Cibersegurança, Inteligência Artificial e Novas Tecnologias na Área de Defesa

Rio de Janeiro
2022

Cibersegurança, Inteligência Artificial e Novas Tecnologias na Área de Defesa

ISBN: 978-65-00-48550-9

Rio de Janeiro, 2022

Dados Internacionais de Catalogação na Publicação (CIP)

C748 Conferência de Direitos dos Colégios de Defesa Ibero-Americanos (23.: 2022: Rio de Janeiro).

Cibersegurança, inteligência artificial e novas tecnologias na área de defesa / organização Maria Célia Barbosa Reis da Silva. - Rio de Janeiro: ESG, 2022.

362 p.: il. - color.; 17 x 23 cm.

ISBN: 978-65-00-48550-9

1. Segurança cibernética – Ibero-América. 2. Inteligência artificial. 3. Tecnologia da informação. 4. Defesa cibernética. I. Silva, Maria Célia Barbosa Reis da. II. Escola Superior de Guerra (Brasil). III. Título.

CDD 003-5

Elaborada pela bibliotecária Patricia Imbroizi Ajus – CRB-7/3716

SUMÁRIO

Prefácio

No ano de 2022, quando o Brasil comemora duzentos anos de Independência, a Escola Superior de Guerra recebe, no período de 29 de agosto a 2 de setembro, a XXIII Conferência de Diretores dos Colégios de Defesa Ibero-Americanos, um fórum de integração acadêmica na área de Defesa decorrente da constatação de que há uma identidade cultural entre os países americanos de Línguas Espanhola e Portuguesa e os da Península Ibérica.

Sediar a XXIII Conferência de Diretores dos Colégios de Defesa Ibero-Americanos muito nos honra. Foi um período de intensa atividade de preparação e de uma rica troca de contribuições acadêmicas. Uma das contribuições desta conferência é a materialização, em forma de livro, das ideias e colaborações dos pesquisadores das Escolas de Defesa.

O lançamento do presente tomo XI dos Livros da CDCDIA, com o título **Cibersegurança, Inteligência Artificial e Novas Tecnologias na área de Defesa**, busca fornecer uma visão ampla desse campo, abordando teorias e debates clássicos e contemporâneos, que vão desde a teoria da guerra clausewitziana até o poder da inteligência artificial, levando em conta os acontecimentos recentes.

Várias reflexões provocativas sobre o tema, de grande significado para o campo da Defesa, podem ser encontradas neste livro, configurando um subsídio relevante para compreender que a guerra moderna "não está circunstanciada ao campo de batalha", pensamento já expressado pelo Marechal Osvaldo Cordeiro de Farias – o primeiro Comandante da Escola Superior de Guerra do Brasil.

Os autores dos capítulos deste livro – Acadêmicos Militares e Civis oriundos das diversas Escolas participantes da XXIII Conferência de Diretores dos Colégios de Defesa Ibero-Americanos – basearam-se em suas experiências pessoais no combate a ameaças avançadas. A arquitetura de segurança cibernética tradicional de defesa de perímetro e a proteção de terminais tradicionais são insuficientes contra os novos agentes de uma guerra híbrida. Os autores percebem a necessidade cada vez maior de recursos, os quais não se limitam à configuração da arquitetura de defesa cibernética, mas também envolvem treinamento dos múltiplos utilizadores e sensibilização dos tomadores de decisão.

A segurança cibernética nacional prepara nossas instituições com programas de segurança cibernética de ponta ou com soluções apropriadas para se defenderem contra a crescente ameaça de ataques cibernéticos direcionados a alvos estratégicos. Este livro mostra-se bem-vindo, ao apresentar subsídios para o estabelecimento de uma estrutura abrangente de segurança cibernética.

O desafio de desenvolver um programa de defesa cibernética envolve muito mais do que simplesmente a obtenção e a utilização de tecnologias de segurança. Sem uma comunicação clara, o apoio dos executores e decisores não será obtido. O processo de comunicação exige uma boa organização. Um programa de segurança

cibernética bem-sucedido precisa facilitar a coordenação entre política, ciclo de vida da tecnologia de informação e estimativas de segurança cibernética.

A relação humana com a violência e a guerra é complexa e contraditória. A humanidade sempre tomou decisões quanto a conflitos, mas, agora, a Inteligência Artificial (IA) está modificando a dinâmica do processo, o que pressupõe consequências dramáticas para as relações internacionais.

Neste livro, os autores também investigam as origens evolutivas da estratégia humana e apresentam um argumento provocativo de que a Inteligência Artificial alterará fundamentalmente o caráter da guerra, modificando a base psicológica para a tomada de decisões violentas. Lendo neste livro os artigos que abordam tal tema, é possível identificar como a Inteligência Artificial revolucionou intensamente a dinâmica dos acontecimentos nas primeiras décadas do século XXI.

Nossas mentes foram moldadas pela necessidade de preocupar-se com os conflitos, que eram uma ameaça constante para os primeiros humanos. Como resultado, desenvolveu-se uma inteligência sofisticada e estratégica. As transformações da Inteligência Artificial são profundas porque se afastam radicalmente da base biológica da inteligência humana, pois nos levarão não apenas a uma guerra radicalmente diferente – decorrente da evolução dos armamentos – mas também acelerará drasticamente a tomada de decisões, o que pode significar o aumento na violência direta ou indireta. A Inteligência Artificial tem o potencial de mudar a estratégia, a organização das forças armadas e a ordem internacional.

Este livro é uma contribuição necessária, com temas que nos são caros, particularmente diante dos últimos acontecimentos no cenário internacional. Para nós, o conteúdo deste compêndio é enriquecedor, por conta da colaboração de vários intelectuais de diversas formações e origens, portadores de uma experiência substancial, materializada nesta obra, a qual servirá como subsídio para pesquisadores, acadêmicos, e tomadores de decisão na área de segurança internacional e defesa.

Como Comandante da Escola Superior de Guerra, expresso minha satisfação por nossa Escola ser a organizadora desta obra relevante e atual. Desejo a todos uma boa leitura.

General de Divisão ADILSON CARLOS **KATIBE**
Comandante da Escola Superior de Guerra

A GUERRA AEROESPACIAL: GEOGRAFIA, TEORIA, ESTRATÉGIAS E TECNOLOGIAS

Carlos Eduardo Valle Rosa*

RESUMO
O capítulo introduz a discussão sobre a guerra aeroespacial. Conceitua ambiente aeroespacial, com o suporte da epistemologia da geografia. Apresenta os fundamentos da guerra aeroespacial com base na teoria do poder aeroespacial. Empiricamente, sustentando as aproximações teóricas anteriores, evidencia estratégias empregadas na guerra no espaço e aponta algumas tecnologias que têm sido desenvolvidas e utilizadas nesse tipo de confronto. O Capítulo conclui destacando a propriedade da utilização do conceito de guerra aeroespacial, em face de o fenômeno se realizar no contínuo representado pelo ambiente aeroespacial.
Palavras-chave: Ambiente aeroespacial; Fenômeno da Guerra; Guerra Aeroespacial.

LA GUERRA AEROESPACIAL: GEOGRAFÍA, TEORÍA, ESTRATEGIAS, Y TECNOLOGÍAS

RESUMEN
El capítulo introduce el debate sobre la guerra aeroespacial. Conceptualiza el ambiente aeroespacial, con el apoyo de la epistemología de la geografía. Presenta los fundamentos de la guerra aeroespacial basados en la teoría del poder aeroespacial. Empíricamente, apoyando los planteamientos teóricos anteriores, destaca las estrategias empleadas en la guerra espacial y señala algunas tecnologías que se han desarrollado y utilizado en este tipo de enfrentamientos. El capítulo concluye destacando la conveniencia de utilizar el concepto de guerra aeroespacial, dado que el fenómeno se desarrolla en el continuo que representa el ambiente aeroespacial.
Palabras clave: Ambiente aeroespacial; Fenómeno de la guerra; Guerra aeroespacial.

1 INTRODUÇÃO

Em todo conflito militar o contexto geográfico é fundamental para se conhecer os movimentos das forças em combate, os desafios de relevo e vegetação, as condições climáticas e tantos outros elementos. Colin Gray (1999, p. 40) entente que "sempre há uma dimensão geográfica nos conflitos". Por esse motivo, discutir a guerra aeroespacial demanda, inicialmente, a compreensão do domínio geográfico no qual se opera esse tipo de guerra: o ambiente aeroespacial. Consoante com

* Doutor em Geografia (Geopolítica), Coronel Aviador da Reserva da Força Aérea Brasileira, Professor Permanente do Programa de Pós-Graduação em Ciências Aeroespaciais, Universidade da Força Aérea (UNIFA). Contato: eduvalle80@hotmail.com

as iniciativas históricas da ciência geográfica, isso se dá a partir de um requisito epistemológico.

A inserção da aerostação e da aviação no contexto das guerras e, mais recentemente o acesso ao espaço exterior, consolidaram essa necessidade. Alguns geógrafos, inclusive, já apontaram a conveniência dessa episteme. Gray (1999, p. 40) destacou que "o fator relevante da geografia nos conflitos atuais se expandiu, [entre outros], para o domínio do ar e do espaço". João Santiago (2013, p. 99) considerou como questões atuais a "expansão do horizonte geográfico para a conquista do espaço extraterrestre, conquista da Lua e perspectiva de colonização de Marte". Joan-Eugeni Sanchéz (1992, p. 182) destacou que "o termo espaço geográfico permite estender-se mais além do próprio Planeta". Consequentemente, o desafio que se impõe é propor um domínio da guerra que seja suscetível a análises não só da geografia, mas da ciência política, das relações internacionais e dos estudos estratégicos, além de, obviamente, das ciências militares.

A fim de dar termo a essa problemática, o estudo inicia apresentando o conceito de ambiente aeroespacial. Do ponto de vista teórico, trata-se de *geografizar* esse domínio como forma de viabilizá-lo como objeto de estudo da guerra. Configurada essa base geográfica, o Capítulo analisa os fundamentos da guerra aeroespacial como *locus* na condução de conflitos militares. Esse é um esforço teórico de recorrer à teoria do poder aeroespacial e observar como ela direciona o tema para o ambiente aeroespacial. Por fim, buscando demonstrar evidências empíricas da guerra nesse novo domínio, o texto revelará algumas estratégias e tecnologias que podem ser aplicadas a esse tipo de disputa militar.[1]

2 O AMBIENTE AEROESPACIAL

A Geografia tem-se preocupado em estudar a atmosfera e o espaço exterior desde a Antiguidade. Notadamente entre os gregos houve uma preocupação em estender o objeto dessa ciência a esses ambientes não convencionais no estudo corográfico que caracterizou a geografia daquele período da história. Aristóteles, em *Meteorologica*, descreveu zonas climáticas e "desenvolveu um modelo primitivo do fluxo de ventos em todo o mundo conhecido" (BONNETT, 2008, p. 48). Ptolomeu empreendeu um estudo astronômico em *Almagesto*, no qual tratou da esfericidade da Terra e observou o movimento aparente das estrelas, enunciando um modelo geocêntrico do Universo. Erastóstenes de Cirene foi responsável por "calcular a distância da Terra ao Sol, catalogar 675 estrelas, medir o raio da Terra e o seu perímetro de circunferência máxima" (CAVALCANTI; VIADANA, 2010, p. 29).

Expoentes da Geografia Moderna empreenderam estudos em direção

1 O capítulo atualiza conclusões do Autor advindas da Tese de Doutorado - ROSA, C. E. V. Geopolítica Aeroespacial. 2020. Tese (Doutorado em Geografia) – Programa de Pós-Graduação e Pesquisa em Geografia da Universidade Federal do Rio Grande do Norte, Natal, 2020.

semelhante. Alexander von Humboldt teve "uma visão holística da natureza e, em *Cosmos*, descreveu sua ampla visão sobre o Universo" (HUGGETT; ROBINSON, 1996, p. 2). Samuel Sark (1887, p. 6) empreendeu um estudo de geografia física sobre o espaço exterior, denominado *Geografia Astronômica*, estudando "a Terra em relação ao Universo e ao Sistema Solar". Richard Hartshorne (1959, p. 25) conjecturou sobre a expansão da definição de superfície terrestre e a admissibilidade da extrapolação do termo para além do planeta Terra, afora não excluir a possibilidade de "utilizar ferramentas e métodos da geografia no melhor conhecimento do espaço exterior". Denis Cosgrove (1994) analisou, na Geografia, o impacto das fotografias da Terra tiradas da espaçonave *Apollo*.

Apesar desses esforços, ainda hoje, há dissensos em torno de muitos conceitos na Geografia. Antonio Moraes (2005, p. 4), adotando uma perspectiva histórica, afirma que a a ciência geográfica é "um campo do conhecimento científico, onde reina enorme polêmica [conceitual]". Por esse motivo, o Capítulo busca, inicialmente, conceituar ambiente aeroespacial como um espaço geográfico.

Neste estudo, a palavra *ambiente* (domínio ou dimensão) é definida como um espaço geográfico caracterizado pelos seus "arredores, pela matéria constitutiva, pelos elementos químicos e propriedades físicas, além dos organismos" (MAYHEW, 2003, p. 171). Trata-se de uma "esfera ou área de atividade (*wirkungsraum* ou *bereich*)" ou um "*milieu* (meio)" (HERRMANN; BUCKSCH, 2014, p. 401 e 475). De acordo com Vladimir Kotlyakov e Anna Komarova (2007, p. 228) ambiente refere-se à "gama completa de condições externas (físicas e biológicas) com as quais as pessoas interagem nas suas vidas e com as atividades econômicas".

A palavra *aeroespacial* também exige clarificação. O Dicionário de Engenharia Geotécnica define aeroespaço (*aerospace,* no original em inglês) como "um termo mnemônico derivado de aeronáutica + espaço e que denota a atmosfera da Terra e o espaço além como uma unidade única" (HERRMANN; BUCKSCH, 2014, p. 25). O Dicionário Aeroespacial de Cambridge define aeroespaço como um "*Continuum* essencialmente sem limite que se estende para fora e através da superfície da Terra em direção às partes mais distantes do universo observável, em especial aquelas que abrangem porções atingíveis do sistema solar" (GUNSTON, 2009, p. 22).

Além de essencialmente geográfico, o debate sobre a questão da integração do ar com o espaço, segundo Peter Hays e Karl Mueller (2001, p. 42) também é uma "questão filosófica, que em decorrência da crescente importância do contexto militar, transforma a demanda por integração nos campos teórico, doutrinário e operacional um assunto cada vez mais importante".

Consideramos que também na esfera da geoestratégica (a aplicação da estratégia militar condicionada pela geografia) essa integração tem se tornado

tema de grande relevância. Frank Jennings (2001, p. 49) expõe conclusões vigorosas da Força Aérea norte-americana sobre essa integração. O ar e o espaço são considerados "um meio operacional sem costuras", ou seja, sem limites, um campo contínuo. Não é por menos que, ainda hoje, tal integração pode ser observada. O Comando de Defesa Aeroespacial Norte-Americano mantém a ideia de uma defesa aeroespacial (NORAD, 2020), ao invés de defesa aérea e espacial.

Portanto, requisitos epistemológicos são obtidos na configuração do conceito de ambiente aeroespacial. Na delimitação do tema que sugerimos, esse ambiente é a conjugação de elementos da superfície terrestre (naquilo em que se relaciona aos objetos geográficos pertinentes ao estudo), a atmosfera (ao abrigar os voos com as aeronaves convencionais), e uma porção do espaço exterior (compreendida entre o ponto mais próximo sobre a superfície no qual um satélite pode orbitar e as órbitas entre a Lua e o Sol). Espaço aéreo e espaço exterior formam um contínuo conceitual na perspectiva que aqui concebemos, representado por eventos semelhantes, correlatos e, na maioria das vezes, interdependentes.

Tal procedimento metodológico de caracterização do ambiente aeroespacial nos permite inferir algumas possibilidades de análise. Esse ambiente ainda é, na perspectiva concreta, um espaço inexplorado ou temporariamente ocupado, onde predominam elementos e fenômenos naturais (tanto atmosféricos como espaciais), especialmente quando compararmos à realidade da superfície terrestre. Contudo, elementos relacionais, potencialmente conflituosos, são observados em grande intensidade. A questão dos espaços aéreos e a soberania sobrejacente aos territórios dos Estados; a questão do acesso às órbitas geoestacionárias; ou a exploração de recursos naturais em corpos celestes são exemplos da suscetibilidade desse domínio ao fenômeno da guerra. Na verdade, transformam-no em um espaço cada vez mais disputado. Por esse motivo, compreender como se daria a dinâmica conflituosa na perspectiva militar torna-se questão essencial nos debates em torno de segurança e defesa, donde se percebe a contribuição original do texto aos estudos estratégicos.

3 A EVOLUÇÃO DA TEORIA PARA O PODER AEROESPACIAL

Além da Geografia, outra importante fundamentação teórica para este estudo é a teoria de poder. Os precursores de teorias clássicas de poder, tais como Alfred Mahan, Friedrich Ratzel, Halford Mackinder, Rudolf Kjellén ou Karl Haushofer, não incluíram em seus estudos as possibilidades que o ambiente aeroespacial, na época deles ocupado pela aerostação ou a aviação, descortinava para a realidade da guerra.

Caberia, inicialmente, ao engenheiro italiano Giulio Douhet, que viveu entre 1869 e 1930 (contemporâneo aos citados anteriormente), alertar para aquilo que

já havia se transformado em realidade desde os aeróstatos e se consolidava com os aeroplanos: a demanda por uma nova teoria de poder que trouxesse o emprego da aviação para o palco da geopolítica e da guerra. O alerta surgiria em 1921, quando foi publicada sua principal obra: *O domínio do ar*.

A forma como Douhet conduziu o debate sobre poder aeroespacial refletia a visão de espaço aéreo contíguo, sem fronteiras físicas, que expunha as nações à guerra total por meio do bombardeio aéreo. A percepção que se evidenciava era a possibilidade do avião atingir o interior do território inimigo, principalmente seus centros populacionais, superando clássicas barreiras físicas da superfície (DOUHET, 1988).

Também William Mitchell e Hugh Trenchard procuraram demonstrar essa nova percepção geopolítica e geoestratégica. A principal contribuição de Mitchell foi o livro de 1925, *Defesa alada: o desenvolvimento e as possibilidades do poder aéreo moderno – econômico e militar*, no qual busca reforçar a ideia da necessidade de uma nação, no caso os Estados Unidos da América (EUA), voltar-se por completo para uma mentalidade aeronáutica (BIDDLE, 2019). O próprio Mitchell (2009, p. 6) declararia que a aviação traria "um novo conjunto de regras para a condução da guerra". Um documento muito importante produzido por Trenchard foi o *Memorando sobre o objeto da guerra para a Força Aérea*, de maio de 1928, onde ele deixa claro que o "poder aéreo poderia dispensar o passo intermediário, passando sobre a marinha e exército inimigos, penetraria o espaço aéreo e atacaria diretamente os centros de produção, transportes e comunicações pelos quais o esforço de guerra do oponente seria mantido" (TRENCHARD, 2008, p. 142).

Porém, o elemento de maior contundência nas proposições dos teóricos pioneiros do poder aeroespacial seria a ideia de domínio do ar. Esse conceito, derivado da ideia de Mahan (1890) sobre o controle do mar[2], e da formulação de área-coração terrestre, originária de Mackinder (1904), sugeria que o domínio (ou controle) do ar, agora, não mais seguiria a lógica bidimensional, constante nas proposições seja do poder naval ou do poder terrestre.

Dominar o ar significava "estar em condições de impedir o voo do inimigo, ao mesmo tempo em que garantíssemos esta faculdade para nós mesmos" (DOUHET, 1988, p. 48). Da forma como entendia Douhet o domínio do ar tinha propósito semelhante ao que se propunha no ambiente marítimo ou terrestre. Ou seja, negar movimento, concentração ou operação dos meios do oponente. Essas ideias foram acolhidas na geografia na forma de uma nova representação do mapa-múndi.

2 Mahan defendia a ideia de controle do mar como forma de assegurar linhas de comunicação marítimas, nas quais o trânsito de mercadorias e suprimentos (o comércio marítimo), garantiria "o jogo livre para a riqueza da terra e a indústria do povo" (MAHAN, 1890, p. 123).

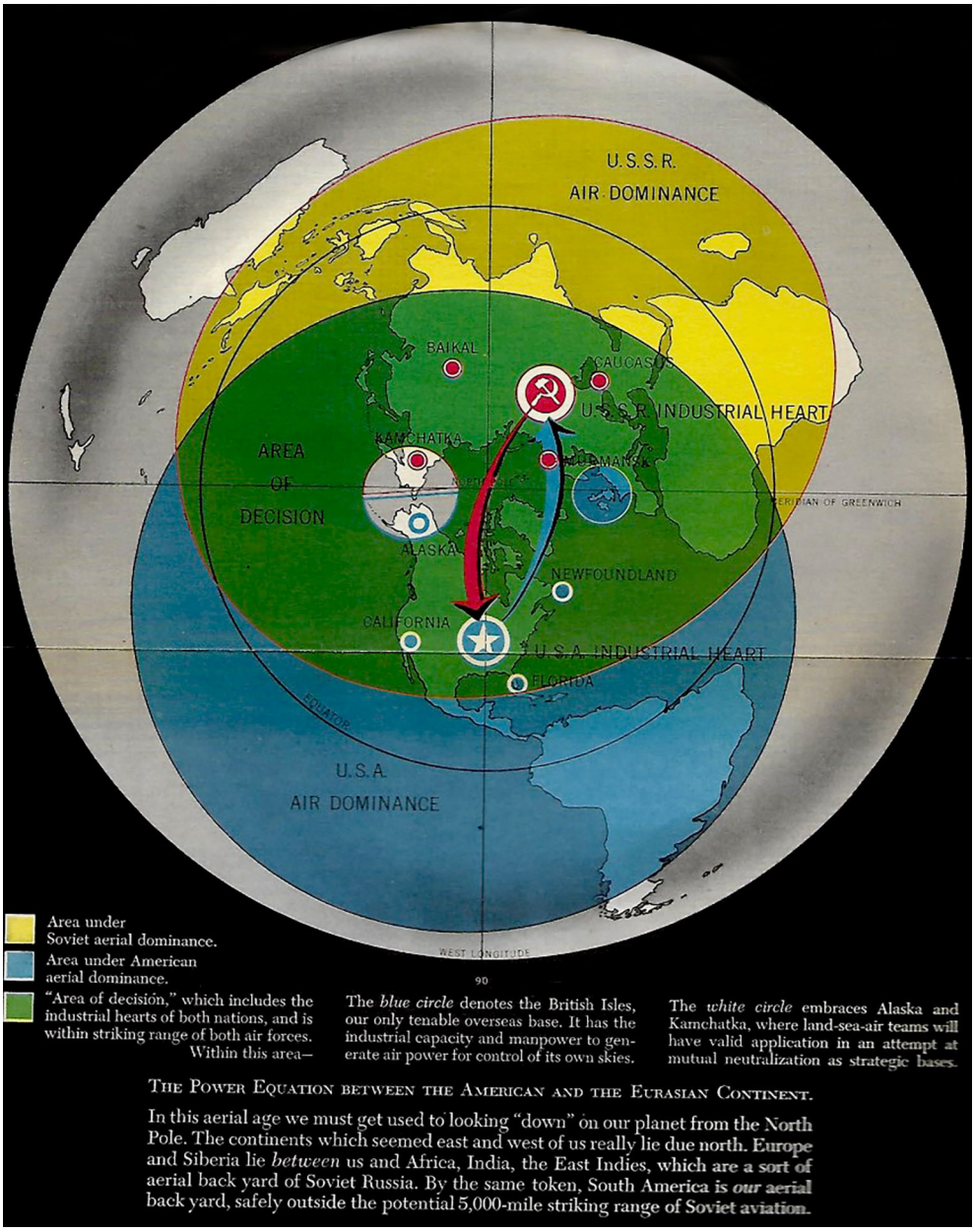
Em 1944, ainda sob forte influência das batalhas da 2ª Guerra Mundial, nas quais o poder aéreo vinha desempenhando papel significativo, Nicholas Spykman (1944) introduziria a percepção cartográfica baseada na projeção azimutal polar. Alexander de Seversky retomaria a ideia de Spykman, considerando o pleno engajamento da nação e criticando a "ilusão do isolamento geográfico" (SEVERSKY, 1950, p. 1). Ainda durante a 2ª GM, Seversky daria uma nova amplitude geográfica à noção de contiguidade do espaço aéreo, "uma guerra entre hemisférios, através dos oceanos, envolvendo a força aérea em operações, não sobre esta ou aquela localidade, mas por longitude e latitude, por toda a parte, no ininterrupto oceano do ar" (SEVERSKY, 1988, p. 20). O que se observa em Seversky é uma ampliação da escala geográfica de atuação da aviação em relação aos precursores Douhet, Mitchell e Trenchard, cujo contexto foi o da 1ª Guerra Mundial, onde a trincheira era o obstáculo a ser transposto pelas aeronaves. Segundo Saul Cohen (2015, p. 28), Seversky desenvolveu uma "visão unitária global", que por meio do poder aéreo poderia levar a nação detentora desses meios a dominância sobre toda a superfície terrestre. Assim, a ênfase que os teóricos originais deram ao bombardeio no interior das nações inimigas, em escala local, Seversky amplia a visão e infere o bombardeio de escala global.

Seversky, em 1950, já incorporava em sua apreciação toda a experiência da 2ª GM e, principalmente, o prólogo da Guerra Fria. Há que se ressaltar que a 2ª GM, diferentemente do conflito mundial anterior, testemunhou operações aéreas de grandes amplitudes em termos de distância de deslocamento, tais como toda a campanha de bombardeio aliado contra a Alemanha (não só em seu território original, mas também em toda a extensão dos países ocupados a partir de 1939), toda a guerra no Pacífico (que demandava o trânsito das aeronaves em escalas no milhar de quilômetros) e as operações aéreas sobre o Atlântico Sul.

Na Guerra Fria, surgem os mísseis balísticos intercontinentais, cujo alcance aos poucos evoluiu até atingir a escala global. Mísseis balísticos de curto alcance já eram uma realidade desde a V-2 alemã. A visão prospectiva de que o alcance desses mísseis atingiria a escala global já era uma realidade para os norte-americanos que, com o grupo de cientistas liderados por Wernher von Braun, "conduziam trabalho nessa direção, para o Exército, no campo de testes de lançamento de White Sands, no Novo México" (CHAPMAN, 2008, p. 8).

Esse contexto deu margem à ampliação da escala de atuação da aviação do local (ou regional) para o global. Stephen Jones (*apud* COHEN, 1963, p. 49) chama de "visão global do homem do ar". Como forma de referenciar esse alargamento de perspectiva, Seversky propôs uma abordagem para o poder aeroespacial, adaptando a projeção azimutal equidistante centrada no polo Norte, de cunho geopolítico e geoestratégico (Figura 1).

Figura 1 – A perspectiva de Seversky quanto ao poder aeroespacial



Fonte: SEVERSKY, 1950, p. 312.

Inicialmente, essa nova perspectiva de Seversky considerava que a relação espacial e de distância seria totalmente diferente em face da realidade tridimensional

incorporada com a aviação (onde ressalta a perspectiva geográfica). Na Figura 1, observa-se o círculo na cor azul e a elipse em amarelo, onde Seversky representava áreas de dominação aérea, respectivamente sobre controle norte-americano e soviético. Na prática, essas representações seriam, do ponto de vista aeroespacial, espaços geopolíticos de influência, sob os quais os EUA e a União das Repúblicas Socialistas Soviéticas (URSS) poderiam prevalecer (perspectiva geopolítica).

No mapa de Seversky, na observação da área verde se denota um espaço de confluência ou de interseção entre as zonas de influência norte-americana e soviética (azul e amarela), configurando um espaço de conflito potencial (perspectiva geoestratégica). Seversky (1950, p. 308) considerava que nessa zona verde estariam "as áreas industriais vitais de ambas as nações ao alcance do poder de ataque aéreo". Essa área verde é, efetivamente, uma nova visão de zona de fronteira na qual, por meio da perspectiva tridimensional do autor, localiza-se um *território* contestado.

Aliando os argumentos de sua nova perspectiva e da reinterpretação das fronteiras sob o ponto de vista aeroespacial, Seversky abre espaço para um novo raciocínio. Agora, em virtude da *era aeronáutica*, o correto seria olhar o globo terrestre de cima do Polo Norte, substituindo a ultrapassada projeção de Mercator pelo que denominou de "projeção polar" (SEVERSKY, 1950, p. 307).

Essa inovadora perspectiva, delineada na Figura 1, demandaria grandes modificações nas análises políticas dos Estados, em face da realidade da aviação (e incipientemente, do espaço exterior). Sobre essa nova perspectiva, Seversky diria que, "vistos a partir do Polo Norte, os continentes que pareciam se situar a Leste e a Oeste de nós (no caso os EUA), realmente situam-se a Norte" (SEVERSKY, 1950, p. 307). Ou seja, os grandes movimentos políticos e estratégicos não seriam mais interpretados no sentido longitudinal (Leste-Oeste), mas no sentido latitudinal (Norte-Sul).

No estudo de Seversky o que se coloca é, baseado na experiência até então acumulada, uma *teoria do poder aéreo*, que viria ora a se justapor, ora a se contrapor aos postulados da teoria do poder terrestre e do poder marítimo. Em síntese, essa teoria propunha: a) uma alternativa para os postulados sobre o controle do mar e o controle do *heartland*; b) uma visão geográfica do todo, superando as barreiras físicas existentes e alterando o conceito de fronteira; c) a inclusão nas relações de poder de um novo modal de transporte e vetor militar representado pelo avião.

Na verdade, as ideias de Seversky podem ir além. Como afirma Pedro Correia (2018, p. 188), elas mereceriam nova atenção, "com o aparecimento dos mísseis intercontinentais, com o alcance e raio de ação ilimitados dos meios aéreos [...] e com o domínio do novo elemento de circulação que é a dimensão espacial, o poder aéreo adquiriu nova projeção". Essa visão estenderia o "oceano aéreo uno e indivisível" de Seversky (1988, p. 352) ao espaço exterior, formando um conjunto integrado, o ambiente aeroespacial, espaço geográfico de atuação de uma nova

forma de poder. Assim é que pensamos que esse seria um momento de adequada transição para uma teoria do poder aeroespacial.

Antonio Tomé (2009), em clara citação que evidenciaria a evolução do poder aéreo para o poder aeroespacial, destaca que a aeronave hipersônica, capaz de voar a velocidades superiores a Mach 5 (cerca de 6.175 km/h), em camadas superiores da atmosfera, seria uma verdadeira

> [...] aeronave espacial, que constituirá seguramente a concretização de uma etapa importante e decisiva na projeção do poder aéreo para o espaço orbital, como que um trampolim que permitirá transpor de forma firme e consolidada a fronteira mesosférica da atmosfera pelos meios e tripulações pioneiros os quais, libertando-se da gravidade, irão estabelecer diretamente a continuidade e o prolongamento dos altos voos atmosféricos para o ambiente do Espaço próximo. (TOMÉ, 2009, p. 276).

As características inerentes a essas novas tecnologias e a essa nova dimensão geográfica representada pelo ambiente aeroespacial fariam da aviação um vetor cada vez mais influente nas guerras. Como observamos acima, em 1991, um conflito no Oriente Médio daria vazão à aplicação do espaço exterior nessa nova perspectiva teórica. A Guerra do Golfo foi um ponto de inflexão na comunhão entre atmosfera e espaço exterior, legitimando a transição da teoria de poder aéreo para poder aeroespacial.

O fato novo que a Guerra do Golfo revelaria, e que acompanhou os movimentos de dissolução da URSS e o consequente esmaecimento e término da Guerra Fria, foi uma verdadeira revolução tecnológica aeroespacial. Essa revolução teria efeitos não somente no campo militar, mas também no desenvolvimento da ciência, na economia e na relação entre os Estados.

Conflitos posteriores, como a Guerra no Afeganistão, em 2001, e a invasão norte-americana no Iraque, em 2003, testemunhariam a aceleração do processo de integração de capacidades militares espaciais (e, também, algumas de natureza civil) nos embates militares. Segundo Rick Sturdevant e Haithe Anderson (2011, p. 25), o *gap* operacional de 12 anos que separou os conflitos no Iraque (1991 e 2003), apesar de não ter significado grande salto técnico nos sistemas espaciais utilizados, "modificou tremendamente a forma de utilizá-los nas operações militares". Autores como Benjamin Lambeth (2000), Max Boot (2006), David Jordan *et al.* (2008), John Olsen (2010 e 2018), John Baylis, James Wirtz e Colin Gray (2013), além de reforçarem o impacto operacional dos sistemas espaciais nas operações militares, destacam a grande vantagem estratégica que esses sistemas oferecem aos seus usuários.

O emprego dos sistemas espaciais em operações militares na superfície, inclusive a partir do ar, é assunto plenamente explorado e demonstrado nas obras

acima citadas. Alguns fatos demonstram que essa é uma tendência ainda a curto prazo.

A consolidação da ideia de perspectiva geográfica aeroespacial, cujo fato precursor foi a ascensão de aeróstatos, e o fato atual, a presença de satélites de observação e de aquisição de imagens, cumprindo, essencialmente, a mesma função originária de reconhecimento aeronáutico pelo alto. Em segundo lugar, a recente criação de novo ramo das forças armadas nos EUA, denominada *Space Force* (Força Espacial), que tem por propósito organizar a capacidade militar norte-americana para o emprego de sistemas espaciais em suporte aos comandos militares combatentes (USSF, 2020a). Essa tendência de denominação de forças aeroespaciais tem sido seguida em vários países. Por fim, ainda que assunto cercado de sigilo e restrições de acesso à informação, surgem as armas antissatélite (*Anti-satellite Weapons* – ASAT). Segundo Bert Chapman (2008, p. 143), as ASAT são "armas cujo propósito é destruir ou interferir no funcionamento de satélites pertencentes a forças hostis".

Voltando nossa atenção para a questão da integração do poder aéreo e do poder espacial, consideramos importante observar o tema a partir de em um único construto conceitual: o poder aeroespacial. O Brasil, considerado um dos pioneiros na integração desse conceito, viu em Murillo Santos, influente pensador do poder aéreo nacional, a contundente afirmação de que o poder aéreo haveria se "tornado poder aeroespacial na medida em que os marcos deixaram de ser a baixa atmosfera" (SANTOS, 1989, p. 15, grifo nosso). Mesmo nos EUA, onde houve intenso debate sobre o significado do termo *aerospace* (aeroespacial), influentes pensadores retomam o assunto tendendo a concordar com essa integração, como é o caso do general da USAF David Deptula (2018, p. 14), quando afirmou que "com a perspectiva do poder aéreo ascendendo ao espaço, uma teoria da indivisibilidade do poder aeroespacial se materializa com a fusão das aplicações tecnológicas no ar e no espaço".

A utilização de veículos aéreos em camadas cada vez mais elevadas da atmosfera terrestre vem se tornando uma realidade crescente. A tecnologia da velocidade hipersônica habilita veículos aéreos a transitar à cerca de 90Km de altura da superfície, portanto, no trecho que compreende a transição entre espaço aéreo e espaço exterior. Além disso, o sistema de propulsão hipersônico mistura uma motor de compressão de ar, característico das aeronaves modernas, com um foguete acelerador, típico de sistemas de propulsão próprio dos veículos lançadores de satélites. Na verdade, os mísseis balísticos de longo alcance (intercontinentais) percorrem parte significativa de sua trajetória em subórbitas, deixando a atmosfera terrestre nesse segmento do voo e nela reentrando para prosseguir na direção do alvo selecionado. Alguns desses mísseis atingem o apogeu de 2.000km de altura.

Do ponto de vista operacional, consequentemente, tais veículos poderiam ser considerados como elementos de um poder aeroespacial, pois seria difícil negligenciar essas características de operação próprias. Além do mais, como são

veículos essencialmente de emprego militar, a neutralização de suas funcionalidades poderia ocorrer em diferentes segmentos geográficos: ainda na superfície, por meio da destruição da capacidade de lançamento; no deslocamento pelo atmosfera terrestre, por meio de dispositivos de intercepção, tais como mísseis ar-ar lançados por aeronaves; no percurso orbital, por meio de armas ASAT; ou na reentrada em órbita, no estágio final do deslocamento, por meio de sistemas de defesa antiaérea, como mísseis superfície-ar.

O que se analisa nessa contextualização é a dificuldade de se compreender a utilização do espaço exterior apenas sob a perspectiva de poder espacial. O que existe, de fato, é uma integração entre os segmentos da atmosfera terrestre e o espaço exterior (em especial, naquilo que se refere às órbitas terrestres) que caracteriza o ambiente aeroespacial e, por conseguinte, um poder aeroespacial. Não se pode deixar de citar que, no caso brasileiro, a própria Constituição Federal de 1988 cita a palavra aeroespacial três vezes (letra "c" do inciso XII do Art. 21; inciso X e XXVIII do Art. 22), relacionando-a com a navegação ou com a defesa. Nesse último caso, fica clara a integração dos contextos aéreo e espacial em um só conceito, pois a carta magna atribui à União a responsabilidade pela "defesa aeroespacial" (ao invés de falar em defesa aérea ou defesa espacial) (BRASIL, 2016).

Essa revolução tecnológica é um dos fundamentos pelos quais o espaço exterior se insere no debate sobre o poder aeroespacial e influencia o fenômeno da guerra. Tal aporte passa a justificar uma evolução no conceito de poder aéreo para poder aeroespacial. Isso se justifica também pelo fato de inexistir, até o momento, uma teoria essencialmente de poder espacial, no que concordamos com Nayef Al-Rodhan (2012, p. 20) quando cita que "não há, ainda, uma teoria de poder espacial". Peter Hays (2011a, p. 30) também entende que, "apesar de vários esforços para se apropriar ou adaptar conceitos-chave oriundos da teoria do poder marítimo e do poder aéreo, atualmente ainda estamos à deriva, sem uma teoria de poder espacial abrangente para nos guiar".

Concluindo essa apreciação teórica, é importante afirmar que poder aeroespacial é aqui compreendido como uma síntese entre o poder aéreo e o poder espacial. Autores como Daniel Goure e Christopher Szara (1997), já debateram essa integração, que é um assunto comumente abordado sob o ponto de vista doutrinário ou teórico. Autores como Tony Mason (1994), Philip Meilinger (1997), Benjamin Lambeth (2000), Clayton Chun (2004) e John Olsen (2018) exploram as formas de se melhor compreender o que seria essa integração. No Brasil, André Almeida já defendeu que o poder aeroespacial é fruto da integração entre o poder aéreo e a possibilidade desse poder aéreo atuar no espaço exterior. Nas palavras do autor, a partir do lançamento do primeiro satélite artificial, em 1957,

> [...] o espaço exterior passou a ser incluído como um novo teatro no qual a guerra poderia ser travada. Assim, diante desta nova

> percepção do espaço, começou-se a realizar formulações para o uso do espaço sideral, baseadas na teoria do poder aéreo. O poder aeroespacial pode, assim, ser definido a partir da definição do poder aéreo como a capacidade de um país de empregar o espaço aéreo e o espaço exterior a fim de atingir um objetivo militar, político ou diplomático. (ALMEIDA, 2006, p. 34).

A guerra aeroespacial revela-se no ambiente aeroespacial, sintetizado como a conjugação entre o espaço aéreo e o espaço exterior. Em grande parte, isso se explica pela continuidade histórica que permitiu à humanidade a adquirir a capacidade aeronáutica (inicialmente na forma de aerostação, e depois pelo voo aerodinâmico) e, em seguida, ir mais além, ao espaço exterior, com a astronáutica (por meio dos foguetes e da astrodinâmica). O que se propõe, finalmente, é considerar a conquista do ambiente aeroespacial como um marco na história das guerras. No próximo segmento do capítulo, apresentaremos algumas evidências concretas dessa realidade.

4 ESTRATÉGIAS E TECNOLOGIAS DA GUERRA AEROESPACIAL

Este segmento do capítulo tem por finalidade identificar estratégias e tecnologias que já tem sido evidenciadas, ou em desenvolvimento, para a guerra aeroespacial. À guisa de síntese, e por considerar que o segmento aéreo de nosso ambiente aeroespacial já é extensivamente qualificado quando se fala de guerra (refiro-me essencialmente às aeronaves), nosso esforço analítico concentrar-se-á nas evidências da guerra aeroespacial no segmento do espaço exterior.

Apesar disso, insistimos que a repartição dos segmentos (aéreo e espacial) tem finalidade meramente didática, até porque instrumentos como os mísseis balísticos, por exemplo, são lançados da superfície, transitam pela atmosfera, ingressam no espaço exterior (alguns com apogeu que pode chegar a mais de 4.000 km), realizam deslocamentos entre os espaços orbitais, retornam à atmosfera e atingem o alvo pré-determinado. Nesse sentido, é difícil classificar se tal equipamento militar é de natureza terrestre, aérea ou espacial. Um outro forte argumento é o arcabouço jurídico internacional, quando trata da delimitação (ou da fronteira) entre espaço aéreo e espaço exterior. Nem a Organização da Aviação Civil Internacional (OACI) nem o Comitê das Nações Unidas para o Uso Pacífico do Espaço Exterior (COPUOS), trazem uma definição do ponto de transição entre atmosfera e espaço exterior. Isso pode trazer questões de natureza jurisdicional, política e, até mesmo, militar.

Uma primeira constatação é a de que o ambiente aeroespacial é um ambiente disputado. A principal argumentação nesse contexto de contenda decorre de constatações em torno da ideia de expansão de fronteiras e da busca por espaços geográficos estratégicos (donde se buscam recursos naturais e/ou posições

politicamente vantajosas), ambos processos que centralizam a discussão em torno do Estado.

A expansão do território de um Estado foi estudada por Friedrich Ratzel, no final do século XIX. Ratzel estabeleceu leis do crescimento estatal que são fundamentos teóricos da geopolítica, identificando que esse crescimento se daria na direção das fronteiras (RATZEL, 1892). Os movimentos de colonização, como por exemplo das navegações ibéricas dos séculos XV e XVI, as navegações aéreas em direção aos polos Norte e Sul, a corrida espacial que levou o homem à Lua, e o interesse mais recente pelo planeta Marte, revelariam intrinsecamente a teoria do antropólogo e geógrafo alemão. Para Ratzel (1892, p. 178) "as dimensões do Estado crescem com sua cultura (que também significa tecnologia)". Em seu crescimento, o Estado "luta para alcançar posições politicamente valiosas (recursos naturais ou localização geográfica relevante). O crescimento territorial é efetuado na periferia do estado pelo deslocamento da fronteira (no caso, a periferia do planeta Terra)".

À ideia do espaço vital e da expansão do território, agrega-se a conceituação de espaço geográfico estratégico. Colin Gray e Geoffrey Sloan (1999) têm defendido a ideia da influência da geografia na geopolítica sob o ponto de vista desse espaço estratégico. Quando afirmam que "os objetivos políticos são uma consequência das escolhas feitas pelos formuladores de políticas" e que "é a partir dessas escolhas que a importância política e estratégica é agregada às configurações e localizações geográficas" (GRAY; SLOAN; GEOFFREY, 1999, p. 2), o que os autores propõem é a ideia de uma escolha seletiva.

O qualificativo "estratégico" do espaço geográfico implicaria da decisão política, que decorre, naturalmente, da demanda por mais território. Cria-se, assim, um vínculo entre ambas as ideias. O espaço estratégico é reclamado como um fenômeno de expansão do território a partir de uma decisão política. Parafraseando o famoso pensador militar Carl von Clausewitz (1984), a expansão do território para os espaços geográficos estratégicos é a continuação da política por outros meios.

O que se infere até aqui é que, em função dessas características, o ambiente aeroespacial é objeto de estratégias estatais de expansão. Mas quais seriam evidências concretas dessas estratégias? Isso nos leva a apreciar o que seriam, onde estariam e quais as características desses espaços estratégicos na geografia do ambiente aeroespacial. Faremos isso a partir de algumas analogias.

A exemplo dos espaços geográficos estratégicos da superfície, o ambiente aeroespacial também é amplo, prolífico em recursos naturais, mas, em alguns casos, encerra a ideia de finitude, ou de limitação, percepção diferente do senso comum que atribui ao espaço exterior a ideia de infinitude. As órbitas terrestres são espaços finitos. Especificamente, as órbitas geoestacionárias são um bom exemplo dessa afirmação. A se considerar que essas órbitas seriam preferenciais para satélites militares e de comunicações, assim como para aqueles que tem por função detectar o movimento de mísseis balísticos (funções essenciais em um

conflito militar), podendo também servir para comunicações globais e meteorologia (serviços, hoje, imprescindíveis à sociedade), percebe-se o quão significativas são essas órbitas. Estima-se em um máximo de 1.800 slots geoestacionários disponíveis no total, sendo que até 2021, cerca de 565 deles já estariam ocupados, por satélites ativos e tantos outros por satélites defuntos. A conclusão óbvia que se chega a partir dessa realidade é que órbitas geoestacionárias são um recurso natural limitado àqueles que se apropriarem inicialmente. Tal conclusão enseja uma questão: qual a estratégia do Estado para assegurar o direito de ocupação desses espaços finitos?

Outra evidência, que também demandará estratégias, encontra-se na praticabilidade de exploração comercial dos asteroides ou dos cometas, autores como Hans Mark (2003, p. 600) consideram que em comparação com as dificuldades logísticas de empreendimentos na Lua, os asteroides próximos à Terra, "devido a sua imensa riqueza e diversidade de recursos, têm emergido como fontes mais atrativas de materiais para exploração". Segundo Martin Elvis (2012, p. 549) "o apelo econômico para a mineração de asteroides é claro: um pequeno asteroide com 200 m de diâmetro e rico em alumínio pode valer algo em torno de US$ 30 bilhões".

Há de se supor, caso reconheçamos a evolução do fenômeno da guerra e de suas causas, que a disputa por recursos naturais demandará estratégias estatais de ocupação desses nichos. Fato que também pode ser observado em características geográficas do ambiente aeroespacial que se assemelham aos estreitos, estrangulamentos ou *chokepoints.* No espaço exterior, também existem localizações privilegiadas, como por exemplo, os Pontos Lagrange, que são pontos de equilíbrio gravitacional e espaçonaves posicionadas nesses pontos seriam favorecidas pela baixa necessidade de correção de órbitas por meio do uso dos foguetes e, por conseguinte, de combustível.

Ainda sobre esses espaços geográficos privilegiados, a exemplo das rotas marítimas e das rotas aéreas, verdadeiras linhas de comunicação, que viabilizam conexões das mais variadas formas, há, no ambiente aeroespacial, realidade semelhante. Talvez a mais contundente seja aquela que conecta o planeta por meio das telecomunicações e da tecnologia da informação. Por meio dos satélites, surgem redes conectadas que favorecem um sem-número de serviços de interesse da sociedade. Um exemplo concreto dessas linhas de comunicação são as Órbitas de Transferência de Hohman, uma rota de comunicação entre órbitas distintas, utilizada nas manobras das espaçonaves. Essa órbita atua como uma catapulta gravitacional, reduzindo o consumo de combustível na manobra espacial de reposicionamento de um veículo espacial entre órbitas distintas, por exemplo entre a Lua e Marte.

Outra demanda de estratégia para lidar com eventuais conflitos militares no ambiente aeroespacial será a ambiental que, a exemplo das questões relacionadas à superfície terrestre, tem potencial para gerar antagonismos estatais. No dilema entre o desenvolvimento e a preservação dos biomas terrestres, um grande debate mundial

tem colocado em polos opostos àqueles que defendem a ideia de que o planeta é um bem comum da humanidade, ou uma *res communis*. Possivelmente, a discussão que mais reverbera nos fóruns internacionais é a questão do lixo espacial, ou *debris*. Segundo Daniel Deudney (1982, p. 49) "os *debris* orbitais crescem a uma taxa de 11% ao ano". Peter Hays (2011b, p. 91) alerta que com "a permanência de tendências atuais, há um risco crescente de que os *debris* tornem o espaço, em particular as órbitas baixas da Terra, progressivamente não utilizável". O lixo espacial pode gerar problemas de colisão contra satélites ou outras espaçonaves, inclusive os próprios foguetes conduzindo astronautas ou turistas espaciais, com efeitos catastróficos. Ou ainda, gerar problemas quando da colisão com a superfície terrestre.

Potencialmente, fóruns internacionais seriam espaços de amortização de conflitos. Porém, a se perceber alguns exemplos recentes, como no caso do COPUOS, questões cruciais ficaram sem soluções definitivas. Em primeiro lugar, porque o Tratado sobre os Princípios Reguladores das Atividades dos Estados na Exploração e Uso do Espaço Exterior, inclusive a Lua e demais Corpos Celestes (UNITED NATIONS, 1966), aprovado pela Assembleia Geral da ONU, em vigor desde 10 de outubro de 1967, ratificado pelo Brasil, comumente denominado Tratado do Espaço Exterior, tem recebido críticas e demandado revisões.

Por exemplo, no caso do Art. I, na visão de que a exploração e o uso do espaço exterior, não expressaria corretamente a relação custo x benefício, pois àqueles que se lançam à empresa espacial teriam que dividir as benesses com aqueles que seriam meros espectadores. Tanto é que o recente Ato de Exploração e Utilização de Recursos Espaciais (UNITED STATES OF AMERICA, 2015, p. § 51303), do governo dos EUA, flagrantemente veio de encontro ao Tratado do Espaço Exterior, ao legislar que "qualquer recurso obtido em asteroides no espaço exterior é propriedade da entidade que obteve tal recurso".

O outro exemplo que tem potencial conflituoso, pois toca na questão da soberania do território, foi a Declaração de Bogotá, de 1976, a respeito das órbitas geoestacionárias, documento onde ficou explícito que "os segmentos da órbita síncrona geoestacionária fazem parte do território sobre o qual os Estados equatoriais exercem sua soberania nacional" (BOGOTA DECLARATION, 1976), ressaltando que o Brasil foi signatário dessa declaração. A se considerar que as órbitas geoestacionárias são finitas em termos de disponibilidade de ocupação, pode-se perceber a relevância da declaração que indica um movimento de extensão da soberania territorial no espaço aéreo para o espaço exterior. A partir dessa possibilidade, o território estatal seria efetivamente um território aeroespacial.

Todos esses fatos, em tese, demandariam estratégias para a eventualidade de uma guerra no ambiente aeroespacial. As evidências apontam que alguns estados já pensam seriamente nessa possibilidade. Isso no leva a analisar as tecnologias que estariam disponíveis, ou em desenvolvimento, na atualidade, a fim de atender demandas militares nesse novo domínio da guerra.

Há que se reconhecer que o processo de militarização e de armamentização do espaço exterior dá-se sob um viés realista das relações internacionais (PLANO; OLTON, 1988). Por esse motivo, autores como Everett Dolman (2002, p. 4) entendem que "a militarização e a corrida armamentista [ou a armamentização] do espaço não é somente um fato histórico, mas também um processo em curso".

Importante distinguir militarização de armamentização. A militarização já ocorre desde o início da corrida espacial, que remonta à Guerra Fria, e é, a cada dia, um fenômeno que se intensifica. Mesmo o Brasil, hoje, já faz parte desse processo em curso, quando posicionou em órbita o Satélite Geoestacionário de Defesa e Comunicações, em 2017, com o propósito de fornecer comunicações seguras para suas forças armadas. O segundo fenômeno, ainda incipiente, trata da postura de armas em órbita ou do desenvolvimento de capacidades que tenham efeitos neutralizadores dos aparatos postados no espaço exterior.

Nossa ênfase no Capítulo será em torno do processo de armamentização. Mesmo que incipiente, perceberemos que há evidências fortes de um caminhar a passos largos. Relatórios oficiais, análises de *think thanks* e o noticiário internacional apontam, por exemplo, diversos testes de armas antissatélite. Um dos mais recentes, à época da redação deste Capítulo, foi o teste da Rússia que teria destruído o satélite defunto Cosmos-1408, entre 14 e 15 de novembro de 2021 (EUSST, 2021). Contudo, existem relatos mais antigos de testes de ASAT por parte da China, dos EUA, Rússia e Índia. Em 2007, revelou-se o teste chinês de lançamento da superfície de um míssil que atingiu um satélite desativado a uma altura de cerca de 800km (SHEEHAN, 2007, p. 167). Os EUA já haviam conduzido um teste de ASAT no início dos anos 1980, por meio do lançamento de "um veículo miniatura, a partir de uma aeronave F-15 *Eagle*, com capacidade de seguir o curso do satélite e destruí-lo fisicamente no impacto" (CHAPMAN, 2008, p. 144). David Ziegler (1998) aponta que também os russos possuíram programas de armas ASAT. Em 2018, a Índia testou uma ASAT, exitosamente destruindo um satélite defunto em LEO, transformado em lixo espacial (URRUTIA, 2017).

Sobre as ASAT, importante é recorrer ao *Space Threat Assessment* (HARRISON *et al.*, 2021) para se compreender a natureza dessas armas. Mais do que ASAT, o que esse estudo propõe é uma classificação de armas que contrapõe a atividade espacial. Na classificação proposta existem quatro tipos de ASAT: a) As de efeito cinético, voltadas para o impacto físico contra satélites, acarretando danos destrutivos e catastróficos; b) Aquelas que causam danos físicos aos satélites (ou instalações terrestres), porém sem contato físico com eles e, em geral, podem utilizar emissões de *laser*, micro-ondas de alta potência ou energia nuclear; c) O terceiro grupo de armas é representado por sistemas que agem no espectro eletromagnético, impedindo, interferindo, adulterando a transmissão de dados entre satélites e suas estações terrestres, ou vice-e-versa; d) O grupo final está enquadrado nas capacidades de guerra cibernética, haja vista que os dados transitam por sistemas

computacionais que podem ser vulneráveis aos ataques em equipamentos nos satélites ou estações terrestres.

Na verdade, já existem várias concepções de como se lidar com as ameaças aos satélites e as estações na superfície que se relacionam com a atividade espacial. Nesse rol estariam defesas passivas e ativas. Algumas se estruturam na arquitetura das constelações satelitais, como por exemplo a "desagregação de constelações, que é a separação de missões distintas em diferentes plataformas ou cargas úteis, efetivamente dividindo satélites multimissão em satélites separados para missões específicas que operam em paralelo" (HARRISON; JOHNSON; YOUNG, 2021, p. 11). No campo das defesas ativas estariam o *jamming* (interferência eletrônica) ou o uso de laser que cegue sensores dos satélites.

Dentre essas ações no âmbito da guerra aeroespacial, possivelmente, a mais importante seria o *Space Domain Awareness* – SDA (Consciência Situacional Espacial). A exemplo do que já acontecia na guerra aérea, a capacidade de identificar os atores da batalha é essencial, assim como possuir condições de comandar e controlar esses atores, com a finalidade de que executem determinadas funções. O SDA é uma rede de sensores e estações de controle que apresentam um panorama da situação espacial. O sistema provê informações sobre a posição e movimentação de aparatos espaciais (inclusive sobre *debris*).

Uma forma adequada de se evidenciar esses tipos de tecnologia é observar algumas iniciativas de determinados estados na direção do desenvolvimento de capacidades de armas para a guerra aeroespacial, sem a pretensão de esgotar o assunto. Um recente estudo sobre capacidades *counterspace* (contraespacial)[3] listou diversas iniciativas de vários países que desenvolvem algum tipo de tecnologia que pudesse ser utilizada na guerra aeroespacial (WEEDEN; SAMSON, 2021). Concentraremos nossa análise nos EUA, China e Rússia. O estudo se desenvolve em torno de capacidades relacionadas ao seguinte:

> a) Ascensão direta: armas que utilizam mísseis lançados do solo, ar, ou mar interceptadores que são utilizados para destruir cineticamente satélites através da força de impacto, mas não são colocados em órbita elas próprias;
> b) Coorbital: armas que são colocadas em órbita e depois manobradas para se aproximar do alvo para atacá-lo por vários meios, incluindo meios destrutivos e não destrutivos;
> c) Energia dirigida: armas que utilizam energia focalizada, tais como o laser, partículas, ou feixes de micro-ondas para interferir ou destruir sistemas espaciais;
> d) Guerra eletrônica: armas que utilizam energia de

3 O termo counterspace deriva de abordagens teóricas e doutrinárias sobre a guerra espacial, referindo-se às ações de contraposição a iniciativas militares para se obter determinados efeitos nos sistemas espaciais do oponente.

> radiofrequência para interferir ou bloquear as comunicações de ou para os satélites;
> e) Cibernética: armas que utilizam software e técnicas de rede para comprometer, controlar, interferir ou destruir sistemas informáticos. (WEEDEN; SAMSON, 2021, p. xxxi)

Além dessa importante classificação, o estudo também aponta o estágio atual de desenvolvimento das capacidades, distinguindo entre as fases de: a) pesquisa & desenvolvimento; b) em testes; c) com condição operacional; e d) utilizada em conflito.

4.1 ESTADOS UNIDOS DA AMÉRICA

Os EUA têm desenvolvido capacidades militares espaciais desde a Guerra Fria. O X-37B, classificado como uma capacidade coorbital, é uma espaçonave que se assemelha ao ônibus espacial, mas é muito menor e completamente robótico (não tripulado). Tem potencial limitado para transportar armas e sua principal função parece ser a de sensoriamento remoto, embora, provavelmente, tenha capacidade de manobrar no espaço. Porém, até o momento, o X-37B não se aproximou ou se encontrou com qualquer outro objeto espacial (WEEDEN; SAMSON, 2021).

O *Rods of God*, ou as "Varas de Deus", é um conceito de arma espacial que se encaixaria, no contexto de ascensão direta porém no sentido reverso. Composto por feixes de hastes de tungstênio de cerca de 6 metros de comprimento, lançadas da órbita terrestre, atingiriam uma velocidade de até dez vezes a velocidade do som, capaz de penetrar bunkers endurecidos ou locais subterrâneos secretos (STILWELL, 2019).

O ASM-135 é um míssil atmosfera-espaço capaz de destruir fisicamente satélites, classificado como arma de ascensão direta. De acordo com Peter Grier (2009) o míssil foi testado pela primeira vez em 1985, lançado a partir de uma aeronave da Força Aérea dos EUA. O míssil, que continha uma cabeça explosiva convencional, atingiu o alvo (o satélite *Solwind* P78-1), a uma altitude de 548 km (portanto além da Linha Kármán), destruindo-o.

Uma capacidade coorbital norte-americana é o XSS-10, e sua versão mais recente o XSS-11, um satélite manobrável capaz de se aproximar de outros satélites e realizar operações nas suas proximidades. Não está claro até o momento, que tipo de manobra esse satélite executará· Brian Weeden e Victoria Samson (2021, p. 3-10) afirmam que o XSS-11, "entre abril de 2005 e outubro de 2006, fez uma série de manobras para se aproximar do estágio superior do foguete *Minotaur*, que o havia colocado em órbita. Em seguida, realizou um movimento adicional se aproximando de outros objetos espaciais dos EUA em órbitas baixas".

Por fim, o Programa de Consciência Situacional Espacial Geossincrônica – GSSAP, que certamente já complementa o sistema de SDA dos EUA, usa dois pares

de pequenos satélites em órbitas GEO, o que lhes permitiria "realizar rigorosas inspeções de objetos na região das órbitas geoestacionárias" (WEEDEN; SAMSON, 2021, p. 3-7). A se considerar que um dos satélites do par possua algum tipo de capacidade cinética, não cinética, de energia dirigida ou de guerra eletrônica, estaríamos falando de uma arma espacial em potencial.

Na análise do *Global Counterspace Capabilites* - GCC, estudo citado acima, os EUA teriam significativas capacidades operacionais de guerra eletrônica e SDA para a guerra aeroespacial, além de alguma capacidade em fase de testes nos campos da ascensão direta para órbitas baixas e de energia dirigida.

4.2 CHINA

A China tem se revelado um ator muito importante no campo espacial, buscando acelerar seus programas nativos e alcançar as potências tradicionais (EUA e Rússia). Apesar de possuir muitos projetos, alguns deles de natureza militar, a maior parte das informações disponíveis origina-se de sites especializados ou da mídia convencional, o que dificulta sobremaneira o acesso às informações precisas. Esse é o caso, por exemplo da estação espacial *Tiangong*. A par das especulações de que essa seria uma estação espacial militar, diferentemente da Estação Espacial Internacional, de natureza científica, Sakshi Tiwari (2022) aponta que "os EUA estariam apreensivos quanto à possibilidade de a *Tiangong* hospedar um braço mecânico capaz de capturar satélites", o que se enquadraria tal capacidade na classificação de arma coorbital.

Outra relevante tecnologia chinesa seria um veículo similar ao X-37B norte-americano, aparentemente podendo acoplar com a estação *Tiangong*. Segundo Brian Weeden e Victoria Samson (2021, p. 1-6) "em 4 de setembro de 2020, a China lançou em órbita o que chamou de nave experimental reutilizável, utilizando um foguete CZ-2F do Centro de Lançamento de Satélites de Jiuquan". Joseph Trevithick e Tyler Rogoway (2020) destacam a preocupação de autoridades norte-americanas quanto à possibilidade dessa aeronave possuir capacidades militares, tais como o uso de armas cinéticas ou a captura de outros satélites.

No campo missilístico, a China desenvolveu o míssil antissatélite SC-19, capaz de neutralizar satélites em órbitas baixas terrestres. Weeden e Samson (2021, p. 1-12) informam que "em 11 de janeiro de 2007, o SC-19 foi testado pela terceira vez a partir de Xichang e destruiu um defunto satélite meteorológico chinês, o FengYun 1C, a uma altitude de 865 km, criando milhares de pedaços de detritos orbitais".

No campo das armas coorbitais, o satélite de captura de objetos Shijan SJ-17, que possuiria ganchos para abordar outros objetos no espaço. Esteban Pardo (2022) afirma que uma satélite chinês, que denomina SJ-21 (porém, mais provavelmente seja o SJ-17), teria sido observado no espaço capturando um outro satélite e transportando-o para uma outra órbita. Tal capacidade é significativa,

pois a manobra satelital em órbita, mesmo que exija um planejamento meticuloso, avançaria na hipótese de neutralização de capacidades dos meios do oponente.

A China também possui uma forte cultura no desenvolvimento de equipamentos capazes de interferir eletronicamente em sistemas de navegação global por satélite (*Global Navigation Satellite System* – GNSS), como aparenta ser um dispositivo instalado, em 2018, nas Ilhas Spratly, no Mar do Sul da China (GORDON; PAGE, 2018). Na classificação anteriormente apresentada, trata-se de uma inciativa no campo da guerra eletrônica.

Um tema que tem gerado grande repercussão atualmente é a suposta capacidade chinesa de lançamento de um míssil hipersônico, com característica de bombardeamento orbital fracionado (*Fractional Orbital Bombardment System* – FOBS). Ele é um míssil que utiliza uma baixa órbita terrestre (até 150 Km) em direção ao seu alvo, à velocidade hipersônica. Em face dessas características, a imprevisibilidade da trajetória de navegação do míssil e a impossibilidade de neutralização dele, torna-o uma arma de grande relevância na guerra aeroespacial.

Com relação ao que aponta o GCC, a China já possui significativas capacidades operacionais de ascensão direta contra satélites em órbitas baixas, guerra eletrônica e de SDA, ao passo que certa capacidade pode ser observada, em fase de testes, na questão de ASAT nas órbitas média e geoestacionária. Tal diagnóstico leva autores como Harrison *et al.* (2021, p. 10) a afirmar que "A China pode ameaçar qualquer satélite dos EUA em órbitas baixas, e provavelmente em órbitas médias e geoestacionárias da mesma forma".

4.3 RÚSSIA

A Rússia tem sido um ator relevante nesse campo desde a Guerra Fria, com a corrida espacial. No caso da capacidade cinética física, já existiriam equipamentos como o PL-19 Nudol, um míssil antissatélite com efetividade em órbitas baixas terrestres. Além disso, há grande expectativa com relação ao S-500, também uma ASAT. De acordo com Weeden e Samson (2021, p. 2-22) "existem poucas informações sobre o S-500 no domínio público, mas parece ser um interceptador exoatmosférico, capaz de destruir não apenas mísseis balísticos antes da reentrada, mas também objetos em órbita".

No campo da guerra eletrônica, a Rússia tem desenvolvido muitos equipamentos. Um deles é o Tirada-2, especialista em interferir em comunicações satelitais. O Tirada-2 poderia ser usado para infligir "danos permanentes aos sistemas de comunicações via satélite a bordo, e projetado para cobrir diferentes partes do espectro eletromagnético, no *uplink* (transmissão da superfície para o satélite) das comunicações" (HENDRICKX, 2020).

Um fato muito interessante, com grande potencial de análise para a guerra aeroespacial, foi a ação conjunta de dois satélites russos. O satélite Cosmos 2542

transportou um outro satélite, o Cosmos 2543 e, este, teria disparado uma arma no espaço. De acordo com Gunter Krebs (2022) "em julho de 2020, um objeto separado do Cosmos 2543 apresentava características de uma arma antissatélite baseada no espaço".

Outra capacidade relevante é o dispositivo *Peresvet*, um sistema avançado de laser móvel brilhante, que parece ser projetado para proteger os misseis balísticos móveis de serem fotografados a partir do espaço exterior, cegando sensores dos satélites de observação.

De acordo com os autores do relatório GCC "há fortes evidências de que a Rússia embarcou em um conjunto de programas, desde 2010, para recuperar muitas capacidades *counterspace* da era da Guerra Fria" (WEEDEN; SAMSON, 2021, p. xvii). No relatório, aponta-se que a Rússia já teria utilizado em conflito militar as capacidades de guerra eletrônica. Teria condições operacionais efetivas em torno de SDA e estaria realizando testes com armas coorbitais de órbitas baixas. Além disso, estariam em desenvolvimento, em uma fase avançada, as ASAT cinéticas para órbitas baixas e com relação à energia direcionada.

5 CONCLUSÃO

Apesar das evidências em torno da guerra aeroespacial, segundo Rebecca Reesman e James Wilson (2021) ela ainda será "frustrante para os fãs de Guerra nas Estrelas", ao menos com as tecnologias disponíveis nos próximos anos. No espaço exterior, o movimento é lento e meticuloso, apesar da velocidade dos satélites em órbita estar em torno de 3 a 8 km/s (comparativamente, um projetil de arma de fogo se desloca a 0,75 km/s). A movimentação dos atuais satélites é previsível e rastreável e o volume representado pelas órbitas baixas e geoestacionárias é 190 vezes maior que o volume da Terra.

Contudo, mesmo que a ficção científica não seja um bom parâmetro para a guerra aeroespacial de hoje, ela não deixa de apontar importantes elementos que devemos considerar sobre esse espaço estratégico que é o ambiente aeroespacial. Até porque, já existem conceitos em doutrinas militares que tratam do espaço como um ambiente de batalha. Apenas para citar dois exemplos, o Dicionário de Termos Militares e Associados do Departamento de Defesa dos EUA (UNITED STATES OF AMERICA, 2020b, p. 198) cita o "controle do espaço como [o campo] de operações para garantir liberdade de ação no espaço para os EUA e seus aliados e negar a um adversário a liberdade de ação no espaço". O outro exemplo advém do *Primer* da Força Aérea dos EUA. Nesse documento, que é uma iniciação de doutrina militar, cita-se que

> O valor inerente do espaço é como meio de comunicação; portanto, a guerra espacial deve funcionar direta ou

> indiretamente para assegurar o comando do espaço ou impedir que o inimigo o assegure. O domínio do espaço não significa que o adversário não possa agir, apenas que ele não pode interferir seriamente em nossas ações. Além disso, o domínio do espaço normalmente estará em disputa. (ACSC, 2009, p. 38).

Também no campo da teoria já existem consensos em torno dessas ideias, mesmo que ainda não haja integralmente uma teoria do poder espacial, como observamos acima. John Klein (2006, p. 60) considera o "comando do espaço como a capacidade de garantir o acesso e uso de linhas celestiais de comunicação quando necessário para apoiar os instrumentos do poder nacional – diplomático, econômico, informativo e militar".

O capítulo procurou lidar com essas questões sob as perspectivas geográfica, de estratégias e tecnológica. Incialmente, apresentou o conceito de ambiente aeroespacial. Apropriando-se da epistemologia da geografia, sob o ponto de vista teórico, tratou-se de geografizar esse domínio como forma de viabilizá-lo como objeto de estudo da guerra. Em seguida, com a percepção do substrato geográfico sob o qual repousa a discussão e complementando a estruturação teórica dos argumentos, percebemos que a o ambiente aeroespacial foi, gradativamente, se configurando com um domínio da guerra. Para tanto, recorremos à evolução da teoria do poder aeroespacial para observar como ela direciona o tema da guerra para o ambiente aeroespacial.

Este texto termina com um levantamento sobre como se pensa estratégia militar no espaço exterior, assim como no apontamento de tecnologias que têm sido desenvolvidas, algumas delas já em operação, por países como os EUA, China e Rússia. Essa caracterização procurou dar uma visão abrangente, sintética e, principalmente, relacionando-as às capacidades antevistas para a guerra nesse domínio. Nesse sentido, confirmamos que ela se dá não somente no, ou a partir do espaço exterior, constatação que nos levaria a recomendar o uso do conceito de guerra aeroespacial.

Pensar o ambiente aeroespacial como uma fronteira final abre espaço para uma série de considerações: fronteira final de expansão dos territórios nacionais; de exploração de recursos naturais; de um novo processo colonialista; de desenvolvimento da tecnologia e de uma nova doutrina de poder. E por que não, de novos conflitos de natureza militar. Por esse motivo, nunca é demais relembrar as palavras do escritor romano do século VI, Flávio Vegécio: *Si vis pacem para bellum!*

REFERÊNCIAS

ACSC. *AU-18 Space Primer.* Maxwell Air Force Base: Air University Press, 2009. Air Command and Staff College.

ALMEIDA, A. L. D. *A evolução do poder aeroespacial brasileiro.* São Paulo: Universidade de São Paulo, 2006. Dissertação.

AL-RODHAN, N. R. F. *Meta-Geopolitics of outer space:* an analysis of space power, security and governance. Hampshire: Palgrave Macmillan, 2012.

BAYLIS, J.; WIRTZ, J. J.; GRAY, C. S. (Eds.) 4th. ed. *Strategy in the contemporary world:* an introduction to strategic studies. Oxford: Oxford University Press, 2013.

BIDDLE, T. D. *Air power and warfare:* a century of theory and history. Carlisle: US Army War College Press, 2019.

BOGOTA DECLARATION. *Declaration of the first meeting of equatorial countries adopted in 3 december 1976.* Bogota, 1976. Disponível em: https://www.jaxa.jp/library/space_law/chapter_2/2-2-1-2_e.html. Acesso em: 31 jul. 2020.

BONNETT, A. *What is Geography?* London: Sage Publications, 2008.

BOOT, M. *War made new:* weapons, warriors, and the making of the modern world. New York: Gotham Books , 2006.

BRASIL. *Constituição da República Federativa do Brasil.* Texto constitucional promulgado em 5 de outubro de 1988. Brasília: Senado Federal, Coordenação de Edições Técnicas, 2016. Com as alterações determinadas pelas Emendas Constitucionais de Revisão nº 1 a 6/94, pelas Emendas Constitucionais nº 1/92 a 91/2016 e pelo Decreto Legislativo nº 186/2008.

CAVALCANTI, A. P. B.; VIADANA, A. G. Fundamentos históricos da Geografia: contribuições do pensamento filosófico na Grécia antiga. In: GODOY, P. R. T. (Ed.) *História do pensamento geográfico e epistemologia em geografia.* São Paulo: Cultura Acadêmica, 2010.

CHAPMAN, B. *Space warfare and defense:* a historical encyclopedia and research guide. Santa Barbara, Denver, Oxford: ABC Clio, 2008.

CHUN, C. K. S. *Aerospace power in the 21st century:* a basic primer. Maxwell Air Force Base: Air University Press, 2004.

CLAUSEWITZ, C. V. *On War.* Tradução de Michael Howard e Peter Paret. Princeton: Princeton University Press, 1984.

COHEN, S. B. *Geography and politics in a divided world.* Methuen, London: Methuen & Co. Ltd. , 1963.

COHEN, S. B. *Geopolitics:* the geography of international relations. 3rd. ed. London: Rowman&Littlefield, 2015.

CORREIA, P. D. P. *Manual de Geopolítica e Geoestratégia*. Lisboa: Edições 70, 2018.

COSGROVE, D. Contested global visions: one-world, whole-earth, and the Apollo space photographs. *Annals of the Association of American Geographers*, Oxford, v. 84(2), p. 270-294, 1994.

DEPTULA, D. A. The St. Andrews proclamation: a pragmatic assessment of 21st century airpower. *Mitchell Institute Policy Papers*, v. 12, p. 1-15, June 2018.

DEUDNEY, D. Space: The high frontier in perspective. *Worldwatch Paper*, Washington, v. 50, 1982.

DOLMAN, E. C. *Astropolitik.* Classical geopolitics in the Space Age. London, Portland : Frank Cass, 2002.

DOUHET, G. *O domínio do ar.* Tradução de Escola de Aperfeiçoamento de Oficiais. Rio de Janeiro: INCAER, 1988.

ELVIS, M. Let's mine asteroids – for science and profit. *Nature*, v. 485, p. 549, May 2012.

EUSST. EU SST confirms the fragmentation of space object COSMOS 1408. *European Union Space Surveillance and Tracking*, 2021. Disponível em: https://www.eusst.eu/newsroom/eu-sst-confirms-fragmentation-cosmos-1408/ . Acesso em: 18 mar. 2022.

GORDON, M. R.; PAGE, J. China installed military jamming equipment on Spratly Islands, U.S. says. *The Wall Street Journal*, 2018. Disponível em: https://www.wsj.com/articles/china-installed-military-jamming-equipment-on-spratly-islands-u-s-says-1523266320. Acesso em: 17 nov. 2021.

GOURE, D.; SZARA, C. M. *Air and space power in the new millennium.* Washington: The Center For Strategic & International Studies, 1997.

GRAY, C. S. *Modern strategy.* Oxford: Oxford University Press, 1999.

GRAY, C. S.; SLOAN; GEOFFREY (Eds.). *Geopolitics, geography and strategy.* London: Frank Cass Publishers, 1999.

GRIER, P. The flying tomato can. *Air Force Magazine*, 2009. Disponível em: <https://www.airforcemag.com/article/0209tomato/>. Acesso em: 25 nov. 2021.

GUNSTON, B. *The Cambridge aerospace dictionary.* 2nd. ed. Cambridge: Cambridge University Press, 2009.

HARRISON, T. et al. *Space threat assessment 2021.* Washington: Centre for Strategic & International Studies, 2021.

HARRISON, T.; JOHNSON, K.; YOUNG, M. *Defense agaisnt the dark arts in space:* protecting space systems from counterspace weapons. Lanham, Boulder, New York, London: Center for Strategic & International Studies, 2021.

HARTSHORNE, R. *Perspectives on the nature of geography.* Chicago: Rand McNally & Co., 1959.

HAYS, P. L. *Space and security:* a reference handbook. Santa Barbara: ABC-CLIO, LLC, 2011a.

HAYS, P. L. National security space. In: SADEH, E. *The politics of space:* a survey. London, New York: Routledge, 2011b. p. 29-57.

HAYS, P.; MUELLER, K. Going boldly – where? Aerospace integration, the Space Comission, and the Air Force's vision for space. *Aerospace Power Journal*, p. 34-49, spring, 2001.

HENDRICKX, B. Russia gears up for electronic warfare in space (part 1). *The Space Review*, 2020. Disponível em: https://www.thespacereview.com/article/4056/1. Acesso em: 22 mar. 2022.

HERRMANN, H.; BUCKSCH, H. *Dictionary of geotechnical engineering.* 2nd. ed. Berlin, Heidelberg: Springer-Verlag, 2014.

HUGGETT, R.; ROBINSON, M. Introduction. In: DOUGLAS, I.; HUGGETT, R.; ROBINSON, M. *Companion encyclopedia of geography.* London, New York: Routledge, 1996.

JENNINGS, F. W. Genesis of the aerospace concept. *Air Power History*, p. 48-55, spring, 2001.

JORDAN, D. et al. *Understanding modern warfare.* Cambridge: Cambridge University Press, 2008.

KLEIN, J. J. *Space warfare:* strategy, principles and policy. New York, London: Routledge, 2006.

KOTLYAKOV, V. M.; KOMAROVA, A. I. *Elsevier's dictionary of geography.* Moscow : Elsevier, 2007.

KREBS, G. D. Kosmos 2542, 2543. *Gunter's Space Page*, 2022. Disponível em: https://space.skyrocket.de/doc_sdat/kosmos-2542.htm. Acesso em: 22 mar. 2022.

LAMBETH, B. S. *The transformation of american air power.* Ithaca, London: Cornell University Press, 2000.

MACKINDER, H. J. The geographical pivot of history. *The Geographical Journal*, London, v. 170, n. 4, 2004, p. 298-321, dec. 1904.

MAHAN, A. T. *The influence of sea power upon history - 1660 - 1783.* 12th. ed. Boston: Little, Brown and Company, 1890.

MARK, H. (Ed.). *Encyclopedia of space science and technology.* Hoboken: John Wiley & Sons, v. 1, 2003.

MASON, T. *Air power:* a centennial appraisal. London: Brassey's Ltd., 1994.

MAYHEW, S. *Oxford dictionary of geography*. Oxford: Oxford University Press, 2003.

MEILINGER, P. S. (Ed.). *The paths of heaven:* the evolution of airpower theory. Maxwell Air Force Base: Air University Press, 1997.

MITCHELL, W. *Winged defense:* the development and possibilities of modern air power - economic and military. Tuscaloosa: University of Alabama Press, 2009.

MORAES, A. C. R. *Geografia:* pequena história crítica. 20. ed. São Paulo: Annablume, 2005.

NORAD (NORTH AMERICAN AEROSPACE DEFENSE COMMAND). About NORAD. *www.norad.mil*, 2020. Disponível em: https://www.norad.mil/About-NORAD/. Acesso em: 03 ago. 2020.

OLSEN, J. A. (Ed.). *A history of air warfare*. Washington: Potomac Books, 2010.

OLSEN, J. A. (Ed.). *Routledge handbook of air power.* London, New York: Routledge, 2018.

PARDO, E. Satélite chinês de "limpeza espacial" flagrado no espaço. *Deutsche Welle*, 2022. Disponível em: https://www.dw.com/pt-br/sat%C3%A9lite-chin%C3%AAs-de-limpeza-espacial-flagrado-no-espa%C3%A7o/a-60792233. Acesso em: 17 fev. 2022.

PLANO, J. C.; OLTON, R. *The international relations dictionary*. 4th. ed. Santa Barbara, Oxford: ABC-Clio, 1988.

RATZEL, F. As leis do crescimento espacial dos estados. In: MORAES, A. C. R. (Ed.) *Ratzel.* São Paulo: Ática, 1892.

REESMAN, R.; WILSON, J. Physics gets a vote: no starcruisers for space force. *War on the Rocks*, 2021. Disponível em: https://warontherocks.com/2021/06/physics-gets-a-vote-no-starcruisers-for-space-force/. Acesso em: 30 jun. 2021.

SÁNCHEZ, J.-E. *Geografia política*. Madrid: Editorial Síntesis, 1992.

SANTIAGO, J. P. *Espaço geográfico e geografia do estado em Friedrich Ratzel.* Vitória da Conquista: Edições UESB, 2013.

SANTOS, M. *Evolução do poder aéreo.* Belo Horizonte, Rio de Janeiro: Itatiaia, INCAER, 1989.

SARK, S. M. *Astronomical geography.* Circleville: Union-Herald Publishing House, 1887.

SEVERSKY, A. N. P. D. *Air power:* key to survival. New York: Simon and Schuster, 1950.

SEVERSKY, A. P. D. *A vitória pela força aérea.* Tradução de Asdrubal Mendes Gonçalves. Belo Horizonte, Rio de Janeiro: Itatiaia, Instituto Histórico-Cultural da Aeronáutica, 1988.

SHEEHAN, M. *The international politics of space.* Oxon, New York: Routledge, 2007.

SPYKMAN, N. J. *The geography of the peace.* New York: Harcourt, Brace and Company, 1944.

STILWELL, B. The US Air Force's 'rods from god' could hit with the force of a nuclear weapon — with no fallout. *Insider*, 2019. Disponível em: https://www.businessinsider.com/air-force-rods-from-god-kinetic-weapon-hit-with-nuclear-weapon-force-2017-9. Acesso em: 26 nov. 2021.

STURDEVANT, R. W.; ANDERSON, H. Space effects in Operation Iraqi Freedom. *Quest*, v. 18:4, p. 25-27, 2011.

TIWARI, S. Chinese space station: why US remains 'highly apprehensive' of Tiangong & fears ceding military edge to Beijing. *The Eurasian Times*, 2022. Disponível em: https://eurasiantimes.com/chinese-space-station-why-us-tiangong-fears-ceding-military-edge/. Acesso em: 18 mar. 2022.

TOMÉ, A. J. V. A. *O domínio aeroespacial nas manifestações de poder:* efeitos nas relações internacionais. Lisboa: Universidade Lusófona de Humanidades e Tecnologias, 2009. Tese.

TRENCHARD, H. Memorandum by the Chief of the Air Staff for the Chiefs of Staff Sub-Committee on the war object of an air force, 2nd May 1928. In: THIN, J. *The pre-history of Royal Air Force area bombing, 1917-1942.* Canterbury: University of Canterbury, 2008. p. 141-144 (Appendix 6). Tese.

TREVITHICK, J.; ROGOWAY, T. China's secret spacecraft looks to have landed at this remote base with a massive runway. *The Drive/The War Zone*, 2020. Disponível em: https://www.thedrive.com/the-war-zone/36270/this-remote-base-with-a-massive-runway-looks-to-be-where-chinas-secretive-spacecraft-landed. Acesso em: 18 mar. 2022.

UNITED NATIONS. *Treaty on principles governing the activities of states in the exploration and use of outer space, including the Moon and other celestial bodies.* Geneva: Office of Outer Space Affairs, 1966. Disponível em: http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html. Acesso em: 13 out. 2019.

UNITED STATES OF AMERICA. *Space resource exploration and utilization act of 2015. H.R. 1508. June 15th, 2015.* Washington: House of Representatives, 2015.

UNITED STATES OF AMERICA. Fact Sheet. *www.spaceforce.mil*, U.S. Space Force, 2020a. Disponível em: https://www.spaceforce.mil/About-Us/Fact-Sheet. Acesso em: 11 maio 2020.

UNITED STATES OF AMERICA. *DOD Dictionary of military and associated terms.* Washington: Department of Defense, 2020b.

URRUTIA, D. E. Hurricane watch: how satellites track huge storms from space. *space.com*, 2017. Disponível em: https://www.space.com/38097-how-satellites-track-hurricanes-from-space.html. Acesso em: 27 mar. 2020.

WEEDEN, B.; SAMSON, V. *Global counterspace capabilities.* Washington: Secure World Foundation, 2021.

ZIEGLER, D. W. *Safe heavens:* military strategy and space sanctuary thought. Maxwell Air Force Base: Air University Press, 1998.

CYBER POLICY PAPERS - UMA TENDÊNCIA ATUAL?

Fernando Jose Soares da Cunha Mattos*

RESUMO
Neste século XXI, a digitalização de processos nas sociedades organizadas tem impactado em escala global. O indivíduo percebe, em suas rotinas, a presença deste fenômeno invisível aos olhos, porém onipresente. Como usuários deste universo digital, as pessoas – e os Estados – são, ao mesmo tempo, beneficiados pela denominada "Era da Informação", mas também vítimas dos ilícitos perpetrados nesta dimensão, o ECiber (Espaço Cibernético). Ainda diante de novas tecnologias ("Big Data", Inteligência Artificial e a Computação Quântica, para citar algumas), novas percepções sobre o ECiber são buscadas, bem como sua normatização. Em consequência, diversos países, recentemente, têm publicado seus posicionamentos próprios na forma de *policy papers*, como um instrumento de comunicação externa sobre a percepção desses Estados sobre o tema, e como este é entendido por cada um deles. Um comparativo de tais abordagens é objeto deste artigo.
Palavras-chave: Espaço Cibernético; Normatização; "Policy Papers"

CYBER POLICY PAPERS – UNA TENDENCIA ACTUAL?

RESUMEN
En este siglo XXI, la digitalización de procesos en las sociedades organizadas ha tenido un impacto a escala global. El individuo percibe, en sus rutinas, la presencia de este fenómeno invisible a los ojos, pero omnipresente. Como usuarios de este universo digital, las personas - y los Estados - son, al mismo tiempo, beneficiados por la llamada "Era de la Información", pero también víctimas de los actos ilícitos perpetrados en esta dimensión, el ECiber (Espacio Cibernético). Incluso de cara a las nuevas tecnologías ("Big Data", Inteligencia Artificial y Computación Cuántica, por nombrar algunas), se buscan nuevas percepciones sobre ECiber, así como su estandarización. Como resultado, varios países han publicado recientemente sus propias posiciones en forma de policy papers, como instrumento de comunicación externa sobre la percepción de estos Estados sobre el tema, y cómo es entendido por cada uno de ellos. Una comparación de tales enfoques es el objeto de este artículo.
Palabras clave: Espacio cibernético; Estandarización; Policy Papers.

* General de Divisão (R1), Assessor de Governança no Comando de Defesa Cibernética, Exército Brasileiro. Contato: cunhamattos@cdciber.eb.mil.br.

1 INTRODUÇÃO

Em 2020, foi aprovado o relatório do *Group of Governmental Experts (GGE) on Advancing responsible State behaviour in cyberspace in the context of international security* (Grupo de especialistas governamentais para promover o comportamento responsável do Estado no ciberespaço, no contexto da segurança internacional - abordado nesta análise), com a participação do BRASIL; embora um avanço, o citado relatório ainda não definiu temas importantes para a convivência pacífica entre Estados, na dimensão cibernética. Segundo compilação de várias fontes, por empresa dedicada à *cibersegurança*, a Varonis, no artigo *Cybersecurity Statistics and Trends for 2021***,** observa-se, entre outros dados (fonte origem sublinhada):

a) a grande maioria (86%) das violações (intrusões) em redes ou meios de Tecnologia de Informação e Comunicações (TIC), têm motivação financeira e 10% foram motivadas por espionagem. (*Verizon*);

b) o tempo médio para identificar uma intrusão, em 2020, foi de 207 dias. (*IBM*);

c) o pagamento médio de *ransomware* (intrusão para sequestro e resgate de dados) aumentou 33% em 2020, em relação a 2019, para U$ 111.605,00 (*Fintech News*); e

d) em 2023, o número total de ataques *DDoS* (ataques de negação de serviços de TIC) em todo o mundo será de 15,4 milhões. (*Cisco*).

Estes e outros dados atestam que os ilícitos no ECiber (ilícitos cibernéticos) têm em comum Técnicas, Táticas e Procedimentos (TTPs) em suas intrusões; o que os difere estão na origem, motivação e objetivo de tais ataques. Sob estes aspectos, os ilícitos cibernéticos a seriam compilados como:

a) o crime cibernético (mais comum);

b) o *hacktivismo* (pessoas ou grupos em busca de notoriedade ou divulgação);

c) a espionagem cibernética (obtenção de dados sigilosos de empresas ou países);

d) o terrorismo cibernético (executado por indivíduo ou grupos terroristas); e

e) a guerra cibernética (sujeita ao Direito Internacional dos Conflitos Armados-DICA / Direito Internacional Humanitário-DIH).

Neste século, a partir de 2007, mais especificamente, o noticiário internacional registra exemplos da ocorrência destes diferentes tipos de ilícitos, isolados ou em combinação, conforme exemplos da Figura 1:

Figura 1 – Giro no tempo: ilícitos cibernéticos marcantes

Fonte: O AUTOR, 2022.

Observa-se que a natureza dos ilícitos é variada: emprego em conflitos armados interestatais, o enfrentamento a grupos armados/terroristas, ou o sequestro de dados sobre infraestrutura crítica (*Colonial Pipeline*). Vale destacar que a participação dos Estados ocorre de modo dissimulado (atuação via grupos "apoiados", as APTs (*Advanced and Persitent Threats*). Em 2010, no ataque ao Irã via *Stuxnet* havia indícios de que Israel e os EUA fossem os responsáveis para sua atribuição, mas ninguém admitiu sua participação.

O *NotPetya* (2017) seria de origem russa, de acordo com relatórios confidenciais citados por funcionários da inteligência dos EUA. Este *malware*, bem como e o *WannaCry*, são exemplos de disseminação fora de controle de seus próprios (supostos) criadores, pois sistemas de TIC dos países de provável origem do artefato malicioso acabaram sendo infectados e/ou comprometidos. Dado interessante é que, neste momento, há tensões e conflitos – ainda – entre a Ucrânia e Rússia e têm tornado o primeiro país alvo de atividades maliciosas originárias do segundo.

Conclui-se parcialmente que há a conjugação da crescente ameaça dos ilícitos cibernéticos, por um lado, e a falta de regulamentação internacional assertiva para alguns destes ilícitos. Uma exceção positiva é a "Convenção de Budapeste" (2001), contra os crimes cibernéticos, à qual o Brasil aderiu, em 15 de dezembro de 2021. Também em atendimento às lacunas existentes na norma internacional, alguns países expediram documentos – aqui qualificados como *policy ou position papers* – sobre o tema cibernético. Tais diplomas têm normalmente com a participação

dos segmentos de relações exteriores e/ou defesa. A intenção é apresentar uma maior transparência sobre o tema perante a comunidade internacional, facilitando a comunicação entre os Estados envolvidos.

Neste artigo, alguns aspectos/princípios são importantes e recorrentes na comparação a seguir, são eles: atribuição (de responsabilidade); soberania; diligência devida; uso da força; autodefesa; contramedidas; e o de não intervenção. Para facilitar ao leitor, esses termos estarão apresentados em negrito, ao longo do texto.

2 ANÁLISE SUMÁRIA DE DOCUMENTOS SUPRANACIONAIS

2.1 RELATÓRIO DO "*GGE ON ADVANCING RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE IN THE CONTEXT OF INTERNATIONAL SECURITY*" (ONU, 2021)

2.1.1 Escopo

O Grupo (GGE) foi estabelecido em 2018 de acordo com o parágrafo 3º da resolução 73/266 da Assembleia Geral (AGe). Nesta resolução, a AGe solicitou que um grupo de peritos governamentais fosse estabelecido em 2019 com base na distribuição geográfica equitativa, proveniente das avaliações e recomendações contidas nos relatórios consensuais do GGE de 2010, 2013 e 2015, para continuar a estudar, com vista a promover entendimentos comuns e implementação efetiva, possíveis medidas cooperativas para enfrentar ameaças existentes e potenciais na esfera da segurança da informação, incluindo normas, regras e princípios de comportamento responsável dos Estados, medidas de fortalecimento da confiança e capacitação, bem como sobre como o direito internacional se aplica ao uso de tecnologias de informação e comunicação pelos Estados. De acordo com os termos da resolução, foram nomeados especialistas de 25 Estados, incluindo o BRASIL, os EUA, Rússia e China. Assinou o embaixador Guilherme de Aguiar Patriota.

Durante este trabalho o *Comitê Internacional da Cruz Vermelha* (CICV) encaminhou, em 2019, um *Position Paper*, (o CICV é uma Organização Humanitária, daí adotado termo *position*), intitulado *International Humanitarian Law and Cyber Operations during Armed Conflicts*. Temas com base neste documento são assinalados com a observação (CICV).

2.1.2 Destaques

A atividade maliciosa sobre sistemas de TIC, por parte de atores de ameaças persistentes, incluindo Estados e outros atores, pode representar um risco significativo para a segurança e estabilidade internacionais, o desenvolvimento econômico e social, bem como a segurança e o bem-estar dos indivíduos.

A atividade prejudicial de TIC contra infraestruturas críticas que fornecem serviços no mercado interno, regional ou global, que foi discutida em relatórios anteriores do GGE, está se tornando cada vez mais séria. Uma preocupação específica é a atividade maliciosa de TIC que afeta a infraestrutura de informação, a infraestrutura que fornece serviços essenciais ao público, a infraestrutura técnica essencial para integridade da Internet e entidades do setor de saúde. A pandemia COVID-19 demonstrou os riscos e consequências de atividades maliciosas de TIC que buscam explorar vulnerabilidades em tempos em que nossas sociedades estão sob enorme pressão.

É amplamente aceito que as operações cibernéticas com expectativa de causar morte, ferimentos ou danos físicos constituiriam ataques de acordo com o DIH. Na opinião do CICV, isso inclui danos devido aos previsíveis efeitos diretos e indiretos (ou ditos "reverberantes") de um ataque; por exemplo, a morte de pacientes em unidades de terapia intensiva causada por uma operação cibernética em uma rede de eletricidade que resulta no corte de um fornecimento de eletricidade ao hospital. Além disso, os ataques que interrompem significativamente os serviços essenciais sem necessariamente causar danos físicos constituem um dos riscos mais importantes para os civis. *Existem pontos de vista divergentes, no entanto, sobre se uma operação cibernética que resulta em uma perda de funcionalidade sem causar danos físicos se qualificaria como um ataque*, (grifo nosso) conforme definido no DIH **(**CICV).

O GGE reafirma que *a soberania do Estado e as normas e princípios internacionais decorrentes da soberania se aplicam à conduta dos Estados em atividades relacionadas às TIC e à sua jurisdição sobre a infraestrutura de TIC em seu território* (grifo nosso). Os Estados exercem jurisdição sobre a infraestrutura de TIC em seu território, *inter alia* (entre outros) definindo políticas e leis e estabelecendo os mecanismos necessários para proteger a infraestrutura de TIC em seu território contra ameaças relacionadas às TIC.

Quanto à atribuição, o GGE não especifica norma, porém, destaca-se que de acordo com o direito internacional, um Estado é responsável pela conduta que lhe é atribuída, incluindo possíveis violações do DIH. Isso inclui: conduta de órgãos do Estado, incluindo suas forças armadas ou serviços de inteligência; a conduta de pessoas ou entidades, tais como empresas privadas, quando o Estado concedeu poderes para exercer elementos de autoridade governamental; conduta de pessoas ou grupos, como milícias ou grupo de *hackers*, agindo de fato sob as instruções do Estado, ou sob sua direção ou controle (as ATP); e a conduta de particulares ou grupos que o Estado reconhece e adota como sua própria conduta (CICV).

Como conclusão parcial, o relatório foca nos temas de *proteção* de TIC e de *cooperação e* não aborda os conceitos de uso da força e de contramedidas no espaço cibernético. Entretanto, o CICV, assinala, no resumo executivo do seu *position paper* que:

> A interpretação das regras existentes do DIH pelos Estados determinará até que ponto o DIH protege contra os efeitos das operações cibernéticas. Em particular, os *Estados devem assumir posições claras* sobre seu compromisso de interpretar o DIH de modo a preservar a infraestrutura civil de interrupções significativas e proteger os dados civis. A disponibilidade de tais posições também influenciará a avaliação se as regras existentes são adequadas ou se novas regras podem ser necessárias. Se os Estados virem a necessidade de desenvolver novas regras, eles devem desenvolver e fortalecer a estrutura legal existente - incluindo o DIH. (CICV, 2019, p.2, grifo nosso).

2.1.3 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

É um documento elaborado pelo CCDCOE (*NATO Cooperative Cyber Defence Centre of Excellence* ou Centro de Excelência em Defesa Cibernética Cooperativa da Organização do Tratado do Atlântico Norte-OTAN), órgão com sede em Talin, Estônia. Embora o manual tabule um total de 154 possíveis regras, os princípios/ regras analisados neste resumo são: soberania; diligência devida; uso da força; autodefesa e o de não intervenção.

2.2 SOBERANIA

O princípio da soberania do Estado se aplica ao ciberespaço (Regra 1). Uma definição bem aceita foi estabelecida na *Sentença Arbitral da Ilha de Palmas*, a qual cita que: "A soberania nas relações entre os Estados significa independência. Independência em relação a uma parte do globo é o direito de exercer nela, com exclusão de qualquer outro Estado, as funções de um Estado. " (HUBER, Max. *Corte Permanente de Arbitragem em Haia*, 1928).

O ciberespaço tem sido descrito de várias maneiras como um "domínio global" ou 'quinto domínio' que carece de fisicalidade e é de natureza virtual. Também, às vezes, sugerido que deveria ser comparado ao alto mar, ao espaço aéreo internacional, ou ao espaço exterior no sentido de constituir um 'comum global' (*a res communis omnium*). Embora tais caracterizações possam ser úteis em contextos diferentes dos jurídicos, o GIP (Grupo Internacional de Peritos) que elaborou o manual não as adotou.

Atividades cibernéticas ocorrem no território e envolvem objetos, ou são realizadas por pessoas ou entidades, sobre as quais os Estados podem exercer suas prerrogativas de soberania. Em particular, o GIP observou que, embora as atividades cibernéticas possam cruzar múltiplas fronteiras ou ocorrer em águas internacionais, no espaço aéreo internacional ou no espaço sideral, todas são

conduzidas por indivíduos ou entidades sujeitas à jurisdição de um ou mais Estados.

Um Estado goza de autoridade soberana com relação à infraestrutura cibernética, pessoas e atividades cibernéticas localizadas em seu território, sujeito às suas obrigações legais internacionais (Regra 2). No que diz respeito à soberania interna de um Estado, seria irrelevante para o direito internacional se a infraestrutura cibernética em questão é de caráter público ou privado. Por exemplo, um Estado tem direitos/atribuições sobre um *Internet Service Provider* (provedor de *internet ou* ISP) localizado em seu território, mesmo se o ISP estiver domiciliado no exterior.

Um Estado é livre para conduzir atividades cibernéticas em suas relações internacionais, sujeito a qualquer norma contrária do direito internacional que o vincule (Regra 3). A soberania externa deriva da igualdade soberana de Estados, conforme reconhecido no Artigo 2º da Carta das Nações Unidas; os Estados são juridicamente iguais. Soberania externa significa que um Estado é independente em suas relações externas de outros Estados e é livre para se envolver em atividades cibernéticas fora de seu território, sujeito apenas ao direito internacional. Entretanto, *Estados são livres para decidir se optam por regimes de tratados cibernéticos específicos ou emitem manifestações de opinio juris sobre a natureza do direito consuetudinário de qualquer prática cibernética de um Estado* em particular (grifo nosso).

Um Estado não deve realizar operações cibernéticas que violem a soberania de outro Estado (Regra 4). Sobre esta regra houve análise em três níveis distintos:

a) dano físico;

b) perda de funcionalidade; e

c) violação da integridade territorial abaixo do limite de perda de funcionalidade.

Em primeiro lugar, a maioria dos especialistas concordou que as operações cibernéticas constituem uma violação da soberania no caso de resultar em danos físicos ou ferimentos, como no caso de *malware* que causa o mau funcionamento dos elementos de resfriamento do equipamento, levando a superaquecimento, o qual resultaria em componentes destruídos. Também a presença física não consensual no território de outro Estado para realizar operações cibernéticas equivale à mesma violação. Os peritos observaram que tais operações também podem, ainda, constituir intervenção proibida (Regra 66), um uso ilegal da força (Regra 68) ou mesmo um ataque armado (Regra 71).

2.2.1 Diligência Devida (due diligence)

Um Estado deve exercer diligência devida de modo a não permitir que seu território, ou infraestrutura cibernética sob seu controle governamental, sejam usados para operações cibernéticas que afetem os direitos de outros Estados e que produzam graves consequências adversas para estes países (Regra 6). A obrigação

da diligência devida aplica-se a todo o território do Estado. Observe que a parte que está iniciando a operação cibernética em questão pode estar operando remotamente de um terceiro país. Por exemplo, considere um grupo de *hackers* localizado no Estado A que realiza uma operação cibernética destrutiva contra o Estado B usando infraestrutura cibernética localizada no Estado C; caso C saiba de tal uso e não tomar medidas viáveis para encerrar a operação, seria violação do princípio de diligência devida.

O princípio supracitado exige que um Estado adote todas as medidas viáveis para pôr fim às operações cibernéticas que afetam um direito de outros Estados e produzem graves consequências adversas para estes países (Regra 7). Considere um caso em que uma agência de inteligência se infiltrou em um fórum *online* fechado usado por um grupo terrorista baseado em seu território. A agência descobre que o grupo instalou *malware* destrutivo na infraestrutura cibernética da bolsa de valores de outro estado que está prestes a ser ativada. Nesta situação, o Estado deve agir para interromper a operação cibernética, pois é muito provável que venha a acontecer. Os especialistas concordaram que a diligência devida seria uma regra de direito internacional (Regras 6-7),

A Holanda é bem explícita sobre esta regra; o país reserva-se o direito de solicitar a um país cujos servidores estão sendo usados para cometer um ataque cibernético que desligue esses servidores, independentemente de o Estado estar realmente patrocinando o ataque (MALAGUTTI, 2019); esta é uma posição que vários outros países também adotam, tais como: Áustria, Chile, Equador, Guatemala, Guiana, Japão, Peru, República da Coréia, República Dominicana e República Tcheca. Em outro entendimento há declarações contrárias feitas até agora pela Argentina, Israel, Nova Zelândia e Reino Unido, que rejeitam ou questionam a aplicabilidade dos deveres de diligência devida se aplicada às TIC (COCO; DIAS, 2021, p. 782). Assim, tal critério ainda não teria alcançado o status de regra vinculativa do direito internacional, mas é um princípio mais "consuetudinariamente" aceito perante os outros atributos e regras abordados neste artigo.

2.2.2 Uso da Força

Uma operação cibernética *constitui um uso da força quando sua escala e efeitos são comparáveis a operações não cibernéticas que chegam ao nível do uso da força* (Regra 69, grifo nosso). Alguns conceitos para análise são mais concretamente aceitos em caracterizar tal uso são:

a) Grau de impacto - as consequências que envolvem danos físicos a indivíduos ou a propriedades irão por si mesmas qualificar uma operação cibernética como um uso de força; aqueles que geram mera "inconveniência" não se enquadrariam; assim, quanto mais consequências afetam os interesses nacionais críticos, mais elas

contribuirão para a sua descrição como de uso da força; *nesse sentido, o escopo, a duração e a intensidade das consequências terão grande influência* na avaliação de sua gravidade; o grau de impacto (gravidade do ato) *é o fator mais significativo* na análise (grifo nosso);

b) Caráter militar - um nexo entre a operação cibernética em questão e as operações militares aumenta a probabilidade de caracterização como um uso da força; esta afirmação é apoiada pelo fato de que a Carta da ONU está particularmente preocupada com ações militares. Além disso, tal uso tem sido tradicionalmente entendido como implicando de que a "força" seja empregada por militares ou forças armadas;

c) Envolvimento do Estado - a extensão da participação de um Estado em uma operação cibernética está ao longo de um *continuum* de operações conduzidas pelo próprio Estado (por exemplo, as atividades de suas forças armadas ou agências de inteligência), até aquelas em que seu envolvimento é periférico; quanto mais claro e próximo for o nexo entre um Estado e as operações cibernéticas, mais provável é que outros Estados as caracterizem como uso da força por esse Estado; e

d) Legalidade presumida - o direito internacional é geralmente de natureza proibitiva. Atos que não são proibidos são permitidos; na ausência de um tratado expresso ou de uma proibição do direito consuetudinário aceita, um ato é presumivelmente legal. Por exemplo, o direito internacional não proíbe propaganda, operações psicológicas ou mera pressão econômica *per se*; portanto, os atos que se enquadram nessas e em outras categorias seriam presumivelmente legais.

A regra 69, portanto, auxiliaria a definir características que caracterizariam o uso da força no ECiber, especialmente em seu grau de impacto, como visto.

2.2.3 **Autodefesa**

Um Estado que é alvo de uma operação cibernética, se esta chega ao nível de um ataque armado, poderia exercer seu direito inerente de autodefesa. Já se uma operação cibernética constitui um ataque armado depende de sua *escala e efeitos* (Regra 71, grifo nosso). De acordo com o Artigo 51 da Carta das Nações Unidas:

> Nada na presente Carta prejudicará o direito inerente à legítima defesa individual ou coletiva se ocorrer um ataque armado contra um Membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para manter a paz e a segurança internacionais. As medidas tomadas pelos Membros no exercício deste direito de autodefesa serão imediatamente comunicadas ao Conselho de Segurança e não afetarão de forma alguma a autoridade e responsabilidade do Conselho de Segurança sob a presente Carta de tomar a qualquer momento as medidas que julgar convenientes,

> julgar necessário para manter ou restaurar a paz e a segurança internacionais. (CARTA DAS NAÇÕES UNIDAS, 1945).

Este artigo reconhece e reflete o direito de legítima defesa. O GIP observou que os termos "ataque armado" e "agressão" devem ser distinguidos. Esta regra trata da autodefesa, para a qual a condição precedente é um ataque armado. A agressão, por outro lado, é uma das situações em que o Conselho de Segurança da ONU pode usar seus poderes de acordo com o Capítulo VII da Carta da ONU. Embora um ato de agressão possa constituir um ataque armado, nem sempre o é.

O direito de empregar força em autodefesa vai além de ataques armados cinéticos, para àqueles que são perpetrados exclusivamente por meio de operações cibernéticas. O grupo de especialistas concluiu por unanimidade que algumas operações cibernéticas podem ser suficientemente graves para justificar sua classificação como um "ataque armado" no sentido da Carta da ONU (grifo nosso). Por exemplo, é universalmente aceito que ataques químicos, biológicos e radiológicos da escala e efeitos necessários para constituir ataques armados desencadeiam o direito de autodefesa, apesar de sua natureza não cinética, porque as consequências daí resultantes podem incluir sofrimento grave ou morte. Raciocínio idêntico aplicar-se-ia às operações cibernéticas.

A unanimidade do GIP sobre este aspecto foi um caso raro de consenso nos trabalhos; porém, os parâmetros de caracterizar o "ataque armado cibernético" (e o direito à autodefesa) ou uma "agressão" continuariam, quase sempre, motivo de debates.

2.2.4 Não Intervenção

Um Estado não pode intervir, inclusive por meios cibernéticos, nos assuntos internos ou externos de outro Estado (Regra 66). O ciberespaço apresenta aos Estados oportunidades de intervenção nos assuntos internos ou externos de outros Estados, em particular devido ao aumento da conectividade global e à crescente dependência dos Estados da tecnologia da informação. Esta regra proíbe a intervenção coercitiva, inclusive por meios cibernéticos, por um Estado nos assuntos internos ou externos de outro. Baseia-se no princípio da soberania do direito internacional, especificamente no aspecto do princípio que prevê a igualdade soberana dos Estados (Regras 1–3). O GIP concordou que a proibição de intervenção é uma norma do direito internacional consuetudinário.

A ONU não poderia intervir, inclusive por meios cibernéticos, em assuntos que são essencialmente da jurisdição interna de um Estado. Este princípio não prejudica a adoção de medidas de coação decididas pelo Conselho de Segurança da ONU de acordo com o Capítulo VII da Carta das ONU (Regra 67). Este é um ponto especialmente importante com relação às operações cibernéticas porque

a natureza interconectada da infraestrutura e das atividades cibernéticas significa que as atividades relacionadas ao ciberespaço realizadas em um Estado geralmente afetam as de outro.

2.2.5 Conclusão Parcial

Na maioria das regras analisadas, não houve unanimidade do grupo de especialistas. Ainda assim, considerações sobre autodefesa, efeitos cinéticos ou causadores de baixas sobre a população como sendo de natureza grave, podem ser elencados como subsídios extraídos deste manual. A aplicabilidade da soberania como regra de direito internacional decorre também de jurisprudência da Corte Internacional de Justiça (CIJ) em casos como do Canal de Corfu (Albânia x RU_1949) e Nicarágua x EUA (1986).

A versão 3.0 do citado manual já está com sua pesquisa iniciada, segundo o *site* do CCDCOE[1].

3 OS *POLICY/POSITION PAPERS* ANALISADOS

Os três países analisados, todos europeus, têm características distintas, entretanto, o que produz variedade na abordagem do tema cibernético, como Estados soberanos. A França, embora membro da OTAN (Organização do Tratado do Atlântico Norte), tem uma política externa mais independente como ator, além de membro permanente do Conselho de Segurança da ONU e sua capacidade nuclear. A Itália também é integrante da OTAN, mas sem as qualificações francesas já citadas. A Suíça é caracterizada por sua neutralidade (desde 1815) e de sua independência; só ingressou, completamente, à ONU, em 2002.

3.1 FRANÇA

O país expediu, em 2019, uma declaração significativa como país soberano, sobre a aplicação do direito internacional no ciberespaço, o *Droit International Appliqué aux Opérations dans le Cyberspace.* Considera que sendo um espaço de oportunidade propício para o progresso, mas também para confronto, o ciberespaço oferece amplas possibilidades de ação aos atores que lá investem. Se a França pretende prevenir, proteger, antecipar, detectar, reagir e ter meios para atribuir *ciberataques*, também se reserva o direito de responder aos ataques.

A declaração destaca algumas *key messages* (pontos chave) nesta comunicação à comunidade internacional, a saber:

1 O Tallinn Manual 3.0 manterá a abordagem de seus predecessores. É um trabalho acadêmico de renomados acadêmicos e profissionais de direito internacional que se destina a fornecer uma reafirmação objetiva do direito internacional aplicado no contexto cibernético.

a) A França reserva-se o direito de responder a qualquer ataque cibernético que infrinja o direito internacional;

b) Ataques cibernéticos podem constituir uma violação da soberania, pois algumas operações cibernéticas podem violar a proibição de ameaça ou uso de força (no espaço digital, cruzar o limiar do uso da força não depende dos meios digitais empregados, mas dos efeitos que a operação cibernética causar);

c) Um ataque cibernético que causa danos de escala ou gravidade significativa pode constituir um ataque armado que dá direito ao uso de autodefesa. Tal uso, entretanto, *não reconhece a legalidade do uso da força com fundamento na legítima defesa preventiva* (grifo nosso); em resposta a um ataque armado realizado por meio de um vetor digital, a resposta, via meios digitais ou convencionais deve atender aos critérios de necessidade e proporcionalidade;

d) O não cumprimento por outro Estado de seu requisito de diligência devida não é motivo suficiente para o uso da força contra ele no contexto de ataques cibernéticos realizados a partir de seu território; e

e) A atribuição de um ataque cibernético com origem em outro Estado é uma *decisão política* nacional (grifo nosso).

Uma operação cibernética pode constituir ataque, na acepção do DIH (ao contrário da definição dada pelo Manual de Tallinn, a França não caracteriza um ataque cibernético apenas com base em critérios materiais; assim, nessa visão, uma operação cibernética constitui um ataque se o equipamento ou sistemas visados não puderem mais fornecer o serviço para o qual foram implementados).

Sobre o quesito soberania, a França assertivamente aponta, como uma questão de lei e política, da soberania como regra. Sobre o uso da força há limites; a regra geral é a adoção de contramedidas. Nos casos mais graves, constituindo uma ameaça à paz e segurança, a França também pode levar a questão ao Conselho de Segurança ao abrigo do Capítulo VI da Carta da ONU, ou mesmo do Capítulo VII, se houver uma ameaça à paz ou violação da paz.

A atribuição de responsabilidade a um Estado como autor de um ataque cibernético, foi interessantemente abordada como sendo uma decisão política do governo francês (influencia na narrativa), pois um ataque cibernético é considerado instigado por um Estado se perpetrado por um órgão estatal, uma pessoa ou entidade que exerce elementos de autoridade governamental, ou uma pessoa ou grupo de pessoas agindo sob as instruções ou sob a direção ou controle daquele Estado, em suma, um agente do estado.

No quesito diligência devida, a comunidade internacional está dividida quanto à questão de saber se a esta é uma obrigação vinculativa no ciberespaço. A França e vários outros Estados-chave no discurso normativo - como a Holanda, a Estônia e a Finlândia - endossam seu status como regra legal; porém, a França diz que o não cumprimento por outro Estado de seu requisito de diligência devida, não é motivo suficiente para o uso da força contra o mesmo.

No tema de autodefesa, a decisão de responder é, ao cabo, uma decisão política, e tomada em conformidade com o direito internacional. Essa resposta pode incluir o uso de força, dependendo da gravidade do ataque cibernético. A França pode considerar respostas diplomáticas a certos incidentes, contramedidas ou mesmo ações coercitivas das forças armadas, se um ataque constituir agressão armada.

No quesito da não intervenção, a França coloca-se em posição de, caso atacada, a escala deste pode ensejar a violação deste princípio, a ser respeitado à luz do direito internacional. Em síntese, o *policy paper* francês traduz a reconhecida independência do país em suas posturas nas relações internacionais.

3.2 ITÁLIA

Em setembro de 2021, foi a vez de a Itália trazer a púbico o seu *position/ policy paper* a respeito da aplicabilidade da Lei Internacional e o Ciberespaço, por intermédio do documento denominado *Italian Position Paper on International Law and Cyberspace*; A Itália considera que o direito internacional é aplicável ao ciberespaço e o considera a disciplina jurídica existente e uma ferramenta fundamental para garantir o comportamento responsável do Estado no ciberespaço.

Os seguintes tópicos foram considerados separadamente: a proteção da soberania no ciberespaço e as violações do princípio de não intervenção; a aplicação da lei da responsabilidade internacional dos Estados às atividades realizadas no ciberespaço; operações cibernéticas e uso da força; a aplicação do direito internacional dos direitos humanos, o papel das partes interessadas privadas; e cooperação internacional no ciberespaço. No que se refere especificamente ao uso da força, ao mesmo tempo em que reafirma os princípios gerais e a validade do *jus ad bellum* e do *jus in bello*[2] no ciberespaço, a Itália destaca que o Direito Internacional Humanitário (DIH) é restritivo, pois visa limitar a conduta dos beligerantes que afeta civis e objetos civis em um conflito armado. Portanto, o reconhecimento de sua aplicabilidade ao ciberespaço não significa incentivar ou permitir o uso da força como instrumento de agressão e/ou meio de solução de controvérsias internacionais.

A Itália também atribui importância fundamental à aplicação do princípio da soberania ao ciberespaço, incluindo suas regras acessórias, como o direito à autodeterminação interna. A Itália considera que tanto os aspectos internos como externos da soberania se aplicam no ciberespaço. O princípio da soberania

2 Jus ad bellum e jus in bello - A diferença mais importante é a que se estabelece entre o jus in bello (ou DIH), que regula a forma como as hostilidades são conduzidas, e o jus ad bellum, que se refere aos motivos da guerra. Em alguns aspectos, existem superposições entre o DIH, o Direito Internacional dos Direitos Humanos e o Direito dos Refugiados. Disponível em: https://cvbrn.org/site/direito-internacional-humanitario/.

é uma regra primária do direito internacional, cuja violação equivale a um ato internacionalmente ilícito.

A Itália acredita, ainda, que as operações cibernéticas constituem uma violação do princípio consuetudinário de não intervenção nos assuntos internos de outros Estados quando um Estado emprega meios coercitivos para obrigar outro Estado a empreender ou desistir de uma ação específica, em questões que se enquadram no seu *domaine réservé*[3].

Já atribuir responsabilidade por atividades cibernéticas é uma questão complexa que levou a diferentes abordagens na comunidade internacional. A Itália considera que a *atribuição é uma prerrogativa da soberania nacional* (grifo nosso) e também a decisão de a tornar pública ou não, caso a caso. A Itália concorda com a opinião de que a atribuição de atos ilícitos cibernéticos de um Estado a outro é regida pelas regras gerais do direito internacional sobre a conduta do Estado, conforme codificado pelos artigos da Comissão de Direito Internacional (ILC) sobre a responsabilidade dos Estados por atos internacionalmente ilícitos Atos (ARSIWA). Ainda assim, *a Itália reconhece as dificuldades de aplicar o ARSIWA em um ambiente peculiar como o ciberespaço* (grifo nosso).

A Itália considera que essas obrigações de diligência se aplicam no ciberespaço, conforme definido no caso do *Canal de Corfu* pelo Tribunal Internacional de Justiça (CIJ), segundo o qual todo Estado tem a obrigação de não permitir, conscientemente, que seu território seja usado para atos contrários ao direito de outros Estados. Portanto, a diligência devida exige que os Estados tomem todas as medidas razoáveis em relação às atividades no ciberespaço sob sua jurisdição, a fim de prevenir, eliminar ou mitigar danos potencialmente significativos aos interesses legalmente protegidos de outro Estado, ou do direito internacional como um todo. A diligência *é uma obrigação de conduta, não de resultados* (grifo nosso). Consequentemente, enquanto fizer seus melhores esforços, um Estado não pode ser responsabilizado se, em última instância, não puder prevenir, mitigar ou encerrar atividades cibernéticas ilícitas lançadas de ou em trânsito em seu território.

Quanto ao uso de contramedidas, o país é da opinião que, quando um Estado é vítima de um ato ilícito internacional perpetrado por outro Estado, pode tomar medidas defensivas em resposta. A Itália considera que as *contramedidas são respostas adequadas às operações cibernéticas que constituem um ato ilícito internacional abaixo do limiar de um ataque armado* (grifo nosso); isto sem prejuízo do direito inerente dos Estados à legítima defesa. A resposta a uma operação cibernética ilícita pode ser de mesmo tipo/modelo (mas não necessariamente, de acordo com a legislação internacional), com a condição de que a resposta seja

3 A noção de domaine réservé (domínio reservado) descreve as áreas de atividade do Estado que são assuntos internos ou internos de um país e dentro de sua jurisdição ou competência (Oxford University). Disponível em: https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1398.

proporcional ao dano sofrido e se limite ao objetivo de garantir o cumprimento das obrigações violadas. Em qualquer caso, as contramedidas não devem representar uma ameaça ou uso de força e devem ser consistentes com outras normas imperativas, bem como com os direitos humanos e o direito humanitário.

3.2.1 **Operações Cibernéticas E O Uso Da Força:**

a) não existe uma definição estabelecida ou limite de operações cibernéticas hostis que caiam no âmbito da proibição do uso da força, no sentido do artigo 2º da Carta da ONU. Essa avaliação será determinada caso a caso, dependendo das consequências. A Itália considera *uma operação cibernética conduzida por um Estado contra outro como sendo com "uso da força", quando sua escala e efeitos* são comparáveis aos do uso convencional da força, resultando em *danos físicos à propriedade, ferimentos humanos ou morte* (grifo nosso). Entretanto, já consideramos controversa desta qualificação as operações cibernéticas que meramente causam perda de funcionalidade; e

b) em consonância com as conclusões da Corte Internacional de Justiça (CIJ) no caso *Nicarágua x Estados Unidos*, a Itália considera que a forma mais grave de uso da força constitui um ataque armado. Não há uma definição estabelecida ou limite de operações cibernéticas hostis abrangidas por "ataque armado", no sentido do artigo 51 da Carta das Nações Unidas; *tal avaliação será determinada caso a caso* (grifo nosso), dependendo das consequências de qualquer operação cibernética; assim, a ocorrência de um ataque armado desencadeia o direito à legítima defesa, podendo o Estado vitimado recorrer a todos os meios necessários e proporcionados para pôr fim à agressão.

3.2.2 Outros Aspectos:

a) Operações cibernéticas e a lei da neutralidade - a lei da neutralidade se aplica no ciberespaço no contexto de um conflito armado internacional com base no direito consuetudinário internacional existente. De acordo com a lei de neutralidade, as partes de um conflito armado internacional não podem lançar operações cibernéticas ilícitas a partir de uma infraestrutura de TIC localizada no território ou sob o controle exclusivo de um Estado neutro. Em um conflito armado, qualquer ação tomada por um Estado neutro deve ser aplicada igualmente a todos os beligerantes. Por exemplo, um Estado não pode fornecer ou negar acesso à sua infraestrutura de TIC a uma parte, mas não à (s) outra (s);

b) Direitos humanos no ciberespaço - considera-se que o direito internacional dos direitos humanos se aplica no ciberespaço da mesma forma que se aplica ao mundo analógico. O Estado é obrigado a proteger os direitos humanos *on line* e *off line*, protegendo os indivíduos de possíveis violações desses direitos,

incluindo, mas não se limitando à liberdade de opinião e expressão, o direito de acesso à informação e o direito à privacidade;

c) Papel das partes interessadas privadas no ciberespaço – dada a fundamental atuação do setor privado no ciberespaço, a Itália *considera a cooperação público-privada como a chave para garantir a segurança cibernética* (grifo nosso). Atividades ilícitas no ciberespaço também podem afetar as partes interessadas privadas, tanto como indivíduos quanto como parceiros/membros de parcerias público-privadas que administram infraestruturas de TIC; e

d) Cooperação internacional – cabe promover a cooperação internacional para melhorar a resiliência cibernética e a estabilidade internacional; o país deseja enfatizar a relevância da construção de confiança como meio de fomentar a cooperação e a necessidade de operacionalizar atividades de capacitação e compartilhamento de informações.

3.3 SUÍÇA

A motivação do país ao organizar seu *policy paper* (*Switzerland's position paper on the application of international law in cyberspace*) vem do conceito de que "A Suíça vê as posições nacionais dos Estados como uma contribuição importante para dar corpo à aplicação do direito internacional no ciberespaço". O uso do termo "ciberespaço" no presente documento se refere apenas à parte do espaço digital que diz respeito à dimensão da segurança. A Parte I aborda questões relativas ao direito internacional em geral, incluindo direitos humanos. A Parte II dá ênfase especial às questões relacionadas ao Direito Internacional Humanitário (DIH). A Suíça considera a lei internacional aplicável ao ciberespaço. Como um país neutro com longa experiência, o país enfatiza o objetivo primordial de garantir que o ciberespaço seja usado apenas para fins pacíficos.

3.3.1 **Direito Internacional Geral**

Sob o tema da soberania, este princípio também se aplica ao ciberespaço. "A soberania é uma regra primária vinculativa do direito internacional"; tais violações são, portanto, consideradas atos internacionalmente ilícitos. O país considera dois critérios a seguir em tais avaliações: (I) o incidente viola a integridade territorial do estado e, (II) constitui interferência ou superação de uma função inerentemente governamental.

Os temas do uso de força e autodefesa (resposta) são analisados conjuntamente. Um dos princípios fundamentais da Carta das Nações Unidas é a proibição do uso da força (Art. 2º, parágrafo 4º). Há apenas duas exceções: se autorizado pelo Conselho de Segurança da ONU (Art. 42) ou se as condições estritas sob as quais o direito de legítima defesa pode ser exercido forem cumpridas (Art.

51). O direito de legítima defesa só pode ser exercido se ocorrer primeiro um ataque armado. De acordo com a jurisprudência da CIJ, nem toda violação da proibição do uso da força constitui um ataque armado, mas apenas em sua forma mais grave. Para se qualificar, a escala e o efeito do ataque devem atingir um certo "limite de gravidade". Se o limite para um ataque armado não for atingido, os Estados podem recorrer a contramedidas não violentas imediatas e proporcionais.

No aspecto da não intervenção, a Suíça considera este ser o corolário da igualdade soberana de todos os estados (Art. 2º da Carta da ONU) e é considerada no direito internacional consuetudinário. Neste contexto, entende-se por intervenção a interferência direta ou indireta de um Estado soberano nos assuntos internos ou externos de outro por meio de medidas coercivas. Os temas de atribuição, uso de contramedidas e da diligência devida são tratados sob o prisma da "Responsabilidade do Estado", assim:

a) **atribuição**: atribuir a autoria de um incidente de cibersegurança refere-se à identificação do perpetrador e descreve um processo holístico e interdisciplinar. Isso inclui a análise dos aspectos técnicos e jurídicos do incidente, levando em consideração o contexto geopolítico e usando todo o espectro de inteligência para fins de coleta de informações. Usando essa abordagem, um Estado pode atribuir um incidente cibernético a outro Estado ou ator privado, publicamente ou não, e pode decidir tomar outras medidas políticas;

b) **contramedidas**: tem uma abordagem de uso mais restritivo, pois se um ato viola o direito internacional (e possa ser legalmente atribuído a outro Estado), o país lesado também pode atuar na forma de represálias, observadas regras; e

c) a **diligência devida**: é devida no ciberespaço; aplica-se em particular a ações de indivíduos/grupos que violam os direitos de outros Estados (por exemplo, *hackers*) e não podem ser (claramente) atribuídas ao outro Estado.

3.3.2 Direito Internacional Humanitário (DIH)

Os países beligerantes devem, em particular, buscar cumprir os princípios de distinção, proporcionalidade e precaução:

a) Distinguir entre objetivos militares, por um lado, e civis ou objetos civis, por outro e, em caso de dúvida, presumir o status civil;

b) Avaliar se o dano incidental que se espera infligir à população civil ou aos objetos civis seria excessivo em relação à vantagem militar direta e concreta prevista desse ataque em particular; e

c) Tomar todas as precauções possíveis para poupar civis e objetos civis.

Ainda a respeito do DIH, há a obrigação de avaliar a legalidade de uma nova arma prevista no art. 36 do Protocolo Adicional I às Convenções de Genebra (o BRASIL assina todas as convenções e os 3 protocolos adicionais) e é um elemento importante para prevenir ou restringir o desenvolvimento e o emprego de novas

armas cibernéticas que não cumpririam, em particular, as obrigações estabelecidas acima.

4 CONCLUSÃO

• Apresenta-se na tabela 1 uma análise sumária de alguns aspectos abordados nesse resumo, de modo a, comparativamente, levantar princípios de possível uso por ato normativo do País.

Tabela 1 – Comparativo dos documentos analisados

Tema/Aspecto	GGE/2021	Tallinn 2.0	França	Itália	Suíça
Soberania	Sim	Sim	Sim	Sim	Sim
Contramedidas	-	Sim	Sim	Sim	Sim
Autodefesa	-	Sim[1]	Sim	Sim[5]	Sim[6]
Uso da Força	-	Sim[2]	Sim[1] [3]	Sim[5]	Sim[6]
Diligência	Sim	Sim	Sim	Sim	Sim
Ñ intervenção	Sim	Sim	Sim	Sim	Sim
Atribuição	-	-	Sim[4]	Sim[4]	Sim[5]
Outros	Cooperação			Neutralidade	

Legenda:

[1] ator estatal necessário.
[2] ciberataque comparável a cinético
[3] não considera espionagem
[4] decisão política/soberana
[5] análise caso a caso
[6] em conflitos armados

Fonte: O AUTOR, 2022.

• A soberania é quesito entendido como a ser explicitado em um policy/position paper; é elemento natural da existência dos Estados.

• Em relação aos temas de contramedidas, autodefesa e uso da força, quando de uma resposta a ser executada, face a um ilícito cibernético, vimos que o efeito causado é o fator de análise preponderante, a saber:

a) à luz do DICA/DIH, o uso da força é restritivo e deve ser evitado; quando em resposta (e não apenas cibernética) tende a ser mais adequado em casos de conflito armado;

b) a autodefesa, princípio irrevogável, seria resposta a um ataque armado (cibernético) mas, nesse caso, quais os parâmetros? Acredita-se que a existência de dano físico resultante da ação cibernética é um quesito melhor aceito. Lembremos

que, um Estado tem o direito de legítima defesa quando "provado" que outro Estado cometeu um ato internacionalmente ilícito contra ele, tendo assim o direito de preservar sua segurança nacional e de seu povo;

c) assim, o uso da força e a autodefesa estão relacionadas; e

d) por fim, as contramedidas oferecem um campo mais amplo de causa/efeito (agressão é diferente de ataque armado) e de respostas (diplomáticas, "*hackear* de volta"), porém sempre proporcionais e adequadas no tempo e na gravidade.

• A caracterização da espionagem cibernética parece, até o presente, não prosperar como ação cibernética de vulto para resposta, pois apenas os meios de busca e obtenção seriam via redes de TIC.

• Ao abordar a atribuição, julga-se relevante apreciar as soluções francesa e italiana, cujo ato de atribuir é uma decisão política (ou soberana, no caso italiano) e não apenas dependentes de critérios técnicos. Assinala uma narrativa do Estado sobre o fato; as consequências (respostas) decorrentes serão adotadas caso a caso.

• Cabe ressaltar a importância de destacar princípios relacionados ao direito, como a diligência devida, o respeito à não intervenção e ao DICA/DIH, em particular.

• A legislação penal brasileira aplicável no ECiber, embora atualizada recentemente, ainda não inibe adequadamente a maioria dos crimes cibernéticos (exceção feita a ato terrorista cometido contra o País); por outro lado, a ratificação pelo Congresso Nacional da adesão à Convenção de Budapeste foi objetivo alcançado.

• Do sumário apresentado podemos concluir que, perante a comunidade internacional, no escopo do direito, há poucas certezas na aplicação do DICA/DIH no ECiber. Não haveria garantias palpáveis que um ilícito cibernético perpetrado contra um Estado soberano seria reconhecido como tal pela ONU e, principalmente, pelo CS, pois sempre há o poder de veto cedido aos cinco membros permanentes (e aos seus próprios posicionamentos).

• Como país soberano, indubitavelmente o BRASIL precisa ter o Setor Cibernético de Defesa como uma capacidade permanente a desenvolver. Os atributos de resiliência em suas estruturas críticas e a cooperação público-privada são os elos permanentes da segurança cibernética nacional.

• Por fim, fica um questionamento. O BRASIL deveria posicionar-se, também, por intermédio de um policy paper sobre o tema da Segurança e Defesa cibernéticas? Ou aguardar um consenso internacional? Melhor Comunicação Externa x Perda de Liberdade de Ação sobre o tema são aspectos a observar.

REFERÊNCIAS

BRASIL. Senado Federal. *Decreto Legislativo nº 37, 16 dez 2021. Aprova o texto da convenção sobre o crime cibernético, celebrada em Budapeste, em 23 de novembro de 2001.* Brasília: 2021. Disponível em: https://legis.senado.leg.br/norma/35289207. Acesso em: 18 Jan 2022.

CLARKE, Richard A.; KNAKE, Robert K. *Cyber War:* the next threat to national security and what to do about it. [S.l: s.n.], 2010.

COCO, Antonio; DIAS, Talita de Souza. *'Cyber due diligence':* a patchwork of protective obligations in international law. European Journal of International Law, Oxford: v. 32, n. 3, p. 771–806. 2021. Disponível em: https://doi.org/10.1093/ejil/chab056. Acesso em: 20 Jan 2022.

CONFEDERAÇÃO SUISSA. *Switzerland's position paper on the application of international law in cyberspace*: Annex UN GGE 2019/2021. [Berna]: 2019. Disponível em: https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf . Acesso em: 20 jan. 2022.

FRANCE. *Droit international appliqué aux opérations dans le cyberespace*, [Paris]: 2019. 19 p. Disponível em: https://pt.calameo.com/books/000009779eb0b65c5284f. Acesso em 19 jan. 2022.

INTERNATIONAL COURT OF JUSTICE. *Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America).* 1986. 206 p. Disponível em: https://www.icj-cij.org/en/case/70. Acesso em: 20 jan. 2022.

INTERNATIONAL COURT OF JUSTICE. *The Corfu channel case (UK v. Albania).* 1949. p. 4-169. Disponível em: https://www.icj-cij.org/en/case/1. Acesso em: 20 jan. 2022.

INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC). *International humanitarian law and cyber operations during armed conflicts*. [Genebra]: 8 Nov 2019. Disponível em: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts. Acesso em: 18 jan. 2022.

ITALIA, *Italian position paper on 'international law and cyberspace'*. [Roma]: 2021. 11p. Disponível em: https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/italian-position-paper-on-international-law-and-cyberspace.html. Acesso em: 20 jan. 2022.

MALAGUTTI, Larissa. *Famous cyberattacks in light of countries positions regarding principles of international law*. Dissertação (Master of Arts in International Security Studies) Department of Politics and International Relations, University of Reading. Reading: 2020. 47p.

SCHMITT, Michael; VIHUL, Liis. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge: Cambridge University Press, 2017. 598p. Disponível em: https://ccdcoe.org/research/tallinn-manual/. Acesso em: 19 jan. 2022.

UNITED NATIONS. Assembleia-Geral, 76ª Sessão. *Group of governmental experts (GGE) on advancing responsible state behaviour in cyberspace in the context of international security.* New York: [*S.n*.], 14 Jul 2021. Disponível em: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030S-1.pdf. Acesso em 18 jan. 2022.

UNITED NATIONS. *Charter of the United Nations*. New York: 26 Jun 1945. Disponível em: https://www.un.org/en/about-us/un-charter. Acesso em: 17 jan. 2022.

UNITED NATIONS. *Reports of international arbitral awards island of Palmas case*. Netherlands: 4 Abr 1928. Disponível em: https://legal.un.org/riaa/cases/vol_II/829-871.pdf. Acesso em: 21 jan. 2022.

UNITED NATIONS. *Responsibility of states for internationally wrongful acts*. 2001. Disponível em: http://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf. Acesso em: 20 jan. 2022.

LA TECNOLOGÍA MILITAR COMO MOTOR DE DESARROLLO: UNA FÓRMULA POSTERGADA

Fulvio Queirolo Pellerano*

"Los satélites artificiales. El horno microondas. Los radares. El GPS. Internet. Los drones. Todos estos inventos surgieron gracias a la investigación militar, y luego han pasado a formar parte de la vida del común de la ciudadanía".
(El País, 2017)

RESUMEN

Convengamos que la humanidad ha prosperado luego de revoluciones industriales y, en dicho contexto, la sociedad actual se encuentra envuelta por la cuarta (4RI) (SHAWAB, 2016). En ellas, la fórmula *I + D + i* ha constituido una base fundamental para el progreso de la Aldea Global. En este ámbito, se puede admitir que las revoluciones han sido responsables de la modificación de estructuras organizacionales vinculadas a la seguridad y defensa, así como de la transformación de modelos económicos, sociales y laborales, entre los más destacados. Es en este espacio donde la tecnología militar se ha abierto camino para generar valor a través de ingenios tecnológicos que, buscando dar respuesta a problemas de seguridad y bélicos, también han permitido transferir conocimiento aplicado. En consecuencia, el objeto del trabajo es comprobar lo gravitante que representa, para un Estado y, en lo particular, para países latinoamericanos, el propiciar el desarrollo tecnológico militar, a partir del gasto en *I + D + i,* identificando factores que han influido, positiva y/o negativamente, en la capacidad militar.

Palabras clave: Revolución industrial; I + D + i; Clúster; Defensa.

* Licenciado en Ciencias Militares. Es profesor de Academia en la asignatura de "Historia y Estrategia Militar". Magíster en "Ciencia Política, Seguridad y Defensa", en la Academia Nacional de Estudios Políticos y Estratégicos (ANEPE). Magíster en "Ciencias Militares con mención en Planificación y Gestión Estratégica" (ACAGUE). Posee grado de Diplomado en "Seguridad Internacional y Operaciones de Paz" y "Estudios Internacionales de Defensa" (ANEPE). Doctorando en "Seguridad Internacional" en la Universidad Nacional de Educación a Distancia, UNED, España. Actualmente, Jefe de Estudios Estratégicos del Centro de Investigaciones y Estudios Estratégicos (CIEE-ANEPE). Mail: fqueirolo@anepe.cl ; ORCID: https://orcid.org/0000- 0001-6837-0962

A TECNOLOGIA MILITAR COMO MOTOR DE DESENVOLVIMENTO: UMA FÓRMULA POSTERGADA

RESUMO
É certo *que a humanidade prosperou após as revoluções industriais e, neste contexto, a sociedade atual está rodeada pela quarta (4RI) (SHAWAB, 2016). Nelas, a fórmula de I + D + i tem se constituído em uma base fundamental para o progresso da Aldeia Global. Nesta área, pode-se admitir que as revoluções têm sido responsáveis pela modificação das estruturas organizacionais ligadas à segurança e defesa, bem como pela transformação dos modelos econômicos, sociais e trabalhistas, entre os mais proeminentes. É neste espaço que a tecnologia militar tem feito o seu caminho para gerar valor através de dispositivos tecnológicos que, procurando dar resposta aos problemas militares e de segurança, têm permitido também a transferência de conhecimentos aplicados. Consequentemente, o objetivo do trabalho é verificar a importância que representa, para um Estado e, em particular, para os países da América Latina, promover o desenvolvimento tecnológico militar, com base nos gastos em I + D + i, identificando os fatores que têm influenciado, positivamente e / ou negativamente, na capacidade militar.*
Palavras-chave: Revolução industrial; I + D + i; Cluster; Defesa.

1 INTRODUCCIÓN

Admitamos que el desarrollo de ingenios militares, en vastos períodos de la humanidad, ha generado impactos que trascienden la esfera netamente belicista. En efecto, desde que el hombre controló el fuego, se inicia una dualidad de prestaciones de carácter circular que vincula el bienestar comunitario con la seguridad colectiva. Como ejemplos de regímenes de reciprocidad podríamos destacar, inicialmente, que los colectivos humanos se sirven del fuego para fundir minerales y así confeccionar herramientas de trabajo para una agricultura primaria, y seguidamente, estos utensilios son innovados para utilizarlos como instrumentos de caza.

Más adelante, el ingenio humano prospera con la manipulación de la pólvora, un insumo que revolucionó el arte de la guerra y por consiguiente las conquistas, provocando diferencias asombrosas entre los contendores. Sin embargo, en nuestro análisis coincidiremos que la máquina a vapor, de manera decisiva, catapultó a la humanidad a una era industrial sin precedentes, instancia que socavó los pilares de la matriz productiva, hasta ese entonces conocida, un espacio que fue bien explotado por la industria bélica utilizando para sus fines medios como en tren y el barco.

Del mismo modo, otro período que marcó los destinos de la humanidad fue descrito como "la conquista del espacio". Un programa que se enmarcó en una carrera espacial por llegar con humanos a la Luna, impulsando un fuerte desarrollo tecnológico que transformó, prontamente, la industria de la aeronáutica (PEDRAZA, 2017).

En tiempos más cercanos, la re-evolución de la computación y la irrupción del internet de las cosas (IoT, sigla en inglés), así como la Inteligencia Artificial (IA) y *Big Data*, repiten el modelo anterior. Esta nueva dimensión ha estimulado a las sociedades a cruzar el umbral del mundo análogo hacia uno digital -aún en transformación- cuyos últimos avances se pueden observar con la irrupción de la robótica, el análisis cuántico de datos, o bien, en los sistemas autónomos, entre otros.

Sin desmerecer los esfuerzos dados por la ciencia y tecnología, en otros campos del saber, se ha pretendido enfatizar que, en diferentes etapas de desarrollo humano, la sociedad ha participado de los dividendos aportados por la tecnología e ingenio militar, un sector que abrigando objetivos de carácter bélico también produce capacidades que permiten responder a necesidades que la sociedad demanda. Con todo, el énfasis del desarrollo tecnológico militar ha estado condicionado por la disponibilidad de presupuestos, un aspecto que se ha transformado en el "talón de Aquiles" sectorial, causando brechas que demoran en ser corregidas.

En consecuencia, el objeto de este trabajo está destinado a analizar lo gravitante que representa, para un Estado, en este caso Latinoamericano, el propiciar un desarrollo tecnológico militar como actividad que, junto con generar capacidades de Defensa, agregue valor residual en la sociedad, favoreciendo al bienestar comunitario. Postulando que este modelo de transferencia que puede ser logrado mediante clúster tecnológicos (públicos y privados)[1].

Por otra parte, se pretende identificar aquellos factores que han influido, positiva y/o negativamente, en la evolución de la capacidad tecnológica militar, situando como temporalidad a partir del segundo mileno. Así formulado, se pretende responder a: ¿Constituye la investigación, el desarrollo y la innovación (I + D +i) factores dominantes para el progreso de un Estado? y, ¿Qué espacio ocupa, en esta fórmula, la tecnología militar latinoamericana?

El trabajo pretende aportar a la Conferencia de Directores de Colegios de Defensa Iberoamericano 2022, considerando la variable tecnológica como factor relevante en materias de "ciberseguridad, IA., y nuevas tecnologías en el ámbito de

1 Clúster: Como concepto se comprenderá a la "*agrupación de empresas y organizaciones asociadas que están localizadas en un entorno geográfico determinado y que por sus características y complementariedades conforman una red productiva*". Para mayor profundidad se sugiere consultar texto. REYES, Mirlis. "*Los Clusters Industriales de Defensa como Impulsores de la Innovación Tecnológica en América Latina*". En: Revista del Colegio Interamericano de Defensa, 2015. Ed. Julio 2014 – Junio 2015. Vol. 1. p. 100 – 114. http://publications.iadc.edu/wp-content/uploads/sites/5/2019/08/revista-del-cid-2015.pdf

la Defensa". Para llevar a cabo el cometido se empelará una metodología de estudio de casos de países latinoamericanos que, previamente seleccionados, presenten acceso a índices del gasto en ciencia, tecnología y desarrollo militar desde el año 2000.

La dificultad del estudio estará asentada en el acceso a información, que usualmente es restringida para estas temáticas. En este contexto, se cotejará la información publicada en sitios oficiales de la selección de países seleccionados con aquellas publicadas por Naciones Unidas y otras instituciones, como la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), el Banco Interamericano de Desarrollo (BID), Banco Mundial (BM) y la Comisión Económica para América Latina y el Caribe (CEPAL).

Para validar la metodología empleada se ha considerado como países representativos de la muestra a Argentina, Brasil, Colombia, Chile y México. Países que presentan fuentes de información adecuadas para el estudio, permitiendo examinar el comportamiento que han tenido en la aplicación de la fórmula *I + D + i,* respondiendo adecuadamente a las preguntas formuladas.

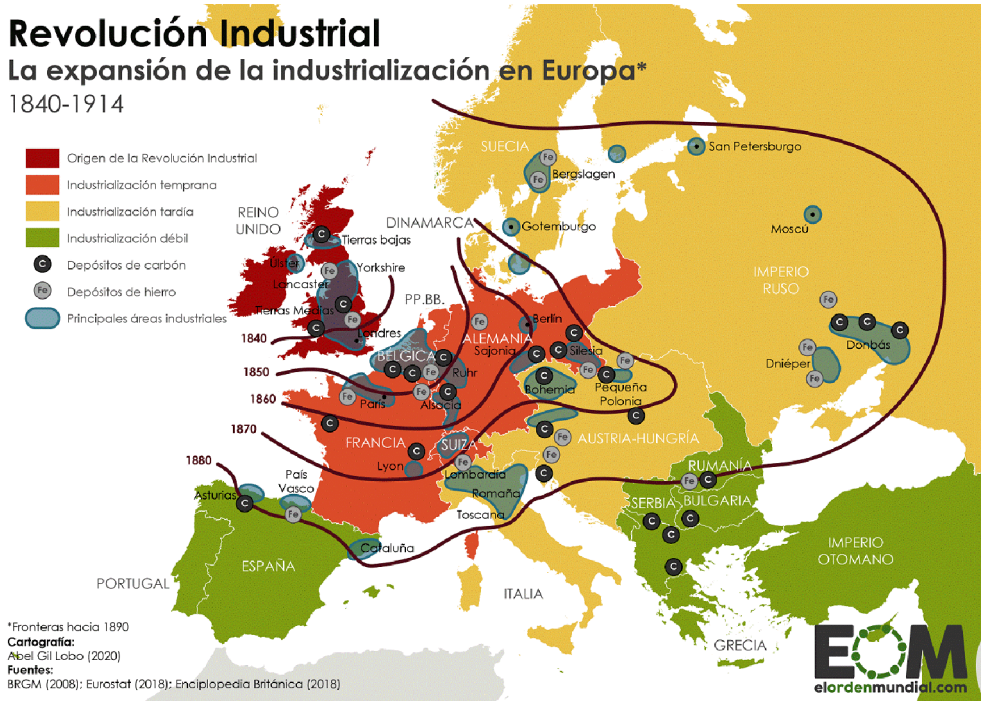
De esta manera, la data obtenida será sistematizada en ítem gastos/inversión en ciencia y tecnología, permitiendo identificar la manera en que los "clústeres tecnológicos" confieren transferencias a la comunidad. Esta técnica, pretende validar la existencia de una correlación entre desarrollo tecnológico de la Defensa y beneficios que puede disponer un Estado para otros fines multisectoriales.

2 LA IMPORTANCIA DE LA FÓRMULA *I + D + I* EN LA SOCIEDAD GLOBAL

Como punto de inicio de este apartado nos concentraremos en el impacto que generó la máquina a vapor en la sociedad. Un ingenio tecnológico considerado como fuente propulsora de las teclas del desarrollo fabril, propiciando la primera revolución industrial (1760 - 1840). En dicho período se pasó, paulatinamente, desde un modelo económico agrícola y rural a una actividad comercial urbana liderada por la industria textil y siderúrgica londinense que se propagó por Europa (Cuadro 1). La precariedad extractiva de la tierra quedaba atrás frente a la mecanización e industrialización de bienes y servicios, produciendo una transformación en la sociedad que veía como íconos del progreso estas máquinas, y que más adelante movieron ferrocarriles y buques.

Por su parte, la industria militar adoptó un enorme capital tecnológico cuya transferencia se manifiesta en manufacturas de pistolas, fusiles y cañones, un cúmulo de artificios que modificaron sustancialmente el rendimiento de sus predecesores (arcabuces), incorporando materiales más confiables. Mientras que las plataformas de hierro (ferrocarril y barcos) sirvieron de soporte para la movilidad de contingentes y pertrechos en épocas de conflictos.

Cuadro 1: Expansión tecnológica en la primera revolución industrial

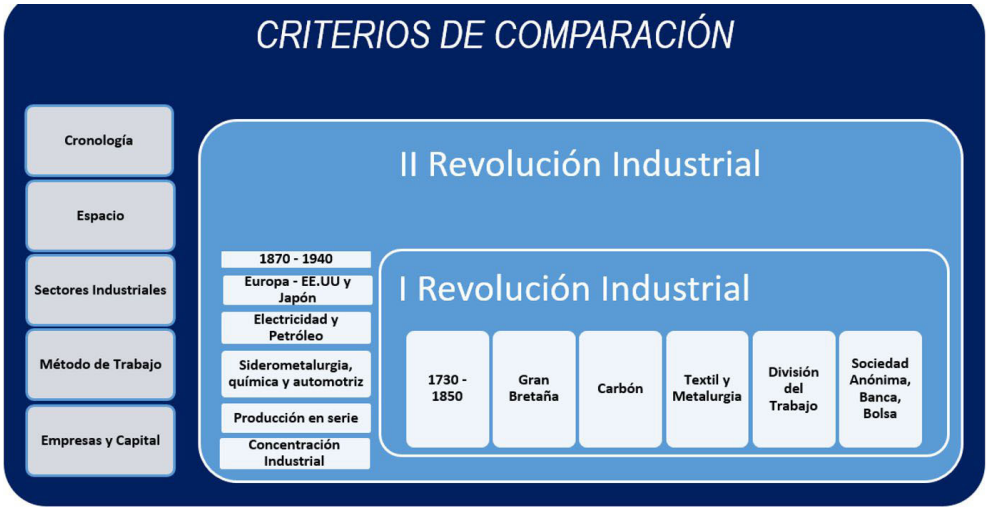


Fuente: Gil, 2018.

La segunda revolución (mediados del S.XIX a Primera Guerra Mundial), fue una época más bien marcada por la búsqueda de nuevas fuentes de energía (petróleo, gas) que potenciaran los sistemas de transporte e industria manufacturera ya en marcha. Sin embargo, el costo de las distancias geográficas había que reducirlas. La ciencia contribuyó a la solución mediante el empleo de las ondas electromagnéticas. Por otra parte, el impacto en el trabajo, la producción y el comercio continuaron un asombroso ascenso y sus beneficios se expandieron por toda Europa, alcanzando América y Asia. Símbolos de este período de desarrollo se evidencia en el teléfono, la radio, el automóvil y avión (Cuadro 2).

Otro enorme salto tecnológico se posesionó entorno a la Gran Guerra. Se puede afirmar que la fórmula *I + D + i* fue fundamental para el desarrollo de instrumentos bélicos que favorecieron, finalmente, a dar solución a temas geopolíticos, sin desconocer los costos humanos. En este escenario, el avión fue utilizado para lanzar bombas desplazando a los lentos y anticuados dirigibles, mientras que en el campo de batalla emergía el tanque, sumándose a sofisticadas piezas de artillería y otros artilugios.

Cuadro 2: Síntesis comparativa entre primera y segunda revolución industrial



Fuente: Elaboración propia en base a fuentes abiertas.

Si los tiempos tecnológicos de las dos primeras revoluciones iban a ritmo regular, visto desde la perspectiva actual, habría que poner atención a la tercera revolución (1960 – 1990). Una época que modificó, sustantivamente, esta cadencia. El responsable de este quiebre, para nuestro análisis, se sitúa en la carrera por la conquista del espacio. La evidencia recogida permite concluir que, a través del impulso dado por la ciencia y tecnología militar, se contribuyó al éxito de facilitar la presencia del hombre en la Luna y cumplir con el sueño de Julio Verne y su anhelado viaje astral.

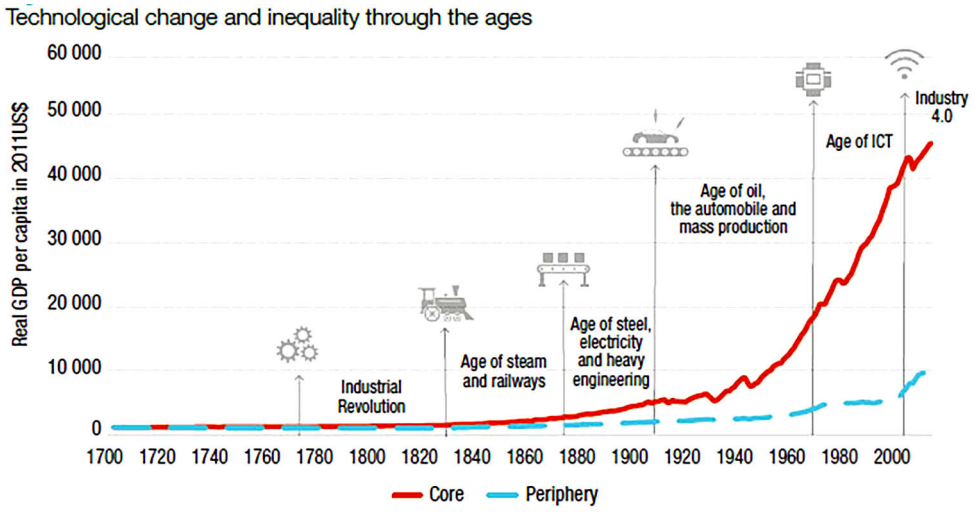
En efecto, en pleno período de Guerra Fría el ejercicio del poder de los principales contendores globales (EE.UU. y la ex URSS), se traslada al espacio. El interés de estas potencias estimula programas como *Sputnik I, Explorer, Saturno, Apolo*, entre otros proyectos, que se nutrían de los logros militares alcanzados en plataformas de misiles balísticos intercontinentales, sin negar el avance sobre la fusión nuclear. Así del "temor" a una tercera conflagración mundial se avanza, virtuosamente, en beneficio de la sociedad, otorgando soluciones tecnológicas aplicadas como los escáneres en tratamientos médicos, sistemas de posicionamiento (GPS) para medios de transporte, o bien purificación de agua y el aprovisionamiento de comida deshidratada, por señalar algunos.

Sin embargo, estos éxitos no tuvieron el mismo impacto de transferencia tecnológica en la Aldea Global. Sus consecuencias se pueden evaluar décadas después, conclusión que se obtiene del análisis de datos de desarrollo humano en dicho período, evidenciando la existencia de brechas al comparar antecedentes del

centro (países de alto desarrollo) y la periferia global (países con bajo desarrollo). Como factor dominante en este complejo panorama ha sido invertir/gastar en I + D + i, como porcentaje del producto interno bruto - PIB (BANCO MUNDIAL, 2022). Un guarismo que debe incentivar a los Estados a otorgar prioridad para dar un paso firme y evitar el estancamiento.

De esta manera, se puede afirmar que mientras algunas sociedades se beneficiaban por contar con imágenes satelitales de la tierra que les permitía modelar y anticiparse a escenarios complejos, o bien mejoraron su eficiencia de sus sistemas de transporte (GPS), así como agradecer el empleo de un utensilio tan básico como el microondas; otras sociedades continuaban sumergidas en la realidad análoga de la segunda revolución industrial. (Cuadro 3).

Cuadro 3: Re-evolución e impacto en el desarrollo global



Source: UNCTAD, based on data from Maddison Project Database, version 2018, Bolt et al. (2018), Perez (2002), and Schwab (2013).
Notes: "Core" corresponds to Western Europe and its offshoots (Australia, Canada, New Zealand and the United States) with Japan. "Periphery" corresponds to the world, excluding the "core" countries.

Fuente: NACIONES UNIDAS, 2020.

En consecuencia, si las tres revoluciones anteriores causaron impactos positivos y negativos, en la actualidad se debe considerar las que acarrea(rá) un superlativo nuevo milenio. Como se puede deducir del cuadro anterior, la tendencia es que los períodos inter-revoluciones ahora se estrechan acarreando, de paso, un elemento que tensiona a las sociedades del conocimiento y, por ende, los Estados. Empíricamente hablando se refleja en el lapso de tiempo transcurrido entre el uso masivo del ordenador (computadora), y la irrupción de la tecnológica digital.

Esta nueva dimensión, para la Aldea Global, constituye una invocación a

propiciar inversión en *I + D + i*. No hacerlo constituiría una renuncia fatal en tiempos de enfrentar nuevos riesgos, amenazas donde irrumpen escenarios complejos e híbridos. Del mismo modo, cooperar en el cumplimiento de la agenda compartida de ONU (NACIONES UNIDAS, 2015), un compromiso que suscribe 17 Objetivos de Desarrollo Sostenible al 2030. El salto tecnológico dado por la IoT, la Nanotecnología, robótica e Inteligencia Artificial, ya están modificando profundamente algunas estructuras sociales, económicas, laborales, hasta ahora conocidas. Cuestionarse sobre la manera que impacta(rá) el campo de tecnología en las organizaciones de la Defensa, es una pregunta, que requiere de respuestas diferentes a las que usualmente se han otorgado en este campo.

Para responder, inicialmente, recurriremos al texto de Guillem Colom, quien se referirse al concepto de "Revolución en Asuntos Militares" (RMA, por sus siglas en inglés): "…es un profundo cambio en la forma de operar de los ejércitos que resulta de la integración de nuevas tecnologías, doctrinas, procedimientos, tácticas o formas de organización en las fuerzas armadas" (COLOM, 2008, p.47). Un acertado análisis si se contrasta con la evidencia actual.

Seguidamente, nos situaremos en la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA, por sus siglas en inglés), una organización dedicada a "realizar inversiones fundamentales en tecnologías innovadoras para la seguridad nacional" (DARPA, 2019, p.1-8). Sus éxitos se circunscriben a la carrera espacial, en pleno período de Guerra Fría, y se extiende hasta nuestros días, aportando con innumerables desarrollos científicos y tecnológicos como el computador, la IA, sistemas autónomos, Big Data y tecnologías cuánticas, etc.

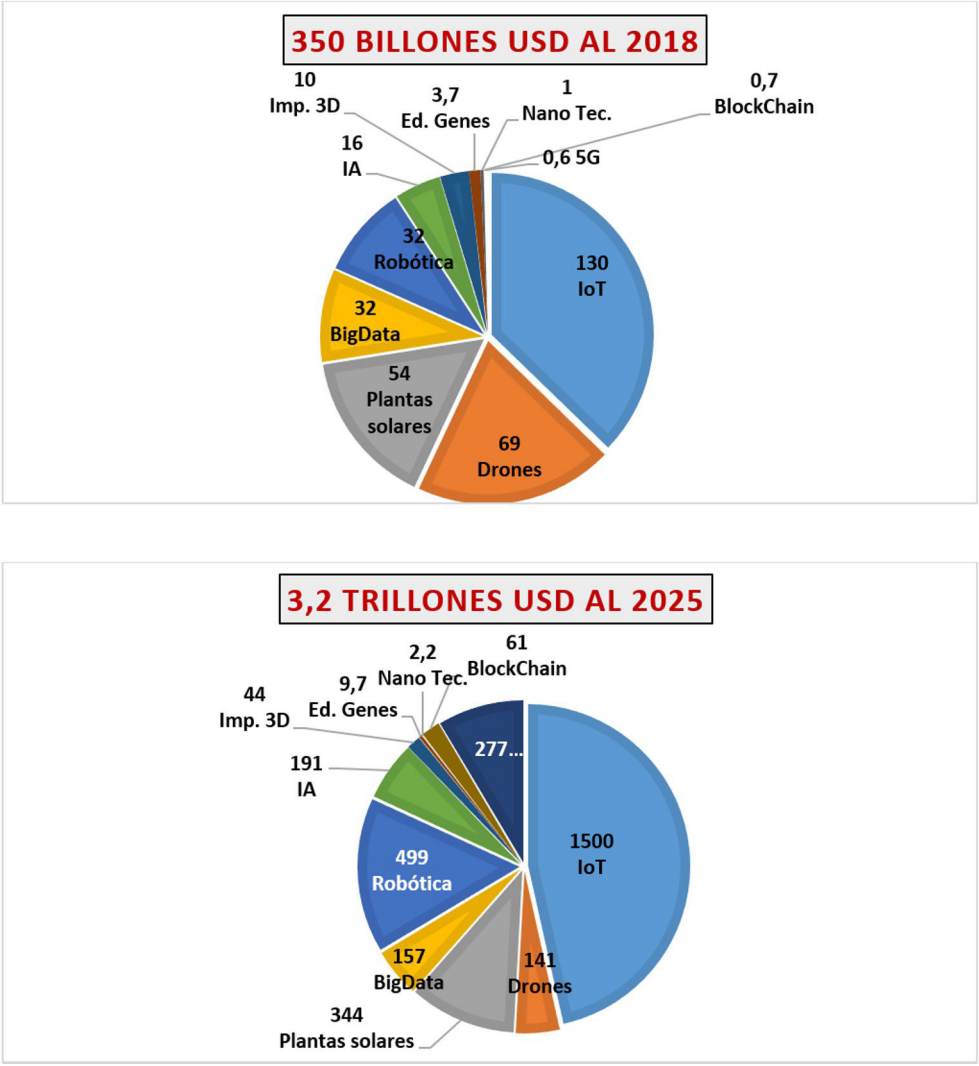
Finalmente, pondremos la mirada sobre Israel, otro país que ha apostado por la inversión en *I + D + i* por años. El resultado de esta decisión política, es que ha escalado al sitial de las grandes potencias que producen tecnología de alto nivel de impacto. Según "La Vanguardia" (OTTO, 2016), para alcanzar este nivel se debe reconocer cuatro ingredientes fundamentales: i) educación; ii) conexión universidad-empresa; iii) cultura militar; y, iv) I + D e inversión público-privada. Todo indica que el camino correcto está trazado y quienes mejor han interpretado las señales ya corren la maratón donde otros aún caminan.

En resumen, tal ha sido el desarrollo y penetración de las nuevas tecnologías que se reconoce que la Aldea Global ha sido abrazada por la cuarta revolución industrial (4RI) (SCHWAB, 2016). Un escenario que impone desafíos a la sociedad en general y al sector Defensa en lo particular, contexto sobre el cual no puede restarse ninguna organización (pública o privada). Las consecuencias de un rezago tecnológico implicarían un divorcio con el mundo digital/lógico en curso, relegando a las Fuerzas Armadas a mantenerse en el campo análogo, conllevando al fracaso (LODEIRO, 2021, pp.36-50).

Según los datos entregados por la Conferencia para el Comercio y Desarrollo de Naciones Unidas (UNCTAD), el tamaño del mercado tecnológico al año 2025

(ver Cuadro 4), para ingenios que se basan en IA, IoT, *Big Data*, *blockchain*, 5G, 3D impresión, robótica, drones, edición de genes, nanotecnología y energía solar fotovoltaica pasaría de la módica suma de USD 350 mil millones a USD 3,2 trillones. ¿Qué Estado o sector de la industria renunciará a esta realidad? ¿La industria de la Defensa no califica en este nicho o polo de desarrollo? Preguntas que requieren respuestas gubernamentales y sectoriales, y de esta forma integrar diferentes capas estatales que requieren una mirada de país y estrategias que las avalen.

Cuadro 4: Mercado tecnológico



Fuente: Elaboración propia en base a datos de UNCTAD, 2020.

En consecuencia, el impulso dado por la ciencia y tecnología revela, por ahora, que próximamente la Aldea Global ingresaría a una "quinta revolución industrial", mucho antes de lo previsto. Por lo tanto, el desafío para el sector de la industria de la Defensa –en condición de clúster– se sitúa en visualizar la manera de adaptarse, oportunamente y rápidamente, a un nuevo campo de acción, esta vez digital/lógico. ¿Habrá respaldo político y financiero adecuado para cumplir con líneas de trabajo estratégicas que asegure un incremento sostenido en *I + D + i*, como lo han concebido otros actores internacionales?

A mayor abundamiento, compartiendo que las (re)evoluciones en asuntos militares se han llevado a cabo en contextos clave para la humanidad, la 4RI ya ha instalado una dimensión muy diferente a las anteriores. Primordialmente destacan el ciberespacio, espacio exterior y, últimamente, el espacio mental - donde Chile es pionero en legislar sobre esta materia (CHILE, 2021).

Las dimensiones antes señaladas han sido identificadas como posibles y nuevos campos de batalla del futuro, tal como fue establecido en la Agenda para la Conferencia de Seguridad de Estocolmo, el pasado noviembre del 2021 (SIPRI, 2021), y que abordó, entre otros, dichos tópicos.

En consecuencia, podríamos establecer *a priori*, como hipótesis alternativa a este estudio, la necesidad de considerar *I + D + i*, como variable dependiente de la Seguridad Nacional) (LISA INSTITUTE, 2019). Esta conjetura se sustenta luego de constatar el grado de vinculación que posee la ciencia y tecnología sobre el desarrollo humano, el cual ha podido medirse a través de las transferencias que se generan.

En el caso de la Seguridad y Defensa estatal, el resultado de esta ecuación distingue el progreso, o bien rezago, de los Estados para hacer frente a riesgos y amenazas, en un escenario internacional cada vez más difuso y que, según el Director de Inteligencia Nacional de EE.UU. (COATS, 2019, p.4-23), requiere de originales y modernas respuestas. Un estadio donde la ciencia y tecnología, por medio de *I + D + i* posee enormes fortalezas (ver Cuadro 5).

Para otorgar validez a lo indicado precedentemente se recurrirá a la noción, globalmente aceptada, del *Democratic Control for Armed Forces* (DCAF, por sus siglas en inglés), sobre esta materia, sosteniendo: "La política de seguridad nacional es una descripción formal de la comprensión de un país de sus principios rectores, valores, intereses, metas, entorno estratégico, amenazas, riesgos y desafíos con miras a proteger y promover la seguridad nacional" (DCAF, 2015). Este criterio permite inferir que uno de los roles primordiales de un Estado se funda en aspirar a la generación de condiciones de estabilidad de su entorno, tanto interno como externo, para mitigar amenazas a su soberanía.

Cuadro 5: Principales amenazas (para occidente) desde la noción de EE.UU.

Principales amenazas para Occidente	***Instrumentos para enfrentar amenazas***
Amenazas cibernéticas	• ***Establecidos por el Estado:*** *Andamiaje de Seguridad y Defensa estatal sustentada principalmente en: Capacidades estratégicas de Fuerzas Armadas – Capacidades Operativas de Fuerzas Policiales – Capacidades Operativas de Organismos de Inteligencia – Capacidades Legales de Organismos de Persecución Judicial – otras funcionales al objeto.*
Tecnologías emergentes y amenazas a la competitividad	
Seguridad en el espacio y contra espacio	
Seguridad económica y energética	
Crimen organizado transnacional	
Terrorismo	
Seguridad Humana	
Contraespionajeycontrainteligencia	
Proliferación de armas de destrucción masiva	• ***Nuevas capacidades y dimensiones de origen estatal y /o privado:*** *IA – IoT – Big Data – realidad aumentada – Blockchain – computación cuántica - 5G – 3D printing – robótica – Drones (UAV) – Nano tecnología – biotecnología – entre las de mayor relevancia.*

Fuente: Elaboración propia en base a datos de Lisa Institute, DCAF, y UNCTAD.

En consecuencia, ¿El gasto en *I + D + i* contribuiría a dicho objetivo? La respuesta, a nuestro entender, es afirmativa, por consiguiente, la hipótesis sería positiva. ¿Qué tan alejada se encuentra esta conclusión de lo descrito en el Informe de la Comunidad de Inteligencia Norteamericana el 2019? En palabras expresadas por un comité de expertos, se señala:

> Para 2019 y más allá… la brecha de capacidad entre las tecnologías comerciales y militares se evapora; y los actores extranjeros aumentan sus esfuerzos para adquirir los mejores talentos, empresas, datos y propiedad intelectual por medios lícitos e ilícitos. Muchos líderes extranjeros, incluido el presidente chino Xi Jinping y el presidente ruso Vladimir Putin, impulsan el desarrollo de capacidades científicas y tecnológicas autóctonas como clave para la soberanía de su país, perspectiva económica y poder nacional (COATS, 2019, p.15).

Se puede concluir que los principales actores internacionales han renovado sus respectivas visiones geopolíticas, otorgando vigor a la inversión/gasto en I + D + i como fórmula para enfrentar una nueva época, esta vez concebida bajo el sombrero 4RI. Lamentablemente aquellas sociedades que no inviertan prontamente en esta ecuación, se mantendrán en la periferia de las transferencias que se generen. Evidencia de ello ha sido la dicotomía revelada con ocasión del COVID-19, que apremia a quienes pueden acceder a tan anhelada protección y así evitar un descalabro económico, social y gubernamental. ¿Quiénes están más propensos? Las respuestas más acertadas provienen desde la ciencia y tecnología.

3 LA IMPORTANCIA DE I + D + I EN LA REGIÓN

Iniciaremos el análisis situándonos en las discusiones llevadas a cabo durante la Tercera Reunión de la Conferencia de Ciencia, Innovación y Tecnologías de la Información y las Comunicaciones de la CEPAL, materializada de manera virtual y con auspicio del gobierno de Argentina (CEPAL, 2021, p.19). Para nuestro análisis, resulta fundamental un párrafo conclusivo el cual establece, como aspecto clave, para la recuperación de América Latina y El Caribe, aumentar el esfuerzo en materia de I + D.

El mencionado informe rescata la idea que llevan a cabo países más avanzados en este asunto, así como en otras regiones, afirmaciones que debiesen producir efectos en las respectivas administraciones, buscando evitar la tradicional receta de firmar acuerdos que, al final del día, no se cumplen. Resulta de enorme trascendencia, para nuestro estudio, el alcance dado en dicha conferencia:

> […] mientras que Estados Unidos, la Unión Europea, los países de la Organización de Cooperación y Desarrollo Económicos (OCDE) y China tienen un nivel de gasto en I+D relativo al producto interno bruto (PIB) superior al 2%, en América Latina y el Caribe el gasto en I+D relativo al PIB es unas cuatro veces inferior, el que incluso se ha reducido en los últimos años, pasando de un 0,65% del PIB en 2013 al 0,56% en 2019. (CEPAL, 2021).

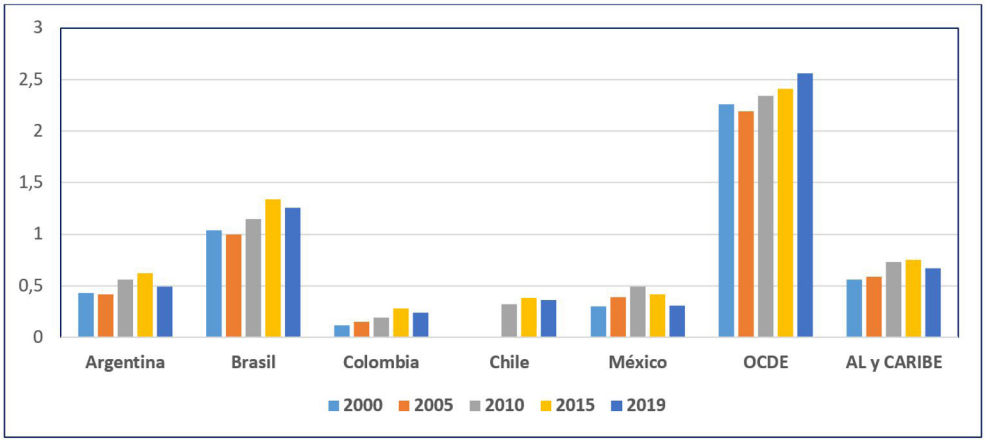
Este conciso resumen posiciona la fórmula *I + D + i*, como condicionante para la transformación de la sociedad. Nuevamente, el cuestionamiento se instala en la mesa de los tomadores de decisión. Recordemos que, una década antes, el BID mostraba ciertas preocupaciones al momento de estudiar la evolución en ciencia y tecnología de la región latinoamericana, coligiendo: "…el estado actual de la ciencia, la tecnología y la innovación en América Latina y el Caribe… pone de manifiesto una cruda realidad: las economías de América Latina y el Caribe no están preparadas para enfrentar los desafíos de la sociedad del conocimiento" (BANCO INTERAMERICANO DE DESARROLLO, 2010, p. 1).

Un lustro más tarde, la UNESCO, nuevamente, pone la alerta sobre la "distribución sectorial directa en tecnología" (IED, por sus siglas en inglés). En este caso, se evaluó la manera en que los países propician las inversiones en tecnología. El resultado de dicho estudio arrojó que al 2014 la inversión orientada a tecnología se concentraba en: i) proyectos de bajo nivel tecnológico (18%); ii) mediano impacto (22%); iii) medio alto (56%); y, iv) de alta tecnología (4%) (UNESCO, 2015).

Al avanzar al 2020 las noticias no son alentadoras. La brecha observada no ha sido posible cerrar y, en algunos casos, se ha ensanchado. El reproche sobre esta realidad se sitúa en develar las razones de esta tendencia. Los datos revelan una baja asignación presupuestaria en *I + D + i*, un indicador que denuncia la (ir)relevancia otorgada por quienes están llamados a priorizar esta fórmula, asumiendo que las autoridades reconocen la factibilidad de transferencias multisectoriales.

Estos valiosos antecedentes permiten cruzar datos con otras organizaciones y así establecer como evidencia la existencia de rezagos generados en el sector de la industria de la Defensa. Entendiendo que esta actividad industrial forma parte de clústeres tecnológicos de un país. La observación se puede colegir luego del análisis de antecedentes aportados por el BM., institución que expresa el gasto en I + D como porcentaje del PIB, para este caso, de aquellos países seleccionados durante el período 2000 – 2019 (ver Cuadro 6).

Cuadro 6: Gasto en I + D como % del PIB 2000-2019



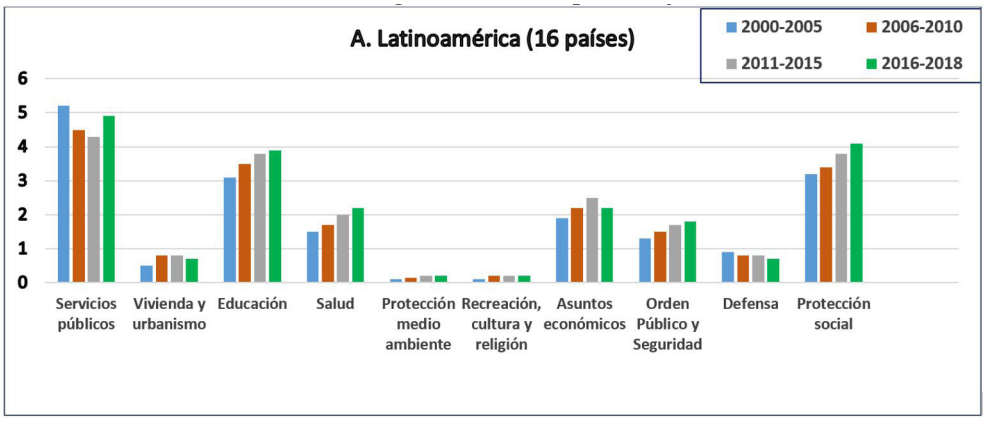
Fuente: Elaboración propia en base a datos del BM., 2020.

Lo sorprendente de la muestra es la gran coincidencia con lo expresado por la Dra. Mirlis Reyes (2014), quien señalara: "El reto en este caso (defensa) es contar con fuentes de financiamiento cada vez más reducidas, cuestión que se refleja con la disminución de los presupuestos estatales para la defensa en la mayoría de los países. Esta limitación ha hecho que los distintos ministerios de defensa adapten la tecnología creada fuera del sector, reduciendo los costos y riesgos de la

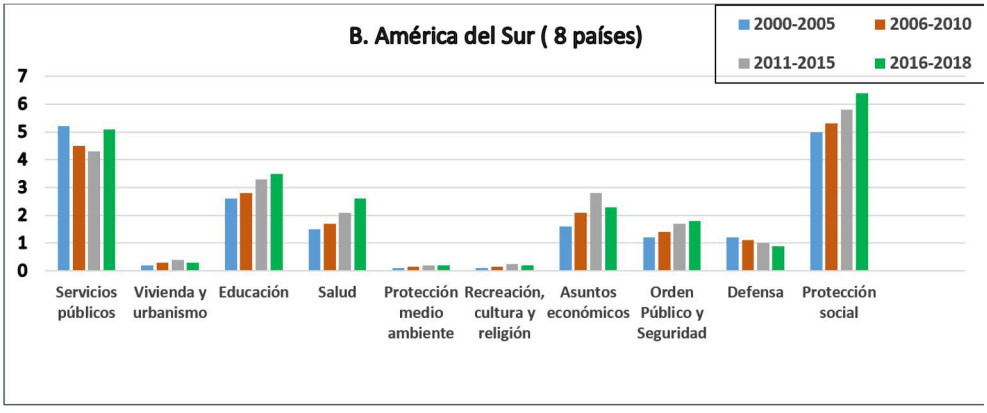
inversión". Si bien, los datos no se encuentran desagregados, el indicador del gasto es fundamental y que aclararemos más adelante.

Así las cosas, uno de los mayores impactos para las Fuerzas Armadas se posesiona en la capacidad de generar nuevas capacidades, las que aún poseen componentes de bajo y/o mediano estándar tecnológico. Esta condición, prácticamente, demanda la (re)formulación proyectos que propicien una constante actualización de sistemas o bien, si el grado de obsolescencia es tan alto, acudir a la adquisición de ingenios tecnológicamente acabados, una opción que limita la posibilidad de estructurar clústeres públicos y/o privados locales (ver Cuadros 7 A - B).

Cuadros 7 A - B: Evolución del gasto Estatal, en porcentajes del PIB 2000-2018



Nota: Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Nicaragua, Panamá, Paraguay, Perú, México, República Dominicana y, Uruguay.
Fuente: Elaboración propia a partir de datos (CEPAL, 2019).

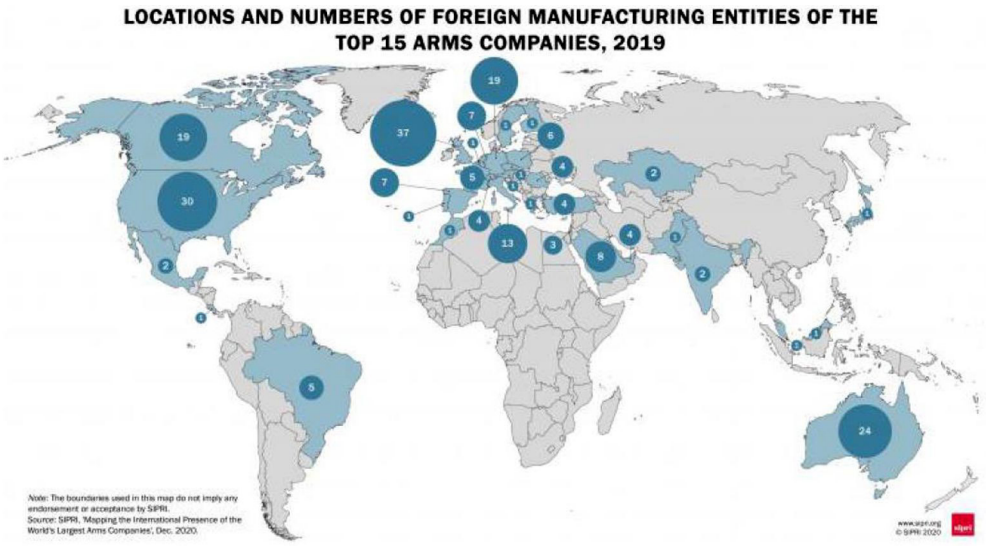


Nota: Argentina, Brasil, Chile, Colombia, Ecuador, Paraguay, Perú y Uruguay.
Fuente: Elaboración propia a partir de datos (CEPAL, 2019).

Se puede comprobar que la tendencia regional, en gastos de Defensa, es "a la baja", repercutiendo no solo en el sostenimiento de los sistemas de armas para mantener capacidades estratégicas, sino que limita acciones que impulsan la elaboración de proyectos que posean alto nivel tecnológico. Por ahora, salvo excepciones, el desarrollo de IA (*software*), fabricar vehículos no tripulados (aéreos, terrestres, náuticos), entre otros ingenios avanzados (computación cuántica), permanecen supeditados a la adquisición en el extranjero.

El reporte entregado por Instituto Internacional de Investigación para la Paz de Estocolmo (SIPRI, por sus siglas en inglés), confirma esta lastimosa tendencia, destacando que entre las 100 compañías dedicadas a la producción de armas y proveer servicios adicionales (transferencias), conocido como industria de la Defensa, se advierte una reducida participación de corporaciones regionales. Panorama que según la experiencia internacional identifica como nichos de clústeres tecnológicos aquellos orientados a salud, seguridad, inteligencia, industria digital y espacial, transporte y movilidad, energía, clima, campos donde el sector Defensa debiese estar presente, en virtud de sus fortalezas y ventajas comparativas, (ver Cuadro 8).

Cuadro 8: Ubicación y número de consorcios extranjeros entre los más destacados 2019 - 2020



Fuente: SIPRI (2020).

Pese a este obscuro escenario global, algunas empresas (públicas/privadas) regionales, han recibido el estímulo para formalizar clústeres nacionales y

extranjeros, que van en la línea señalada y que analizaremos más adelante. De esta manera, con los antecedentes aportados por SIPRI, dan cuenta que entre el 2002 y 2020, únicamente, el consorcio EMBRAER-Brasil ha participado en este tipo actividades (2010 – 2016) (SIPRI, 2020).

Lo indicado, ratifica lo que Castaldi y Dosi señalaron en la investigación cuyo objeto fue comprobar el impacto que genera el desarrollo tecnológico sobre el crecimiento económico de un país y, en lo particular, para los países en desarrollo (CASTALDI, DOSI, 2009. p. 81-129). Un escenario que mantiene un registro tendencial bajo.

4 LA FÓRMULA *I + D + I* APLICADA A DEFENSA EN PAÍSES SELECCIONADOS

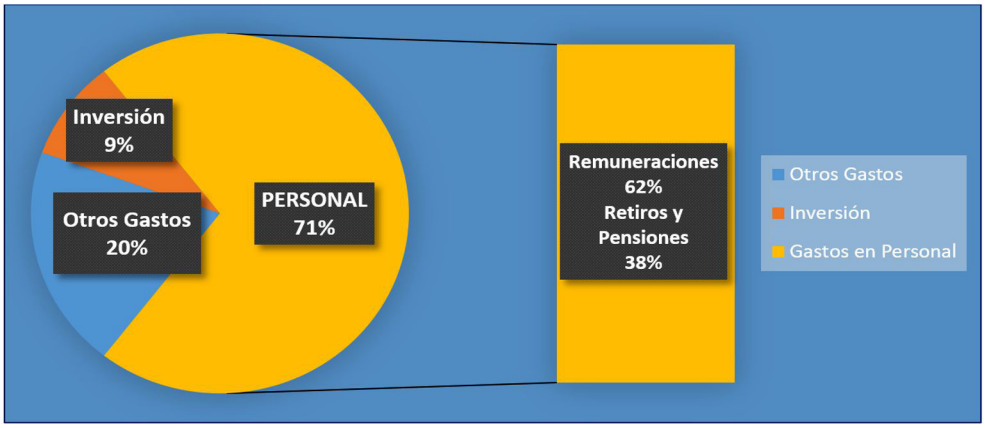
En el trabajo de recolección de datos, que sean representativos para este estudio, se ha considerado como fuente inicial el reporte que, anualmente y hasta el 2016, publicaba la Red de Seguridad Latinoamericana (RESDAL). De esta manera, al examinar las "partidas" presupuestarias más importantes asignadas a las Fuerzas Armadas latinoamericanas, se identifica un ítem destinado a inversiones. Este rubro, considera como segmento de la inversión estudios e investigaciones y adquisición de sistemas de armas y equipos.

Se puede evidenciar la inclusión de I + D, aunque como un indicador genérico y que, para nuestro trabajo, habrá que despejar. Interesante es observar que durante el lapso de 10 años se ha mantenido un comportamiento que bordea el 9% del total del gasto de Defensa, una cifra que parece abultada, sin embargo, se encuentra influida por otros factores que se aprecian en Cuadro 9 A.

Con el fin de aclarar la duda que ocasiona la interpretación del ítem "inversiones", se recurrirá al último reporte elaborado por el Centro de Estudios Estratégicos de Defensa (CEED)[2], organismo que, hasta el 2018 y bajo auspicio de la Unión Suramericana de Naciones (UNASUR), elaboraba investigaciones de este tipo. En dicho caso, el informe del 2017 es más específico que el anterior (RESDAL), estableciendo: "…la composición del gasto en defensa a nivel regional permite afirmar que la mayor parte del gasto de la jurisdicción se encuentra destinado al rubro Personal, con un promedio de 59,57% para la década, seguido por el de Operaciones y Mantenimiento (22,60%), Inversiones (17,18%) e Investigación y Desarrollo (0,47%)", (ver Cuadro 9 B).

2 CEED. Registro Suramericano de Gastos Agregados en Defensa. Edición Especial 2006 – 2015. Centro de Estudios Estratégicos de Defensa. Consejo de Defensa Suramericano. Unión de Naciones Suramericanas. 2017.

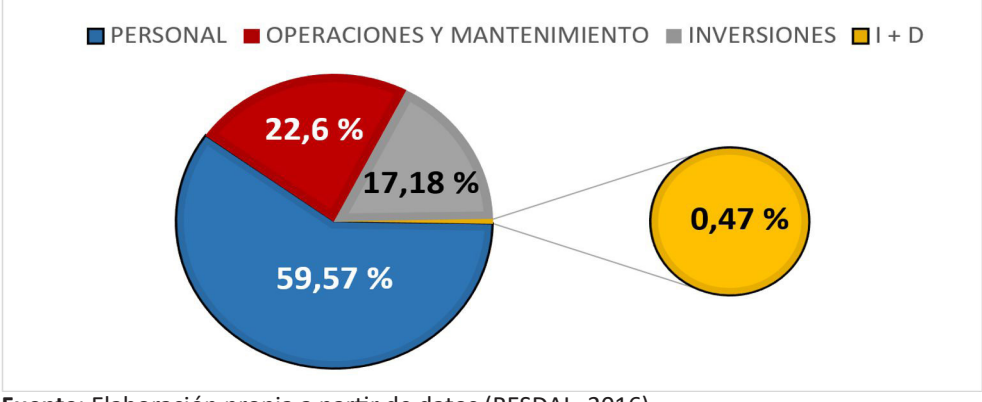
Cuadros 9 A: "Distribución de partidas del presupuesto de Defensa en Latinoamérica" 2016



Fuente: Elaboración propia con datos (RESDAL, 2016).

Fuente: Elaboración propia con datos (RESDAL, 2016).

Cuadro 9 B: Porcentajes del gasto (promedio) I + D + i (2006 – 2015)



Fuente: Elaboración propia a partir de datos (RESDAL, 2016)

En consecuencia, el cruce de información permite constatar que la tendencia en gasto en *I + D + i* como porcentaje del PIB de un Estado, es directamente proporcional a la inversión en Defensa, además el ítem Defensa continúa con una sostenida baja en desarrollo tecnológico.

Para sostener lo señalado, recurriremos al portal Infodefensa.com (CAIAFA, 2021) cuyo análisis se refieren a los retos que enfrentará Latinoamérica para el 2022. Se puede comprobar la presencia de la misma tendencia ya señalada, es decir la mayoría de los casos se orientan a proyectos que buscan "renovar sistemas" manteniendo una reducida inversión en *I + D + i*.

Así, para Argentina el foco estaría en definir el tipo de aviones de combate y vehículos blindados en reemplazo de anticuados modelos; en el caso de Brasil (excepción), las autoridades adoptarán decisiones tecnológicas para carros blindados (8 x 8), la construcción de cuatro fragatas (según programa) y avances en el "know-how" del proyecto de aviones F-39 Gripen, así como el desarrollo del eVOLT (avión eléctrico), el único país que muestra inversión en tecnología (CAIAFA, 2021).

Por su parte, Colombia, se encuentra muy retrasada en la renovación de sistemas de Defensa que han llegado al límite de la obsolescencia tecnológica. Chile, se focaliza en reemplazar los vetustos carros de combate "Mowag", la actualización de sistemas a medios acorazados (Briaco), avanzar en plan de construcción de buques (por ahora rompe hielos y OPVs), y fortalecer el programa Satelital Chileno, recientemente estrenado por las autoridades. Finalmente, México se centrará en la Feria Aeroespacial 2023, así como concreción de planes de construcción naval muy postergados.

¿Cómo se ha comportado la industria tecnológica militar durante estos últimos 20 años? ¿Qué planes de desarrollo tecnológico han dominado? ¿Cómo ha sido el tránsito de generar valor a través de clústeres? Respuestas que serán focalizadas mediante una tabulación de aquellos principales proyectos generados por el sector Defensa, y así cotejar el avance que se ha logrado en I + D + i. (ver Anexo 1)

Del análisis temporal 2000-2015 (Anexo 1) se confirma una tendencia estatal de privilegiar la adquisición de sistemas en el extranjero por sobre desarrollar soluciones nacionales. Si bien se presentan proyectos complejos, como los requeridos en la construcción de plataformas aéreas, marinas o terrestres, finalmente la gestión se ha centrado en complementar los proyectos. La principal razón para que esto ocurra es el presupuesto que cada Estado, anualmente, está dispuesto a distribuir de su erario para financiar la industria de la Defensa.

Sin embargo, se advierte que en el período 2016-2030 (aun en evolución), un síntoma de cambio tendencial. En este sentido, se destacan las apuestas de Brasil y México por sobre el resto de los países (SHERVI, 2020). Del mismo modo, se instala el concepto de "co-producción", reconociendo el fomento hacia la participación

de agentes internacionales en proyectos o bien como proveedores de soluciones militares y servicios multisectoriales. En este ámbito irrumpen empresas privadas (nacionales y extranjeras), constituyendo un pilar fundamental para establecer robustos clústeres de la industria de la Defensa, ya que han sido éstas empresas las que han ocupado un espacio que otrora era exclusivo de empresas estatales.

La mayor crítica sobre este evolutivo proceso es constatar la brecha en proyectos y programas que sustenten, como primera opción, invertir mayores recursos en I + D + i. Tal como se indicó en el Cuadro 5 (previo), no se aprecia una simbiosis de IA – IoT – *Big Data* – *Blockchain* – computación cuántica - 5G – 3D *printing* – robótica – Drones – Nano tecnología – biotecnología, en soluciones que provengan desde la industria de la Defensa local, y lo poco que se ha producido no redunda en niveles considerados aceptables, pese a que se han instalado como fundamentales para enfrentar nuevas amenazas en escenarios híbridos en la era de la 4RI.

5 LA TRANSFERENCIA CIRCULAR ENTRE *I + D + I* Y LA SEGURIDAD NACIONAL

En este apartado se retomará el postulado, previamente establecido en nuestro estudio, que se encamina en acreditar el grado de dependencia que surge entre gastar/invertir en *I + D + i* y Seguridad Nacional. A partir de las nociones de DCAF (DCAF, 2015) e instituto LISA se evitará contaminar el análisis con visiones que permanecen ancladas en la Guerra Fría. En este contexto, y sin pretender reinstaurar una nueva conceptualización de "carrera espacial", como modelo de desarrollo científico y tecnológico, nos concentraremos en aquellos elementos que sustentan nuestro axioma.

Para ninguna persona podría pasar inadvertido los recientes lanzamientos de misiones espaciales en dirección al planeta Rojo (Marte), teniendo por objeto, entre otros, "analizar si hubo vida". En efecto, en esta oportunidad las agencias interesadas pertenecen a Estados Unidos, China, India, y, por primera vez, Emiratos Árabes Unidos (ABBANY, 2021), a los que próximamente se unirá la Agencia Espacial Europea en colaboración con la Representación Espacial Rusa (ROUQUETTE, 2020). ¿Qué los ha unido para asumir una empresa espacial que enfrenta enormes desafíos para llegar a Marte? Fuera de descubrir nuevos horizontes (científicos, tecnológicos, geopolíticos), también existen otros factores, que se vincularían a la Seguridad Nacional en la perspectiva de 4RI.

Los proyectos de las distintas agencias espaciales se concentran en: identificar la conformación atómica de la superficie marciana; crear mapas de zonas de interés a partir de 3D; intentar producir oxígeno en la atmósfera de Marte, y otros. Sin embargo, quedan temas pendientes por resolver, como la duración del viaje (aproximadamente 9 meses), suministros para la tripulación, la enorme exposición a la radiación solar de los mismos, entre otros factores (ACHENBACH, 2016). Como

respuesta a esta incertidumbre viene por el lado del empleo de robots, apoyados de IA y así disponer de vehículos no tripulados, artilugios que se desarrollan reservadamente.

Si bien dichos proyectos pretenden objetivos "científico-humanitario", es importante señalar que para el éxito de cada uno de ellos depende, en gran medida, contar con comunicaciones seguras y permanentes. En el entorno descrito, se reconoce la preponderancia que han adquirido los satélites y por tanto es dable cuestionarse: ¿Qué pasaría si estos sistemas, satélites, comunicaciones, etc. sean afectados por "virus cibernéticos" o, lisa y llanamente, sean víctimas de ataques cibernéticos, como el perpetrado últimamente a laboratorios biotecnológicos en Europa? (MIT, 2020).

La solución podría venir desde Francia, país que ha incursionado en tecnologías cuánticas buscando otorgar mayor seguridad a sus sistemas de comunicaciones. De este modo, ha puesto interés por evitar "interferencias no deseadas", un vector responsable de las desconexiones. En este plano, ha avanzado en reducir la elevada dependencia de satélites. Otras prestaciones que ha identificado el país Galo se sitúan en áreas descritas como "de interés militar" (precisión de armas) e "inteligencia estratégica" (*Big Data*, ruptura de algoritmos, realidad aumentada). En este contexto, según el sitio *Defense News* la tarea estará a cargo del Instituto Nacional de Investigación en Ciencia y Tecnología Digitales (INRIA, por sus siglas en francés), y será acogido por la Comisión de Energías Alternativas y Energía Atómica (CEA), en instalaciones tecnológicas militares (MACHI, 2022).

El ejemplo descrito permite corroborar que el Estado francés aplica la noción de Seguridad Nacional como principio rector en áreas de repercusión estratégica, en este caso el espacio ultraterrestre. Un principio adoptado para otros proyectos duales como el desarrollo de vehículos no tripulados o Drones con prestaciones civil-militares.

En el estudio de Sistemas de Armas Autónomas Letales (LAWS, por sus siglas en inglés), llevado a cabo el año 2019 (QUEIROLO, 2019), se aportaron antecedentes para identificar algunas implicancias jurídicas y bélicas sobre el empleo de sistemas autónomos. Tal ha sido el interés que luego de dos años el avance tecnológico ha alcanzado el empleo de "enjambres de drones", que por ahora no poseen la condición de autónomos.

Sin entrar en materia de discusión jurídica (se sugiere leer el artículo), se puede afirmar que la operación de enjambres ha presentado mejores prestaciones que los drones solitarios. En pruebas del sistema la efectividad de ubicación de personas extraviadas en ambientes complejos como montaña o zonas afectadas por incendios, entre otros, es superior, es decir el beneficio supera la esfera de operaciones militares (MCMULLAN, 2019). La mayor dificultad que ha presentado el uso de enjambres de drones es su sistema de comunicación, requiriendo una conectividad fina para que la IA *interdrone* logre efectividad y evite colisiones en sus

misiones (INTERESTING ENGINEERING, 2021). Lo importante es resaltar los pasos dados para integrar, sincronizar y multiplicar beneficios en pro de un Estado que sustente una renovada conceptualización de Seguridad Nacional.

El análisis de los antecedentes permite, nuevamente, evidenciar la relación directa entre gastar/invertir en *I + D + i* y beneficios que se obtienen. Observemos a los satélites, radares, drones, robots, e IA, desarrollados por la industria de la Seguridad y Defensa cuyo objetivo ha sido prestar servicios en operaciones militares y, de acuerdo a sus capacidades, también han sido utilizados para otras funciones de importancia civil. En efecto, catástrofes, emergencias, ayudas humanitarias y evacuaciones, son solo algunos de los fenómenos en que ingenios tecnológicos militares han contribuido a resolver necesidades estatales. ¿Qué tan lejos están estas actividades de aquellas que se derivan del cumplimiento de los Objetivos de Desarrollo Sostenible 2030 (ODS)[3]? ¿Cuál sería la relación con la Seguridad Nacional?

Del análisis a los diecisiete (17) ODS, se puede observar múltiples tareas vinculadas con áreas tan diversas como salud, cambio climático, educación, desarrollo de industria e innovación, vida marina y energía, como ambientes donde *I + D + i* de Defensa debiese estar presente, apelando a ventajas comparativas. El fundamento se sostiene en lo señalado en el reporte de la CEPAL al indicar:

> En los países de la región, los planes y estrategias nacionales se han ido alineando con la Agenda 2030, y en la mayoría se han establecido mecanismos institucionales de seguimiento y evaluación; no obstante, aún no se ha generado gran parte de la información estadística necesaria para elaborar los indicadores que permitan evaluar el avance hacia las metas, dado que se requiere producir datos en áreas nuevas y con una mayor desagregación para centrar el análisis en los grupos más vulnerables. (CEPAL, 2020, pp. 7-8)

Aplicando estas orientaciones la aplicaremos sobre el Continente Antártico, que, para el caso de Chile, permite evidenciar una manifiesta relación circular *I + D + i* y Defensa. Como país reclamante de soberanía, y al igual que otros signatarios del Tratado Antártico[4] y el Protocolo sobre Protección al Medio Ambiente[5], posee bases militares y científicas. Desde ellas, se patrocinan diferentes actividades e investigaciones cuyos resultados son internacionalmente reconocidos. Estudios sobre el comportamiento humano en climas extremos, experimentos sobre

3 (CEPAL, 2015). ODS. Disponible en: https://www.cepal.org/es/temas/agenda-2030-desarrollo-sostenible/objetivos-desarrollo-sostenible-ods

4 INACH. Tratado Antártico, 1959. Disponible en: https://www.inach.cl/inach/wp-content/uploads/2009/10/treaty_original.pdf

5 INACH. Protocolo sobre Protección al Medio Ambiente, 1991. Disponible en: https://www.inach.cl/inach/wp-content/uploads/2010/01/protocolo_medio_ambiente.pdf

enfermedades, análisis de la variable clima, control de vida marina y áreas protegidas, resguardo a disponibilidad de recursos y otros (REBOLLEDO, 2022), son solo algunas de las tareas que requieren de tecnología de punta para cumplir con el cometido.

De esta manera, podemos afirmar la importancia que resulta el propiciar clústeres de Defensa en esta titánica tarea. En esta ruta la construcción de plataformas navales (buques antárticos), aéreas (aeronaves, satélites), y terrestres (bases), constituyen una necesidad que el Estado debe impulsar y cautelar, en el marco del ejercicio soberano (MINDEF, 2021). Sin duda que el comprender el alcance de llevar a cabo este tipo de funciones allana la comprensión sobre la Seguridad Nacional en la era de 4RI.

Otra materia que se entrelaza I + D + i con la Seguridad Nacional es la dimensión del ciberespacio. Un dominio virtual que revela riesgos y amenazas nunca antes visto, cuya mayor evidencia han sido los ataques cibernéticos, y pese a diferentes medidas adoptadas por los usuarios, sean gobiernos u organizaciones (públicas o privadas), no han cesado. Ahora todos integran la lista de posibles objetivos, principalmente aquellas infraestructuras estratégicas (EITB.EUS, 2021).

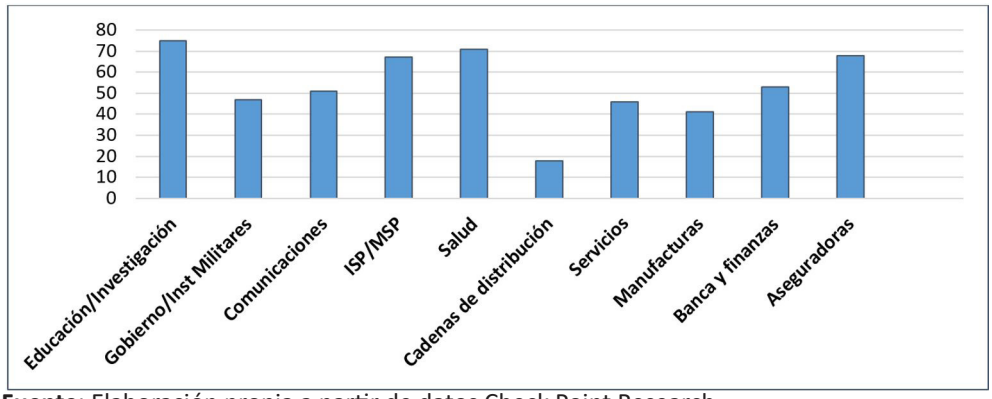
En el caso de infraestructuras estratégicas o críticas, como se identifica a aquellas instalaciones o servicios fundamentales para un Estado, cualquier alteración podría generar graves consecuencias, incluso provocar parálisis estratégica como fue el ataque a Estonia (MCGUINNES, 2017). Últimamente, los objetivos han sido un gaseoducto en EE.UU., una empresa de alimentos en Brasil y hospitales alrededor del mundo, evidencias que revelan la necesidad de adoptar medidas integrales (SONICWALL, 2021, p.3).

Ya no se trata del robo de datos personales o acceder a cuentas bancarias, que aún persisten, sino que se busca hacer daño con otros fines. Algunos ataques han traspasado las fronteras físicas con la intención de quebrantar sistemas democráticos. De este modo, la protección de fórmulas biológicas/químicas, de proyectos civiles o militares estratégicos e incluso evitar la manipulación de información o alteración de procesos electorales, han pasado a liderar la lista de riesgos y amenazas de Seguridad Nacional.

Para el sector Defensa, el ambiente cibernético descrito, representa un verdadero desafío, toda vez que forma parte del grupo objetivo. Asumiendo que constituye una infraestructura crítica requiere desarrollar estructuras robustas que protejan sus inventarios, en este ámbito, propiciar clústeres permitiría integrar capacidades (civiles y militares) con suficiente sinergia. Es aquí donde se constata la creación de Comandos Cibernéticos o Ciberespaciales y otros afines que, siguiendo pautas de Seguridad Nacional, han apostado al desarrollo de sistemas de *IA*, *Big Data*, computación cuántica y otros que enfrenten de manera eficiente esta nueva era digital.

Según el sitio *Check Point Research*[6], durante el 2021, se experimentó un alza importante de ciberataques afectando, en orden de prioridades, sectores como educación/investigación, gubernamental/militar, y la industria de las comunicaciones. Se puede deducir del reporte la configuración de ataques a infraestructuras críticas que un Estado debe proteger con medios tecnológicamente adecuados (ver Cuadro 10). Comprobando que la fórmula *I + D + i* constituye una variable que impacta en la Seguridad Nacional.

Cuadro 10: Porcentaje promedio de ataques por organización (2021)



Fuente: Elaboración propia a partir de datos Check Point Research.

6 CONCLUSIONES

La información recogida permite aseverar que la investigación, el desarrollo y la innovación (I + D +i) constituye un factor dominante para el progreso de un Estado. Sin duda que se pudo demostrar la existencia de un virtuosismo sinérgico entre dichos elementos, respondiendo así a la primera pregunta. Los Estados que se aparten de esta ecuación continuarán arrastrando una carga que se hará más pesada, un gravamen que estará propiciado, esta vez, por fenómenos políticos, sociales, económicos, laborales, culturales y ambientales que requieren soluciones integradoras como propicia la fórmula I + D + i. Esta vez el Covid-19, y otras crisis sanitarias sin resolver, así como el Cambio Climático, son solo la punta del iceberg de fenómenos que requieren de ciencia y tecnología para sobrellevarlos.

Tal como la propulsión a vapor, la electricidad, el auto y el computador, fueron ingenios que marcaron diferentes épocas de desarrollo humano, ahora son las "tecnologías disruptivas" vinculadas a la IA, Big Data, robótica, biotecnología, nanotecnología, la IoT y comunicaciones 5G/6G. Una nueva dimensión que

6 (Check Point Research, 2021). Disponible en: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/

imprimirá un sello generacional. Un mundo digital/virtual/lógico que requiere contar con estructuras y organizaciones (públicas y privadas), robustas, un ámbito que demandará de capital humano de excelencia para este nuevo entorno.

Concordando que el Estado es la organización política que debe proveer seguridad a sus ciudadanos y ejercer soberanía en su territorio, de la misma manera que propiciar su desarrollo y bienestar, para la industria de la Defensa constituye un impulso a una labor esencial que ha perfeccionado por décadas, actividad que no debiese menguar. En efecto, se constata una real oportunidad que ofrece una nueva época, conocida como 4RI, para reimpulsar clústeres de la Defensa. Para cumplir con este objetivo, se requiere de políticas estatales que propicien la transferencia de conocimiento a través del gasto en I + D + i, tal como se reconoce en Brasil y, en cierta medida México. Proyectos espaciales, cibernéticos, plataformas marítimas y otros campos asociados, son la evidencia que se ha alcanzado a través de una sinergia circular civil – militar, con réditos multisectoriales plausibles.

Se puede concluir que el piso requerido para alcanzar un nivel tecnológico que permita generar consistentes réditos en la sociedad, es propiciar un gasto/inversión del 1% del PIB en I + D + i y procurar avanzar al 1,5% en breve período. Una receta que ya ha dado utilidades en otras regiones. Este dato permite validar ambas preguntas del estudio, del mismo modo el postulado que sustenta la directa relación con la Seguridad Nacional en la 4RI.

Para evitar los vaivenes políticos que repercuten en la asignación presupuestaria, las administraciones debiesen considerar la fórmula I + D + i como factor dependiente para la elaboración de una Política de Seguridad Nacional. El reconocimiento gubernamental de esta ecuación fortalecería directamente el cumplimiento de varios, sino todos, los Objetivos de Desarrollo Sustentable que la Aldea Global se ha propuesto al 2030.

Como clústeres tecnológicos que la industria de la Defensa evidencia ventajas comparativas son: Ciberespacio – ciberinteligencia (señales, imágenes, data) – desarrollo de plataformas (aire, mar, tierra) – gestión de recursos estratégicos – data para cumplimiento de ODS, que se suman a los actuales nichos que únicamente deben desarrollarse por industrias estatales.

REFERENCIAS

ABBANY, Zulfikar. Estados Unidos, China y Emiratos Árabes: tres misiones en la carrera por Marte. *DW*, 09 Feb. 2021. Disponible en: https://www.dw.com/es/estados-unidos-china-y-emiratos-%C3%A1rabes-tres-misiones-en-la-carrera-por-marte/a-56513827. Accedida en: 3 feb. 2022

ACADEMIA NACIONAL DE ESTUDIOS POLÍTICOS Y ESTRATÉGICOS. Balance Estratégico 2020-2021. [Santiago]: ANEPE, 2021. Disponible en: https://www.publicacionesanepe.cl/index.php/balance/article/view/945/609. Accedida en: 11 feb 2022.

ACHENBACH, Joel. La conquista de Marte. *National Geographic*, 11 nov. 2016. Disponible en: https://www.nationalgeographic.com.es/ciencia/grandes-reportajes/conquista-marte_10848. Accedida en: 3 feb. 2022

BANCO INTERAMERICANO DE DESARROLLO. Ciencia, Tecnología e Innovación en América Latina y el Caribe. New York: BID, 2010. Disponible en: https://publications.iadb.org/publications/spanish/document/Ciencia-tecnolog%C3%ADa-e-innovaci%C3%B3n-en-Am%C3%A9rica-Latina-y-el-Caribe-Un-compendio-estad%C3%ADstico-de-indicadores.pdf. Accedida en: 4 feb. 2022

BANCO MUNDIAL. Gasto en investigación y desarrollo (% del PIB). [*S.l.*]: Banco Mundial, 2020. Disponible en: https://datos.bancomundial.org/indicator/GB.XPD.RSDV.GD.ZS. Accedida en: 3 feb. 2022.

CAIAFA, Roberto. BAE Systems y Embraer exploran el potencial de la aeronave Eve e VTOL en el mercado de defensa. *Infodefensa.com*, 23 dic. 2021. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/3349446/bae-systems-embraer-exploraran-posibles-variantes-defensa-eve-evtol. Accedida en: 20 ene. 2022.

CASTALDI, Carolina y DOSI, Giovanni. *Algunas lecciones de pautas seculares y algunas conjeturas sobre el impacto actual de las tic*. *Revista Economía*: teoría y práctica, Nueva época, v. 1, n. especial, nov. 2009. Disponible en: http://www.scielo.org.mx/pdf/etp/nspe1/nspe1a5.pdf. Accedida en: 20 ene. 2022

CENTRO DE ESTUDIOS ESTRATÉGICOS DE DEFENSA. Consejo de Defensa Suramericano. *Registro Suramericano de Gastos Agregados en Defensa*. Edición Especial 2006-2015. Buenos Aires: CEED, 2017.

CHILE. Senado. *Protección de los neuroderechos*: inédita legislación va a la Sala. [Santiago]: Senado, 2021. Disponible en: https://www.senado.cl/proteccion-de-los--neuroderechos-a-un-paso-de-pasar-a-segundo-tramite. Accedida en: 26 ene 2022

COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE. Informe de la Conferencia de Ciencia, Innovación y Tecnologías de la Información y las Comunicaciones "Innovación para el Desarrollo". *In*: CONFERENCIA DE CIENCIA, INNOVACIÓ Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, 3. 2021, Buenos Aires, 2021. *Actas* […]. Santiago: CEPAL, 2021. Disponible en: https://innovalac.cepal.org/3/sites/innovalac3/files/c2100805_web.pdf. Accedida en: 20 ene. 2022

COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE. *In*: CONFERENCIA DE CIENCIA, INNOVACIÓ Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, 3. 2021, Buenos Aires, 2021. *Actas* […]. Santiago de Chile: CEPAL, 2021. Disponible en: https://www.cepal.org/es/comunicados/paises-abogaron-un-rol-mas-activo-la-ciencia-innovacion-nuevas-tecnologias-politicas. Accedida en: 13 feb 2022.

COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE. *Objetivos de Desarrolo Sostenible (ODS)*. Santiago de Chile: CEPAL, 2015. Disponible en: https://www.cepal.org/es/temas/agenda-2030-desarrollo-sostenible/objetivos-desarrollo-sostenible-ods. Accedida en: 20 ene. 2022

COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE. *Gasto público para impulsar el desarrollo económico e inclusivo y lograr los Objetivos de Desarrollo Sostenible*. Santiago de Chile: CEPAL, 2020. Disponible en: https://www.cepal.org/sites/default/files/publication/files/46276/S2000670_es.pdf. Accedida en: 25 ene. 2022

COATS, Daniel R. *Worldwide Threat Assessment of the US Intelligence Community*. [*S.l.*]: DNI, 2019. Disponible en: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf. Accedida en: 4 ene. 2022.

COLOM, Guillem. P. *Entre Ares y Atenea.* El debate sobre la Revolución en Asuntos Militares. Madrid: IUGM, 2008. Disponible en: https://iugm.es/wp-content/uploads/2016/07/Libro_Entre_ares.pdf. Accedida en: 4 ene. 2022.

CHECK Point Research: cyber attacks increased 50% year over year. *Check Point*, [2022]. Disponible en: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/ Accedida en: 12 ene. 2022:

CHILE. Ministerio de Defensa Nacional. Ministerios de Defensa y Ciencia firman convenio para fomentar la investigación y la innovación en ciencia y tecnología. Disponible en: https://www.defensa.cl/noticias/ministerios-de-defensa-y-ciencia-firman-convenio-para-fomentar-la-investigacion-y-la-innovacion-en-c/. Accedida en: 11 feb. 2022.

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY. [Condado de Arlington]: DARPA, 2019. Disponible en: https://www.darpa.mil/attachments/DARPA-2019-framework.pdf. Accedida en: 25 ene. 2022

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY. *OFFSET swarms take flight in final field experiment*. [Condado de Arlington]: DARPA, 2021 Disponible en: https://www.darpa.mil/news-events/2021-12-09. Accedida en: 12 ene. 2022

DONADIO, Marcela. *Atlas comparativo de la defensa en América Latina y Caribe*. Buenos Aires: RESDAL, 2016. Disponible en: https://www.resdal.org/assets/atlas-2016-esp-completo.pdf. Accedida en: 01 feb. 2022.

GENEVA CENTRE FOR SECURITY SECTOR GOVERNANCE. National Security Policy. DCAF, Disponible en: https://securitysectorintegrity.com/defence-management/policy/#_ftn1 Accedida en: 16 feb. 2022.

GIL, Abel. La Revolución Industrial en Europa. *El Orden Mundial (blog)*. 2020. Disponible en: https://elordenmundial.com/mapas-y-graficos/revolucion-industrial-europa/ Accedida en: 01 feb. 2022.

INSTITUTO ANTARTICO CHILENO. *Protocolo sobre Protección al Medio Ambiente*. [Santiago]: INACH, [2010]. Disponible en: https://www.inach.cl/inach/wp-content/uploads/2010/01/protocolo_medio_ambiente.pdf. Accedida en: 10 ene. 2022.

LA UE, Estados Unidos y la OTAN reclaman a China que tome medidas para frenar los ciberataques. *EITB.EUS*, 21 jul. 2021. Disponible en: https://www.eitb.eus/es/noticias/internacional/detalle/8200773/la-ue-estados-unidos-y-otan-reclaman-a-china-que-tome-medidas-para-frenar-ciberataques/ Accedida en: 12 ene. 2022

LEMARCHAND, Gillermo A. America Latina. *In*: INFORME de la UNESCO sobre la ciencia, [2015]. Disponible en: https://en.unesco.org/sites/default/files/usr15_latin_america_es.pdf. Accedida en: 11 ene. 2022.

LISA INSTITUTE. *¿Qué es la Seguridad Nacional? Riesgos y Amenazas.* Madrid: LISA Institute, 2019. Disponible en: https://www.lisainstitute.com/blogs/blog/seguridad-nacional-riesgos-amenazas. Accedida en: 15 ene. 2022.

LOS RETOS del sector de la defensa en Latinoamérica para el 2022. *Infodefensa.com*, 23 dic. 2021. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/3350959/retos-sector-defensa-latinoamerica-2022?utm_source=dlvr.it&utm_medium=linkedin. Accedida en: 20 ene. 2022.

MACHI, Vivienne. Eying military gains, France goes big on national quantum technology. *Defense News*, 5 Jan. 2022. Disponible en: https://www.defensenews.com/global/europe/2022/01/05/eying-military-gains-france-goes-big-on-national-quantum-technology/?utm_source=Linkedin&utm_medium=social&utm_campaign=Socialflow+DFN. Accedida en: 11 feb. 2022.

MCGUINNESS, Damien. Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país. *BBC News*, 6 mayo 2017. Mundo. Disponible en: https://www.bbc.com/mundo/noticias-39800133. Accedida en 11 ene. 2022.

MCMULLAN, Thomas. Cómo los enjambres de drones cambiarán la estrategia de las guerras del futuro. *BBC News*, 19 mar. 2019. Mundo. Disponible en: https://www.bbc.com/mundo/noticias-47595525 . Accedida en: 3 ene. 2022.

NACIONES UNIDAS. Objetivos de Desarrollo Sostenible 2030. [*S.l.*]: ONU, 2015. Disponible en: https://www.un.org/sustainabledevelopment/es/2015/09/la-asamblea-general-adopta-la-agenda-2030-para-el-desarrollo-sostenible/. Accedida en: 11 feb. 2022.

NACIONES UNIDAS. Technology and Innovation Report 2021: Catching technology waves, innovation with equity. United Nations Conference on Trade and Development. 2020. Disponible en: https://unctad.org/system/files/official-document/tir2020overview_en.pdf
Accedida en: 11 feb. 2022.

NAVARRO, José María. La evolución tecnológica de los sistemas de armas. *Defensa.com*, 24 jun. 2018. Disponible en: https://www.defensa.com/reportajes/evolucion-tecnologica-sistemas-armas. Accedida en: 11 feb. 2022.

O'NEILL, Patrick Howell. Traducido por Ana Milutinovic. Un ciberataque ha robado datos confidenciales de la vacuna de Pfizer. *MIT Technology Review*, 11 dic. 2020. Disponible en: https://www.technologyreview.es//s/12964/un-ciberataque-ha-robado-datos-confidenciales-de-la-vacuna-de-pfizer. Accedida en: 13 feb. 2022.

OTTO, Carlos. Los secretos silicon wadi: el milagro de Israel: así es la fórmula que lo convirtió en el nuevo Silicon Valley. *La Vanguardia*, 20 jun. 2016. https://www.lavanguardia.com/tecnologia/20160618/402597185310/israel-emprendedores-startups-silicon-wadi.html. Accedida en: 22 ene. 2022.

PARRA, David. Lo nunca visto. Un enjambre de drones controlados por una IA. AZ *ADSL ZONE*, jul. 2021. Disponible en: https://www.adslzone.net/noticias/ia/en-jambre-drones-militares-ia/. Accedida en: 1 feb. 2022.

REYES, Mirlis S. Los Clúster Industriales de Defensa como Impulsores de la Innovación Tecnológica en América Latina. *Revista del Colegio Interamericano de Defensa*, v. 1, jul. 2014 / jun. 2015. Disponible en: http://publications.iadc.edu/wp-content/uploads/sites/5/2019/08/revista-del-cid-2015.pdf . Accedida en: 4 feb. 2022.

QUEIROLO, Fulvio. Sistemas de armas autónomos letales (LAWS). Reflexiones para un debate. *Revista Política y Estrategia*, n. 134, jul./dic 2019. Disponible en: https://www.politicayestrategia.cl/index.php/rpye/article/view/790 Accedida en: 10 ene. 2022

PEDRAZA, Jacobo. Talento Digital, 3 de octubre 2017. Nosotros inventamos, los militares lo aprovechan (y viceversa). *El País*, Madrid, 3 oct. 2017. Disponible en: https://elpais.com/elpais/2017/09/07/talento_digital/1504735775_608262.html. Accedida en: 4 ene. 2022.

REBOLLEDO, Lorena. La importancia del monitoreo continuo del sistema climático en Antártica y sus desafíos futuros. *Elmostrador*, 9 enero, 2022. Disponible en: https://www.elmostrador.cl/cultura/2022/01/09/la-importancia-del-monitoreo-continuo-del-sistema-climatico-en-antartica-y-sus-desafios-futuros/. Accedida en: 3 feb. 2022.

ROUQUETTE, Pauline. China, Estados Unidos, Emiratos Árabes... a toda marcha en la carrera hacia Marte. FRANCE 24, 25 jul. 2020. Disponible en: https://www.france24.com/es/20200724-carrera-exploracion-marte-china-eeuu-emiratos-india. Accedida en: 1 feb. 2022.

SHERVI, Eshan. Ciencia, tecnología e innovación en la defensa: los casos de Brasil y México (2007-2020). *Cuaderno de Trabajo*, n. 7, 2020. Disponible en: https://www.publicacionesanepe.cl/index.php/cdt/article/view/858. Accedida en: 10 ene. 2022.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE. SIPRI arms industry database. Stockholm: SIPRI, 2020. Disponible en: https://www.sipri.org/databases/armsindustry. Accedida en: 12 feb. 2022

STOCKHOLM SECURITY CONFERENCE, 2021, Stockholm. *Proceedings* […]. Stockholm; SIPRI, 2021. Theme: Battlefields of the Future: Trends of Conflict and Warfare in the 21st Century. Disponible en: https://www.sipri.org/events/2021/2021-stockholm-security-conference. Accedida en: 18 feb. 2022.

SCHWAB, Klaus. La Cuarta Revolución Industrial. *In*: WORLD ECONOMIC FORUM ANNUAL MEETING, 2016. *Anales* […]. Davos-Klosters: WEF, 2016. Disponible en: https://www3.weforum.org/docs/WEF_AM16_Report.pdf. Accedida en: 10 feb. 2022.

SONICWALL. Cyber Threat Report. Mid-Year Update, 2021. Milpitas, CA: SONICWALL, 2021. Disponible en: https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2021-cyber-threat-report.pdf. Accedida en: 15 ene. 2022.

ANEXO

PAIS	2000-2015	2016-2030
Argentina	• Proyecto y desarrollo: – C.Conjunto Ciberdefensa – UAVs – Pampa III/GT – Sistemas comunicaciones satelitales • Adquisición de HE Bell 412 • Mantenimiento y Modernización: – Plataformas aéreas (C-130--Tucano-A4, Pampa I/II. – Misiles – Plataformas terrestres (TAM2C) – Plataformas navales (submarinos, rompehielos)	• Adquisición de: – HE Sea King, Bell 412, radares RPA200M, camiones, • Modernización: – TAM2C, Corbetas • Proyecto cofabricación blindados • Desarrollo avión IA-100B
Brasil	• Plan de Articulación y Equipamiento (PAED, 2012 - 2031) • Desarrollo de proyectos: – Construcción de submarinos Scorpene modificados (S-BR) – Construcción de avión de reemplazo de C-130 “Hércules” por KC-390 “Millennium” – Desarrollo UAV “Atobá” – Proyecto y desarrollo de Centro de Defensa Cibernética • Modernización de carros de combate (M-60, Leopard 1A 1, M113, Urutu, Cacavel) • Actualización de sistemas de defensa A.A. • Adquisición de misiles y cohetes • Actualización de tecnología de aviones F-5, KC-130, C-95, P-95, P-3. • Proyecto de adquisición de aviones caza, C-295, helicópteros H-60, y UAVs	• Construcción de Submarinos Scorpene Clase Riachuelo y S-42 / S-43 • Coproducción de: – Submarino propulsión nuclear (SN – BR) – Corbetas Clase Tamandaré – EMBRAER-SAAB (36 Gripen) – UAVs • Construcción de Aeronaves KC-390 • Creación de Centro de Operaciones Satelitales • Construcción de Navíos de soporte antártico. • Estructuración de Sistema de ciberdefensa (Comando) • Producción de satélite de observación terrestre “Amazonía 1-2-3” diseño, integración, prueba y operación propia de Brasil. (1 lanzado). • Proyecto lanzadores espaciales VLM1 – Aquila 1 y 2.

Colombia	• Adquisición: – Aviones Kfir – Aviones SuperTucano • Mantenimiento y modernización: – VBL M113A2, EE-9 – Aviones Kfir – HE UH-60 • Fabricación Patrulleras Fluviales	• Adquisición: – Aviones Boeing 737-700/800, T-6 Texan II, King Air, HE Bell 412, Drones FVR-90, sistema guerra electrónica – VBL M-1117 • Mantenimiento y modernización: – HE UH-60 – M113A2, HMMWV – Aviones Kfir – Corbetas • Fabricación VLC Cobra 3.0 • Proyectos adquisición: – Caza F-16 OPVs
Chile	• Recuperación y servicios de armamento menor, cohetes, misiles, municiones y propelentes. • Mantenimiento y actualización: – Sistemas de material acorazado Leopard 1V, M113, M548, LAR 160mm. – Aeronaves y componentes (Mirage, F-5e, HE-UH 1H) • Adquisición de: – Leopard 2 A4, Marder 1A 3 – Caza F-16 (10 nuevos /36 usados) – HE-Bell 412 (12) • Construcción: – buques de apoyo logístico y auxiliares – embarcaciones de servicio general. • Modernización: – destructores, fragatas, misileras y submarinos. • Desarrollo e integración de sistemas C4I • Fabricación de aviones de entrenamiento (Pillán), partes y piezas especiales. • Desarrollo y lanzamiento de satélite Fasat Charlie • Proyectos: – cofabricación de fusiles – simuladores – sistemas autónomos Fragatas	• Mantenimiento y modernización: – Sistemas material acorazado Leopard 1V, Leopard 2 A4, M113, M548, LAR 160mm. – Plataformas aéreas – Plataformas marítimas. • Adquisición: – Aviones Super Tucano – HE UH-60 • Construcción de buques multipropósito OPVs • Proyecto de implementación del Sistema Nacional Satelital • Coproducción de 10 satélites (2021 y 2025)

México	• Adquisición: – HE Bell 412, UH-60, CH53, Super Cougar, AW109 Augusta – Aviones C-27 Spartan, T-6C, Texan, Embraer 145 AEW&C, Pilatus, CASA-295 – Buques Patrulla Oceánica – Patrulla Costera – Buques Asalto • Mantenimiento – Aviones F5E • Proyecto: Radares largo alcance	• Mantenimiento y modernización: – UH-60 – C-130 “Hércules” • Construcción vehículos blindados. • Coproducción de: – UAVs, Buques de largo alcance POLA, OPVs (Offshore Patrol Vessel, siglas en inglés) – Sistemas de mando y control, de inteligencia de radares y vigilancia aérea. • Estructuración de Sistema de ciberdefensa (Comando) • Adquisición – HE Bell 407 • UH-60

RIESGO CIBERNÉTICO DEL SECTOR DEFENSA EN LA CUARTA REVOLUCIÓN INDUSTRIAL

Lucas Adolfo Giraldo-Rios*

RESUMEN
El desarrollo de tecnologías y usos aumenta el ecosistema digital interconectado. Esto va acompañado de un uso intensivo de datos. Dondequiera que haya datos digitales disponibles, los ataques cibernéticos están amenazados y aumentan la necesidad de prevención de la seguridad cibernética. El hecho de que el combustible básico de la Industria 4.0 sean datos indica que el riesgo de ciberataque seguirá aumentando. En este capítulo, las fuentes de amenazas a la ciberseguridad en el ecosistema de la Industria 4.0 se examinan en las dimensiones corporativa y de usuario final. Se ha determinado que las vulnerabilidades de seguridad cibernética más evidentes en los sistemas de la Industria 4.0 incluyen vulnerabilidades en los protocolos de los sistemas de control, conexiones de dispositivos o elementos desprotegidos, descuido de las pruebas de infiltración periódicas, incapacidad para administrar los dispositivos de red de manera efectiva y personal no capacitado. Se han determinado las estrategias de ciberdefensa y los requisitos para estas vulnerabilidades. Al mismo tiempo, se les ha dicho a las empresas y usuarios finales cómo implementar estas prevenciones. Como resultado, no es posible prevenir por completo los ciberataques dentro del ecosistema de la Industria 4.0. Prevenir las vulnerabilidades identificadas en el estudio garantizará que el daño sea mínimo en los ataques.
Palabras Clave: Ciberseguridad; Ciberataque; Estrategias de defensa; Evaluación de riesgos; Industria 4.0.

RISCO CIBERNÉTICO DO SETOR DE DEFESA NA QUARTA REVOLUÇÃO INDUSTRIAL

RESUMO
O desenvolvimento e uso de tecnologias aumenta o ecossistema digital interconectado, acompanhado de um intenso uso de dados. Onde existir dados digitais disponíveis, há a ameaça de ciberataques, aumentando a necessidade de prevenção de segurança cibernética. O fato de que o combustível básico da Indústria 4.0 sejam dados indica que o risco de ataques cibernéticos seguirá aumentando. Neste texto, as fontes de ameaças à cibersegurança no ecossistema da Indústria 4.0 se examinam nas dimensões corporativa e de usuário final. Foram determinadas

* Especialista en Finanzas, Magister en Innovación, Magister en Administración y Candidato a Doctor en Ingeniería de la Universidad Nacional de Colombia, Docente Investigador de la ESDEG.

que as vulnerabilidades de segurança cibernética mais evidentes nos sistemas da Indústria 4.0 incluem fragilidades nos protocolos de sistema de controle, conexões de dispositivos ou elementos desprotegidos, descuido das provas periódicas de infiltração, incapacidade para administrar os dispositivos de rede de maneira efetiva e equipe não treinada. Ao mesmo tempo, empresas e usuários foram informados como implementar essas prevenções. Como resultado, não é possível prevenir por completo os ciberataques dentro do ecossistema da Indústria 4.0. Prevenir as vulnerabilidades identificadas no estudo garantirá que o dano seja mínimo nos ataques.
Palavras-chave: Cibersegurança; Ciberataque; Estratégias de defesa; evolução de riscos; Indústria 4.0.

1 INTRODUCCIÓN

Hace siglos, la Industria 1.0 había surgido con la invención y el uso de las máquinas de vapor (LASI *et al.*, 2014). La Industria 2 surgió con el desarrollo de dispositivos eléctricos y producidos en masa (LEE *et al.*, 2015). La Industria 3.0, con el uso de robots y computadoras en la línea de producción (LU, 2017). El paso final, la Industria 4.0, llamada la cuarta fase de la revolución industrial, es un período de fabricación inteligente en el que se minimiza la influencia humana en el proceso de fabricación, junto con la inteligencia artificial, Internet de las cosas y *Big Data*. La Industria 4.0 se basa en los principios de interoperabilidad, virtualización, gestión independiente, modularidad y tiempo real (GORECKY *et al.,* 2014). Hoy en día, el impacto de la gran revolución industrial, denominada Industria 4.0, sigue aumentando a nivel mundial (ALMADA-LOBO, 2016).

Los Sistemas Ciberfísicos (CPS[1]- por sus siglas en inglés) son el conjunto de estructuras que incluyen sistemas de fabricación inteligente y proporcionan comunicación y coordinación entre el Internet de las cosas industriales (IoT) y el mundo físico, que también se utiliza en la Industria 4.0 (LU, 2017). Los CPS se utilizan en procesos de fabricación, investigación y desarrollo, diseño y ventas en la Industria 4.0. Si bien los sistemas de fabricación inteligente brindan una gran comodidad en nuestras vidas, también conducen a la aparición de riesgos significativos, como los ataques cibernéticos (ZHOU *et al.*, 2015). En la Industria 4.0, todos los sistemas inteligentes están interconectados con redes cableadas o inalámbricas por su propia identidad. Los ciberataques a estas redes provocarán fallos de producción irreparables o daños graves. Para minimizar los riesgos cibernéticos, los fabricantes que adoptan la Industria 4.0 deben abordar los riesgos cibernéticos e identificar estrategias de seguridad cibernética (JAZDI, 2014).

1 Cyber-Physical Systems.

Para el desarrollo de este capítulo se examinaron los estudios sobre ciberseguridad dentro de las redes de Industria 4.0 en la literatura. En la Industria 4.0, los ataques cibernéticos se llevan a cabo en IoT (LU; DA XU, 2018), *Cyber-Physical Systems* (CPS) (HSU; MARINUCCI; VOAS, 2015) fabricación (WELLS *et al*., 2014) y capas de red (GUPTA; KULARIYA, 2016). Se han desarrollado soluciones para prevenir ataques a estas capas (LEZZI; LAZOI; CORALLO, 2018).

Aunque existen diferentes vulnerabilidades de seguridad en CPS, se han solucionado las vulnerabilidades de día cero. Estos han sido investigados en todas las capas de intercambio de información. En particular, las vulnerabilidades de seguridad de los sistemas SCADA son las siguientes (LEZZI; LAZOI; CORALLO, 2018).

- Servidores de aplicaciones y bases de datos.
- Interfaces hombre-máquina.
- Controladores lógicos de programa (PLC[2] - Por sus siglas en inglés).
- Unidades terminales remotas.
- Protocolos de comunicación y red.

La transferencia segura de datos es un tema importante en la comunicación entre dispositivos. El problema de producción se debe a su modificación, eliminación o interrupción de estos datos (KOGISO; FUJITA, 2015). La literatura se centra en la protección DDOS y las prevenciones de cifrado para una comunicación segura (SEMERCI; CEMGIL; SANKUR, 2018). En particular, las características de seguridad de los dispositivos IoT deben considerarse sin necesidad de compra. Se deben identificar contraseñas seguras y únicas para las cuentas de estos dispositivos. También se recomienda utilizar VPN al acceder a redes inalámbricas (LIU *et al*., 2012).

Como resultado, los ataques cibernéticos hacen que las instituciones reduzcan su productividad y competitividad. Además, los usuarios finales sufren pérdidas financieras y robo de sus datos personales en estos ataques. Cuando se examinan los estudios en la literatura, se han propuesto o desarrollado soluciones para prevenir ataques cibernéticos. Pero estas soluciones están dirigidas a capas individuales o específicas. No se ha introducido una prevención que cubra todo el ecosistema de la industria 4.0.

2 OBJETIVOS DE ATAQUE EN LA INDUSTRIA 4.0

La Industria 4.0 es una revolución industrial en la que los procesos de fabricación y la manufactura se llevan a cabo mediante sistemas inteligentes. En este proceso de producción, las etapas desde el diseño hasta la producción se pueden

2 Program Logic Controllers

controlar y gestionar desde cualquier lugar (BAHRIN *et al.*, 2016). La Industria 4.0 también proporciona un entorno en el que el producto y la producción se pueden llevar a cabo a través de simulaciones (ZHENG *et al.*, 2018) y generalmente se basa en los principios de interoperabilidad, virtualización, gestión autónoma, tiempo real, orientación al servicio y modularidad (ZHONG *et al.*, 2017).

Para desarrollar estrategias de defensa contra ciberataques, es necesario identificar las fuentes del ataque. Los ataques están dirigidos a CPS e IoT en Industria 4.0 (PETRASCH; HENTSCHKE., 2016).

3 SISTEMAS CIBERFÍSICOS – CPS

El ecosistema de la Industria 4.0 está conectado entre si través del mundo físico e internet a través de sistemas de ciberseguridad (*Cyber-Physical System*, CPS). Además, los CPS recopilan rastros de sensores y actuadores en el espacio y les permite interactuar entre sí. El modelo CPS consta de dispositivos que interactúan entre sí y se comunican con el mundo físico (WANG *et al.*, 2010). Las aplicaciones de CPS se pueden encontrar en muchas áreas, como sistemas de fabricación, redes inteligentes, robótica, sistemas de transporte, dispositivos médicos, espacio militar, edificios inteligentes, entre otros (ÉL; JIN, 2016).

El primer paso en el desarrollo de sistemas CPS en la industria es la recuperación de datos precisos y confiables de los objetos. El punto importante a destacar aquí es que los datos provienen directamente de sensores o de sistemas de producción como ERP, MES, SCM y CMM. En el paso de transformación de información-datos, la información significativa se extrae de los datos leídos a través de varias herramientas o metodologías. La ciberarquitectura es el centro de información del CPS (WANG *et al.*, 2010). Aquí se llevan a cabo procesos como construir redes de máquinas, registrar su desempeño y predecir su comportamiento futuro. En el cuarto nivel del CPS, se presentan datos a usuarios expertos, se visualizan situaciones de la máquina y se toman decisiones sobre el proceso. En el último nivel se retroalimenta el espacio físico y se reconfiguran las máquinas.

4 INTERNET DE LAS COSAS (IOT)

IoT es la comunicación y gestión en tiempo real de sensores, actuadores, sistemas de control y redes de máquinas en la industria, desde la producción hasta la comercialización (LEE, I; LEE, K., 2015). La arquitectura IoT consta de 3 capas. Estas son las capas de detección, comunicación y aplicación respectivamente (GUBBI *et al.*, 2013). Los riesgos y amenazas que pueden ocurrir en las capas de los sistemas IoT se dan en la Tabla 1.

Tabla 1: Riesgos y amenazas en las capas IoT

Tipo de capa IoT	Amenazas de ciberseguridad
Detección	Señales inalámbricas, ataque físico, topología IoT
Redes	Análisis de tráfico, escucha oculta, pasiva monitoreo, diferencias de hardware y protocolos de red
Aplicación	Políticas de Seguridad, Sistemas de Autenticación

Fuente: GUBBI *et al.* 2013

Las tecnologías de comunicación utilizadas para conectar dispositivos IoT y sus estándares se proporcionan en la Tabla 2. Estas tecnologías de comunicación se utilizan a menudo en la capa de enlace de datos, la capa de red, la capa de comunicación y la capa de aplicación (MADAKAM; RAMASWAMY; TRIPATHI, 2015).

Tabla 2: Tecnologías y estándares de comunicación IoT

Comunicación	Estandar
Wifi	IEEE 802.11a/c/b/d/g/n
WiMAX	IEEE 802.16
LR-WPAN	IEEE 802.15.4 (ZigBee)
Onda Z	Alianza Z-Wave ZAD12837 / ITU-T G.9959
Celular	2G-GSM, CDMA 3G-UMTS, CDMA2000
Bluetooth	4G-LTE
lora	IEEE 802.15.1
NFC	LoRaWAN R1.0
sigfox	ISO/CEI 18092:2004, ISO/CEI 18000-3
Neul	sigfox Neul RFC6282
6BajoPAN	Subproceso, basado en IEEE802.15.4 y
Hilo	6BajoPAN
LAN	Red de área local (LAN)

Fuente: MADAKAM, RAMASWAMY, TRIPATHI, 2015.

La expansión de los dispositivos *plug-and-play* que le facilita la vida al usuario final trae consigo un crecimiento difícil de predecir. La cantidad de dispositivos IoT disponibles en Internet es aproximadamente el 10% de la cantidad total de dispositivos IoT, según consultas del motor de búsqueda de Internet de las cosas *Shodan* (Sentient Hyper-Optimized Data Access Networkshodan). En consecuencia, se prevé que la cantidad de dispositivos IoT, que es de 6 000 millones en 2016, supere los 20 000 millones en 2025 (BARNAGHI; SHETH, 2016). El mayor problema que trae este crecimiento es que el espacio creado por las cosas no está asegurado (PANCAROGLU, 2018). Estos dispositivos se enfrentan a una grave amenaza de seguridad cuando no se cambian las contraseñas predeterminadas.

Los dispositivos o elementos dentro del ecosistema y que están conectadas a Internet deben tener estrategias de seguridad predeterminadas. La rápida inclusión de dispositivos en el ecosistema de Internet de las cosas está provocando una reducción de la prevención de la seguridad. Los temas a considerar para determinar las estrategias de seguridad de las cosas utilizadas en el espacio de la Industria 4.0 se resumen a continuación (PANCAROGLU, 2018):

- Intimidad: Los datos generados por los objetos deben ser accesibles solo por la autoridad (usuario u otros dispositivos). La comunicación de cosas interconectadas debe hacerse sobre una topología específica.
- Integridad: Garantizar que los datos provengan del lugar correcto y de un extremo a otro de manera segura y sin cambios.
- Usabilidad: Para asegurar la disponibilidad de los datos que necesitan los dispositivos o servicios en la red dentro del sistema.
- Autorización: Es la identificación de cosas dentro de la red y la edición del mecanismo de verificación.
- Soluciones de iluminación: Es la determinación de la compatibilidad de las funciones de IoT, como la cantidad de dispositivos en la red y la capacidad de energía para determinar las soluciones de seguridad.
- Heterogeneidad: Representa que las cosas con diferentes fabricantes tienen arquitecturas de trabajo colaborativo.
- Política: Establecer estándares de IoT para la gestión, protección y comunicación de datos dentro de IoT.
- Sistema de cifrado: La identificación de algoritmos de cifrado para la protección de datos durante los datos de los dispositivos.

REFERENCIAS

ALMADA-LOBO, F. The Industry 4.0 revolution and the future of Manufacturing Execution Systems (MES). Santiago, *Journal of Innovation Management,* v.3, p.16-21, 2016.

BAHRIN, M. A. K.; OTHMAN, M. F., AZLI, N. N.; TALIB, M. F. Industry 4.0: a review on industrial automation and robotic. Malaysia, *Jurnal Teknologi*, v.78, p.137-143, 2016.

ÉL, K.; JIN, M. *Cyber-Physical systems for maintenance in Industry 4.0*, Jönköping, School of Engineering, Jönköping University, 2016.

GUBBI, J.; BUYYA, R.; MARUSIC, S.; PALANISWAMI, M.; Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Amsterdam, Elsevier, *Future Generation Computer Systems*, v.29, p.1645-1660, 2013.

GORECKY, D., SCHMITT, M., LOSKYLL, M.; ZÜHLKE, D. *Interacción hombre-máquina en la era de la Industria 4.0*. In: International Conference on Industrial Informatics (INDIN), nº12, 2014, Porto Alegre, Institute of Electrical and Electronics Engineers, p.289-294, 2014.

GUPTA, G. P.; KULARIYA, M. A framework for fast and efficient cyber security network intrusion detection using apache spark. *Procedia Computer Science*, Amsterdam, Elsevier, v.93, p.824-831, 2016.

JAZDI, N. Cyber Physical Systems in the Context of. Industry 4.0. Cluj-Napoca, *Institute of Electrical and Electronics Engineers*, 2014.

HSU, MARINUCCI, VOAS. Ciberseguridad: Hacia un ecosistema cibernético seguro y sostenible. *Informática*, v.4, p.12-14, 2015.

KOGISO, K. Y FUJITA, T. Cyber-security enhancement of networked control systems using homomorphic encryption. In: 2015 54th IEEE Conference on Decision and Control (CDC). Osaka, p. 6836-6843, 2015.

LASI, H.; FETTKE, P.; KEMPER, H. G.; FELD, T. Y.; HOFFMANN, M. Industria 4.0. Marburg, *Business & Information Systems Engineering*, v.6, p. 239-242, 2014.

LEE, J; BAGHERI, B; JIN, C. Introduction to cyber manufacturing. United States of America, *Manufacturing Letters*, v.8, p.11-15, 2016.

LEE, J.; BAGHERI, B.; KAO, H. A. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. United States of America, *Manufacturing Letters*, v.3, p.18-23, 2015.

LEE, I.; LEE, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, Indiana University, v.58(4), p.431-440, 2015.

LEZZI, M.; LAZOI, M.; CORALLO, A. Cybersecurity for Industry 4.0: in the current literature: a reference framework. *Computers in Industry*, Amsterdam, Elsevier, v.103, p.97-110, 2018.

LU, Y. Industry 4.0: a survey on technologies, applications and open research issues. Amsterdam, *Journal of Industrial Information Integration*, Elsevier, v.6, p.1-10, 2017.

LU, Y.; DA XU. Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. Dartmouth, *IEEE Internet of Things Journal*, v.6, p. 2103-2115, 2018.

LIU, J.; XIAO, Y. ; LI, S. ; LIANG, W.; CHEN, CP (2012). *Cyber Security and Privacy Issues in Smart Grids*, IEEE Communications Surveys & Tutorials, v.14(4), p. 981-997, 2012.

MADAKAM, S.; RAMASWAMY, R.; TRIPATHI, S. Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, Obour, Misr International University, v.3(05), p.164-173, 2015.

PANCAROGLU, D. *An Analysis on the Current State of Security in the Internet of Things*. In: International Conference on Cyber Security and Computer Science (ICONCS 2018), Safranbolu, Turquía, 2018.

PETRASCH, R.; HENTSCHKE, R. Process modeling for Industry 4.0 applications: Towards an Industry 4.0 process modeling language and method. In: *Computer Science and Software Engineering (JCSSE)*, Thailand. 2016, 13th International Joint Conference, p. 1–5.

SEMERCI, M.; CEMGIL, AT; SANKUR, B. An intelligent cyber security system against DDoS attacks in SIP networks. *Computer Networks*, v.136, p.137-154. 2018. Disponible en:https://academics.boun.edu.tr/bulent.sankur/sites/bulent.sankur/files/inline-files/Jour_Semerci_SIP-DDOS_Compute%20Netw.pdf.

WANG, E. K.; YE, Y.; XU, X.; YIU, S. M.; HUI, L. C. K.; CHOW, K. P. *Security issues and challenges for cyber physical system*. In: Conference on Green Computing and Communications & International Conference on Cyber, Physical and Social Computing, Baltimore, p.733-738, 2010.

WELLS, L. J.; CAMELIO, J. A.; WILLIAMS, C. B.; WHITE, J. Desafíos de seguridad cibernética en los sistemas de fabricación. United States of America, *Cartas de fabricación*, v.2, p.74-77, 2014.

ZHENG, P.; SANG, Z.; ZHONG, R. Y.; LIU, Y.; LIU, C.; MUBAROK, K.; XU, X.. Smart manufacturing systems for Industry 4.0: Conceptual framework, scenarios, and future perspectives. Lausanne, *Frontiers of Mechanical Engineering*, v.13, p.137-150, 2018.

ZHONG, R. Y.; XU, X.; KLOTZ, E.; NEWMAN, S. T. Intelligent Manufacturing in the Context of Industry 4.0: A Review. *Engineering*, v.3 (5), p.616-630, 2017. Disponible en: https://doi.org/10.1016/J.ENG.2017.05.015.

ZHOU, K.; LIU, T; ZHOU, L. Industria 4.0: Hacia futuras oportunidades y desafíos industrials. In: International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), n. 13, Xi'an, p. 2147-2152, 2015.

PROCESO DE GESTIÓN DE RIESGO CIBERNÉTICO

Manuel Humberto Santander*

RESUMEN
Frente a la era del progresivo avance tecnológico y los ciberataques, este artículo pretende informar sobre los procesos de gestión de riesgos, desde su relevancia a nivel personal e institucional hasta las técnicas de seguridad, la clarificación entre los conceptos de apetito y tolerancia al riesgo y virtual. y evaluaciones de defensa. Como estrategia de protección digital, se destacan consideraciones sobre el escenario actual de las ciberinvasiones, así como reseñas de actividades consideradas comunes en el campo de los ciberataques, mientras que con base en ellas se propagan a lo largo del texto probabilidades y sugerencias defensivas.
Palabras clave: Riesgo cibernético; ciberseguridad; Defensa; tecnología; apetito y tolerancia al riesgo

PROCESSO DE GESTÃO DE RISCO CIBERNÉTICO

RESUMO
Diante da era de progressivo avanço tecnológico e ataques cibernéticos, o presente artigo intenta informar sobre os processos de gestão de riscos, desde sua relevância a nível pessoal e institucional às técnicas de segurança, ao esclarecimento entre os conceitos de apetite ao risco e tolerância ao risco e avaliações de defesa virtual. Enquanto estratégia de resguardo digital, são sinalizadas considerações sobre o presente cenário de invasões cibernéticas, assim como expostas revisões de atividades consideradas comuns no campo de ciberataque, ao passo que embasadas por esses, probabilidades e sugestões defensivas se propagam ao longo do texto.
Palavras-chave: Risco cibernético; cibersegurança; Defesa; tecnologia; apetite e tolerância ao risco

1 INTRODUCCIÓN

La gestión de riesgos es tanto un proceso de apoyo a la toma de decisiones como una herramienta vital para la planificación militar y la toma de decisiones (NORTH ATLANTIC TREATY ORGANIZATION, 2013). Proporciona los fundamentos necesarios para la toma de decisiones estratégicas, tácticas y operativas en el ámbito militar, pues permite anticipar posibles escenarios adversos a los intereses de las entidades del sector defensa y cómo anticiparlas.

* Magister en Administración en la Universidad EAFIT, Magister en Ingeniería de Seguridad de la Información de SANS Technology Institute y Estudiante de Doctorado en Information Security Assurance de University of Fairfax

Los distintos pasos que componen la gestión de riesgos han sido utilizados en escenarios de múltiples industrias desde 1950 para anticipar situaciones que pudieran generar algún peligro y la implementación del correspondiente plan para la mitigación del escenario identificado y evaluado (ANDREWS; MOSS, 2002). La gestión de riesgos en las organizaciones pertenecientes al sector defensa se analiza bajo la categoría de la gestión de riesgos operativos (*Operational risk management, ORM) (*NAVAL POST GRADUATE SCHOOL, 2002) o la gestión de riesgos compuestos (COMPOSITE RISK MANAGEMENT, 2006). Sin embargo, no existe una diferencia sustancial entre estos métodos y la gestión de riesgos en general.

La gestión de riesgos puede definirse como la aplicación de políticas, procesos, procedimientos y prácticas de gestión para controlar posibles situaciones adversas que puedan afectar un sistema. Comprende tres aspectos principales: (a) un análisis de riesgos; (b) una evaluación de riesgos; y (C) reducción y control de riesgos. Consulte la Figura 3 para ver una ilustración de la gestión de riesgos militar típica y sus componentes y subcomponentes.

La estrategia de tratamiento para un análisis de riesgos debe siempre considerar el apetito y tolerancia al riesgo (AVEN, 2012; NUR AINI, LUTFI, 2019) expresado por la organización. Otros criterios que pueden ser considerados son: la confiabilidad del sistema, la situación financiera de la institución y las ganancias potenciales que puedan surgir de una situación particular. Es comín ver toma de decisiones aceptando riesgos importantes en caso de que el potencial de ganancia sea considerable (COMPOSITE RISK MANAGEMENT, 2006).

En general, las evaluaciones de riesgo que involucran la revisión de probabilidades de ocurrencia en la situación correspondiente proporcionan una base estructurada que permite evaluar actividades que involucran algún tipo de peligro para uno o varios procesos de una institución. Sin embargo, la práctica involucra métodos especializados con algún grado de complejidad. Esto implica que su adopción no es rápida y requiere formar la capacidad de auditoría al interior de la organización para garantizar que se haya adoptado un enfoque lógico y coherente en la estrategia y transversalidad del proceso de gestión de riesgo (ANDREWS; MOSS, 2002).

En el sector defensa, la evaluación de riesgos se ejecuta de igual manera frente a un conjunto de criterios de evaluación y aceptación de riesgos (INTERNATIONAL MARITIME ORGANIZATION, 2018), los cuales son definidos directamente por la fuerza correspondiente en virtud de las circunstancias que rodean el escenario evaluado. Si bien es normal ver que existen criterios implícitos de alto nivel objeto de evaluación, claramente estos implican subjetividades que pueden distorsionar el producto del mismo. Es por esto que existe una tendencia actual para el desarrollo de criterios de evaluación explícitos, como la cuantificación del riesgo máximo tolerable para las tropas que se encuentran en combate, en las bases y el personal civil potencialmente involucrado en las operaciones (SKJONG, 2002).

El ciberespacio es el nuevo teatro de operaciones donde el sector defensa desarrolla sus actividades. En virtud de los aspectos discutidos en los párrafos

anteriores, es importante anotar que los mismos principios se cumplen aquí y que en múltiples ocasiones la materialización del riesgo cibernético trae consigo la materialización de hechos físicos que pueden tener impacto en la población civil, en la sociedad y en las mismas tropas.

El país se comporta como una gran organización donde pueden presentarse dos hechos que son comunes en cualquier otra institución: (a) Posee información sensible, la cual si llega a caer en las manos equivocadas puede traer impactos relevantes al funcionamiento de la infraestructura crítica y, por tanto, desestabilizar el funcionamiento del país y (b) Un ataque cibernético sofisticado dirigido a comprometer estos activos de información tiene altas probabilidades de ser exitoso, pues el riesgo cibernético nunca será cero y siempre existirá la manera de lograrlo. Considerando que no existe un método único para gestionar de forma óptima el riesgo cibernético, la mejor opción de una organización para detectar y disuadir estas amenazas es una estrategia integral de defensa estructurada a partir de una evaluación exhaustiva del riesgo cibernético. Esto implica la necesidad de identificación de: (a) los activos de información, (b) las distintas vulnerabilidades que pudieran tener inmersas, (c) probabilidad de ocurrencia y el impacto de estas. Esto permitirá establecer los controles óptimos que permitan definir si el riesgo cibernético se acepta, disminuye, transfiere o se evita.

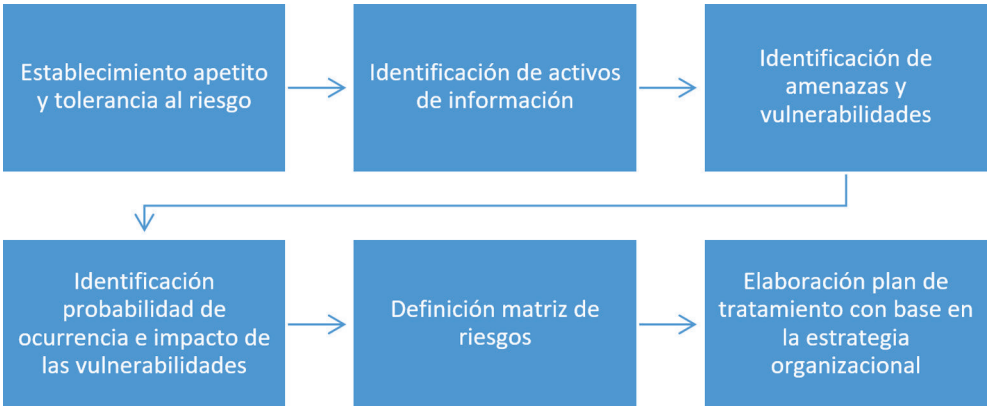
Resumiendo los conceptos definidos, el proceso de gestión de riesgo cibernético define las siguientes etapas, las cuales pueden evidenciarse en la figura 1:

- Establecimiento del apetito y tolerancia al riesgo cibernético: Define cuánto está dispuesta la organización a perder por impactos sufridos a raíz de la materialización de amenazas cibernéticas y cuál es el máximo impacto que puede sufrir antes de llegar a consecuencias irreversibles.
- Identificación de activos de información: Determina la lista de activos de información susceptible al riesgo cibernético en el desempeño de las funciones de la organización.
- Identificación de amenazas y vulnerabilidades: De acuerdo con las características de los activos de información y la implementación de los correspondientes servicios asociados, se determina las posibles formas en que pudieran sufrir un ciberataque, siendo la más recomendada las tácticas, técnicas y procedimientos establecidos en MITRE ATTACK (MITRE, 2021)
- Identificación de probabilidad de ocurrencia e impacto de las vulnerabilidades: Con base en las circunstancias particulares de la organización tales como los controles instalados, la forma de despliegue de las soluciones y los procesos organizacionales, se establece la probabilidad de materialización del riesgo y el impacto en las distintas áreas de la organización.
- Definición matriz de riesgo: Se plasma la información obtenida de activos de información, vulnerabilidades, probabilidad e impacto en caso de la materialización de alguna amenaza cibernética.

- Elaboración plan de tratamiento: Con base en el apetito y tolerancia al riesgo definido por la organización más la consideración de factores adicionales como el impacto a la sociedad y a las tropas, se establecen los criterios para aceptar, disminuir, transferir o evitar el riesgo y se procede a definir el detalle de la correspondiente acción.

El establecimiento del inventario de los activos de información es una tarea retadora que posee dificultades en su obtención por las circunstancias de operación de la compañía, lo cual lleva a que la perspectiva que se obtenga de los mismos sea limitada y, por tanto, conduzca a evaluaciones de riesgos de seguridad inexactas. Al revisar en detalle las deficiencias, es posible identificar tres puntos relevantes (SHEDDEN *et al*., 2016): (a) Los inventarios de activos de información suelen adoptar una visión tradicional basada en las responsabilidades organizaciones, la cual considera categorías de información discretas y estáticas que se pueden enumerar con fines de auditoría, lo cual deja por fuera nuevas funciones dinámicas que van surgiendo en la organización que no se encuentran formalmente documentadas y oficializadas ante todos los grupos de interés: (b) Los inventarios de activos de información tienden a estar restringidos a aquellos activos que son visibles a una parte de los procesos críticos de negocio, descuidando aquellos que pudieran tener impacto social y organizacional en otros escenarios; y (c) El enfoque estructural y metodológico que trabajan los analistas de seguridad puede llevarlos a descuidar el conocimiento organizacional menos visible pero esencial que crea procesos críticos de negocio y respalda la operación de los mismos.

Figura 1: Proceso de Gestión de Riesgo Cibernético



Fuente: EL AUTOR, 2022.

Por último y en especial en el sector defensa, se hace indispensable identificar el conocimiento de los distintos miembros de las fuerzas como un activo relevante para proteger, a pesar de su existencia menos tangible en la organización.

La gestión del riesgo cibernético continúa siendo una preocupación clave y un aspecto fundamental de los sistemas tecnológicos y ciberfísicos de las organizaciones. Algunos ejemplos relevantes de ataques cibernéticos recientes han sido T-Mobile (CLARK, 2021), Ucrania (ABIBOK, 2022), Facebook (HOLMES, 2021) y el Gobierno federal de Canadá (COBLE, 2022). Estos hechos afectaron a millones de consumidores y miles de empresas.

Considerando el paradigma de la computación en la nube, el cual fue masificado en esta cuarta revolución industrial y se ha convertido en una importante tendencia para acortar los tiempos de mercado de las nuevas iniciativas, ha aumentado de forma considerable la superficie de ataque sobre los distintos activos de información, pues estos ya se encuentran publicados en Internet. Algunos ejemplos de esto son las API (Application Programming Interface), las cuales son objeto de ataques como la fuga de información debido a problemas en su construcción. Si la correspondiente fuga de información involucra credenciales, permite el escalamiento de la acción criminal al poder involucrar en cadena múltiples sistemas de otras entidades para comprometer de forma integral una persona u organización. Al ser de conocimiento público la información publicada, es posible observar sitios como Hunt (2022), el cual permite determinar si la información de credenciales personal u organizacional ha sido objeto de compromiso, con el fin que los potenciales afectados puedan efectuar las acciones correspondientes de remediación.

Para efectos del tratamiento proactivo de los problemas organizacionales de seguridad y con el fin de ver las amenazas y vulnerabilidades de forma integral, se sugiere trabajarlo bajo la metodología de enfoque de amenazas. Esta define un proceso que establece las amenazas que pueden llegar a afectar los principales activos dentro de un sistema. Permite obtener la evaluación del estado actual de un sistema y el diseño de los requisitos de seguridad para nuevos proyectos en la organización. Esta metodología puede ser combinada con simulaciones de ataques para proporcionar evaluaciones probabilísticas de seguridad en donde se ilustre las circunstancias claras por las cuales puede llegar a ser comprometido un activo, lo cual brinda un valor concreto de la probabilidad de ocurrencia basado en la forma como fue desplegado en la infraestructura tecnológica de la compañía. Sobre la base de dichas evaluaciones objetivas, se pueden elegir controles de seguridad para contrarrestar las amenazas anticipadas.

Los métodos de modelado de amenazas se pueden clasificar en: (a) manual: Ejecutados sin automatización, (b) automático: Ejecutado desde herramientas que realizan el inventario y comprobación de las amenazas y vulnerabilidades, (c) formal: basado en métodos matemáticos y (d) gráfico: Basado en técnicas como árboles de ataque, gráficos de ataque y defensa. Desde la perspectiva de la evaluación de sistemas, a través del modelado de amenazas se representa y analiza la arquitectura, se identifican las posibles amenazas a la seguridad y se seleccionan las técnicas de mitigación apropiadas con base en el estado del arte de las distintas soluciones tecnológicas disponibles en el mercado.

Desde la perspectiva del desarrollo de aplicaciones, el modelado de amenazas se utiliza para ayudarle a los desarrolladores a efectuar la identificación y documentación de las posibles amenazas de seguridad asociadas con un producto de *software*, proporcionando a los equipos una forma de desarrollo una forma estructurada de descubrir fortalezas y debilidades en sus aplicaciones de *software*.

¿Cómo se pueden determinar las amenazas y vulnerabilidades? Para efectos del riesgo cibernético, se hace necesario considerar aquellas acciones que sean posibles materializar de forma ilícita en los activos de información, las cuales causan impactos a nivel organizacional. El estado del arte actual define la matriz MITRE ATT&CK, el cual corresponde a una base de conocimiento de tácticas y técnicas del adversario basadas en observaciones del mundo real y a un insumo fundamental para el desarrollo de modelos de amenazas específicos.

MITRE ATT&CK Enterprise Matrix contiene 12 tácticas que representan el objetivo táctico de un adversario para actuar (MITRE, 2021):

- Acceso Inicial: Su objetivo es el establecimiento de un punto de compromiso inicial para el ciberataque. Algunos ejemplos de técnicas a utilizar en esta táctica son *phishing*, compromiso por *malware* en medios extraíbles, entre otros.
- Ejecución: Luego del acceso al punto de compromiso inicial, los adversarios buscan ejecutar código malicioso utilizando técnicas como la ejecución a través de una interfaz gráfica o de línea de comandos.
- Persistencia: Los puntos de apoyo ganados por los adversarios a través del acceso inicial pueden ser fácilmente eliminados por acciones como el cambio de contraseña de los usuarios comprometidos. Con el fin de poder conservar el acceso, los adversarios pueden implementar mecanismos de acceso irregular a través de código malicioso en el dispositivo objetivo para permanecer y profundizar en el ciberataque correspondiente.
- Escalamiento de privilegios: Los adversarios suelen entrar a un sistema objetivo sin accesos privilegiados. Considerando que su objetivo es tener dominio total sobre el correspondiente activo de información, se busca explotar alguna vulnerabilidad del activo que no se encuentre parchada.
- Evasión de Defensa: Esta táctica busca evitar la detección del adversario y eludir cualquier tipo de control de seguridad. Es normal que borren las pistas de ejecución para continuar con sus actividades maliciosas.
- Credencial de acceso: Esta táctica busca habilitar la capacidad de capturar más nombres de usuario y contraseñas con el fin de mantener el acceso al dispositivo objetivo. Algunos ejemplos donde se puede encontrar esta información es el historial de Bash o el llavero de una computadora comprometida.
- Descubrimiento: Una vez fue posible efectuar el compromiso inicial de un dispositivo, los adversarios intentarán efectuar exploraciones y recop-

ilar más información sobre el entorno de la infraestructura tecnológica para encontrar un camino que les permita lograr sus objetivos.

- Estos intentos incluyen descubrir vulnerabilidades potenciales para explotar datos almacenados en el sistema y recursos de red a través de *Network Service Scanning*.
- Movimiento lateral: Después del compromiso inicial de un activo, los adversarios intentaran comprometer otros activos dentro de la misma infraestructura tecnológica a través de técnicas como *Internal Spearphishing*, buscando con esto lograr obtener cuentas internas que sean confiables para aumentar la probabilidad de engañar a otros usuarios.
- Colección: Esta técnica busca habilitar en adversarios la capacidad de recopilar datos de su interés para los objetivos con los que planearon el ciberataque. La información puede ser recopilada desde un equipo previamente comprometido que permita movimientos laterales o incluso desde los mismos dispositivos periféricos para ya continuar con la exfiltración de datos.
- Comando y control: Esta táctica permite a los adversarios monitorear la operación de los dispositivos objetivo de forma remota. En caso de contar con el control de múltiples equipos, es posible establecer ejércitos automatizados como lo pueden ser las *botnets*, lo cual les permitirá ejercer acciones hostiles contra otros objetivos.
- Exfiltración: Una vez que se recopilan los datos de interés para los adversarios, se procede a empaquetarlos utilizando técnicas como la compresión de datos y esteganografía para minimizar el tamaño de estos y la posibilidad de detección de transferencias hacia el exterior de la red, logrando grandes probabilidades de éxito al ser menos visible para evadir la detección.

Continuando con la revisión de las actividades en la gestión de riesgo cibernético, estimar la probabilidad es difícil. Las evaluaciones que involucran incertidumbre están sujetas a una amplia gama de fuentes de sesgo. Considerando lo anterior, se hace importante ilustrar cómo abordar la evaluación de la probabilidad. Ninguna técnica es infalible o aplicable a cada situación y, por tanto, cada una de ellas tiene sus propias fortalezas y debilidades. Sin embargo, es recomendado que los analistas de seguridad que evalúen la probabilidad del riesgo tengan conocimiento de la variedad de técnicas disponibles y consideren el uso de una variedad de enfoques diferentes de acuerdo con el caso a evaluar.

La selección de una técnica en particular está influenciada por el nivel de detalle con el que se desarrolle el proceso de gestión de riesgos o el tamaño y la importancia estratégica del activo de información correspondiente.

Se procederá a describir dos enfoques para evaluar la probabilidad de riesgo: (a) Técnicas de definición: Este enfoque incluye técnicas que intentan definir la probabilidad de varias maneras, con el fin de proporcionar un lenguaje inequívoco

para describir la probabilidad y (b) Este enfoque utiliza varios comparadores contra los cuales se puede comparar la probabilidad de un riesgo dado.

Respecto a las técnicas de definición, es necesario mencionar que el rango bajo el cual se define la probabilidad va desde la imposibilidad (0%) hasta la certeza (100%). Existen múltiples formas para describir este espectro. Las técnicas de definición para la evaluación de la probabilidad de riesgo ofrecen diferentes formas de describir la escala para dar a los evaluadores marcos de referencia significativos contra los cuales pueden estimar la probabilidad de un riesgo dado (HILLSON, 2003). También se usan las etiquetas para nombrar los rangos. Algunos ejemplos de escalas mediante el uso de etiquetas son alto, medio o bajo, probable, posible e improbable. Para cada etiqueta se define un rango de probabilidad que le será asignada mediante números, siendo usualmente utilizada la notación de porcentaje.

Existen un problema fundamental bajo este enfoque y corresponde a que tanto las etiquetas como las frases son ambiguas y pueden interpretarse subjetivamente.

Otros enfoques de definición también tienen problemas, ya que las cuotas no son familiares para muchos: la persona promedio tiene algunas dificultades para ordenar una serie de cuotas como 1:2 en contra, 4:3 a favor, 9:13, 15:1, entre otros. Los valores porcentuales o decimales introducen una precisión aparente espuria cuando la realidad es menos cierta, y los rangos fijos son artificiales y no suelen reflejar el rango real de probabilidad para un riesgo dado. Para todos los enfoques de definición, los evaluadores se enfrentan al desafío de justificar qué punto de la escala definida seleccionan, ya que la evaluación de la probabilidad de riesgo sigue siendo subjetiva.

Respecto a las técnicas comparativas, se han desarrollado varias técnicas para ayudar en la evaluación de la probabilidad del riesgo al proporcionar valores contra los cuales se puede comparar la probabilidad de que ocurra el riesgo, preguntando si la probabilidad de que ocurra el riesgo es mayor, menor o igual que el valor que se está considerando, presentado. El objetivo de todas estas técnicas es ajustar el comparador hasta que el evaluador no pueda distinguir entre la probabilidad de riesgo y el valor que se presenta.

Este valor se toma entonces como la mejor estimación de la probabilidad de riesgo. Hay diferentes formas de presentar las probabilidades contra las cuales se puede comparar la probabilidad de riesgo. Éstas incluyen:

- Apuestas: se le pregunta al evaluador qué probabilidades daría si se produjera el riesgo (aunque la respuesta se ve afectada por la curva de utilidad del individuo, que debe conocerse para que la apuesta se interprete correctamente).
- Orientado al valor: la probabilidad de riesgo se compara con un evento cuya probabilidad se conoce, por ejemplo, si es mayor o menor que la posibilidad de obtener 10 caras en un experimento de lanzamiento de una moneda. Se presentan diferentes eventos hasta que el evaluador no ve ninguna diferencia.

- Probabilidad relativa: similar al enfoque orientado al valor, se le pregunta al evaluador qué tan probable es que ocurra el riesgo que algún otro evento cuya probabilidad se conoce. El proceso puede continuar usando un enfoque basado en valores hasta que se alcance la igualdad, o se puede agregar la probabilidad diferencial al comparador para dar la probabilidad estimada de que ocurra el riesgo.

Si bien los enfoques comparativos parecen ser fáciles de usar, existen varias dificultades, incluidos problemas para comprender los comparadores. Además, las evaluaciones que utilizan técnicas comparativas están particularmente sujetas a sesgos de percepción y heurísticas, como se mencionó anteriormente.

Respecto a la estimación del impacto, es requerido la existencia en la organización de documentación y conocimiento detallado sobre cada uno de los procesos existentes. A través de estos elementos, será posible efectuar un análisis que permita estimar en detalle el impacto en el que incurre la empresa, independiente del objeto de impacto. Estos pueden ser reputacional, operacional, financiero, cibernético, entre otros.

Por último, la definición de la estrategia de gestión del riesgo va a estar influenciada por al menos los siguientes criterios: (a) apetito al riesgo; (b) Tolerancia al riesgo; (c) Beneficio por permitir la situación de riesgo; y (d) Costeo del impacto del riesgo. A partir de las distintas combinaciones que puedan presentarse, la organización toma la decisión de gestión que mejor se ajuste a su perfil de riesgo.

2 CONCLUSIÓN

El proceso de gestión de riesgo cibernético es demandante y consume una cantidad importante de recursos para las siguientes tareas: (a) Identificación de activos de información: La organización tiene conciencia de un número limitado de activos de información. Sin embargo, hechos como la masificación del *shadow IT* (SILIC; BACK, 2014) y la responsabilidad de los activos de información (EACHEMPATI, 2017) hacen que en la mayoría de las ocasiones no haya claridad del número de activos disponibles y por tanto se garantiza que el riesgo cibernético permanezca oculto a los ojos del proceso; y (b) Identificación de amenazas y vulnerabilidades presentes en los distintos activos de información: Al igual que con el inventario de activos de información, es indispensable contar con un inventario detallado y pormenorizado de la configuración de cada uno de los activos de la infraestructura tecnológica, tales como sistema operativo, el *software* allí instalado y la configuración de *software* de base como lo son las bases de datos y los API GW (Application Programming Interface Gateway). Las vulnerabilidades pueden ser creadas fácilmente mediante la instalación de un software con vulnerabilidades documentadas en alguno de los nodos o la configuración de parámetros inseguros como contraseñas por defecto o triviales, lo cual permitiría fácilmente la acción

de cualquier adversario. Esto implica la necesidad de explorar nuevas tecnologías que permitan automatizar estos elementos para poder establecer controles que gestionen de forma adecuada el riesgo encontrado.

¿Qué tecnologías podrían ser pertinentes implementar para apoyar el proceso de gestión de riesgo cibernético?

REFERENCIAS

ABIBOK, Y. *Cyberattacks Undermine Ukraine's Security*. United Kingdom/ Washington, DC: Institute for War and Peace Reporting, 27 ene 2022. Disponible en: https://iwpr.net/global-voices/cyberattacks-undermine-ukraines-security Accedido en: 27 feb. 2022.

ANDREWS, J. D.; MOSS, T. R. *Reliability and risk assessment*. London: Professional Engineering, 2ed. 2002

AVEN, Terje. On the meaning and use of the Risk Appetite Concept. *Risk Analysis*, v. 33, ed. 3, p. 462-468. 2012. https://doi.org/10.1111/j.1539-6924.2012.01887.x

CLARK, M. *Another T-Mobile cyberattack reportedly exposed customer info and SIMs*. New York: The Verge, 28 dec 2021. Disponible en: https://www.theverge.com/2021/12/28/22857619/t-mobile-cyberattack-data-breach-december-2021-cpni-sim-swap Accedido en: 28 feb 2022.

COBLE, S. Cyber-Attack on Global Affairs. Canada. *Infosecurity Magazine,* 2022. Disponible en: https://www.infosecurity-magazine.com/news/cyberattack-on-global-affairs/ Accedido en: 3 feb. 2022.

COMPOSITE RISK MANAGEMENT. *FM 5-19*. [S. l]: Headquarters Department of the Army, 2006. Disponible en: https://www.globalsecurity.org/military/library/policy/army/fm/5-19/fm5-19.pdf Accedido en: 22 sep. 2021.

EACHEMPATI, P. Change Management in Information Asset. *Journal of Global Information Management*, v.*25*(2), p. 68-87, 2017. https://doi.org/10.4018/jgim.2017040105.

INTERNATIONAL MARITIME ORGANIZATION. *Revised Guidelines for Formal Safety Assessment (Fsa) For Use in The Imo Rule-Making Process*. London: United Nations, 2018. Disponible en: https://wwwcdn.imo.org/localresources/en/OurWork/HumanElement/Documents/MSC-MEPC.2-Circ.12-Rev.2%20-%20Revised%20Guidelines%20For%20Formal%20Safety%20Assessment%20(Fsa)For%20Use%20In%20The%20Imo%20Rule-Making%20Proces...%20(Secretariat).pdf Accedido en: 28 dec.2021.

HOLMES, A. 533 million Facebook users' phone numbers and personal data have been leaked online. New York*: Business Insider*. 2021. Disponible en: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 Accedido en: 19 jul. 2021.

HUNT, T. *Have i been pwned?* Disponible en: https://haveibeenpwned.com/ Accedido en: 23 feb 2022

MITRE ATT&CK. *ICS tactics*, 2021. Disponible en: https://attack.mitre.org/. Accedido en: 11 dec. 2021.

NORTH ATLANTIC TREATY ORGANIZATION. *Comprehensive Operations Planning Directive V2.0*. Nato Supreme Headquarters Allied Powers Europe, Belgium, 2013. Disponible en: https://www.cmdrcoe.org/download.cgf.php?id=9 Accedido en: 12 ago. 2021.

NAVAL POSTGRADUATE SCHOOL. *Operational risk management.* California: University Circle, Safety, 2002. Disponible en: https://nps.edu/web/safety/orm Accedido: 15 ene. 2021.

NUR AINI, N. S. ; LUTFI, L. The influence of risk perception, risk tolerance, overconfidence, and loss aversion towards investment decision making. *Journal of Economics, Business & Accountancy Ventura*, v. *2,* n.3, 401- 413, p. 401 – 413, 2019. Disponible en: https://pdfs.semanticscholar.org/5890/4ca9ea7f5f8f4d0258c770b92d1769130193.pdf?_ga=2.203943058.320665634.1655738543-740256354.1653320705 Accedido en: 23 mayo 2021.

SHEDDEN, P.; AHMAD, A.; SMITH, W., TSCHERNING, H.; SCHEEPERS, R. Asset Identification in Information Security Risk Assessment: A Business Practice Approach. *Communications of the Association for Information Systems*, v.*39*, p.297–320, 2016. https://doi.org/10.17705/1cais.03915

SILIC, M.; BACK, A. Shadow IT – A view from behind the curtain. *Computers & Security*, v.45, p.274-283, 2014. https://doi.org/10.1016/j.cose.2014.06.007

SKJONG, R. *Risk Acceptance Criteria: current proposals and IMO position*. Surface transport technologies for sustainable development. Valencia, Economics, 4-6 june, 2002. Disponible en: http://research.dnv.com/skj/Papers/SkjValencia.pdf Accedido en: 20 nov. 2021.

EL IMPACTO DE LA CIBERSEGURIDAD EN LA SEGURIDAD Y DESARROLLO NACIONAL DE EL SALVADOR

Eva María Peña Daura*

RESUMEN

El auge de las nuevas tecnologías de la información y comunicación ha supuesto un cambio en las relaciones e interacciones de la sociedad actual, la popularidad del internet y de sus servicios van en rápido aumento, como demuestra la existencia de usuarios globales de Internet - son 4.66 mil millones en todo el mundo. El continuo incremento de la población conectada a internet hace que aumente también el número de víctimas en potencia y de delincuentes. Es difícil calcular cuántas personas emplean internet para efectuar actividades ilegales. En los últimos años, se ha podido observar el aumento del riesgo de ataques cibernéticos por diferentes actores; con las más diversas motivaciones. Los países tienen que estar preparados para enfrentar esta nueva amenaza, puesto que el uso indebido del conocimiento de la seguridad de la información muestra un escenario en donde tal vez una persona puede acceder oculta e ilegalmente a una computadora generando daños incalculables. La posibilidad que en el ciberespacio ocurran ataques está siempre presente dada la facilidad con que algunas personas han podido manipular computadoras con impunidad, convirtiéndose las *ciberamenazas* en uno de los principales riesgos para la seguridad de los países, como se ha podido apreciar de forma permanente en los últimos tiempos. La ciberseguridad es un reto a la Seguridad y Desarrollo Nacional, que exige la adopción de un enfoque integral en su análisis, que contemple los aspectos que han transformado el ciberespacio en un campo de sofisticación delictual, en uno de los principales desafíos a la estrategia nacional de ciberseguridad que deben de adoptar los países.

Palabras Clave: Ciberseguridad; Ciberamenazas; Seguridad Nacional; Desarrollo Nacional; Estrategia Nacional de Ciberseguridad.

O IMPACTO DA CIBERSEGURANÇA NA SEGURANÇA E DESENVOLVIMENTO NACIONAL DE EL SALVADOR

RESUMO

O surgimento de novas tecnologias de informação e comunicação significou uma mudança nas relações e interações da sociedade atual, a popularidade da Internet

* Licenciada en Ciencias Jurídicas, Máster en Derecho Penal Económico Internacional, Egresada de Máster en Derecho Penal Constitucional, Graduada del Postgrado en Seguridad y Desarrollo Nacional. Actualmente es Procuradora Adjunta de Defensa Pública Penal de la Procuraduría General de la Republica de El Salvador. Contacto: eva.pena@pgres.gob.sv

e seus serviços estão aumentando rapidamente, como evidenciado pela existência de usuários globais da Internet - são 4,66 milhões em todo o mundo. O aumento contínuo da população conectada à internet também aumenta o número de potenciais vítimas e criminosos. É difícil estimar quantas pessoas usam a internet para realizar atividades ilegais. Nos últimos anos, foi possível observar o aumento do risco de ataques cibernéticos por diferentes atores; com as mais diversas motivações. Os países precisam estar preparados para enfrentar essa nova ameaça, pois o uso indevido do conhecimento em segurança da informação mostra um cenário em que talvez uma pessoa possa acessar um computador de forma secreta e ilegal, causando danos incalculáveis. A possibilidade de ocorrência de ataques no ciberespaço está sempre presente dada a facilidade com que algumas pessoas conseguiram manipular computadores impunemente, tornando as ameaças cibernéticas um dos principais riscos para a segurança dos países, como se tem visto permanentemente nos últimos tempos. A cibersegurança é um desafio para a Segurança e Desenvolvimento Nacional, o que exige a adoção de uma abordagem abrangente em sua análise, que contemple os aspectos que transformaram o ciberespaço em um campo de sofisticação criminal e um dos principais desafios à estratégia nacional de cibersegurança que países devem adotar.
Palavras-chave: Cibersegurança; Ameaças cibernéticas; Segurança Nacional; Desenvolvimento Nacional; Estratégia Nacional de Cibersegurança.

1 INTRODUCCIÓN

Analizar el impacto de la ciberseguridad como componente estratégico para contrarrestar las ciberamenazas a la Seguridad y Desarrollo Nacional, debe pasar por establecer los elementos que componen el concepto de ciberseguridad, así como la definición de otros componentes claves que rodean el concepto de ciberseguridad y la determinación de las principales ciberamenazas (LAIÑO, 1991).

El estudio de investigación es de tipo Básico-Descriptiva, debido a que permitirá realizar un breve análisis del contexto actual del impacto de la ciberseguridad en la Seguridad y Desarrollo Nacional de El Salvador, con algunas incidencias que pueden vincularse con otros países, asimismo tomando en consideración la pandemia por Covid-19 que ha puesto de manifiesto una nueva realidad a nivel mundial.

De ahí la importancia de categorizar a la Seguridad Nacional como clave para la protección del ciberespacio de las ciberamenazas que ponen en peligro las infraestructuras críticas en un país (COLEGIO DE ALTOS ESTUDIOS ESTRATEGICOS, 2018).

Se analiza el contenido sobre la ciberamenazas en las Estrategias de Seguridad Nacional, de forma específica si existen líneas de acción y estrategias que ha adoptado el gobierno de El Salvador para permear el impacto de la ciberdelincuencia que ponen en peligro la seguridad del Estado y si en El Salvador, se han desarrollo

de Políticas o Estrategias de Ciberseguridad que coadyuven el esfuerzo de prevenir y reprimir los ciberataques o ciberamenazas que atentan a la Seguridad y Desarrollo Nacional.

El enfoque está orientado a la exposición de datos e información por medio de búsqueda bibliográfica referida a información doctrinaria, legislación, revistas, informes, notas periodísticas, casos, entre otros registros obtenidos, con el fin de establecer las conclusiones sobre el tema de investigación.

2 MARCO TEÓRICO

El fenómeno de la globalización y las transformaciones económicas, han hecho posible la aparición, desarrollo y masificación de las nuevas tecnologías de la información y la comunicación (Tics) y las redes de conexión a la red mundial. Este avance tecnológico se representa como una herramienta de desarrollo para los países, vitales hoy en día en el campo del sector privado y público.

La incidencia de las tecnologías de la información y la comunicación en los procesos de globalización trae consigo enormes implicaciones sociales, económicas, culturales que se ven reflejadas en escenarios cada vez más complejos y abiertos. Implica que los procesos económicos y la integración de mercados, junto con los procesos locales, tienen un impacto sin precedentes en cualquier interacción humana. La identidad misma se ve mediatizada por las relaciones de comunicación e información, sobre todo, virtuales y a distancia (CONTRERAS, 2017).

Es importante determinar que:

> Las tecnologías de la información y de la comunicación, es un término que contempla toda forma de tecnología usada para crear, almacenar, intercambiar y procesar información en sus varias formas, tales como datos, conversaciones de voz, imágenes fijas o en movimiento, presentaciones multimedia y otras formas, incluyendo aquéllas aún no concebidas. En particular, las Tics están íntimamente relacionadas con computadoras, software y telecomunicaciones. (TELLO, 2008).

La Tecnología de la información y la comunicación (TIC) más difundida y de mayor alcance es el internet, siendo un sistema de intercambio de información a nivel global, al que se puede tener acceso desde cualquier parte del mundo, y que es utilizada para desarrollar distintos programas que permiten el intercambio de mensajes, de información de audios, imágenes y videos, como las hoy conocidas por redes sociales (de las más difundidas Facebook, Instagram, Twitter y otras), pero también correos electrónicos (siendo las más difundidas Gmail, Hotmail y Yahoo!), y el uso de esta Tics en dispositivos móviles también ha permitido el desarrollo de aplicaciones con la misma finalidad (como WhatsApp y otras).

La masificación del uso de las nuevas tecnologías de la información y la comunicación, la interconectividad requerida por la globalización, el crecimiento del internet y de los servicios telemáticos, genera vulnerabilidades que se traducen en amenazas producidas en el ciberespacio, que pueden atentar contra la confidencialidad, integridad y disponibilidad de la información (COLEGIO DE ALTOS ESTUDIOS ESTRATEGICOS, 2017).

Anteriormente:

> La ciberseguridad obedecía a un enfoque de protección de la información (Information Security) donde solamente se trataba de proteger la información a accesos, usos, revelaciones, interrupciones, modificaciones o destrucciones no permitidas. En la actualidad, este enfoque está evolucionando hacia la gestión de riesgos del ciberespacio (Information Assurance) donde la ciberseguridad consiste en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados (CHAMORRO, 2015).

En tal sentido, el ciberespacio, tiene características particulares que facilitan la realización de un ataque, no es necesario desplazarse, moverse o tener que pasar una frontera. Es un entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física; constituye un elemento fundamental del ámbito personal, empresarial y administrativo (COLEGIO DE ALTOS ESTUDIOS ESTRATEGICOS, 2017).

En el mundo actual ha surgido una nueva dimensión donde pueden materializarse las ciberamenazas: “el ciberespacio”. Anteriormente, en el ámbito de la defensa estaba claro que nos movíamos en las tres dimensiones de tierra, mar y aire, e incluso el espacio, actualmente se cuenta con una dimensión adicional y más intangible que las anteriores (EL SALVADOR, 2002).

El ciberespacio fue declarado por *The Economist*, como el quinto dominio después de la tierra, el mar, el aire y el espacio (AGUILAR, 2010).El ámbito donde se desarrollan y actúan las ciberamenazas es el ciberespacio. Entendiendo la ciberamenaza como la potencial ocurrencia de una situación que pudiera convertirse en un ciberataque, es decir, una acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de la materialización de un crimen y mediante la cual, dichos agentes comprometen la seguridad de la información de la entidad.

> Los ciberataques normalmente comparten las siguientes características comunes: Bajo coste, muchas herramientas de ataque se pueden descargar de forma gratuita o con un coste muy bajo para el daño que pueden causar, fácil empleo. Para muchos ataques no son necesarios grandes conocimientos técnicos, existen herramientas con unos interfaces de usuario muy amigables y sencillas de usar. Existe una probabilidad muy alta de alcanzar los objetivos buscados con estos ataques por la ausencia de políticas de empleo o la limitación de recursos existentes en la parte defensiva debido a la falta de concienciación de las organizaciones gubernamentales, empresas y ciudadanos, bajo riesgo para el atacante. Es muy difícil atribuir un ataque con las herramientas de ocultación del origen existentes actualmente en internet y por la diferencia de legislaciones de los diferentes países. (ROMERO, 2010).

Las principales amenazas relacionadas con el ciberespacio se pueden clasificar en dos grandes grupos: las amenazas contra la información y las amenazas contra la infraestructura TIC's (CHAMORRO, 2015). Las amenazas contra la información son aquellas cuya materialización provocan una pérdida, manipulación, publicación o uso inadecuado de información. Entre estas amenazas se encuentran:

> Espionaje dentro de esta categoría se incluyen toda la variedad de espionaje, desde el espionaje de Estado al espionaje industrial; Robo y publicación de información clasificada o sensible; Robo y publicación de datos personales; Robo de identidad digital; Fraude; Amenazas persistentes avanzadas y las amenazas contra la infraestructura TIC's, son aquellas cuya materialización pueden provocar la interrupción temporal, parcial o total de determinados servicios o sistemas. (CHAMORRO, 2015).
>
> Entre estas amenazas se encuentran: los ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, ataques contra sistemas de control y redes industriales, infección con programa maligno y ataques contra redes, sistemas o servicios a través de terceros. (CHAMORRO, 2015).

Ningún sistema de información está libre del riesgo de sufrir un ciberataque, hoy en día la seguridad interna de un país se enfrenta a amenazas delictivas relacionadas con las tecnologías de la información. Las tecnologías de Internet se encuentran en la guerra de la información, cuyos objetivos son principalmente de índole económica y cuya repercusión es importante para el buen desarrollo de las

actividades, por otro lado, favorece las actividades de espionaje y de inteligencia, debido a la facilidad actual de interceptación de la información que se transmite por Internet (UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, 2009).

> Los ataques cibernéticos ya no solamente tienen motivación intelectual o económica, sino también política, por lo que las consecuencias ya no sólo se centran en una pérdida económica, sino en los conflictos entre países que demuestran y miden sus fuerzas, además de las dimensiones de tierra, mar y aire, a través del ciberespacio. En el ámbito de las operaciones militares, los ciberataques también tienen que ser considerados como una amenaza, ya que cada vez resulta más probable que éstas se combinen con ataques informáticos con el objeto de dejar fuera de servicio las redes y sistemas del adversario. (INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS, INSTITUTO UNIVERSITARIO GENERAL GUTIÉRREZ MELLADO, 2010).

La ciberdelincuencia puede tener una dimensión terrorista en la medida 0 en que los sistemas atacados estén implicados en infraestructuras críticas. Efectivamente, las infraestructuras esenciales para el buen funcionamiento de las actividades de un país, (energía, agua, transportes, logística alimentaria, telecomunicaciones, bancos y entidades financieras, servicios médicos, funciones gubernamentales, etc.) ven aumentada su vulnerabilidad por depender cada vez más de las tecnologías de Internet. Es necesario hacer énfasis en la importancia de los sistemas de producción y distribución de electricidad, ya que condicionan el funcionamiento de la mayor parte de las infraestructuras.

El ciberterrorismo como cualquier acto realizado a través de tecnologías de información puede tener como resultado lograr directa o indirectamente causar terror o generar daños significativos a un grupo social o político a través de la destrucción del soporte tecnológico de cualquiera de sus infraestructuras fundamentales. El ciberterrorismo, por lo tanto, se estructura en torno a dos elementos: la presencia de un grupo terrorista y el empleo de medios provenientes de una infraestructura tecnológica para lograr la ampliación de su capacidad operativa (BEJARANO, 2011).

Cabe mencionar que, en nuestro país, por vía jurisprudencial, la Sala de lo Constitucional, ha determinado que:

> [...] son grupos terroristas las pandillas denominadas Mara Salvatrucha o MS-13 y la Pandilla 18 o Mara 18, y cualquier otra pandilla u organización criminal que busque arrogarse el ejercicio de las potestades pertenecientes al ámbito de la soberanía del Estado -v. gr., control territorial, así como el

> monopolio del ejercicio legítimo de la fuerza por parte de las diferentes instituciones que componen la justicia penal -, atemorizando, poniendo en grave riesgo o afectando sistemática e indiscriminadamente los derechos fundamentales de la población o de parte de ella; en consecuencia, sus jefes, miembros, colaboradores, apologistas y financistas, quedan comprendidos dentro del concepto de 'terroristas', en sus diferentes grados y formas de participación, e independientemente de que tales grupos armados u organizaciones delictivas tengan fines políticos, criminales, económicos (extorsiones, lavado de dinero, narcotráfico, etc.), o de otra índole. (SENTENCIA DE INCONSTITUCIONALIDAD, 2015).

Asimismo, es oportuno señalar que, de acuerdo con el tema que nos ocupa, la ley especial contraactos de terrorismo, tipifica las conductas consideradas actos de terrorismo, regulando específicamente el delito informático, que de acuerdo al art. 12 de la referida ley:

> Será sancionado con pena de prisión de diez a quince años, el que para facilitar la comisión de cualquiera de los delitos previstos en esta Ley:a) Utilizare equipos, medios, programas, redes informáticas o cualquier otra aplicación informática para interceptar, interferir, desviar, alterar, dañar, inutilizar o destruir datos, información, documentos electrónicos, soportes informáticos, programas o sistemas de información y de comunicaciones o telemáticos, de servicios públicos, sociales, administrativos, de emergencia de seguridad nacional, de entidades nacionales, internacionales o de otro país; b) Creare, distribuyere, comerciare o tuviere en su poder programas capaces de producir los efectos a que se refiere el literal a), de este artículo. (EL SALVADOR, 2006).

Dicho lo anterior, se prevé en nuestra legislación los diferentes la dimensión terrorista que puede tener la ciberdelincuencia, sobre todo en la medida en que los sistemas atacados estén implicados en infraestructuras críticas de nuestro país o de otro, puesto que actualmente el terrorismo, tal como se menciona en considerando IV de la referida ley, constituye una grave amenaza para la seguridad del país, la paz pública y la armonía de los Estados, afectando directa e indirectamente a sus nacionales en su integridad física y moral, así como en la propiedad, posesión y conservación de sus derechos (EL SALVADOR, 2006).

El control de infraestructuras críticas parece ser uno de los objetivos del ciberterrorismo, prueba de ello es el recrudecimiento de los *scans* (pruebas

de sistemas informáticos para descubrir sus vulnerabilidades a fin de poder penetrar en ellos con posterioridad) dirigidos contra los ordenadores de las organizaciones que gestionan estas infraestructuras (UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, 2009).

> Las Infraestructuras críticas, y compartiendo la definición, puede entenderse como el conjunto de recursos, servicios, tecnologías de la información y redes, que, en el caso de sufrir un ataque, causarían gran impacto en la seguridad, tanto física como económica, de los ciudadanos o en el buen funcionamiento del Gobierno de la Nación. Este impacto se mide según unos criterios horizontales que determinan la criticidad de una infraestructura. Se han establecido: el número potencial de víctimas mortales o de lesiones graves que pueda producir; el impacto económico en función de la magnitud de las pérdidas económicas y/o el deterioro de productos o servicios, incluido el posible impacto medioambiental; y el impacto público, por la incidencia en la confianza de la población, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales. (ROMERO, 2010).

Las infraestructuras críticas se agrupan en sectores entre los que se incluyen la Administración, sector aeroespacial, sector energético, de la industria, nuclear, de la industria química, las instalaciones de investigación, de agua, de la salud, de transporte, de alimentación, financiero y tributario y de las tecnologías de la información y comunicaciones (ROMERO, 2010).

3 IMPACTO DE LAS AMENAZAS

A nivel mundial se hace referencia al ciberataque masivo realizado en 2020 a los Estados Unidos, el hackeo pudo haber afectado al recuento de los votos en las elecciones del Expresidente Donald Trump, los oficiales de ciberseguridad del Departamento de Seguridad Nacional calificaron en un comunicado de “un grave riesgo para el Gobierno federal” (GIMÓN, 2020).

En el campo de la salud, tanto la Interpol como el CNI han alertado del “incremento” de ataques a instituciones médicas a cambio de rescates económicos y ‘aprovechando’ la especial sensibilidad de los datos clínicos, un hospital puede ser ‘bloqueado’ actuando contra una simple máquina de rayos X o fotocopiadora del centro. Las implicaciones no sólo son de índole económica, en Alemania, el hospital universitario *Uniklink* (Dusseldorf) sufrió un ciberataque que paralizó el servicio de Urgencias durante 13 días y provocó la muerte (indirecta) de una paciente (CORNEJO, 2021).

Recientemente, aprovechando la situación de caos generada por la COVID-19, se han producido multitud de ciberataques de todo tipo a hospitales como los siguientes (GARCIA-CORDOBA, J., 2020).

En España se produjo un ataque tipo *ransomware*, llamado Netwalker, que consistía en un correo electrónico que contenía información sobre el virus como señuelo, enviado a personal sanitario, que intentaba acceder a los sistemas de los hospitales para inutilizarlos y posteriormente pedir una recompensa.

En Brno (República Checa) al inicio de la pandemia se produjo otro ataque de tipo *ransomware* que secuestró los dispositivos electrónicos del Hospital Universitario, obligando a posponer intervenciones quirúrgicas de urgencia, así como al traslado de pacientes en situación delicada a otros centros sanitarios próximos. En Estados Unidos, se produjo un ciberataque al sistema informático del Departamento de Salud y Servicios Humanos buscando la ralentización de los sistemas, objetivo que no alcanzaron.

Entre otros hechos recientes se menciona el jaqueo de la plataforma de videoconferencias Zoom, que en el marco de la pandemia por el COVID-19 tomó gran relevancia y tuvo un crecimiento sin precedentes por el amplio uso que le ha dado en empresas, colegios, universidades y otras organizaciones para reuniones remotas, que fue vulnerada mediante *Zoom bombing*. Estos actos comprometieron y expusieron gran cantidad de cuentas, usuarios y claves (alrededor de 500.000) y afectaron las actividades personales, académicas y laborales de muchas personas y organizaciones, al permitir el acceso no autorizado a reuniones privadas para extraer datos, infiltrar información para divulgar información falsa, grosera, discriminatoria o pornográfica para sabotear. Todo ello derivado, aparentemente, de la venta de cuentas, usuarios y contraseñas de la plataforma en la red oscura (CRUZ, 2020).

No se puede obviar, que en el contexto de la pandemia por COVID-19, trajo consigo nuevas formas de realizar actividades laborales en diferentes ámbitos, públicos y privados a nivel mundial, y con ello, el teletrabajo representó en gran medida, el mecanismo por el que se continuarían las labores diarias, lo que implicó usos de aparatos electrónicos, internet, aplicaciones, etc.

Según el Reporte de Seguridad de *Enjoy Safer Technology* (ESET) para Latinoamérica 2020, indica que el 60% de las empresas sufrió al menos un incidente de seguridad en 2019. En el caso de El Salvador sufrió un 58% de ciberataques a empresas. El informe reveló que más del 50% de los usuarios encuestados en la región latinoamericana aseguró que la organización para la que trabajan no brindó las herramientas de seguridad necesarias para migrar hacia el teletrabajo en estas condiciones y casi el 45% recibió intentos de "*phishing*", conjunto de técnicas que persiguen el engaño, relacionados con la pandemia (ALFARO, 2021).

Recientemente en nuestro país, el día 19 de octubre de 2020, se reportó un supuesto ataque informático que provocó inconvenientes en los servicios clínicos y administrativos. El Instituto Salvadoreño del Seguro Social (ISSS) informó sobre

afectaciones en su sistema de programación de citas médicas, así como para la entrega de medicamentos y otros trámites administrativos, luego de registrarse un presunto ataque informático contra los sistemas de la institución. En la misma nota periodística se hace referencia que hace unas semanas, también se reportó que la Policía Nacional Civil (PNC) fue blanco de un ataque informático que vulneró el sistema de la institución y filtró información personal de más de 30 mil agentes policiales, entre ellos sus nombres, números de identificación, lugar donde estaba destacado y números de teléfono (ALVARADO, 2021).

La Superintendencia del Sistema Financiero, en este año 2021 reporta un incremento en fraudes bancarios digitales a los usuarios, debido al crecimiento de la bancarización y los servicios financieros en El Salvador se ha visto también, en los últimos meses se reportan un promedio de 20 casos de estafas (BERNAL, 2021).

Según datos brindados por la Fiscalía General de la República (FGR), las denuncias por delitos informáticos entre enero y septiembre del 2021, se contabilizaron 3,182 sin tener el dato exacto de los casos que se judicializaron. El incremento de denuncias fue a consecuencia de la evolución acelerada que tuvieron los cibercrímenes, actividades ilícitas relacionadas con el manejo de datos y dinero a través de la tecnología, como el hurto por medios informáticos, la estafa informática e incluso el espionaje. Los datos de la FGR afirman que, en el 2021, agosto fue el mes con más denuncias por hurto en cuentas bancarias, lo cual coincidió con una oleada de reclamos por fallas en cuentas bancarias electrónicas en el país. Estos datos no incluían, las denuncias por las operaciones en Chivo Wallet, a través de la cual el gobierno salvadoreño entregó $30.00 a los ciudadanos, eso haría que las cifras a finales del 2021 aumentaran considerablemente (INCREMENTO, 2021).

Los casos anteriormente expuestos, representan sólo una muestra del incremento de los ciberataques ocurridos recientemente en otros países y en El Salvador, sólo basta con ingresar al sitio web *Ciberamenazas Mapa en Tiempo Real* (MAPA EN TIEMPO REAL DE CIBERAMENAZA, 2020), para conocer los tipos de ciberataques que suceden a cada segundo a nivel mundial demostrando diferentes tipos de afectaciones, ubicando con el número 118 a El Salvador como el país más atacado.

4 ESFUERZOS DEL ESTADO SALVADOREÑO PARA CONTRARRESTAR LAS CIBERAMENAZAS

El riesgo a la Seguridad Nacional consecuentemente impacta al Desarrollo Nacional, afectando las mejoras de las condiciones socioeconómicas de la población, el alcance del bien común y la mejora de la calidad de vida de toda la población por los graves efectos de los ataques alas infraestructuras esenciales de un país.

Los incidentes que causan la interrupción de las infraestructuras críticas y de los servicios podrían causar importantes impactos negativos en la sociedad y

en la economía. Asegurar el ciberespacio se ha convertido en uno de los retos más importantes de la actualidad y es considerado como una cuestión nacional a nivel estratégico que afecta a todos los niveles de la sociedad (WITKER, 2002).

Desde el ámbito normativo, específicamente la normativa internacional, el Convenio sobre la Ciberdelincuencia o la Convención de Budapest de 2001, ha sido considerado el primer tratado internacional que busca la armonización normativa en materia de criminalidad informática, este convenio distingue cuatro categorías de infracciones relativas a la ciberdelincuencia: Delitos contra la confidencialidad, la integridad y disponibilidad de los datos y sistemas informáticos, Delitos informáticos, Delitos relacionados con el contenido y Delitos relacionados con infracciones de la propiedad intelectual y de derechos afines (COUNCIL DE EUROPA, 2001).

Este convenio trata en particular de las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de la red. Igualmente se ocupa de una serie de competencias y procedimientos, como la preservación de datos de tráfico y contenido, la búsqueda de las redes informáticas y la interceptación legal. Su principal objetivo, que figura en el preámbulo, es aplicar una política penal común encaminada a la protección de la sociedad contra el Cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional (CARDOSO, 2005).

El Salvador ha logrado un avance significativo en relación a la creación de una normativa referida al delito cibernético con la aprobación de la Ley Especial contra los Delitos Informáticos y Conexos con el objetivo de proteger los derechos legales de las conductas delictivas cometidas utilizando las tecnologías de la información y comunicación, así como de prevenir delitos cometidos contra datos almacenados, procesados y/o transferidos, los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías (EL SALVADOR, 2016).

De tal manera, el Estado ha buscado los mecanismos en el campo normativo, creando un marco jurídico desde diferentes aristas, que tienden a la protección relacionada con la ciberseguridad, así se pueden mencionar: la Ley de acceso a la Información Pública, Ley de la Firma Electrónica (EL SALVADOR, 2015), que determinan que las actividades reguladas en la ley, deberán regirse por principios generales, entre ellos se puede mencionar: autenticidad, con el cual se garantiza que la información contenida en el mensaje de datos o documento electrónico es confiable, si se encuentra suscrito con firma electrónica certificada, sello electrónico y sello de tiempo, y esta garantía perdura a través del tiempo; integridad, por el cual se otorga certeza de que la información contenida en medios electrónicos, no ha sido modificada desde el momento en que se coloca la firma electrónica certificada, sello electrónico o sello de tiempo, o desde el momento en que se desmaterializa un documento; confidencialidad, por medio del cual se garantiza a los usuarios, que

la información proporcionada a los proveedores de servicios no será conocida por terceras personas, sin su expresa autorización.

Con el fin de robustecer la capacidad de proteger, resguardar y regular los datos personales de los salvadoreños, el Pleno Legislativo aprob**ó** el 22 de abril del 2021, la Ley de Protección de Datos Personales y Hábeas Data, que se encuentren en posesión de personas naturales o jurídicas de carácter privado o público, con la finalidad de regular su tratamiento legítimo, esta normativa, estaba orientada a frenar el mal uso de la información como el cometimiento de prácticas abusivas que van más allá del normal uso de la información privada y pública que se ve expuesta a su uso indiscriminado y con fines ajenos a los intereses reales de la sociedad.

La referida Ley, que fue aprobada para entrar en vigencia ciento ochenta días después de su publicación, fue vetada por inconstitucional por el Presidente de la República de El Salvador, fundamentando las principales razones del veto, en una falta de armonía con el marco legal salvadoreño en el diseño de mecanismos jurisdiccionales y no jurisdiccionales para la protección de datos personales, no adecuándose las recomendaciones de organismos internacionales a las instituciones jurídicas del Derecho salvadoreño, particularmente, no han sido armonizadas con otras Leyes aplicables, tales como: la Ley de Firma Electrónica, Ley de Supervisión y Regulación del Sistema Financiero, Código de Trabajo, Ley de Bancos, Ley Orgánica del Registro Nacional de las Personas Naturales y las regulaciones relacionadas con la información de carácter tributario y aduanero. Agrega que tampoco han sido considerados aspectos señalados por la jurisprudencia constitucional relacionada, específicamente, la establecida en los Amparos 934-2007 y 142-2012, sobre el derecho constitucional a la autodeterminación informativa (MENJIVAR, 2021).

Dicho lo anterior, es de suma importancia la creación de un proyecto ley que regule el tratamiento de la protección de los datos personales y el habeas data, en armonía con la legislación secundaria vigente relacionada con el tema, el dato personal es potencialmente vulnerable al ser guardados en un sistema informático, siendo susceptible de pérdida, filtración, fuga o acceso no autorizado de la información, la cual puede ser personal confidencial o sensible, ya que hace posible identificar a su titular o que, crea el riesgo de ser utilizada para el cometimiento de delitos tradicionales como el robo de identidad, fraude u otros delitos y por otro lado, el tipo de accesos no autorizados o ataques cibernéticos, que pueden afectar en el peor de los casos la infraestructuras críticas (BRÚCULO, 2012).

Es de suma importancia mencionar las Normas Técnicas para la Gestión de la Seguridad de la Información, las cuales tienen por objeto, establecer los criterios mínimos para la adopción de políticas y procedimientos relacionados con el desarrollo de metodologías para la gestión de la seguridad de la información y la ciberseguridad de la misma, acordes a las mejores prácticas internacionales, naturaleza, tamaño, perfil de riesgo de las entidades y volumen de sus operaciones (BANCO CENTRAL DE RESERVA, 2019).

Asimismo, dado el contexto actual de la pandemia por Covid-19 el cual ha acelerado la transformación digital y ha masificado el uso de los canales digitales para el desarrollo de los servicios financieros, los sistemas informáticos de las entidades financieras han sido vulnerados tanto a nivel local como internacional, nuestro país con el fin de implementar medidas para prevenir la materialización de eventos de fraudes financieros, ha emitido las normas de carácter temporal para anticipar el cumplimiento de algunas medidas de ciberseguridad reguladas en las Normas Técnicas para la Gestión de la Seguridad de la Información (NRP-23) (BANCO CENTRAL DE RESERVA, 2020). El objetivo de estas normas es reforzar las medidas de ciberseguridad en los sistemas informáticos de las entidades financieras mediante los cuales se recopila, procesa, transmite y se almacena la información de los productos y servicios financieros que las entidades financieras ofrecen a sus clientes, así como también la implementación de medidas para la correcta identificación de los clientes.

De acuerdo al Reporte Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe, determina que El Salvador ha desarrollado la Estrategia de Gobierno Digital 2018-2022, y ha tomado algunas medidas concretas para establecer el gobierno electrónico, lo cual queda de manifiesto con el lanzamiento del proyecto para el Sistema Integrado de Gestión Administrativa y la Política Nacional de Datos Abiertos que se agregó al nuevo portal *Datos El Salvador*, un sitio que contiene más de 20 bases de datos de información pública. Asimismo, en 2016 se creó la Dirección de Gobierno Electrónico, que es la encargada de coordinar iniciativas con las instituciones públicas, y hay una plataforma que está en funcionamiento desde inicios del 2017 para facilitar el intercambio de información del gobierno aplicando los lineamientos de seguridad (INTER-AMERICAN DEVELOPMENT BANK, 2020).

Actualmente, en nuestro país, por medio de la Secretaría de Innovación de la Presidencia de la República, se ha diseñado la ejecución de la Agenda Digital de país 2020-2030, orientada a iniciar la transformación digital, entre los componentes se encuentran: Identidad Digital, Gobernanza Digital, Modernización del Estado, Innovación, Educación y Competitividad (EL SALVADOR, 2020).

Uno de los aspectos importantes relacionados en la referida Agenda es el impacto de esta transformación en el Desarrollo Nacional, específicamente en los aspectos de bienestar social, seguridad y desarrollo, mencionando en este último, la necesaria adecuación tecnológica de muchos procesos productivos y comerciales, considerando que la combinación de infraestructura física, software, sensores, nanotecnología y tecnología de comunicaciones, entre otros, ha generado nuevas configuraciones productivas y laborales, asegurando con ese fortalecimiento de las actividades económicas para asegurar la competitividad de nuestro país.

Esta agenda, además de contener actividades para propiciar un marco legal sobre el tema, también incluye un eje de Gobernanza Digital, que establece lineamientos para la prevención, detección y remediación de posibles

vulnerabilidades a las que se puedan exponer los diferentes recursos de información del país, y proteger la infraestructura crítica nacional (DEVOTO, 2001).

En cuanto a los compromisos y metas de la agenda, es necesario aclarar, que algunas son de cumplimiento a largo plazo. En el caso de la Ciberseguridad las metas son (EL SALVADOR, 2020):

> Elaborar e implementar una Estrategia Nacional de Ciberseguridad y política de seguridad digital del Estado, para proteger la información digital en poder del Estado a través de la adopción de estándares internacionales y el trabajo articulado de las instituciones públicas, Elaborar registro y plan de gestión de infraestructura crítica del Estado para identificar riesgos y mitigar amenazas a la infraestructura que soporta los servicios prioritarios nacionales, Fortalecer la gestión del dominio de nivel superior (TLD por sus siglas en inglés) asignado a El Salvador (.SV) para garantizar la seguridad de los portales e impulsar el uso de dominios nacionales en nuestro país, Implementar Centros de Operaciones de Seguridad (SOC) sectoriales para responder a las necesidades específicas de las diferentes áreas y servicios que administra el Estado, Implementar programas de capacitación en ciberseguridad para empleados públicos para garantizar las competencias mínimas y asegurar la información en poder del Estado, para prevenir y mitigar los riesgos derivados de los delitos informáticos y Fortalecer la gestión y los alcances de SalCERT de forma que el Estado pueda contar con una gobernanza claramente definida y con lineamientos actualizados de ciberseguridad. (EL SALVADOR, 2022).

De aquí la importancia de ejecutar una Estrategia Nacional de Ciberseguridad que deberá ejecutarse en coordinación con los sectores público y privado, ser compatible con los derechos y libertades individuales y ser coordinada con otras acciones para detectar las distintas amenazas, establecer sistemas de respuesta y recuperación ante eventualidades, así como fomentar la cooperación internacional como punto clave para lograr tratados internacionales.

La Estrategia Nacional de Ciberseguridad, se entenderá como: un plan de acción nacional sobre la base de una visión nacional para lograr un conjunto de objetivos que contribuyan a la seguridad del ciberespacio. La importancia de la Estrategia es que se encuentra a un alto nivel en la pirámide organizacional de una nación, y establece una serie de objetivos nacionales y prioridades que deben alcanzarse en un plazo determinado y es en tal sentido que proporciona un marco estratégico para la implementación de un Sistema de Ciberseguridad Nacional, que se entiende como un conjunto de órganos, organismos y procedimientos que permiten la dirección, control y gestión de la Ciberseguridad (LEIVA, 2015).

En este contexto, y dando cumplimiento a los compromisos y metas en el tema de ciberseguridad de la Agenda Digital está considerada elaborar e implementar una Estrategia Nacional de Ciberseguridad y política de seguridad digital del Estado, para proteger la información digital en poder del Estado a través de la adopción de estándares internacionales y el trabajo articulado de las instituciones públicas, El Salvador ha desarrollado una Política de Ciberseguridad (GOBIERNO DE EL SALVADOR, 2021), teniendo como objetivo el de establecer las líneas de acción y estratégicas que permitan al Gobierno de El Salvador definir los aspectos relevantes enfocados en la prevención de riesgos cibernéticos, así como su gobernanza, definición de los criterios de abordaje para el desarrollo de las capacidades de ciberseguridad enfocadas en el aseguramiento de las infraestructuras críticas, el fortalecimiento de los mecanismos de respuesta ante incidentes y el desarrollo de habilidades técnicas y de gestión, para que las instituciones públicas y privadas a nivel nacional y los ciudadanos mismos puedan tomar conciencia del tema de ciberseguridad y los riesgos del uso de las tecnologías de información, que les permitan adoptar medidas de protección ante las ciberamenazas.

Para la ejecución de la Política se han determinado las estrategias, que están orientadas a fortalecer la capacidad de ciberseguridad y proporciona una guía para que las entidades públicas y/o privadas, logren definir y establecer líneas de acción que apoyen el uso de las tecnologías digitales de una manera segura y confiable.

Las estrategias plasmadas en la Política están adecuadas para abordar los temas claves y considerar los aspectos necesarios para lograr cumplir con las metas propuestas por el Gobierno de El Salvador a través de la agenda digital 2030 y la base de un plan nacional de ciberseguridad, en estas se mencionan:

> Creación de la entidad coordinadora de ciberseguridad a nivel nacional, Concientización en materia de ciberseguridad, Reforzar las capacidades en ciberseguridad ante las amenazas, Reforzar el marco jurídico para la persecución del delito en el ciberespacio y la cibercriminalidad, Garantizar la seguridad y resiliencia de activos estratégicos, Identificación, análisis y gestión del riesgo, Contribuir a la ciberseguridad en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable en apoyo a los intereses nacionales y Fortalecimiento del equipo de respuesta ante incidentes. (EL SALVADOR, 2021).

En cuanto a la estrategia de reforzar el marco jurídico para la persecución del delito en el ciberespacio y la cibercriminalidad, partiendo por la revisión del marco jurídico existente, para proponer los ajustes necesarios que permitan responder ante el cometimiento de delitos en el ciberespacio y la ejecución de procedimientos legales que garanticen una adecuada investigación y la realización de juicios justos,

se ha empezado a tener avances en tema, actualmente la Asamblea Legislativa por medio de la Comisión de Seguridad Pública y Combate a la Narcoactividad, se encuentra estudiando una iniciativa de reforma a la Ley Especial Contra Delitos Informáticos y Conexos (EL SALVADOR, 2021) con la finalidad de actualizar el marco normativo, introduciendo modificaciones a algunos tipos penales existentes, incrementando la pena en unos de ellos en razón de la alta lesividad que representan y estableciendo nuevas formas de las conductas delictivas para facilitar su detección, investigación y sanción.

Por lo anterior, toda estrategia nacional de ciberseguridad debe orientarse no sólo a las administraciones es públicas –nacional y local– y a la Fuerza Armada, sino que, naturalmente, debe llegar a las infraestructuras críticas, organizaciones y empresas de todo tipo, la industria ya la sociedad. Es importante mencionar, que los documentos referidos tal como la Agenda Digital 2020-2030 y la Política de Ciberseguridad son de reciente data y constituyen un avance significativo en el tema y un esfuerzo coordinado del Estado, sector público y privado, así como de los ciudadanos (EL SALVADOR, 2021).

De acuerdo con la Política, en cada institución del Estado deberá asignarse el rol de coordinador institucional de implementación del plan de ciberseguridad, el cual deberá tener las siguientes funciones:

> Comprender plenamente las estrategias de ciberseguridad contempladas en la política de ciberseguridad, velar porque se elaboren los planes de acción para que las estrategias definidas en la política de ciberseguridad logren su cometido, coordinar con el responsable de seguridad de la información (RSI) la ejecución de análisis de riesgos y la definición de las líneas de acción a desarrollar para mitigar los riesgos identificados, informar al ente coordinador de la función de ciberseguridad en el país de los proyectos considerados en el plan de implementación de la política de ciberseguridad, en concordancia con los riesgos identificados y reportar al ente coordinador de la función de ciberseguridad en el país los avances del plan. Los titulares de cada institución del sector público deberán enviar al ente coordinador de ciberseguridad nacional, la documentación del nombramiento de la persona que ostentará el rol de coordinador institucional de implementación del plan de ciberseguridad (EL SALVADOR, 2021).

Las instituciones del sector privado podrán adaptar el modelo de estructura organizativa de acuerdo con el entorno propio y la dependencia del uso de las tecnologías de información para el desempeño de sus funciones. Aquellas instituciones del sector privado que administren infraestructuras críticas y que de

ser objeto de ciberataques pudiesen menoscabar el bienestar social y económico de la población en general, deberán implementar un programa de ciberseguridad (EL SALVADOR, 2021). Para el cumplimiento de la referida Política, será necesario la ejecución de las estrategias y sus líneas acción establecidas a corto, mediano y largo plazo, pudiendo determinar las instituciones sus responsabilidades en plazos razonables, pues esta responsabilidad implicaría, impulsar actuaciones conjuntas fortaleciendo las capacidades de respuesta ante incidentes y de inteligencia ante los diferentes tipos de ciberamenazas expuestas, así como también de la dotación o asignaciones presupuestarias para llevar a cabo las líneas de acción que se plantean como posibles soluciones para reducir la ciberamenazas y contar con un andamiaje de ciberseguridad - asimismo, el fortalecimiento de las capacidades técnicas o la cibereducación, en las instituciones públicas y privadas. Por tanto, se vuelve indispensable contar con personal que tenga las capacidades técnicas adecuadas en este campo, en consecuencia, los programas de formación deberían actualizarse constantemente, definiendo y desarrollando nuevos programas, estrategias y tecnologías que refuercen también la seguridad, para respuestas adecuadas ante amenazas estatales y no estatales.

El papel del gobierno, por medio de la Secretaria de Innovación, toma un rol preponderante y activo para el cumplimiento de la Agenda Digital y la Política de Ciberseguridad, para mejorar la ciberseguridad en los sectores que manejan infraestructuras críticas. En tal sentido, debe establecerse la revisión de la política para la verificación del cumplimiento de las estrategias.

En cuanto al registro y plan de gestión de infraestructura crítica del Estado para identificar riesgos y mitigar amenazas a la infraestructura que soporta los servicios prioritarios nacionales, es determinante establecer los planes de acción de los diferentes sectores, así como contar con los Centros de Operaciones de Seguridad (SOC) sectoriales para responder a las necesidades específicas de las diferentes áreas y servicios que administra el Estado.

De igual manera, la potenciación de los mecanismos de Cooperación internacional, estableciendo adecuados canales de comunicación y que se adapten en las legislaciones nacionales los acuerdos en materia de ciberdelito o cibercrimen, es decir su armonización en la normativa interna. Por la naturaleza transnacional que caracterizan a las ciberamenazas y el ciberespacio que facilite la persecución de los ataques, se hace necesario una cooperación internacional para el adecuado abordaje de la problemática.

La ciberseguridad debe plantearse no sólo desde el punto de vista de las amenazas sino también desde los retos que plantean. La implementación de políticas de ciberseguridad servirá no sólo para la Seguridad Nacional sino también para aumentar la eficiencia y rentabilidad de la industria y empresas del sector de la seguridad e incluso en una vertiente mucho más amplia de todos los sectores de la vida nacional que al tener asegurada su ciberdefensa podrán dedicarse, con

tranquilidad, a sus negocios fundamentales, lo que redundará en el aumento de su productividad y beneficiará a sus empleados, clientes, socios, y, en general, a los grupos de interés (AGUILAR, 2010).

5 REFLEXIONES FINALES

Se puede mencionar sin temor a equivocarnos que, en los conflictos tradicionales existen fronteras y límites, mientras que en el ciberespacio no - para realizar un ataque no es necesario desplazarse, moverse o tener que pasar una frontera, este es una de las principales características de este tipo de fenómeno. El ciberespacio es un ambiente único, sin fronteras geográficas, anónimo, asimétrico y puede ser considerado fácilmente clandestino (LEIVA, 2015).

Los ciberataques pueden impactar en los procesos de Seguridad y Desarrollo Nacional, cuando ponen en peligro a la soberanía nacional y la integridad del territorio, especialmente afectando el bien común de la población en ámbitos como económico, social, político y cultural.

El cibercrimen se valdrá de las vulnerabilidades o brechas de los sistemas informáticos para afectar a ciudadanos, empresas y gobierno sin distinción y en este último, constituyéndose perturbaciones que vendrían a limitar el Desarrollo Nacional y la puesta en peligro de los objetivos nacionales.

La ciberdelincuencia puede tener una dimensión terrorista, que puede causar un grave daño a las estructuras críticas de los Estados, en tiempos pasados los ataques eran la guerra en la tierra, en el mar, aire, ahora es una amenaza que también se puede plantear en el ciberespacio y es considerado como una cuestión nacional a nivel estratégico que afecta a todos los niveles de la sociedad.

La importancia de la Estrategia Nacional de Ciberseguridad, es que se encuentra a un alto nivel en la pirámide organizacional de una nación, y establece una serie de objetivos nacionales y prioridades que deben alcanzarse en un plazo determinado y es en tal sentido que proporciona un marco estratégico para la implementación de un Sistema de Ciberseguridad Nacional, que se entiende como un conjunto de órganos, organismos y procedimientos que permiten la dirección, control y gestión de la Ciberseguridad.

La Agenda Digital 2020-2030 y la Política de Ciberseguridad son de reciente creación, constituyen un avance significativo para El Salvador, el cual requerirá de un esfuerzo coordinado del Estado, sector público y privado, así como de los ciudadanos, y de la dotación o asignaciones presupuestarias para llevar a cabo las líneas de acción que se plantean como posibles soluciones para la creación de mecanismos de ciberseguridad.

La Política de Ciberseguridad de El Salvador, busca establecer las líneas de acción y estratégicas que permitan al gobierno salvadoreño definir los aspectos relevantes enfocados en la prevención de riesgos cibernéticos, teniendo como

primordial interés definir los criterios de abordaje para el desarrollo de las capacidades de ciberseguridad enfocadas en el aseguramiento de las infraestructuras críticas, el fortalecimiento de los mecanismos de respuesta ante incidentes y el desarrollo de habilidades técnicas y de gestión, para que las instituciones públicas y privadas a nivel nacional y los ciudadanos mismos puedan tomar conciencia del tema de ciberseguridad y los riesgos del uso de las tecnologías de información, que les permitan adoptar medidas de protección ante las ciberamenazas, lo que se ejecutará por medio de las estrategias.

BIBLIOGRAFÍA

AGUILAR, L, Estado del Arte de la Ciberseguridad, España, *Cuadernos de estrategia,* Ministerio de Defensa, 2011.

ALFARO, Karla. El Salvador con 58% de ciberataques a empresas. *El Economista*, 03 mayo 2021. Tendencias. Disponible en: https://www.eleconomista.net/tendencias/El-Salvador-con-58--de-ciberataques-a-empresas-20210503-0008.html. Accedido en: 23 mayo 2022.

ALVARADO, Irvin. ISS suspende programación de citas y sistema para entrega de medicamentos por ataque informático. *La Prensa Gráfica,* 19 oct. 2021. Disponible en: https://www.laprensagrafica.com/elsalvador/ISSS-suspende-programacion-de-citas-y-sistema-para-entrega-de-medicamentos-por-ataque-informatico-20211019-0069.html. Accedido en: 21 enero 2022.

BANCO CENTRAL DE RESERVA. *Normas Técnicas para la Gestión de la Seguridad De La Información.* San Salvador: BCR, 2019.

BANCO CENTRAL DE RESERVA. *Normas Técnicas para la Gestión de la Seguridad de la Información.* San Salvador: BCR, 2020.

BEJARANO, M. J. *Alcance y ámbitos de la Seguridad Nacional.* Madrid: Unirioja, 2011.

BERNAL, David. Fiscalía registra 3, 182 delitos informáticos en 2021. *La Prensa Gráfica,* 2 nov. 2021. Disponible en: https://www.laprensagrafica.com/elsalvador/Fiscalia-registra-3182-delitos-informaticos-en-2021-20211101-0086.html. Accedido en: 21 enero 2022.

BRÚCULO, C. R. Defensa cibernética en América del Sur. Estrategias en la UNASUR ante ciberguerra y ciberdelito. *In*: CONGRESO DE RALACIONES INTERNACIONALES, 6. 2012, La Plata. *Anales* [...]. La Plata: Instituto de Relaciones Internacionales, 2012. p. 1-14.

CARDOSO, N. El derecho penal del riesgo y la idea de seguridad. Una quiebra del sistema sancionador. *Pensamiento Penal y Criminológico.* Córdoba, v. 6, n. 10, 2005.

CHAMORRO, E. *La ciberseguridad nacional, un compromiso de todos.* [Madrid]: Spanish CiberSecurity Institute, 2015.

CLIMENT BARRERA, J. *Conferencia-La Justicia Penal en Internet:* territorialidad y Competencias Penales*.* San José: Biblioteca Judicial Fernando Coto Albán, 2001.

COLEGIO DE ALTOS ESTUDIOS ESTRATEGICOS. El Ciberespacio y la Seguridad Nacional en El Salvador*. In*: ARTIGA CHICAS, R. *Reflexiones sobre Seguridad y Defensa Nacional.* El Salvador: 1ª Edición, 2017. p. 85-116.

COLEGIO DE ALTOS ESTUDIOS ESTRATEGICOS. Reflexiones sobre Seguridad y Defensa Nacional. *In*: BARQUERO ELÍAS, M. *La ciberseguridad y su incidencia en la seguridad nacional.* El Salvador: 1ª Edición, 2017. p. 117-143. ISBN 978-99961-81-01-6.

COLEGIO DE ALTOS ESTUDIOS ESTRATEGICOS. Conceptualización de la Seguridad, Desarrollo y Defensa Nacional: una aproximación para la identificación de los riesgos y amenazas a la Seguridad Nacional en El Salvador*. In*: GUERRERO MULATO, J. *Desarrollo Nacional*. El Salvador: Primera edición, p. 22, 2018. ISBN 978-99961-81-08-5.

COUNCIL OF EUROPE. Convenio sobre Ciberdelincuencia*.* Budapest*: Serie de Tratados europeos* n. 185, 2001. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf. Accedido en: 23 mayo 2020.

CONTRERAS, R. *Globalización y Derecho Penal Económico.* México; [*S. n*.], 2017.

CORNEJO, A. La otra "ola" de 2020: los ciberataques a hospitales. *Gaceta Médica*, 14 enero 2021. Disponible en: https://gacetamedica.com/profesion/la-otra-ola-de-2020-los-ciberataques-a-hospitales/. Accedido en: 12 ene 2022.

CRUZ, Ariadna. Venden cuentas zoom en la dark web. *El Universal (blog)*, 15 abr. 2020. Disponible en: https://www.eluniversal.com.mx/techbit/millones-de-cuentas-de-zoom-se-venden-en-la-dark-web. Accedido en: 18 mar. 2021.

DEVOTO, M. *Comercio electrónico y firma digital: Las regulaciones del Ciberespacio y las estrategias globales.* Argentina: Editorial La Ley S.A. Primera edición, 2001.

EL SALVADOR. Asamblea Legislativa. Ley Especial Contra Actos de Terrorismo*.* Decreto n. 108. *Diario Oficial*, San Salvador, n. 193, tomo n. 373, 17 octubre 2006.

EL SALVADOR. Asamblea Legislativa. Ley de la Defensa Nacional*.* El Salvador: Decreto n. 948, *Diario Oficial*, San Salvador, n. 184, tomo 357, 2002.

EL SALVADOR. Assemblea Legislativa. Decreto nº 133. Ley de la Firma Electrónica*. Diario Oficial*, San Salvador, n. 196, tomo 409, 2015.

EL SALVADOR. Asamblea Legislativa. Decreto nº 260. Ley de Delitos Informáticos y Conexos*. Diario Oficial*, San Salvador, 26 feb. 2016.

EL SALVADOR. Asamblea Legislativa. *Expediente nº. 320-10-2021-1*. Reformas a la Ley Especial Contra Delitos Informáticos y Conexos. Diario Oficial, San Salvador, 26 oct. 2021.

EL SALVADOR. Gobierno. *Política de Ciberseguridad.* San Salvador: Diario Oficial, 2021.

EL SALVADOR. Gobierno. *Política Nacional de Ciberseguridad.* San Salvador: Diario Oficial, 2021.

EL SALVADOR. Gobierno. *Presidencia de El Salvador*. Disponible en: Ciberseguridad: https://www.presidencia.gob.sv/ciberseguridad/ Accedido en: 18 jun. 2021.

EL SALVADOR. Secretaría de Innovación de la Presidencia. [San Salvador]: Secretaría de innovación de la Presidencia, 2020. Disponible en: https:// innovacion.gob.sv/downloads/Agenda_Digital.pdf. Accedido en: 18 jun. 2021.

GIMÓN, Pablo. Trump resta gravedad al ciberataque masivo a EEUU y apunta a China después de que Pompeo acura a Rusia. *El País,* 2020. Disponible en: https:// elpais.com/internacional/elecciones-usa/2020-12-19/pompeo-acusa-a-rusia-del-ciberataque-masivo-en-estados-unidos.html. Accedido en: 18 jun. 2021.

GARCIA-CORDOBA, J., H.-P. L. La ciberdefensa en los sistemas de información sanitarios militares. San Salvador: El Salvador, 2020.

INCREMENTO en fraudes bancarios digitales. *La Prensa Gráfica,* 4 marzo 2021. Disponible en: https://www.laprensagrafica.com/economia/Incremento-en-fraudes-bancarios-digitales-20210303-0143.html. Accedido en: 17 mayo 2021.

INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS, INSTITUTO UNIVERSITARIO GENERAL GUTIÉRREZ MELLADO. Conclusiones. *In*: AGUILAR, L. *Ciberseguridad. Retos y Amenazas a La Seguridad Nacional en el Ciberespacio.* Madrid: Ministerio de Defensa Nacional, Dirección General de Relaciones Institucionales, 2010. p. 325-335.

INTER-AMERICAN DEVELOPMENT BANK. *Ciberseguridad*: riesgos, avances, y el camino a seguir en América Latina y el Caribe. [S.l.]: Banco interamericano de Desarrollo, 2020. Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf. Accedido en: 28 marzo 2021.

JIMENO MUÑOZ, J. *La responsabilidad civil en el ámbito de los ciberriesgos.* Madrid: Fundación MAPFRE, 2017.

LAIÑO, A. Una aproximación teórica al concepto de defensa. *Centro de Estudios Internacionale (BsAs)*, n. 35, 1991.

LEIVA, E. Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. *Revista Latinoamericana de Ingeniería de Software*, v. 3, n. 4, p. 161-176, 2015. ISSN 2314-2642.

LÓPEZ ORTEGA, J. Conferencia -Libertad de expresión y responsabilidad por contenidos en internet. Cd n.75, 2001.

LÓPEZ, S. *Las transformaciones del sistema jurídico y los significados sociales del derecho en México.* México: UNAM, 1997.

MAPA en tiempo real de ciberamenaza. *Cybermap,* 2 Dic. 2020. Disponible en: https://cybermap.kaspersky.com/es/stats#country=173&type=oas&period=w Accedido en: 28 enero 2021.

MENJIVAR, Juan Carlos. Presidencia veta Ley de Protección de Datos personales y hábeas data. *Derecho y Negocios,* 18 mayo 2021. Disponible en: https://derechoynegocios.net/presidencia-veta-ley-de-proteccion-de-datos-personales-y-habeas-data/. Accedido en: 12 enero 2022.

ROMERO, J. Estrategias nacionales de ciberseguridad. Ciberterrorismo. *In*: I. U. INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS. *Ciberseguridad. Retos y Amenazas a La Seguridad Nacional en el Ciberespacio.* Madrid: Ministerio de Defensa Nacional, Dirección de Relaciones Internacionales, 2010. p. 259-322.

SENTENCIA de inconstitucionalidad. San Salvador: Corte Suprema de Justicia, 2015. Referencia 22- 2007/42-2007/89-2007/96-2007.

TELLO, E. Las tecnologías de la información y comunicaciones y la brecha digital: su impacto en la sociedad de México. *Revista de Universidad y Sociedad del Conocimiento,* Barcelona, n. 3, 2008.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. *Guía de ciberseguridad para los países en desarrollo.* Genebra: UIT, 2009

WITKER, J. *Introducción al Derecho Económico.* México: Editorial Mc Graw Hill, 2002.

EVOLUCIÓN DEL CONCEPTO DE SEGURIDAD EN TORNO A LAS AMENAZAS DESDE LA VISIÓN GEOPOLÍTICA Y GEOESTRATÉGICA DE LOS ESTADOS: LA CIBERSEGURIDAD Y CIBERDEFENSA EN EL ECUADOR

Luis Lara Tapia*

RESUMEN

El objetivo de este trabajo es presentar la evolución del concepto de Seguridad en torno a la presencia de las amenazas y/o riesgos, desde la visión geopolítica y geoestratégica de los estados, a través del análisis en una línea de tiempo propuesta por Eric Hobsbawn, cuando se refiere al largo siglo XIX (1815-1914) y al corto siglo XX (1914-1991); y su vigencia en lo que va del Siglo XXI, de acuerdo al equilibrio de poder y orden mundial vigente en cada época; poniendo énfasis en la respuesta que los estados u organismos internacionales como la ONU, OEA, Unión Europea, OTAN han presentado ya sea como Estrategias de Seguridad Nacional o Estrategias Específicas para enfrentar dichas amenazas; además, se presenta los esfuerzos de Ecuador en el campo de la Ciberseguridad y la Ciberdefensa.

Palabras clave: Seguridad; Geopolítica; Geoestratégica; Ciberseguridad; Ciberdefensa.

A EVOLUÇÃO DO CONCEITO DE SEGURANÇA EM RELAÇÃO A AMEAÇAS A PARTIR DAS VISÕES GEOPOLÍTICAS E GEOESTRATÉGICAS DOS ESTADOS: A CIBERSEGURANÇA E CIBERDEFESA NO EQUADOR

RESUMO

O objetivo deste trabalho é apresentar a evolução do conceito de Segurança sobre a presença de ameaças e/ou riscos, desde a visão geopolítica e geoestratégica dos estados, através da análise em uma linha de tempo proposta por Eric Hobsbawn, quando se refere ao longo do século XIX (1815-1914) até meados do século XX (1914-1991), e sua validade até o século XXI, de acordo com o equilíbrio de poder e ordem mundial vigente em cada época; pondo ênfase na resposta que estados e órgãos internacionais como a ONU, OEA, União Europeia, e OTAN tem apresentado como Estratégias de Segurança Nacional ou Estratégias Específicas para enfrentar tais ameaças, além de apresentar os esforços do Equador no campo de cibersegurança e ciberdefesa.

Palavras-chave: Segurança; Geopolítica; Geoestratégia; Cibersegurança; Ciberdefesa.

* Coronel de Estado Mayor Conjunto, Magister en Seguridad y Defensa, Especialista en Estudios Estratégicos y de Defensa, Licenciado en Ciencias Militares, Licenciado en Comunicación Social; Actualmente Director de la Academia de Defensa Militar Conjunta de Ecuador. Contacto: luislaratapia@hotmail.com

1 INTRODUCCIÓN

Los intereses de los estados a lo largo del tiempo, han sido la base fundamental, en torno a los cuales han girado sus acciones, pues constituyen las aspiraciones de los mismos, que, sin lugar a dudas, estarán circunscritos a alcanzar el bienestar y desarrollo de su pueblo; por lo que, un aspecto fundamental a ser considerado es la Seguridad y Defensa de estos intereses, materializándose como objetivos nacionales, siendo responsabilidad de los gobernantes su vigencia.

En este sentido, un Estado desarrolla su propia identidad que le permitirá definir sus intereses como resultado de una construcción social dinámica y cambiante, los mismos que se reflejan en la normativa legal, planes, acuerdos, políticas y estrategias, así como en las instituciones creadas, es decir, su forma de comportamiento y posicionamiento en el contexto nacional como internacional. Este argumento se basa en la reflexión de Alexander Wendt:

> […] valorar la relación causal entre la práctica y la interacción (como una variable independiente) y las estructuras cognitivas en el nivel de estados individuales y de los sistemas de estados que constituyen identidades e intereses (como variable dependiente) − es decir, la relación entre lo que los estados hacen y lo que son. (WENDT, 2005, p. 33).

Es entonces que, la visión geopolítica y geoestratégica de los estados, marcará sus relaciones internacionales, siempre velando por precautelar sus intereses, por lo que, la Seguridad y Defensa, es un tema que no puede dejarse de estudiar y analizar, siendo necesario abordar temas como: el ámbito de estudio o dimensión de análisis, el papel del sistema internacional y el objeto referente de la seguridad (OROZCO, 2006).

De la misma manera, las amenazas y/o riesgos han ido surgiendo como respuesta a la actualización y modernización de la criminalidad sea esta nacional como internacional, cuyo accionar ha traspasado fronteras en los diferentes dominios: terrestre, naval, aéreo, ultraterrestre y ciberespacio; adaptándose a las acciones de los estados con estrategias que vulneran los sistemas de seguridad nacionales, regionales o globales.

En este contexto de la evolución del concepto de Seguridad y de las amenazas, se visualiza aquellas amenazas que se mantienen en los análisis en forma sostenida como el terrorismo, el crimen organizado transnacional y las armas de destrucción masiva; sin embargo, en la última década del presente siglo, han sido los ciberataques y los conflictos entre Estados los que se han manifestado con más frecuencia, sin perder de vista al cambio climático como una amenaza o riesgo según la concepción de los estados, que permanece como un punto de inflexión en los análisis, ya que sus efectos ha traído consecuencias irreparables en muchos países.

Un aspecto a poner especial atención es la respuesta de los estados a los ciberataques con la implementación de políticas y estrategias, ya que sus efectos

han sido tan letales en los diferentes sistemas políticos, económicos, salud, militar, entre otros, como si se empleara un ataque por una fuerza militar en el campo de batalla tradicional.

En este sentido, se presenta el esfuerzo que el Ecuador ha emprendido en pos de proteger y defender las infraestructuras críticas e información estratégica del Estado, a través de la implementación de la Política de Ciberdefensa en la que se establece su estructura en el sector defensa, el establecimiento de su estrategia y guía política, instrumentos normativos que apuntalan el desarrollo de capacidades en Fuerzas Armadas para combatir en el ciberespacio a las ciberamenazas y la articulación con las demás instituciones del Estado en el marco de la Política de ciberseguridad como el paraguas que la orienta.

2 EVOLUCIÓN DEL CONCEPTO DE SEGURIDAD

Es importante realizar un recuento de la evolución del concepto de seguridad de acuerdo al equilibrio de poder y orden mundial vigente en cada época, para lo cual, se ha considerado la propuesta de Eric Hobsbawn, cuando se refiere al largo siglo XIX (1815-1914) y al corto siglo XX (1914-1991), períodos que permiten identificar la evolución del concepto de seguridad y su relación con el objeto referente de estudio.

Así, partiremos desde 1815, cuando en Europa el concepto del Estado Westfaliano estaba vigente y la territorialidad, soberanía y población, orientaban la preocupación de los gobernantes, considerando, además, la influencia que la primera y segunda revolución industrial tuvieron en la connotación de los diferentes aspectos relacionados a la Seguridad y Defensa de los estados, así:

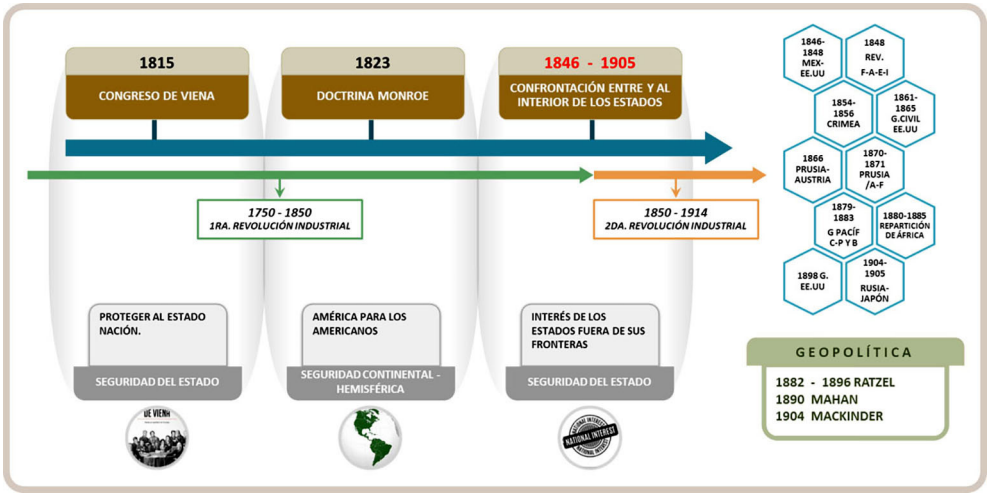
En 1815, la Seguridad estaba orientada bajo la concepción de proteger al Estado Nacional de amenazas externas, encargando esta tarea a la Fuerza Militar, por lo tanto, la *Seguridad Nacional* era la Seguridad del Estado. En el período 1740-1840, se produjo la primera revolución industrial, la misma que estaba en pleno auge y varios procesos históricos habían ocurrido, como la independencia de los EE.UU. (1776) y la revolución francesa (1789).

En 1823, el presidente de los Estados Unidos (EE.UU) James Monroe presentó su discurso al Congreso, cuya frase "América para los americanos" constituiría a la postre la Doctrina Monroe, con lo que se establecería los inicios de la *Seguridad Continental* y *Seguridad Hemisférica*, considerándose como objeto referente al Estado y su integridad territorial. Entre 1846 – 1905, se suscitaron confrontaciones entre Estados y al interior de los mimos, como las revoluciones en: Francia, Alemania, España, Italia (1848); guerra México-EE.UU (1846-1848); guerra de Crimea (1854-1856), que enfrentó a Rusia con Gran Bretaña y Francia; guerra civil de EE.UU (1861-1865); guerra entre Prusia y Austria (1866); guerra Prusia/Alemania con Francia (1870-1871); guerra del Pacífico entre Chile, Perú y Bolivia (1879-1883);

guerra Hispano-Estadounidense (1898); y, guerra ruso-japonesa (1904-1905) - evidenciándose que la Seguridad del Estado estaba vigente.

Finalmente, entre 1850-1914, la segunda revolución industrial estaba en marcha. En este primer período de tiempo presentado, se infiere que la Seguridad del Estado fue la que marcó las acciones de los estados, lo que se resume en el siguiente gráfico:

Figura 1 - Evolución del concepto de seguridad en torno al pensamiento Geopolítico durante el siglo XIX e inicios del Siglo XX



Fuente: AUTOR, adaptado del planteamiento de Eric Hobsbawn, 1999.

Un segundo período de análisis según el planteamiento de Hobsbawn, se inicia con la I Guerra Mundial (I GM) en 1914 y la disolución de la URSS en 1991, período en el cual se evidenció guerras, tensión, crisis, entre estados; así como, crecimiento económico; coyunturas que han marcado los destinos de los estados, según sus propias aspiraciones y sus acciones en torno a la defesa de sus intereses; sin embargo, es necesario precisar que en los años anteriores al inicio de la I GM, varios países decidieron conformar alianzas en torno a la defensa mutua, por ejemplo: La Triple Entente, entre Rusia, Gran Bretaña-Irlanda y Francia, a esta última se unieron Serbia y Bélgica; Reino Unido y Japón; y la Triple Alianza, formada por el Imperio Austro-húngaro, Alemania e Italia. Es así que en este contexto se pueden evidenciar los siguientes acontecimientos:

En 1914, el asesinato del archiduque heredero de la corona del imperio Austro-húngaro, evento que impulsó a que este declare la guerra a Serbia; por su parte Rusia aliada de Serbia declararía la guerra al imperio Austro-húngaro, ante lo cual, Alemania respondería a su pacto de la triple alianza, declarando la guerra a

Rusia y atacando a Francia; con lo que, se dio el ingreso a la guerra de Gran Bretaña, aliada de Francia.

Con esta particularidad de la conformación de alianzas, dio como resultado la *autoayuda*, es decir, el *aumento de la seguridad*, reflejado en la participación de fuerzas militares aliadas en defensa de los intereses comunes de sus miembros, como respuesta a la necesidad de equilibrar las capacidades militares ante un enemigo común más poderoso; con lo que se estaría materializando la *Seguridad Internacional.*

En 1919, se creó la Sociedad de las Naciones (Liga de Naciones), en la que se distinguía los principios de cooperación y *Seguridad Colectiva*, basado en la propuesta del presidente de EE.UU. Woodrow Wilson, con la premisa de que la mejor forma de encontrar respuestas pacíficas para la resolución de conflictos entre estados, son las relaciones internacionales.

En 1939, se produce la invasión de Alemania a Polonia, iniciándose la II Guerra Mundial (II GM) hasta 1945, con aproximadamente 70 millones de víctimas, constituyéndose en la más grave crisis humanitaria vista hasta ese entonces. En 1942, se crea la Junta Interamericana de Defensa (JID), promoviendo la defensa continental y del hemisferio occidental, con principios de reciprocidad y cooperación de las naciones americanas ante cualquier agresión a una de ellas, dando la pauta para la conformación de la Comisión de Seguridad Hemisférica (CSH).

La Organización de las Naciones Unidas (ONU) es creada en 1945. Entre 1945-1991, se produce lo que se conoció como la guerra fría entre las potencias triunfadoras de la II GM, las mismas que liderarían al mundo dividido en dos rivalidades materializadas por ideologías capitalista y comunista, en donde la tensión permanente fue la tónica de los siguientes 46 años.

En 1946, se genera la teoría del Rimland de Spykman mediante la cual, los EE.UU. promovieron alianzas en todo el mundo, creando la barrera contra la expansión de la ideología comunista liderada por la URSS, materializándose la teoría de la contención, lo que permitió la ubicación de bases militares de los EE. UU en diferentes países según las alianzas establecidas.

En 1947, EE. UU propuso la Doctrina Truman, que consistió en brindar ayuda a los países que se resistieran al comunismo, materializándose en el Plan Marshall, que consistió en la contribución de EE.UU. a la reconstrucción de los países de Europa Occidental devastados tras la II GM. En este mismo año, la URSS propuso el Plan Molotov, como respuesta al Plan Marshall, con el cual materializó igual que su contendor de la Guerra Fría, el apoyo a la reconstrucción de los países de la Europa Oriental, a los que consideró aliados política y económicamente, instituyéndose el Consejo para la Mutua Ayuda Económica (COMECON).

En América, se estableció el Tratado Interamericano de Asistencia Recíproca (TIAR), fortaleciendo lo establecido en la JID, lo que permitió sentar las bases de lo que se denominaría Seguridad Hemisférica. En 1948, se establece la conformación

de la Organización de Estados Americanos (OEA), cuyo objetivo fundamental fue establecido en el Artículo 1 de la Carta de su creación: "Un orden de paz y de justicia, fomentar su solidaridad, robustecer su colaboración y defender su soberanía, su integridad territorial y su independencia".

En este contexto de la Guerra Fría, se crearon por parte de EE.UU. y sus aliados varios bloques y alianzas como: la OTAN (1949), la SEATO (1954) y la CENTO (1959); por su parte la URSS, formó la Organización del Tratado de Varsovia (1955), con las Fuerzas Armadas de Albania, Bulgaria, Checoslovaquia, Alemania Oriental, Hungría, Polonia, Rumania y la Unión Soviética, con lo que, se configuró estratégicamente un nuevo orden mundial bipolar, en donde la Seguridad Nacional había dado un paso hacia adelante, pues ahora se hablaba de la Seguridad Internacional; con lo que el realismo en las relaciones internacionales estaba en pleno auge, pues se consideraba que "el conflicto y la guerra son inherentes al sistema internacional" (CHARLES-PHILIPPE, 2008, p. 70).

Posteriormente, se produjeron una serie de acontecimientos, que pusieron a prueba la Seguridad Internacional que se mantenía durante la Guerra Fría, a lo que se le denominó "Détente[1]" (distención), considerándose hasta la década de los 80s, entre los cuales están: Cumbre de Ginebra (1955), con discusiones sobre negociaciones de armas, guerra nuclear, entre otras; crisis de los misiles de Cuba (1962) entre EE.UU. y URSS; los Tratados de no proliferación nuclear (1968), con los cinco países que habían desarrollado hasta ese entonces ensayos nucleares: EE.UU., Reino Unido, Francia, URSS y China (miembros del Consejo de Seguridad Nacional); el Tratado sobre la Limitación de Armas Estratégicas SALT (1972), entre EE.UU. y la URSS.

En este contexto de la distención, se destaca la realización de varias reuniones entre 1972 y 1975, entre las que podemos citar: EE. UU-URSS, URSS-China y la Conferencia de Seguridad y Cooperación en Europa entre los países miembros del Pacto de Varsovia, OTAN y países neutrales, los mismos que reconocieron las fronteras surgidas tras la II GM, acontecimientos que permitieron distender las relaciones entre los países involucrados.

Los acontecimientos antes descritos, tuvieron una connotación adicional, que correspondió a la posición mantenida por la URSS a partir de 1968, en que se estableció la "Doctrina Brezhnew", con la que pretendía y exigía la 'solidaridad socialista internacional', mediante la cual, se les comprometía a intervenir inclusive con la fuerza militar, cuando un Estado miembro era atacado o pretendido pasar al sistema capitalista, entonces, se puede interpretar que esta doctrina, fue la contraparte y respuesta a la Doctrina Truman de los EE.UU.

Ya en los años 70 y 80, se había configurado un nuevo orden mundial y de equilibrio de poder, con lo que se hacía necesario la cooperación internacional

1 "[…] *Détente* caracterizado por la voluntad de evitar una confrontación directa entre las superpotencias […] (VALKI, 1991)

en base a normas y reglas claramente establecidas en el Sistema Internacional; definiéndose en los años 70, con una nueva perspectiva de análisis de los aspectos relacionados al Estado, denominándose Sistema Mundo, tal como lo señala Wallerstein: "Los sistemas-mundo de análisis significaron antes que nada la sustitución de una unidad de análisis llamada "sistema-mundo" en vez de la unidad estándar de análisis, que había sido el estado nacional" (WALLERSTEIN, 2005, p. 15).

Como era de esperarse, esta nueva visión, influyó en la identificación de una multiplicidad de actores en el contexto internacional que configura el Sistema Internacional, en el que los intereses de los estados, producen el requerimiento de interdependencia, trayendo también entonces una nueva conceptualización de la Geopolítica, propuesta que generó una amplia discusión en este campo, pues la dependencia de los estados de la periferia de los centrales era evidente, producto de lo cual la interdependencia era un aspecto de carácter prioritario para los Estados que pretendían ser considerados en este sistema.

Con base en esta perspectiva de análisis, la seguridad se basó en el desarrollo de instituciones y normas internacionales (regímenes internacionales), que sean capaces de promover la paz en el mundo, reconociendo la existencia de otros actores y dando un espacio prioritario al papel que juega la economía en el Sistema Internacional; es decir, la cooperación de los Estados debe reflejarse en las instituciones internacionales, con la convicción de poder superar o eliminar los conflictos, de esta manera, se establecería los conceptos de la Seguridad Global o Seguridad Común.

De la misma manera, en los años 80, se materializó la crítica a la Geopolítica Clásica, pues la discusión generada en torno a la multiplicidad de actores, permitía dar un nuevo enfoque a la dimensión del Estado que permanecía como una entidad estructurada, bajo la cual abarcaba a la sociedad en su conjunto y al interés nacional como un hecho dado; pasando a la idea de:

> […] el sistema internacional es producto de lo que hacen sus actores, y en ese hacer, los actores crean rasgos de identidad que definen sus intereses y su posición en el sistema. La seguridad de cada Estado dependerá, de esta manera, del esfuerzo por ahondar en los lazos de identidad que permitan una mayor cooperación y estimulen la supervivencia de instituciones eficaces a la hora de dirimir los conflictos. (OROZCO, 2006, p. 167).

Con esta reflexión, se materializó la Geopolítica Crítica y como tal se puso énfasis en el proceso en la toma de decisiones de los estados y no solamente en la estructura del mismo, evidenciándose en el enfoque de la teoría constructivista sobre la concepción de la seguridad, cuyos principales autores son: Martha Finnemore (1996), Peter Katzenstein (1996), Emanuel Adler (1997), Barry Buzan (1998), Jutta Weldes (1999), entre otros; en donde fue un aporte importante la Securitización, ya

que el análisis se enmarcó en torno a las ideas, normas e identidades, construidas por los diferentes agentes participantes en este proceso.

A partir de los años 80 y los 90, la Seguridad supera el ámbito militar, pues se pasa a considerar aspectos como la diplomacia preventiva[2], la gestión de la crisis, el control de armamentos, la abstención del uso de la fuerza militar, es decir, la concepción del poder de los estados, pasa de ser considerado como capacidad a ser una relación de dominio(s), según su aplicación, ya sea unilateral o multilateral.

Con la caída del muro de Berlín, el fin de la Guerra Fría en 1989 y la posterior disolución de la URSS en 1991, la conceptualización de la Seguridad de los estados había alcanzado una nueva dimensión, pues, la concepción de la Seguridad Colectiva estaba siendo analizada, en la medida de que la disuasión debía ser superada por la prevención como medida para la resolución de conflictos entre estados.

A partir de la disolución de la URSS, específicamente en los años 1991 y 1992, se realizaron varios estudios en los que se consideró a la cooperación como medida para prevenir, reducir e incluso contener la amenaza de ir a una guerra, es decir, la búsqueda de una forma tal que la confianza mutua entre estados, sea la tónica para resolver las controversias, es así que, los profesores Ashton Carter, William Perry y John Steinbruner, publican un trabajo relacionado a la Seguridad Cooperativa con el título "A new concept of Cooperative Security", cuya idea general se materializó posteriormente en:

> Lo que distingue a la Seguridad Cooperativa de los enfoques tradicionales es su énfasis en la "prevención". En lugar de disuadir amenazas a la seguridad nacional o prepararse para combatirlas si éstas llegan a concretarse, la Seguridad Cooperativa apunta, en primer lugar, a evitar que surjan. (LEYTON, 2008, p. 3).

En definitiva, la Seguridad Cooperativa, busca alcanzar objetivos de Seguridad Común reconocidos entre estados y que, a través de relaciones de cooperación establecidas, se llegue a enfrentar las amenazas, para lo cual la diplomacia preventiva será privilegiada ya que será esta la que alcance la coordinación de acciones y comprometer las capacidades de los estados en la solución de problemáticas comunes.

Es entonces, que el Estado ya no es el único objeto referente para la seguridad, ya que la multiplicidad de actores de un sistema internacional interdependiente, visualiza la necesidad de considerar no solo a las amenazas externas de orden tradicional (estados), sino, a todas aquellas amenazas que afectan al ser humano y al medio ambiente en sus diferentes manifestaciones, ya sea que provengan

2 "[...] puede ser definida como la puesta en práctica del llamado "arte de la negociación política". Esta tiene como objetivo principal la gestión pacífica de los conflictos" (LEYTON, 2008)

del exterior como del interior de un Estado, por lo que fue necesario incorporar aspectos de orden económico y social en los análisis de seguridad.

Así, los debates académicos sobre la reconceptualización del concepto de Seguridad, se plasmaron desde los diferentes enfoques, sean estos los propuestos por los realistas, idealistas, constructivistas y críticos, cada uno de los cuales, difieren en su enfoque sobre quienes deberían ser los actores, pero coinciden en que:

> Esta diversidad de amenazas potenciales incluye la degradación del medio ambiente, el crecimiento de la población, el agotamiento de los recursos naturales, la mala administración y el deterioro económicos; el creciente poder de corporaciones multinacionales, la sustitución de los valores tradicionales de una cultura por influencias culturales «extranjeras», el aumento de la estratificación social y económica, la crisis de los sistemas de salud pública, el autoritarismo y la represión, la violación de los derechos humanos e incluso desastres naturales como terremotos. (CUJABANTE, 2009, p. 104).

Por lo que, la seguridad podría entenderse como lo manifestó Wendt "lo que los Estados quieren hacer de ella" (WENDT, 2005), en este sentido, es importante considerar el aporte de la Escuela de Copenhague, representada por Buzan, Waever y de Wilde (1998), mediante la cual, se considera el proceso de securitización como una herramienta con la que cuentan los Estados para el análisis de temas de seguridad frente a las diversas amenazas; además, "este proceso, mediante el cual se produce la seguridad, está basado en la designación subjetiva de una amenaza a la supervivencia" (CHARLES-PHILIPPE, 2008, p. 84).

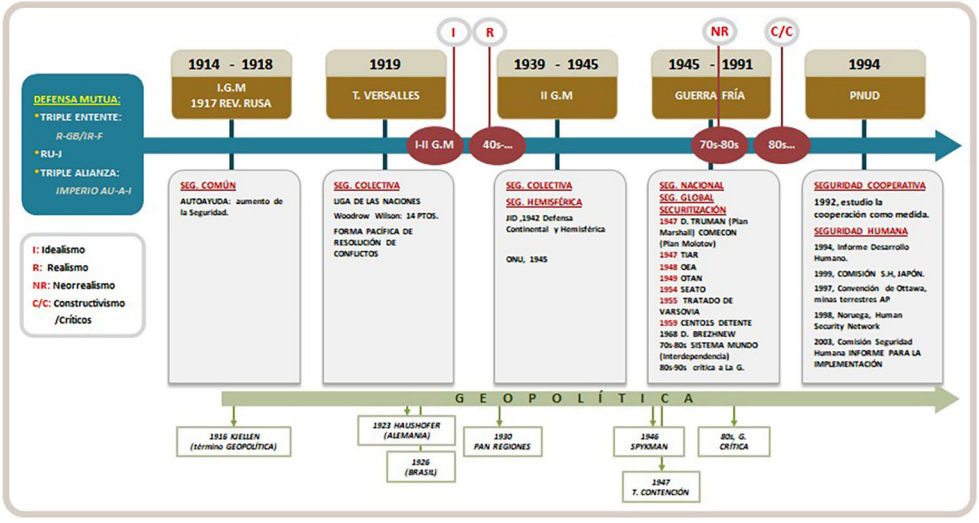
En esta evolución del concepto de seguridad y frente a la necesidad de la humanidad de garantizar la paz, condición indispensable para su desarrollo y bienestar, se ha alcanzado la Seguridad Humana a través del Informe sobre Desarrollo Humano del PNUD de 1994, documento fundador de esta doctrina; en este, se define a la seguridad humana "como una expresión que permite tender un puente entre los conceptos del "freedom from fear" y el "freedom from want" (MORILLAS, 2007).

Es entonces que la Seguridad Humana, ha sido el enfoque que la ONU ha promovido, con el objetivo de priorizar la atención al ser humano por parte de los estados, en el ámbito de la seguridad, en cuyo seno se ha promovido su actualización y fortalecimiento, tal como se refiere en la creación de la Comisión Sobre Seguridad Humana, motivada por Japón en 1999 y materializada dos años más tarde. Esta Comisión publicó en el año 2003, un informe con las diez principales tareas para la implementación de la Seguridad Humana, las mismas que se detallan a continuación:

1. Proteger a las personas inmersas en conflictos violentos.
2. Proteger a las personas de la proliferación de armas.
3. Dar apoyo a la seguridad humana de las personas activas.
4. Establecer fondos de transición para la seguridad humana en situaciones de posconflicto.
5. Promover el comercio justo y los mercados con el fin de beneficiar a las personas en situación de extrema pobreza.
6. Proveer los estándares mínimos de vida en todas partes.
7. Acordar una alta prioridad al acceso universal de los servicios básicos de salud.
8. Desarrollar un sistema eficiente e igualitario de derechos de patentes.
9. Empoderar a todas las personas a través de la educación básica universal mediante mayores esfuerzos en los ámbitos nacional e internacional.
10. Clarificar la necesidad de una identidad humana global al mismo tiempo que se respeta la libertad de los individuos de tener identidades y afiliaciones diversas. (MORILLAS, 2007, p.53).

Todo lo dicho anteriormente se resume en la siguiente figura:

Figura 2 - Evolución del concepto de seguridad en torno al pensamiento Geopolítico durante el Siglo XX



Fuente: AUTOR, adaptado del planteamiento de Eric Hobsbawn, 1999.

Bajo esta premisa de relación de los conceptos de seguridad y geopolítica, es preciso referirnos al planteamiento que Charles-Philippe presenta sobre el pensamiento de Gérard Dussouy, que en lo pertinente dice:

> Las diferentes visiones sobre la seguridad corresponden a las lecturas geopolíticas divergentes. La geopolítica es, globalmente, el estudio de la relación del espacio con la política; en su aspecto geoestratégico, es el lugar donde se entrecruzan (se enfrentan) territorios y potencias. De lo cual se desprende su reflexión, señalando: "… distingue las dos disciplinas de esta manera: la geopolítica es el estudio del Estando del espacio mundial (su organización y sus dinámicas), mientras que la geoestrategia representa el Actuando, o sea, las acciones estratégicas consideradas global o individualmente" (CHARLES-PHILIPPE, 2008, p. 106).

En este sentido, encontramos la Geoestrategia como la rama de la Geopolítica que es "la gestión estratégica de los intereses geopolíticos" (ROSALES, 2005, p.14). En este contexto, se ha conceptualizado a la seguridad desde diferentes enfoques relacionados con las teorías de las relaciones internacionales, dando origen a las escuelas de pensamiento sobre este ámbito, que según Charles Philippe, son el resultado del estudio de varios parámetros característicos de cada escuela, entre los cuales tenemos: la dimensión de análisis, el objeto referente de la seguridad, los supuestos normativos sobre el conflicto y la guerra, la visión sobre la paz y las políticas de seguridad que han diseñado los estados.

El resultado de este análisis, se ve reflejado en el comportamiento de los estados en el sistema internacional, dando como resultado una concepción de seguridad, ante lo cual se han visto decididos a disponer de todos los medios indispensables y recursos necesarios para preservar la paz, el interés nacional, la identidad nacional, el ser humano, el Estado y el medio ambiente. Esta explicación se sintetiza en el Cuadro 1, que a continuación se presenta:

Cuadro 1- Escuelas de pensamiento sobre Seguridad.

Teorías / Fundamentos	Idealista	Realista/ Neorrealista	Liberal/Neoliberal	Constructivista	Críticos
Dimensión de análisis	Ético y Derecho	Poder, Interés nacional Integridad Territorial	Democracia, Interdependencia e instituciones	Ideas, valores, normas, e identidades	Estructuras de poder Emancipación Supervivencia y bienestar
Nivel de Análisis (Objeto referente de la Seguridad)	(OIG), Sociedad Civil	Estado Sistema de Estados	Estados, OIG, Sociedad Civil	Agentes, Estructuras (Colectividades o Grupos)	Individuos, Élites nacionales y Transnacionales.
Supuestos normativos sobre el conflicto y la guerra	El conflicto y la guerra pueden ser eliminados/evitados	El conflicto y la guerra son inherentes al sistema internacional	El conflicto y la guerra pueden ser eliminados/superados	El conflicto y la guerra pueden ser eliminados/evitados	El conflicto y la guerra pueden ser combatidos por cambios radicales
Puntos de vista prospectivos sobre la paz	La paz mediante el Estado de Derecho (paz positiva)	La paz mediante el equilibrio de las potencias (paz negativa)	La paz mediante la cooperación (paz positiva)	La paz mediante la transformación y socialización de los agentes	La paz mediante el comunitarismo y la contestación de los discursos dominantes
Política de Seguridad	Disponer todos los medios indispensables y recursos necesarios para preservar la PAZ	Disponer todos los medios indispensables y recursos necesarios para preservar el INTERÉS NACIONAL	Disponer todos los medios indispensables y recursos necesarios para PREVENIR los conflictos en el marco de la COOPERACIÓN	Disponer todos los medios indispensables y recursos necesarios para preservar la IDENTIDAD NACIONAL en torno a los intereses del Estado	Disponer todos los medios indispensables y recursos necesarios para preservar El SER HUMANO, AL ESTADO Y AL MEDIO AMBIENTE
Concepción sobre seguridad	Seguridad Colectiva	Seguridad Nacional Seguridad Internacional Seguridad Colectiva Seguridad Hemisférica	Seguridad Global Seguridad Común Seguridad Cooperativa	Securitización	Seguridad Humana Seguridad Como Discurso

Fuente: AUTOR, basado en el contenido del libro La guerra y la paz (CHARLES-PHILIPPE, 2008, p. 71).

3 EVOLUCIÓN Y DESARROLLO DE LAS AMENAZAS A LA SEGURIDAD

Se ha visualizado la evolución del concepto de Seguridad, producto de las acciones y reacciones de los estados y la influencia de diferentes actores externos e internos que atentaron y atentan contra la paz y desarrollo de los pueblos a lo largo y ancho del planeta; se ha llegado a comprender que existen como

objetos referentes cuando de seguridad se trata del ser humano, del Estado y del medio ambiente; y, que para protegerlos se emplean según la visión geopolítica y geoestratégica de los estados, la concepción de seguridad que se adapte a la defensa de sus intereses, sea esta colectiva, cooperativa, global, hemisférica, común, humana.

Es importante resaltar lo que sobre amenazas a la seguridad se impulsó en lo que se denominó la nueva agenda internacional de la ONU post Guerra Fría, ya que la connotación estaba basada en la necesidad de abordar nuevas perspectivas, nuevos enfoques sobre este tema; así según (BERMÚDEZ, 2002), es importante considerar aquellos fenómenos que traspasan las fronteras de los estados y que obliga a plantear respuestas comunes a pesar de que sus impactos sean particulares a cada Estado, tal es el caso del crimen organizado, el narcotráfico, la corrupción que se deslinda de estos, el terrorismo, la migración, la degradación ambiental, a las que se las denominó amenazas no tradicionales, sumadas a aquellas que se desprenden de la seguridad humana como amenazas que abordan campos de la salud, económica, alimentaria, comunitaria y política, es decir con un alcance transnacional denominándoles amenazas globales. Finalmente, se consideran aquellos aspectos que deben ser permanentemente monitoreados por los sistemas de alerta temprana y que dependiendo de su incidencia pueden o no ser considerados como amenazas, entre estos constan: incidentes ambientales, riesgo de accidentes nucleares, desastres naturales, movimientos masivos de población, hambre generalizada y propagación de enfermedades.

Pero fueron los atentados del 11 de septiembre del 2001 cuando se produce un punto de quiebre sobre la Seguridad Internacional y las amenazas latentes a esta. Es entonces, que se han producido varios esfuerzos de la comunidad internacional para entender la problemática a la que se enfrenta la humanidad, tal es el caso de la Resolución 1373 de la ONU de 2001 que, en lo particular al terrorismo, tal como lo señala Gomariz (2005) en su artículo sobre Seguridad Internacional y Terrorismo, señala:

> […] constituye, por primera vez, un auténtico código jurídico y político contra el terrorismo, de obligado cumplimiento para todos los miembros de la organización y que concede al Consejo facultades para adoptar medidas coercitivas en caso contrario. Es decir, la lucha contra el terrorismo pasa a ser una obligación de la comunidad internacional, ajustándose al Derecho de la Carta y al Internacional. En la Resolución se observa la estrecha relación entre otras amenazas existentes con el terrorismo internacional, el tráfico ilícito de armas y materiales nucleares, químicos, biológicas y otros letales, el blanqueo de dinero o la delincuencia transnacional. (p.12).

Otro esfuerzo constituye la Declaración de Bridgetown de la Asamblea General de la Organización de los Estados Americanos (OEA) sobre: "Enfoque Multidimensional de la Seguridad Hemisférica" del 4 de junio de 2002, en la que se establece:

> Los Ministros de Relaciones Exteriores y Jefes de Delegación, durante su diálogo en el trigésimo segundo período ordinario de sesiones de la Asamblea General, reconocieron que las amenazas, preocupaciones y otros desafíos a la seguridad en el Hemisferio son de naturaleza diversa y alcance multidimensional y *que el concepto y enfoque tradicionales deben ampliarse para abarcar amenazas nuevas y no tradicionales*, que incluyen aspectos políticos, económicos, sociales, de salud y ambientales. (ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, Declaración de Bridgetown, 2002, p.1). (el resaltado fuera del texto).

Constituyéndose en la base para la Declaración sobre Seguridad en las Américas adoptada en México por la Organización de los Estados Americanos (OEA) en octubre de 2003, que en lo pertinente señala:

> Considerando que la Declaración de Bridgetown reconoce que las amenazas, preocupaciones y otros desafíos a la seguridad en el Hemisferio son de naturaleza diversa y alcance multidimensional y que el concepto y enfoque tradicionales deben ampliarse para abarcar *amenazas nuevas y no tradicionales, que incluyen aspectos políticos, económicos, sociales, de salud y ambientales.* (ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, 2003, p.1). (el resaltado fuera del texto).

Y, al referirse en este documento a los valores compartidos y enfoques comunes, señala:

> La seguridad de los Estados del Hemisferio se ve afectada, en diferente forma, por amenazas tradicionales y por las siguientes nuevas amenazas, preocupaciones y otros desafíos de naturaleza diversa:
> • el terrorismo, la delincuencia organizada transnacional, el problema mundial de las drogas, la corrupción, el lavado de activos, el tráfico ilícito de armas y las conexiones entre ellos;
> • la pobreza extrema y la exclusión social de amplios sectores de la población, que también afectan la estabilidad y la democracia. La pobreza extrema erosiona la cohesión social y

> vulnera la seguridad de los Estados;
> • los desastres naturales y los de origen humano, el VIH/SIDA y otras enfermedades, otros riesgos a la salud y el deterioro del medio ambiente;
> • la trata de personas;
> • los ataques a la seguridad cibernética**;**
> • la posibilidad de que surja un daño en el caso de un accidente o incidente durante el transporte marítimo de materiales potencialmente peligrosos, incluidos el petróleo, material radioactivo y desechos tóxicos; y
> • la posibilidad del acceso, posesión y uso de armas de destrucción en masa y sus medios vectores por terroristas" (ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, 2003, p.4). (el resaltado fuera del texto).

En este mismo sentido, en diciembre del 2003 se conforma el Grupo de Alto Nivel sobre las amenazas, los desafíos y el cambio, por iniciativa del Secretario General de la ONU, con la finalidad de que:

> […] *se evaluarán las actuales amenazas a la paz y seguridad internacionales* y se formularán recomendaciones para fortalecer las Naciones Unidas, a fin de que la Organización pudiera proporcionar *seguridad colectiva* para todos en el siglo XXI. Obedece, por tanto, "al propósito de recomendar medidas claras y prácticas para asegurar una acción colectiva eficaz sobre la base de un riguroso análisis de las *amenazas futuras a la paz y seguridad*, […] Se le pedía una evaluación general de los problemas en materia de seguridad y que recomendase los cambios necesarios para superarlos eficazmente, concibiendo la seguridad en sentido amplio, ya que no se limita estrictamente a lo militar, sino que incluye también los aspectos económicos y sociales relacionados con la seguridad. (GARCÍA; DÍAZ, 2006, p.17). (el resaltado fuera del texto).

Producto de lo cual, en el 2004 el Grupo de Alto Nivel, en su informe al Secretario General de la ONU, señala:

> (…) *una visión nueva y audaz de la seguridad colectiva para el siglo XXI*. Vivimos en un mundo de *amenazas nuevas e incipientes* que no podían haberse previsto cuando se fundaron las Naciones Unidas en 1945, como el terrorismo nuclear y el colapso del Estado por una combinación fatídica de pobreza, enfermedad y guerra civil. […] Hay seis grupos de amenazas

> que deben preocupar al mundo en estos días y en los próximos decenios:
> • Guerras entre Estados;
> • Violencia dentro del Estado, con inclusión de guerras civiles, abusos en gran escala de los derechos humanos y genocidio;
> • Pobreza, enfermedades infecciosas y degradación del medio ambiente;
> • Armas nucleares, radiológicas, químicas y biológicas;
> • Terrorismo; y
> • Delincuencia transnacional organizada" (ORGANIZACIÓN DE LAS NACIONES UNIDAS, 2004, p. 3-4, el resaltado fuera del texto).

Es entonces que la ONU impulsaba la Seguridad Colectiva, bajo la perspectiva de un compromiso compartido de los estados miembros, considerando que las amenazas existentes no respetan fronteras y su acción en un Estado en particular, tiene repercusiones en los demás estados, tal como lo refiere Martínez (2018) en su artículo "Estrategias Nacionales de Seguridad ante los Riesgos y Amenazas Transnacionales", cuando analiza lo palteado en el informe del Grupo de Alto Nivel de la ONU de 2004, que en lo pertinente señala:

> Ello no supone que las amenazas afecten a todos por igual. Es obvio que los Estados con economías menos prósperas padecen mayores riesgos; pero precisamente por ello es necesario un consenso entre países ricos y pobres. "*Sin reconocimiento mutuo de las amenazas no hay seguridad colectiva*". (UN, 2004, p. 12, el resaltado fuera del texto).

Con esta premisa "sin reconocimiento mutuo de las amenazas no hay seguridad colectiva", los estados han generado sus estrategias de seguridad considerando que estas deben ser multiestatales, en donde el compromiso de sus acciones colectivas para enfrentar las amenazas y riesgos, se circunscriban a la necesidad de alcanzar la Seguridad Global y Seguridad Común tan aneladas, en donde la cooperación entre estados, no solo comparta la acción militar sino tambien la acción diplomática, para prevenir y no solo disuadir. En este contexto, de los esfuerzos comunes, los estados han generado Estrategias de Seguridad Nacional (ESN), para multiplicar las acciones y por ende los efectos sobre las amenazas y riesgos identificados; lo que se puede visualizar en la tabla 1 que se presenta a continuación:

Tabla 1 - Tipos de amenazas en las Estrategias de Seguridad

Tipos de amenazas	UE	ONU	Holanda	UE	Alemania	Reino Unido	Reino Unido	OTAN	España	Holanda	España	Reino Unido	UE	Alemania
	2003	2004	2007	2008	2008	2008	2010	2010	2011	2013	2013	2015	2016	2016
Cambio climático		X	X	X	X	X	X	X				X		X
Pandemias		X	X			X	X					X		X
Conflictos entre Estados	X	X					X		X	X	X			X
Armas destrucción masiva	X	X		X	X	X	X	X	X	X	X	X		X
Crimen organizado transnacional	X	X		X		X	X		X		X	X	X	X
Conflictos internos		X												
Terrorismo	X	X		X	X	X	X	X	X		X		X	X
Ciberataques				X			X	X	X		X	X	X	X
Estados Fallidos	X					X								X
Seguridad energética			X	X	X				X		X			X
Vulnerabilidad fronteras			X										X	
Híbridas													X	
Amenazas de terceros no bélicas						X					X		X	
Flujos migratorios descontrolados					X				X		X			X
Catástrofes						X	X		X		X	X		

Fuente: Creación del autor (MARTÍNEZ, 2018, p. 19)

También, en esta tabla se pueden identificar a las tres categorías de amenazas que la Guía Político Estratégica de Ciberdefensa expedida por el Ministerio de Defensa del Ecuador señala, estas son las amenazas convencionales, asimétricas e híbridas a las que las define como:

> Las amenazas convencionales también llamadas amenazas tradicionales son aquellas que están claramente identificadas en el DIH y relacionadas a un conflicto armando internacional […] define como amenaza asimétrica a un "enfrentamiento entre adversarios con recursos, fuerzas y tácticas muy diferentes como guerra de guerrillas a ejércitos regulares y el terrorismo frente a estados" (REAL ACADEMIA ESPAÑOLA, 2021). […] El término amenazas híbrida se refiere a una acción cuyo objetivo es socavar o dañar al influir en su toma de decisiones a nivel local, regional, estatal o institucional. Estas acciones se coordinan, sincronizan y se dirigen deliberadamente a las vulnerabilidades de los Estados e instituciones democráticas. Las actividades se llevan a cabo utilizando una amplia gama de medios y están diseñados para

> permanecer por debajo del lumbral de detección. (ECUADOR, 2021a, p. 41, 42).

Como se ha podido identificar en este apartado, las amenazas han ido evolucionando y han sido identificadas o tipificadas de acuerdo a la concepción de cada Estado u organismo internacional, ante lo cual, se han establecido declaraciones y resoluciones en busca del reconocimiento compartido como tales, ya que es la única manera de aunar esfuerzos para combatirlas; es así que, se han implementado estrategias de seguridad nacional que en la tabla propuesta, da cuenta que amenazas como el terrorismo, el crimen organizado transnacional y las armas de destrucción masiva, han permanecido en el análisis de los últimos 20 años en forma sostenida; sin embargo, los ciberataques y los conflictos entre estados, han tenido una especial atención en la última década, sin dejar de considerar el cambio climático como una amenaza constante.

4 LA CIBERSEGURIDAD Y CIBERDEFENSA EN EL ECUADOR

Como se ha podido evidenciar en la Declaración sobre Seguridad en las Américas de 2003, se consideró a los ataques a la seguridad cibernética como una nueva amenaza a la seguridad de los estados y a partir del año 2008 varios países y organizaciones internacionales han ido incorporando a sus ESN a los ciberataques; así: la Unión Europea (2008-2016); Reino Unido (2010-2015); la OTAN (2010); España (2011-2013; y Alemania (2016). Con lo que, se deduce que, en la segunda década del presente siglo, se han intensificado las acciones de los estados, para enfrentar a esta amenaza.

En el Ecuador, se han desarrollado varias actividades en torno a enfrentar esta amenaza, para lo cual se ha generado normativa legal que permita el accionar de las instituciones involucradas en este tema; sobre la base de las disposiciones constitucionales, así podemos señalar:

> En la Constitución de la República del Ecuador en su artículo 158, esta blece que: "(…) Las Fuerzas Armadas tienen como misión fundamental la defensa de la soberanía y la integridad territorial (…)"; además, en su artículo 261, señala: "El Estado central tendrá competencias exclusivas sobre: 1. La defensa nacional, protección interna y orden público (…)". (ECUADOR, 2008).

En este contexto, en el país se han generado otras normas específicas relacionadas al ámbito de la seguridad y defensa, y que direccionan el accionar del sector defensa para enfrentar este tipo de amenaza, como la Ley de Seguridad Pública y del Estado que en su artículo 2, considera la protección y control de los

riesgos tecnológicos y científicos, la tecnología e industria, es decir, se establece la disposición en base a la necesidad de protección contra amenazas y riesgos vinculados a aspectos técnicos y tecnológicos, poniendo de antemano el requerimiento de la participación activa de las instituciones involucradas en las áreas señaladas, entre las cuales constan el Ministerio de Defensa, Ministerio de Telecomunicaciones, las Fuerzas Armadas, y aquellas que tengan algún tipo de vinculación que por sus competencias deban gestionar los riesgos señalados.

Específicamente en el sector defensa, se expidió el Acuerdo Ministerial N° 281 de 12 de septiembre de 2014, que en el artículo 1 señala:

> Crear el Sistema de Ciberdefensa del Ministerio de Defensa Nacional como el mecanismo que articula las instancias permanentes y de conformación que aborden el tema desde el nivel político - estratégico, estratégico militar y operacional, a fin de coordinar e implementar políticas y estrategias de Ciberdefensa […]; y, en el artículo 7 del mismo, Acuerdo Ministerial señala: "El Comando de Ciberdefensa, se conforma como un comando del CC.FF.AA., integrado por personal técnico y/o operativo civil y militar. *Tendrá la misión de operar las capacidades de defensa, exploración y respuesta en el espacio cibernético para proteger y defender la infraestructura crítica e información estratégica del Estado* (…)". (ECUADOR, 2014, el resaltado fuera del texto).

Con lo dicho anteriormente, se visualiza que se encarga a la Fuerzas Armadas del Ecuador en forma tácita, la tarea de generar las acciones pertinentes en mira de cumplir la misión impuesta en el espacio cibernético, bajo la dirección y coordinación del ente político estratégico de la Defensa que es el Ministerio de Defensa Nacional (MDN).

Un aspecto importante a resaltar en el sector Defensa, es la expedición de la Política de la Defensa Nacional del Ecuador en el 2018, que en lo pertinente señala: "[…] El sector Defensa impulsa la coordinación interinstitucional de la ciberdefensa en el marco de la seguridad cibernética nacional y posee una capacidad considerable para defender la infraestructura crítica digital de las Fuerzas Armadas […]" (ECUADOR, 2018, p. 60).

Es decir, el MDN será el ente coordinador entre las instituciones del Estado relacionadas a alcanzar el direccionamiento político y técnico, así como la respuesta requerida por parte del Estado ante las ciberamenazas; por cuanto, cuenta en su organización al Consejo de Seguridad Sectorial (CSS) como un órgano articulador de temas relacionados a la Seguridad y Defensa del Estado.

Otra normativa generada en el sector defensa del Ecuador, constituye el Plan Nacional de Seguridad Integral (PNSI) 2019-2030, que en el Objetivo General N° 1 establece: "[…] defender la soberanía e integridad territorial (terrestre, marítimo, aéreo, espacio y promoviendo la seguridad y libertad de las personas en el ciberespacio);

mediante la aplicación de estrategias militares multidimensionales sustentadas en capacidades estratégicas conjuntas [...]" (ECUADOR, 2019, p. 108). Esta normativa, orienta de forma específica a las Fuerzas Armadas a generar las capacidades estratégicas conjuntas que le permitan afrontar las operaciones en el ciberespacio.

Cabe recalcar, que el PNSI cuenta como anexos varios planes específicos por cada institución participante en el ámbito de la seguridad del país, en este caso, el sector Defensa cuenta con el Plan Específico de Defensa Nacional, que en su Objetivo 1 establece: "[...] El Estado participará activamente en el control efectivo del territorio nacional (espacios terrestres, marítimos, aéreos y el ciberespacio) impulsando el desarrollo de políticas y estrategias para la ciberseguridad, ciberdefensa y defensa aeroespacial, permitiendo que estas se encuentren en las mejores condiciones para afrontar las amenazas y riesgos que atenten a la paz y seguridad" (ECUADOR, 2019); es decir, la tarea de coordinación interinstitucional del Estado relacionada a la Defensa del mismo, está reflejada en este plan, pues vincula al sector Defensa y de manera particular a las Fuerzas Armadas con otros sectores que operan en el ciberespacio, para lo cual, necesariamente deberá generarse políticas y estrategias para enfrentar las amenazas particulares de este dominio.

Es justamente el ente rector de las telecomunicaciones en el Ecuador, el Ministerio de Telecomunicaciones y Sociedad de la Información quien con Acuerdo N° 025-2019 de 20 de septiembre del mismo año, expidió el Esquema Gubernamental de Seguridad de la Información (EGSI 2.0), cuya implementación es obligatoria en las instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva; mediante el cual, se impulsa la integridad y disponibilidad de la información; así como preservar la confidencialidad, mediante la implementación de procesos de gestión y evaluación de riesgos de seguridad de la información y el establecimiento de controles que permita alcanzar un nivel mínimo de afectación a las instituciones.

Siguiendo esta línea de acciones institucionales, el Gabinete Sectorial de Seguridad como órgano articulador de las instituciones pertenecientes a este cuerpo colegiado como son: Ministerio de Defensa; Ministerio del Interior; Ministerio de Relaciones Exteriores; Centro de Inteligencia Estratégica; Servicio Nacional de Gestión de Riesgos y Emergencias, en la vigésima sesión ordinaria del 1 de abril de 2021, aprueba la Política Nacional de Ciberseguridad (PNC), encargándose al Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) su publicación, cumpliéndose con Acuerdo Ministerial 006-2021 de 17 de mayo de 2021. En la Política Nacional de Ciberseguridad se establece que:

> La seguridad de toda la población ecuatoriana en el ciberespacio -en el "quinto dominio"-, es prioridad estratégica del Gobierno Nacional" [...] La ciberdefensa es un complemento de la ciberseguridad, que provee la defensa contra las amenazas en el ciberespacio en beneficio de toda la población. Esta se fundamenta

> en las líneas de acción estratégica de la Política de Defensa 2018 y en el respeto al Derecho internacional. (MINTEL, 2021, p. 2,34,35).

En concordancia y una vez aprobada la Política Nacional de Ciberseguridad el 1 de abril de 2021, el Ministerio de Defensa Nacional según Acuerdo Ministerial 199 del 11 de mayo de 2021 expide la Política de Ciberdefensa para el Sector Defensa, que en lo pertinente señala "Reformar el Acuerdo Ministerial Nº 281 de 12 de septiembre de 2014, estableciendo una nueva estructura de ciberdefensa del sector defensa, de acuerdo al siguiente detalle.

Cuadro 2- Estructura de Ciberdefensa

ESTRUCTURA DE CIBERDEFENSA		
NIVEL	**RESPONSABLE**	**FUNCIONES**
POLÍTICO ESTRATÉGICO	**Ministerio de Defensa**	• Ejercer la rectoría y direccionamiento político estratégico en ciberdefensa. • Gestionar la ciberdefensa mediante coordinaciones intergubernamentales e interinstitucionales. • Gestionar la cooperación internacional en el ámbito de la ciberdefensa.
ESTRATÉGICO MILITAR	**Comando Conjunto**	• Planificar y conducir las operaciones militares considerando el ciberespacio.
OPERACIONAL	**Comando de Ciberdefensa**	• Planificar y ejecutar operaciones de ciberdefensa para proteger la infraestructura crítica digital y servicios esenciales del Estado e infraestructura crítica digital de defensa.
	Unidades de Ciberdefensa de las Fuerzas	• Ejecutar operaciones de ciberdefensa en cumplimiento al Plan de Ciberdefensa.

Fuente: ECUADOR, 2021b, p.4.

Además, "se crea el Centro de Respuestas a Emergencias de Seguridad Informática (CERT), para coordinar la gestión de incidentes e intercambio de información con el EcuCERT, organismos internacionales y los Equipos de Respuesta a Incidentes de seguridad informática (CSIRT) de las Fuerzas e instituciones a nivel nacional".

Otro aspecto importante de Política de Ciberdefensa, constituye la expedición de la Estrategia de Ciberdefensa en la que:

> […] se establecen objetivos y líneas de acción, para avanzar en el desarrollo de una ciberdefensa capaz de operar de manera individual y colectiva en defensa de los objetivos estratégicos de la nación. Permitiendo disponer de una guía para la planificación, diseño, desarrollo y despliegue de las capacidades de ciberdefensa (…) promulga el establecimiento de un modelo de gestión para la capacidad de ciberdefensa totalmente estructurado, flexible y sólido; al igual, los lineamientos que le permitan crecer y adaptarse en función de las ciberamenazas que puedan presentarse (…) con una visión sistémica, el Estado tendrá la capacidad de conocer, prevenir, proteger, disuadir y responder a las ciberamenazas, en escenarios de alta incertidumbre (…) (ECUADOR, 2021c, p. 12,13).

Figura 3- Estrategia de Ciberdefensa

Fuente: ECUADOR, 2021c

En la Política de Ciberdefensa, también se expide la *Guía Político Estratégica de Ciberdefensa* que busca:

> Orientar el accionar del sector defensa, y su relación con otras instituciones nacionales e internacionales. Alineándose a un marco conceptual del modelo de gestión de ciberdefensa, y estableciendo principios fundamentales que guían el esquema de doctrina para las operaciones militares en el ciberespacio (ECUADOR, 2021a, p.6).

Figura 4- Guía Político Estratégica de Ciberdefensa

Fuente: ECUADOR, 2021a.

En definitiva, en el Ecuador para "la aplicación de la ciberdefensa se establece la rectoría al MIDENA y en el nivel de planificación y ejecución de las operaciones militares en el ciberespacio al CC.FF.AA. y las Fuerzas" (ECUADOR, 2021, p. 64,65).

Como se ha explicado en el desarrollo de este artículo, el concepto de Seguridad ha ido evolucionando a lo largo del tiempo, en la medida en como los estados han reaccionado en defensa de sus intereses y han enfrentado las amenazas y/o riesgos existentes en cada época analizada, en torno al sistema internacional; es decir, la gestión de los intereses geopolíticos de cada Estado, se visualiza en la

geoestratégica aplicada, a través de acciones individuales, bilaterales y multilaterales, con las particularidades propias de cada Estado, con miras a enfrentar los diferentes tipos de amenazas, que como se ha señalado, han ido cambiando conforme se la mutación de los escenarios.

En fin, para cerrar este análisis se ha considerado oportuno lo que Martínez (2018) en su artículo sobre "Estrategias Nacionales de Seguridad ante los riesgos y amenazas transnacionales" publicado en la revista Reflexión Política, señala:

> La seguridad, creo que ha quedado claro, es un concepto poliédrico y ello no la dota únicamente de riqueza en su contenido, sino que lamentablemente le confiere una enorme complejidad que dificulta su logro, puesto que los diferentes ámbitos y sectores de seguridad están interconectados. Por ello, resultan normalmente insatisfactorias las acciones individualizadas en pro de la seguridad, y ya está bastante asumida la necesidad de coordinación intersectorial como vía de éxito. No obstante, las últimas ESN nos están mostrando un paso más allá y, sin negar la autonomía de gestión de cada uno de los ámbitos, comienza a establecer gestiones integradas de todos ellos que permiten multiplicar los efectos perseguidos en el combate contra las amenazas y en la defensa de los intereses que se quieren proteger (p. 18,19).

Sin duda, la tarea de los Estados es ardua ya que en un mundo de alta incertidumbre, la acción coordinada y unificada del Estado y entre estados, parecería ser la única opción para enfrentar las manezas y riesgos a la Seguridad.

5 REFLEXIONES FINALES

El concepto de seguridad ha evolucionado conforme las acciones y reacciones de los estados en torno a la defensa de sus intereses, que se han visto incitados por la presencia de amenazas que han alterado su seguridad y desarrollo; siendo su visión geopolítica y su acción geoestratégica, la pauta necesaria para responder a los desafíos presentes y futuros.

Las amenazas se han desarrollado conforme la dinámica de las variables que las definen, los medios que emplea, y el ambiente en el cual se mueven; sean estas: acciones y reacciones de los estados en torno a la defensa de sus intereses, generarán amenazas como conflictos entre estados, armas de destrucción masiva; la concepción de la influencia de los países considerados como potencias en sus territorios, han generado amenazas como el terrorismo; el tráfico de drogas, generan amenazas como el crimen organizado transnacional y la vulnerabilidad de las fronteras; o el cabio climático en si como una amenaza a toda la humanidad; en

fin, se habla de amenazas convencionales o tradicionales, híbridas, no tradicionales, globales, asimétricas y nuevas amenazas.

Los estados han generado respuestas frente a las amenazas ya sea en forma individual, bilateral, multilateral, con la implementación de resoluciones, declaraciones y estrategias de seguridad nacional o estrategias para un fin específico, lo que prima en esta tarea es cumplir con la premisa "sin reconocimiento mutuo de las amenazas no hay seguridad", es decir, los esfuerzos deben ser comunes, aunque los efectos sean diferentes para cada Estado.

El Ecuador se ha incorporado a los países que han generado normativa legal para enfrentar una de las amenazas más recurrentes en la segunda década del siglo XXI como son los ciberataques, definiendo la necesidad de articular los esfuerzos interinstitucionales con la emisión de la Política de Ciberseguridad como el paraguas que orienta las políticas y estrategias para la Ciberseguridad y la Ciberdefensa. Lo propio el sector Defensa ha generado normativa específica en este campo como: la Política de Ciberdefensa, la Estrategia de Ciberdefensa y la Guía Político – Estratégica de Ciberdefensa, además de la conformación de la Estructura de Ciberdefensa con la definición de responsabilidades en los diferentes niveles político estratégico, estratégico militar y operacional.

REFERENCIAS

ASAMBLEA, N. *Ley de Seguridad Pública y del Estado.* Quito: Asamblea Nacional, 2009.

BERMÚDEZ, L. Nuevas Amenazas a la Paz y Seguridad Internacionales. *Revista Mexicana de Política Exterior*, p. 83-97, 2002.

CHARLES-PHILIPPE. *La Guerra y La Paz, enfoques contemporáneos sobre Seguridad Y Estrategia.* Barcelona: Icaria, 2008.

CUJABANTE, X. La Seguridad Internacional: Evolución de un concepto. *Revista de Relaciones Internacionales, Estrategia y Seguridad*, p. 93-106, 2009.

ECUADOR. *Constitución de la República del Ecuador.* Montecristi: Asamblea Nacional, 2008.

ECUADOR. Ministerio de Defensa Nacional. Acuerdo Ministerial 281. Quito: MDN, 2014.

ECUADOR. Ministerio de Defensa Nacional. *Política de la Defensa Nacional.* Quito: MDN, 2018.

ECUADOR, Ministerio de Defensa Nacional. Plan Nacional de Seguridad Integral. *PNSI,* Quito: MDN, 2019.

ECUADOR, Ministerio de Defensa Nacional. *Guía Político Estratégica de Ciberdefensa.* Quito: MDN, 2021a.

ECUADOR, Ministerio de Defensa Nacional. Acuerdo Ministerial 199. *Política de Ciberdefensa para el Sector Defensa*. Quito: MDN, 2021b.

ECUADOR, Ministerio de Defensa Nacional. *Estrategia de Ciberdefensa.* Quito: MDN, 2021c.

ECUADOR. *Ley de Seguridad Pública y del Estado.* Quito: (s.f.).

GARCÍA, Romualdo Bermejo; DÍAZ, Eugenia López-Jacoiste. Un mundo más seguro: la responsabilidad que compartimos. *UNISCI DISCUSSION PAPERS n. 10*, 17, 2006.

GOMARIZ, A. *Seguridad Internacional y Terrorismo, una nueva era en la lucha contra el terrorismo*. Madri, Espanha: Instituto Universitario General Gutiérrez Mellado De Estudios Sobre La Paz La Seguridad Y La, 2005. Disponible em https://iugm.es/publicaciones/colecciones/estudios/seguridad-y-terrorismo/?id=355 Accedido en: enero 2005.

HOBSBAWM, Eric. *Era dos extremos:o breve século XX – 1914-1991*. Tradução de Marcos Santarrita. São Paulo: Companhia das Letras, 1999.

LEYTON, C. Seguridad cooperativa y seguridad colectiva: ¿cohabitación de la disuasión y la cooperación? *ORPAS UBO del Observatorio Regional de Paz y Seguridad, Serie Documentos de Análisis n. 6*, 1-11, 2008.

MARTÍNEZ, R. Estrategias Nacionales de Seguridad ante los riesgos y amenazas transnacionales. *Reflexión Política, 20* (40), p. 10-20, 2018.

MINTEL, M. d. *Política de Ciberseguridad.* Quito: MINTEL, 2021.

MORILLAS, P. Seguridad humana: conceptos, experiencias y propuestas. *CIDOB*, 49, 2007.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Declaración de Bridgetown. *Enfoque Multidimensional de la Seguridad Hemisférica*. Bridgetown, Barbados: OEA. 2002

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Declaración sobre Seguridad en las Américas. *Conferencia Especial sobre Seguridad*. México, 2003.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resumen, Un mundo más seguro: Una responsabilidad que compartimos. *Informe del Grupo de Alto Nivel sobre las amenazas, los desafíos y el cambio*. ONU. 2004

OROZCO, G. El concepto de la seguridad en la Teoría de las Relaciones internacionales. *CIDOB d'Afers Internacionals*, p.161-180, 2006.

ROSALES, G. *Geopolítica y Geoestrategia Liderazgo y Poder, Ensayos.* Bogotá: Universidad Militar de Nueva Granada, Instituto de Estudios Geoestratégicos, 2005.
VALKI, L. ¿Dónde están aquellos soldados? La evolución en las percepciones de las amenazas en Europa Oriental. *Revista Internacional de Ciencias Sociales*, p. 109-123, 1991.

WALLERSTEIN, I. *Análisis del Sistema Mundo.* México: Siglo Veintiuno, 2005.

WENDT, A. La anarquía es lo que los estados hacen de ella. La construcción social de la política de poder. *Revista Académica de Relaciones Internacionales*, p. 1-47, 2005.

LA TECNOLOGÍA EN EL ESPACIO ULTRATERRESTRE Y SUS IMPLICACIONES EN SEGURIDAD Y DEFENSA

Manuel López-Lago López-Zuazo*

En los últimos 50 años las actividades humanas en el Espacio han creado más residuos que todos los meteoritos llegados del Sistema Solar en miles de millones de años.

Manuel López-Lago López-Zuazo

RESUMEN

En la última década especialmente el espacio ultraterrestre se ha convertido en un espacio de competición en el que han proliferado numerosos actores; no solamente tienen acceso al espacio los países más poderosos, sino que la mayoría de países del mundo tienen algún satélite en el espacio, a lo que hay que añadir el elevado número de empresas comerciales, especialmente en el ámbito de las comunicaciones. El abaratamiento de costes y la evolución exponencial de la tecnología en este ámbito ha supuesto que se desarrollen nuevas capacidades espaciales que afectarán a la seguridad nacional de los países. Ya no sólo existe la capacidad de observación y de comunicaciones, sino que ya las grandes potencias han desarrollado sistemas anti satélites, vehículos de exploración y minado espacial y vehículos supersónicos que supondrán un cambio en las estrategias espaciales de los actores más poderosos. El espacio ultraterrestre, como espacio geopolítico, tendrá una relevancia clave en las relaciones internacionales y, espacialmente, en las operaciones militares.

Palabras clave: Tecnología; seguridad; espacio ultraterrestre; capacidades espaciales; Marte.

A TECNOLOGIA NO ESPAÇO ULTRATERRESTRE E SUAS IMPLICAÇÕES EM SEGURANÇA E DEFESA

RESUMO

Na última década, especialmente, o espaço ultraterrestre se converteu em um campo de competição, no qual se proliferaram numerosos agentes; não apenas

* Doctor cum laude en Navegación Aérea por la Universidad Politécnica de Cartagena y doctor cum laude por la Universidad de Salamanca en Estado de Derecho y Gobernanza Global. Profesor del Departamento de Política de Seguridad y Defensa en el Centro Superior de Estudios de la Defensa (CESEDEN).

têm acesso a esse espaço as grandes potências mundiais, mas a maioria dos países e elevado número de empresas comerciais na área de comunicações possuem, nesse lugar, algum satélite. A redução de custos e a evolução exponencial da tecnologia no setor ultraterrestre podem ter resultado no desenvolvimento de novas capacidades espaciais que afetarão a segurança nacional dos países. Já não há apenas a capacidade de observação e comunicação, mas as grandes potências têm desenvolvido sistemas antisatélite, veículos de exploração, de mineração espacial e supersônicos, que podem significar uma mudança nas estratégias espaciais dos líderes mundiais. O espaço ultraterrestre, enquanto um espaço geopolítico, terá um papel fundamental nas relações internacionais e, especialmente, nas operações militares.
Palavras-chave: Tecnologia; segurança; espaço ultraterrestre; capacidades espaciais; Marte.

1 INTRODUCCIÓN

Aunque no hay un acuerdo unánime sobre que es el dominio espacial, es comúnmente aceptado que es el área por encima de la corteza terrestre donde los efectos atmosféricos sobre los objetos en el aire se vuelven insignificantes. El mando espacial de los Estados Unidos (USSPACECOM) considera que el espacio ultraterrestre es el área que rodea la Tierra a altitudes iguales o mayor de 100 kilómetros (54 millas náuticas) sobre el nivel medio del mar. Aunque no existe un único criterio internacional acerca de la barrera en la que empieza el espacio ultraterrestre, la mayoría de los expertos estiman que esos 100 kilómetros son una buena referencia. Sin embargo, esta falta de definición de la frontera del espacio es un claro ejemplo de la falta de consenso internacional en cualquier aspecto relacionado con el espacio ultraterrestre, véase la regulación de las actividades, la exploración espacial, las orbitas de satélites, la gestión de la basura espacial, la proliferación no controlada de los satélites etc.

Al igual que sucede con el dominio aéreo, el terrestre y el marítimo, el espacio ultraterrestre es un dominio físico dentro del cual se realizan operaciones militares, civiles y se llevan a cabo actividades comerciales. El avance de la tecnología ha supuesto que cada vez se utilice más el dominio espacial; con más relevancia en los últimos años debido al auge del ciberespacio. Más que en cualquier otro dominio, la relación entre el espacio y el ciberespacio es única, en el sentido de que muchas operaciones espaciales dependen del ciberespacio, y una parte crítica del ciberespacio solo se puede proporcionar a través de operaciones espaciales.

El espacio ultraterrestre ha sido considerado durante varias décadas como patrimonio común de la humanidad en el que primaba el entendimiento y la colaboración científica. Prueba de ello son el *Corpus Iuris Spatialis*[1] que, de cierta manera regla la cooperación internacional en el espacio. Ejemplo de esta colaboración son la misión espacial internacional, en la que participan la NASA (Estados Unidos), Roscosmos (Rusia), JAXA (Japón), ESA (Europa), y la CSA (Canadá); así como los numerosos satélites de comunicaciones que proporcionan capacidad de navegación GPS, ancho de banda de conexión internet, información meteorológica, investigación científica etc. (ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL, 2002)

De los acuerdos que conforman el *Corpus iuris spatialis*, el Tratado del Espacio de 1967 constituye la piedra angular del marco legal internacional; sin embargo, no es un derecho impositivo, sino que se basa en las buenas intenciones y colaboración de los actores. En su artículo II afirma que "el espacio ultraterrestre, incluso la Luna y otros cuerpos celestes, no podrá ser objeto de apropiación nacional por reivindicación de soberanía, uso u ocupación, ni de ninguna otra manera", también en este artículo deja abierta la posibilidad de su explotación: "El espacio […] estará abierto para su exploración y utilización a todos los Estados" (PATEIRO, 2021, p. 287). En cuanto a su militarización, el artículo IV afirma lo siguiente: "Los Estados parte en el Tratado se comprometen a no colocar en órbita alrededor de la Tierra ningún objeto portador de armas nucleares ni de ningún otro tipo de armas de destrucción masiva, a no emplazar tales armas en los cuerpos celestes y a no colocar […] armas en el espacio ultraterrestre en ninguna otra forma. […]. Los demás artículos se basan en una mera declaración de buenas intenciones, que no hace más que confirmar que el espacio ultraterrestre se caracterice por una laxa legislación que no dispone ningún tipo de freno a la carrera tecnológica, de exploración e incluso de militarización.

2 DE LA COLABORACIÓN A LA COMPETICIÓN

A pesar de las colaboraciones y tratados de décadas pasadas, recientemente, el espacio ultraterrestre ha pasado a ser un campo de colaboración a un espacio geopolítico de competición en el que se potencia capacidades militares y se explotan recursos de todo tipo. Ciertamente, el espacio exterior y la tecnología

1 Los tratados de las Naciones Unidas que forman el Corpus Iuris Spatialis son los siguientes: Tratado sobre los principios que deben regir las actividades de los Estados en la exploración y utilización del espacio ultraterrestre, incluso la Luna y otros cuerpos celestes; Acuerdo sobre el salvamento y la devolución de astronautas y la restitución de objetos lanzados al espacio ultraterrestre; Convenio sobre la responsabilidad internacional por daños causados por objetos espaciales; Convenio sobre el registro de objetos lanzados al espacio ultraterrestre. Acuerdo que debe regir las actividades de los Estados en la Luna y otros cuerpos celestes.

están íntimamente relacionados; "se puede afirmar que la tecnología está asociada al desarrollo de capacidades militares" (BISBAL, 2021). De hecho, existen numerosos documentos y estudios estratégicos que así lo confirman. En el documento "Entorno Operativo 2035", se argumenta que en el espacio ultraterrestre se albergarán sistemas fundamentales para el desarrollo económico y social de los países, convirtiéndose, por ello, en objetivo valioso para Estados y organizaciones terroristas y criminales, como consecuencia de la progresiva accesibilidad y abaratamiento de la tecnología espacial; así, "el espacio ultraterrestre y su progresiva militarización exigirá el desarrollo y potenciación de sistemas espaciales" (MINISTERIO DE DEFENSA, 2019).

También la doctrina americana, entre otras muchas, advierte que el espacio es un entorno naturalmente peligroso y cada vez más congestionado, controvertido y competitivo. Los activos espaciales se enfrentan a muchas amenazas, tanto naturales como provocadas por el hombre. Estas amenazas pueden ser no intencionadas, por ejemplo, impacto por "basura espacial" o interferencia electromagnética, o intencionadas, a saber: las interferencias de señales, el empleo del láser, los ataques cibernéticos y mediante el uso de armas anti satélite, etc. (UNITED STATES, 2020). La Estrategia de Seguridad Nacional en 2017 (NSS) afirma que los Estados Unidos consideran esencial el acceso sin restricciones al espacio; además de que la libertad de operar en el espacio es un interés vital. Cualquier interferencia dañina o un ataque a componentes críticos de nuestra arquitectura espacial que afecte directamente a este interés vital de los EE.UU. se encontrará con una respuesta deliberada en el momento, lugar, manera y dominio elegido" (UNITED STATES, 2017); una clara declaración de intenciones que pone de manifiesto la relevancia para los EE. UU del espacio ultraterrestre.

En las últimas dos décadas numerosos actores internacionales, desde países como Estados Unidos o la India hasta empresas civiles como Space-X o Amazon, han invertido considerablemente en la explotación del espacio ultraterrestre, bien como inversión comercial en busca de beneficios económicos o como un "nuevo" dominio militar cuyo objetivo es tener una cierta superioridad en el espacio ultraterrestre, como anteriormente sucedió en los dominios tradicionales terrestre, aéreo o naval y, últimamente, el ciberespacio (FERNÁNDEZ-MONTESINOS, 2021). El espacio ya no es solamente utilizado por los países más avanzados tecnológicamente; ciudadanos de todo el mundo hacen uso de los servicios prestados por las capacidades espaciales o dependen de ellas; véase la navegación GPS, Google Maps, comunicaciones a larga distancia, internet, etc. Hoy en día, Google Maps y Bing Maps son servicios gratuitos que proporcionan un mapa de alta resolución de todo el mundo con resoluciones que hace sólo unos años únicamente estaban al alcance de la NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA).

Un ejemplo claro del aumento de la actividad en el espacio es la proliferación de empresas civiles en el ámbito de las telecomunicaciones. Impulsadas por el ritmo de SpaceX y OneWeb, a medida que las dos compañías han desarrollado sus redes de constelación de banda ancha de órbita terrestre baja (LEO), los despliegues de satélites de comunicaciones en 2020 aumentaron un 477% en comparación con 2019 (UNITED NATIONS, 2021). Sin embargo, los satélites de comunicaciones no fueron la única fuente de crecimiento espacial.

Hace ya una década, en el año 2007, China realizó con éxito una prueba anti-satélite (ASAT) sobre uno de sus satélites que orbitaba a una altura de 865 km, creando más de 35.000 piezas de escombros espaciales, lo que ese conoce como basura espacial (BROAD, William J.; SANGER, David E, 2007). La prueba ASAT supuso un notable aumento de la basura espacial en un 20 por ciento y recibió numerosas críticas de la comunidad internacional; sin embargo, no fue suficiente como para impedir que otros países continuaran por esta senda. Desde entonces, otros Estados, incluidos India, Rusia y Estados Unidos, han probado sistemas espaciales con capacidad de ataques cinéticos ASAT. En febrero de 2019, el primer ministro de la India, en una alocución televisada a todo el país, anunciaba que su país había derribado exitosamente un satélite a cientos de kilómetros de distancia, una clara advertencia a su eterno enemigo y vecino Paquistán (URRUTIA, 2019). Ciertamente, este acontecimiento ponía de manifiesto la llegada al espacio de numerosos actores, donde ya no sólo las grandes superpotencias tienen acceso al espacio ultraterrestre.

A finales del año 2019, Estados Unidos decidió crear un nuevo servicio dentro de sus Fuerzas Armadas: el United States Space Command (USSPACECOM). Según su propio mandato, el USSPACECOM tiene capacidades de vigilancia, control espacial y también de agresión o de combate en el espacio (UNITED STATES, 2019). Países como China, Rusia e Irán, entre otros muchos, han desarrollado capacidades militares espaciales de avanzada tecnología que, aunque todas parecen ser de ámbito defensivo, existen ciertas de ellas que son claramente ofensivas: como la citada ASAT o la de espionaje satelital (UNITED STATES, 2021). Aunque todavía no se ha llegado a ningún conflicto militar en el espacio, las estrategias de seguridad nacional de países como China, Estados Unidos o Rusia adelantan que es necesario prepararse para cualquier acción hostil que pudiera venir desde el espacio. Por ejemplo, el USSPACECOM en su estrategia espacial advierte que, debido al aumento de la tecnología, las nuevas amenazas y la situación geopolítica actual, el espacio permanecerá como un componente crítico de la forma de vida occidental y de la seguridad nacional. Evidentemente, un solo día sin las capacidades que ofrecen los satélites, véase comunicaciones, navegación de precisión, internet etc., podría tener consecuencias catastróficas en numerosos ámbitos, especialmente en la economía.

Además de lo anterior, numerosos expertos coinciden en que la expansión científica y militar de China en el espacio, especialmente desde su llegada a Marte, supondrá un cambio notable en las relaciones de colaboración que, hasta ahora, basadas en el *Corpus Iuris Spatialis*, han tenido lugar en el espacio ultraterrestre. La carrera espacial del siglo XXI ya ha comenzado y sus consecuencias pueden ser imprevisibles en un mundo global en el que, contrariamente a la primera carrera espacial donde la URSS y EE. UU eran los únicos competidores, numerosos actores con capacidades espaciales hacen que las consecuencias debidas a este desarrollo sean mucho más difíciles de predecir (DEFENSE INTELLIGENCE AGENCY, 2019). Consecuentemente, la militarización del espacio ultraterrestre parece ser inevitable, prueba de ello son los numerosos avances y las nuevas capacidades que numerosos países ya han desarrollado.

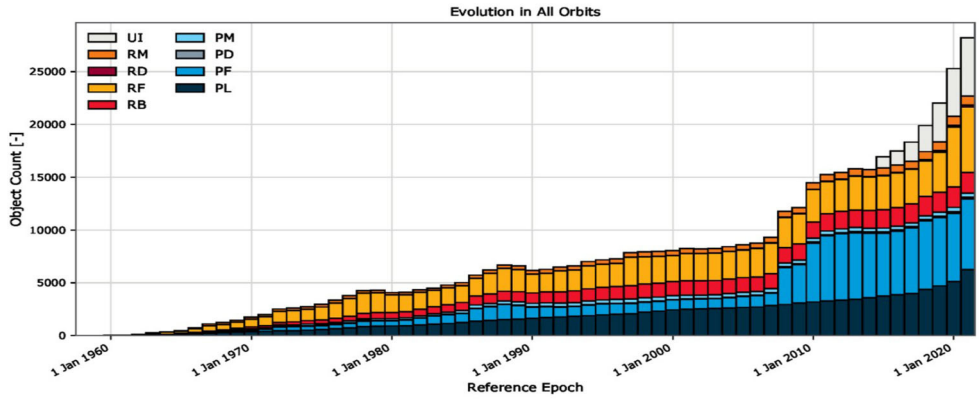
De la misma forma que sucedió con la evolución de las capacidades militares en el ámbito aéreo, se han creado nuevas capacidades, bien ofensivas o defensivas, que demuestran la militarización del espacio ultraterrestre. Al igual que el tratado de Chicago de 1944, que sentó las bases de la aviación comercial (ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL, 1944) no pudo impedir la militarización del espacio aéreo, los escasos tratados en materia del espacio, muy probablemente, no sirvan de freno a la inversión en capacidades militares espaciales (FERNÁNDEZ, 2021).

3 LA EVOLUCIÓN DEL ESPACIO

Los programas espaciales todavía se evalúan como un signo de prestigio nacional; el llegar al espacio supone proyectar el poder geopolítico y militar, así como tener conocimientos científicos y comerciales. Potencias como China, Europa, Francia, Alemania, India, Japón, la OTAN, Rusia, Estados Unidos y Reino Unido han anunciado públicamente sus capacidades espaciales y continúan construyendo infraestructura espacial; existen planes de al menos cinco nuevas estaciones espaciales para el año 2030.

Desde que la Unión Soviética lanzara el Sputnik, el primer satélite hecho por el hombre, en 1957, cada vez se han lanzado más objetos al espacio. Durante la segunda mitad del siglo XX, hubo un crecimiento lento pero constante, con aproximadamente de 60 a 100 satélites lanzados anualmente hasta principios de la década de 2010. En 2020, 114 lanzamientos transportaron alrededor de 1.300 satélites al espacio, superando la marca de 1.000 nuevos satélites por año por primera vez en la historia. Como se puede apreciar en la Ilustración 1. , el número de objetos en el espacio, desde cuerpos de cohetes, hasta escombros generados por el lanzamiento de satélites ha crecido exponencialmente en los últimos años.

Ilustración 1: Objetos en el espacio por tipo



Fuente: THE EUROPEAN SPACE AGENCY, 2020.

[PL = Carga útil (la "carga": generalmente uno o varios satélites que un cohete lanza al espacio); PF = Residuos de fragmentación de carga útil; PD = Residuos de carga útil; PM = Objeto relacionado con la misión de carga útil; RB = Cuerpo del cohete; RF = Escombros de fragmentación de cohetes; RD = Escombros de cohetes; RM = Objeto relacionado con la misión de cohetes; UI = No identificado.]

Hay dos razones principales que explican el crecimiento exponencial de los satélites en órbita en la última década. En primer lugar, nunca ha sido tan fácil lanzar un satélite al espacio desde el punto de vista de acceso a la tecnología. Por ejemplo, el 29 de agosto de 2021, un cohete SpaceX transportó varios satélites, incluido uno construido por estudiantes, a la Estación Espacial Internacional. En segundo lugar, los cohetes pueden transportar más satélites más fácilmente y a menor coste que nunca. Este aumento no se debe a que los cohetes sean más potentes, sino que los satélites se han vuelto más pequeños gracias a la revolución electrónica. La gran mayoría, el 94%, de todas las naves espaciales lanzadas en 2020 fueron satélites *smallsats*, que pesan menos de 600 kilogramos. La mayoría de estos satélites se utilizan para observación científica de la Tierra, para comunicaciones e Internet.

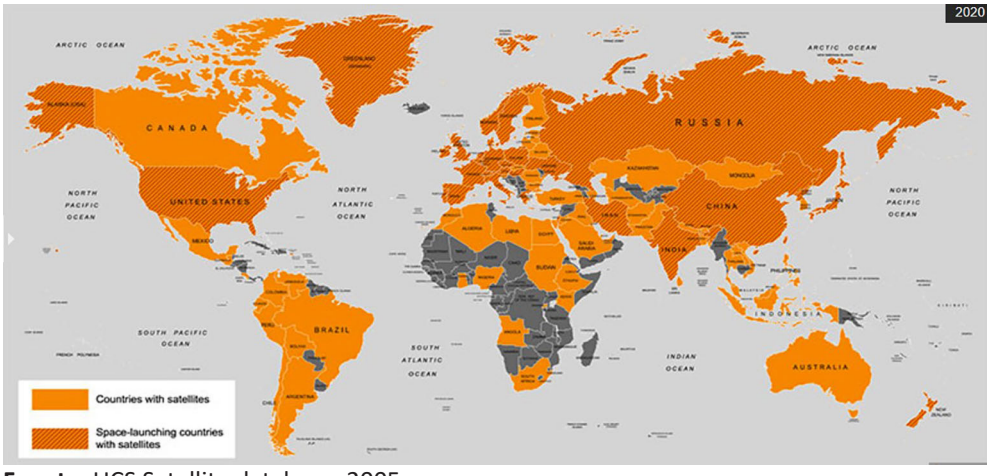
Con el objetivo de llevar Internet a áreas remotas de todo el mundo, dos compañías privadas, Starlink by SpaceX y OneWeb lanzaron casi 1,000 *smallsats* en 2020. Cada una de ellas planea lanzar más de 40,000 satélites en los próximos años para crear lo que se llama "megaconstelaciones" en la baja órbita terrestre. A medida que esta órbita se llena de satélites, especialmente *smallsats*, aumenta la preocupación por los desechos espaciales, al igual que la posibilidad real de colisiones debido a la congestión espacial, que también podría afectar a la seguridad nacional de muchos países.

Hace menos de 10 años, la democratización del espacio era un objetivo aún por alcanzar. Ahora, con proyectos estudiantiles en la estación espacial y más de 105

países que tienen al menos un satélite en el espacio, se podría argumentar que ese objetivo está ya al alcance. Sin embargo, fuera del ámbito comercial, actualmente, sólo nueve países y una organización internacional tienen capacidad para lanzar naves espaciales de forma independiente: China, India, Irán, Israel, Japón, Rusia, Corea del Norte, Corea del Sur, Estados Unidos y la Agencia Espacial Europea. En resumen, el número de objetos en órbita, tanto satélites activos como desechos orbitales, seguirá aumentando rápidamente, con una mayor disponibilidad de satélites pequeños y de menor costo y con la perspectiva de grandes constelaciones que consta de miles de satélites.

Según el Índice de Objetos Lanzados al Espacio Ultraterrestre, mantenido por la Oficina de asuntos del Espacio Ultraterrestre de las Naciones Unidas a finales de abril de 2021, había 7.389 satélites individuales en el espacio; un incremento del 27,97% respecto a 2020. La base de datos también muestra que desde su inicio se han lanzado 11.139 satélites, de los cuales solo 7.389 están en el espacio, mientras que el resto se han quemado en la atmósfera o han regresado a la Tierra en forma de escombros. Los 10 principales países que dominan la industria satelital son Estados Unidos, China, Rusia, Reino Unido, Japón, India, Agencia Espacial Europea, Canadá, Alemania y Luxemburgo; sin embargo, como se puede apreciar en la Ilustración 2, existe una gran cantidad de países con satélites en el espacio. Otros factores de desarrollo que causaron el aumento en el número de lanzamientos de satélites es la carrera por los servicios de banda ancha por satélite, especialmente la constelación de satélites Space X Starlink. En mayo de 2021, SpaceX lanzó 172 satélites Starlink en solo tres lanzamientos, lo que hace que su constelación supere los 1.600, mientras que OneWeb, propiedad parcial del Gobierno del Reino Unido, ha lanzado 72 satélites en 2021. En la Ilustración 3 se puede observar el número de satélites según su propósito declarado.

Ilustración 2: Número de países con satélites en 2020



Fuente: UCS Satellite database, 2005.

Ilustración 3: Número de satélites en órbita según el propósito.

Número de satélites	Propósito principal
1832 satélites	Comunicaciones
906 satélites	Observación de la Tierra
350 satélites	Desarrollo y demostración de tecnología
150 satélites	Navegación y posicionamiento
104 satélites	Ciencia espacial y observación
20 satélites	Ciencias de la Tierra
10 satélites	Otros fines

Fuente: UCS SATELLITE DATABASE, 2005.

Debido al aumento del número de satélites en órbita, el desafío de la congestión espacial será cada vez mayor y los actores espaciales necesitarán mejores capacidades para rastrear e identificar objetos y prevenir colisiones en el espacio. Recientemente, debido a la congestión espacial, China emitió una queja formal, en diciembre de 2021, contra Estados Unidos ante Naciones Unidas en la que asegura que, en dos ocasiones, dos satélites de Starlink, y la estación espacial del gigante asiático, Tiangong, tuvieron un peligroso incidente. Según Pekín, por motivos de seguridad, "la Estación Espacial de China se vio obligada a efectuar una serie de maniobras preventivas para evitar colisiones con dos satélites de Starling" (CHINA PRESENTA UNA QUEJA..., 2021). Por este motivo, las capacidades espaciales se han vuelto fundamentales para muchas operaciones militares, incluida la alerta de misiles, la geolocalización y la navegación, identificación de objetivos, inteligencia, reconocimiento y seguimiento de las actividades del adversario.

4 LA TECNOLOGÍA Y LAS CAPACIDADES MILITARES EN EL ESPACIO

Debido al abaratamiento de costes y a la proliferación de satélites de todo tipo, los satélites cada vez más proporcionan distintas capacidades que la tradicional de exploración aeroespacial, fotografía terrestre y enlace de comunicaciones. Además, la inversión en satélites en el ámbito de la defensa ha supuesto que también evolucionen las prestaciones y capacidades de los satélites.

Los satélites de comunicación proporcionan a usuarios de todo el mundo comunicaciones de voz, transmisión de señal de televisión, internet de banda ancha, servicio de telefonía móvil y servicios de transferencia de datos para civiles,

militares y comerciales. Además de lo anterior, existen muchas otras formas en que se utilizan los satélites de comunicaciones, algunas muy específicas, como los sistemas de comunicación de las redes de loterías nacionales en el Reino Unido y España, las cadenas de comercio de minoristas, los bancos en numerosas partes del mundo, las oficinas postales remotas en pequeños pueblos, el control de oleoductos y gasoductos, la previsión meteorológica, etc.

Cada vez con mayor frecuencia, los satélites se utilizan para sistemas de enseñanza telemática, telemedicina o videoconferencias que conectan a personas desde cualquier parte del mundo; muchos mandatarios de los países más poderosos del mundo tienen videoconferencias a menudo cuya conexión depende de satélites de comunicación. Además, en las partes más remotas y no tan remotas del mundo, las comunicaciones por satélite siguen desempeñando un papel fundamental en la infraestructura de telefonía y en servicios de internet. Los sistemas móviles satelitales, tanto regionales como globales, han sido concebidos para satisfacer nuestra demanda de estar conectados en cualquier momento y en cualquier lugar; en un mundo híper conectado, los satélites de comunicación juegan un papel clave. Las telecomunicaciones por satélite también pueden contribuir a la satisfacción de una amplia gama de requisitos institucionales: desde apoyar el desarrollo de las regiones menos favorecidas hasta la prestación de servicios de telecomunicaciones o telemedicina en situaciones de emergencia o desastre.

En el ámbito militar, las comunicaciones por satélite son esenciales en determinadas operaciones en zonas remotas donde no existe cobertura móvil o las comunicaciones estándares están degradadas. En la guerra de Afganistán, donde en numerosas ocasiones no existía cobertura móvil en zonas remotas, las comunicaciones vía satélite eran la única posibilidad de las tropas de coalición para comunicarse con la cadena de mando, pedir apoyo aéreo o evacuar personal de una determinada zona. El hecho de no tener esa capacidad de comunicación podría suponer el fracaso de la misión y el caer en manos de los talibanes. Este tipo de escenarios, donde sólo es posible comunicarse mediante comunicaciones vía satélite han puesto de manifiesto la relevancia de una robusta red de satélites. Especialmente en la forma de operar de occidente y en particular de la OTAN, donde el control centralizado es un requisito fundamental, la comunicación por satélite es, en la mayoría de los casos, la única forma de proporcionar un sistema de mando y control que funcione en cualquier parte del mundo.

Sin embargo, y a pesar de las ventajas de poseer un sistema potente de comunicaciones basadas en satélites, esto también puede ser una debilidad. El excesivo control por parte de la cadena de mando puede suponer que exista una elevada dependencia de autorizaciones para la ejecución por parte de los niveles superiores que, en un ambiente operacional volátil, incierto, complejo y ambiguo (VUCA por sus siglas en inglés), puede suponer una deficiencia que ponga en peligro cualquier misión. Así, la excesiva dependencia de un control centralizado

proporcionado por las comunicaciones satelitales disponibles hoy en día puede suponer una excesiva dependencia que, en caso de no estar disponible, pudiera traer consecuencias catastróficas. Además de las comunicaciones, el mando militar también depende notablemente de otras muchas capacidades que ofrecen los satélites en tiempo real y otras procedentes de naves espaciales, véase: la inteligencia, vigilancia y reconocimiento (ISR), la detección temprana de misiles, la capacidad anti satélite y la exploración espacial.

Los satélites ISR proporcionan apoyo civil, comercial y militar que son claves en una multitud de ámbitos; no sólo el militar sino también en el científico, como pudiera ser la monitorización del clima, de los cauces de los ríos, el tráfico aéreo o la vigilancia fronteriza, por ejemplo. Los satélites ISR civiles y comerciales proporcionan datos de teledetección, los cuales incluyen datos sobre la tierra, el mar y la atmósfera terrestre. Además, los satélites ISR apoyan una variedad de actividades militares al proporcionar inteligencia de señales, alerta de lanzamiento de misiles balísticos, evaluaciones de daños en el campo de batalla, conocimiento de la situación de las fuerzas amigas y enemigas, evaluación de la efectividad de una misión en una determinada operación, estimación instantánea del daño colateral por el empleo de un determinado armamento, etc.

Los satélites de inteligencia son claves en la mayoría de las operaciones militares que se desarrollan en escenarios VUCA[2] (acrónimo para volatilidad, incertidumbre (*uncertainty* en inglés), complejidad y ambigüedad). Existen una infinidad de operaciones militares en la que una información de inteligencia precisa y reciente es la clave del éxito o fracaso de éstas. Por ejemplo, la localización de los sistemas antiaéreos del oponente son claves para las operaciones aéreas que se llevan a cabo, en las que se incluyen el apoyo aéreo cercano a las tropas (CAS, por sus siglas en inglés). Una inteligencia errónea o incompleta podría suponer la pérdida de una aeronave o incluso de la superioridad aérea en un determinado momento, con las consecuencias que ello tendría en todos los dominios, no sólo el aéreo; sin duda, el dominio terrestre y el marítimo se verían también perjudicados por esta deficiencia.

Otro claro ejemplo de la necesidad de inteligencia son las operaciones contra células terroristas. En los últimos años, las operaciones contra el terrorismo han sido claves en la guerra de Afganistán e Irak, así como en la de Siria. Debido a que estas células suelen operar en zonas urbanas con presencia de población civil, el disponer de imágenes satélites con la suficiente definición como para monitorizar los movimientos de los terroristas es clave para el éxito de la operación. Los satélites "espías" no solamente proporcionan información de la posición de los terroristas, sino que pueden ser determinantes para abortar o "dar luz verde" en tiempo real mientras que las operaciones se están ejecutando.

2 La velocidad rige el mundo actual, y el mundo VUCA se relaciona a los imprevistos y a la velocidad que suceden en el mercado.

El reconocimiento aéreo ha sido durante décadas una de las pocas capacidades existentes para obtener información del enemigo o de la evaluación del resultado de una operación aérea. Sin embargo, con la evolución de los satélites y de su capacidad para fotografiar zonas con una precisión mayor o igual al de las aeronaves ha supuesto que los satélites ISR formen parte imprescindible de las operaciones modernas, en detrimento de las aeronaves de reconocimiento. Esta capacidad que ofrece los satélites ISR supone que el Mando militar tenga una conciencia situacional instantánea del "campo de batalla" y, por lo tanto, pueda tomar decisiones en tiempo real cuando las circunstancias así lo aconsejan. Sin embargo, el no disponer de esta capacidad produce el efecto contrario, ya que la cadena de mando se quedaría "ciega" en cuanto al conocimiento de la citada situación en el campo de batalla, sin poder tomar decisiones o dar órdenes conforme a lo que sucede en el terreno, lo que hace aún más valioso en las operaciones actuales en entornos VUCA.

La relevancia de los satélites ISR ha crecido exponencialmente y de una forma espectacular; ahora mismo es posible monitorizar a una persona e incluso saber la marca del reloj que viste. Lo que se consideraba alta resolución en los años 80, por ejemplo, los datos satelitales de la NASA de Landsat con sus 60 m por píxel, se ha vuelto insuficiente en los estándares actuales. Hoy por hoy, existen satélites comerciales que proporcionan una precisión de 30 cm por pixel. Aunque la resolución de los satélites militares es desconocida, se cree que las grandes potencias pueden poseer satélites que proporcionan resolución de centímetros.

Este aumento de la calidad de las imágenes proporcionadas por los satélites ISR ha supuesto una revolución en el planeamiento de muchas operaciones militares. Existen misiles como el Taurus alemán que basan su navegación en fotografías proporcionadas por satélites, que hace que no dependan de señal GPS o de navegación inercial. Esta capacidad de navegación que proporcionan las fotografías de alta resolución supone que los sistemas de armas no dependan de la señal GPS exclusivamente, por lo que las posibilidades de éxito son más elevadas que si dependiera solamente del GPS. Recientemente, durante una exhibición aérea en Bangalore, la compañía israelí Rafael Advanced Defense System afirmó que uno de sus misiles estrella aire-tierra, conocido como Rocks, utiliza un sistema de navegación para ubicar los objetivos usando sistemas ópticos y algoritmos avanzados de procesamiento de imágenes, lo que asegura alcanzar objetivos con gran precisión, superando la interferencia o negación del GPS. La utilización de este tipo de navegación es una realidad en los sistemas de armas más modernos, especialmente con la proliferación de sistemas perturbadores de GPS que vuelven inútil este tipo de navegación.

5 LOS MISILES HIPERSÓNICOS Y LA DEFENSA ANTIMISILES

Debido a la amenaza que supone la proliferación de misiles balísticos, especialmente si estos tienen cabezas nucleares, la alerta de lanzamiento de misiles

es una de las capacidades en las que más se está desarrollando. Para reaccionar ante un ataque de misiles balísticos, un sistema anti-misiles utiliza sensores espaciales y terrestres para alertar a los centros de control acerca de este tipo de ataque, con el objetivo de tener tiempo para preparar una respuesta. Los sensores espaciales suelen proporcionar la primera indicación de un lanzamiento y los radares terrestres proporcionan información de seguimiento y confirman el ataque.

Recientemente, se han desarrollado nuevas amenazas, como las armas hipersónicas diseñadas para romper la red de defensa antimisiles de los países con mayor desarrollo en este campo. Por ejemplo, algunos países están adoptando el vehículo hipersónico de planeo (HGV, por sus siglas en inglés). Aunque no se sabe con certeza, se cree que el HGV es generalmente difícil de interceptar por un sistema de defensa antimisiles, ya que después de ser lanzado por un misil balístico, vuela a una velocidad ultra rápida, a baja o alta altitud, y con una gran movilidad. Los misiles HGV son proyectiles de una elevada potencia que pueden alcanzar cualquier punto en la tierra y volar a una velocidad entre cinco y veintisiete veces la velocidad del sonido a una altura de hasta cien kilómetros, y cargar ojivas convencionales o nucleares. Este pico elevado de velocidad supone que la detección temprana sea clave, pues una demora podría suponer que ya no se tuviera tiempo material para responder al ataque. Además, el tiempo disponible para una adecuada respuesta se ve disminuido considerablemente; por ejemplo, teniendo en cuenta la distancia entre Corea del Norte y Estados Unidos, el régimen de Kim Jong Un podría alcanzar la costa de California en menos de veinte minutos con uno de estos misiles. Aunque pueda ser una entelequia el disponer de esta tecnología para un país como Corea del Norte, otros como China o Rusia sí podrían disponer de la capacidad requerida.

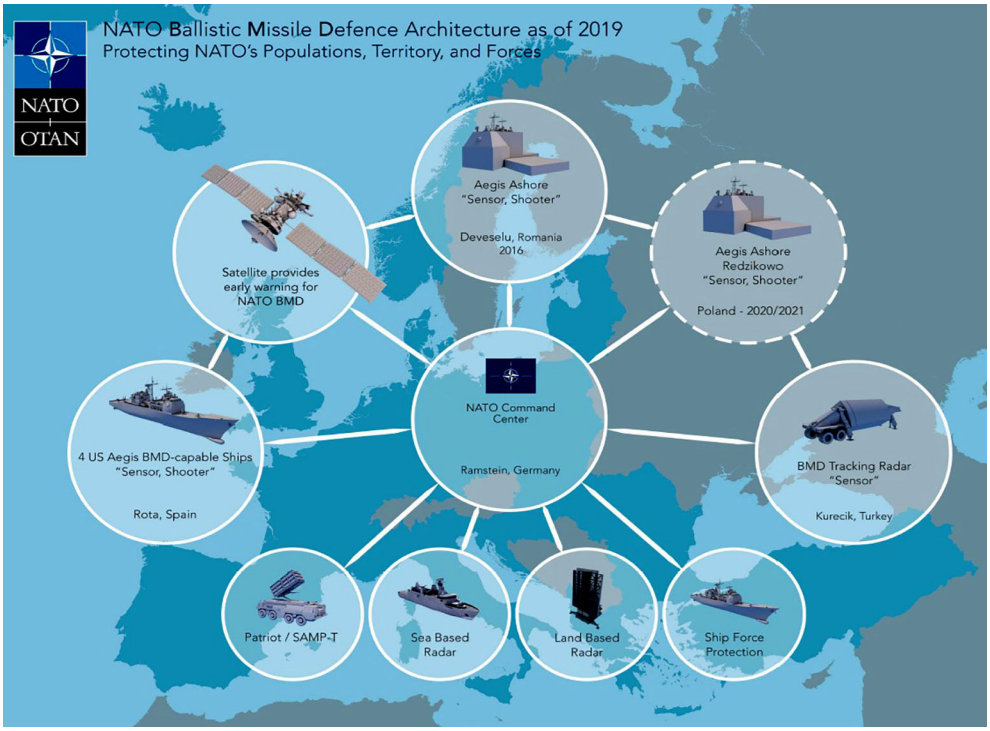
Tanto China como Rusia han invertido en el desarrollo de estos misiles hipersónicos y están en mejor posición que sus competidores occidentales. En marzo de 2018, Moscú afirmó que había lanzado con éxito una de sus seis armas "invencibles". Se trató del misil hipersónico Kinzhal, con velocidades superiores a diez veces la velocidad del sonido y que, según el presidente ruso Vladimir Putin, es invulnerable a los sistemas actuales de defensa aérea y antiaérea de occidente. China, por otro lado, realizó un exitoso test de uno de sus misiles hipersónicos en julio de 2021 en el mar del sur de la China. En este caso, lo más llamativo de la prueba es que el misil fue lanzado desde el aire mediante un vehículo espacial, lo que proporciona al misil un mayor alcance y mayor velocidad.

En resumen, el desarrollo y despliegue de sistemas de armas hipersónicas proporcionará a los Estados una capacidad de ataque significativamente mayor y, potencialmente, los medios para coaccionar a otros Estados que no tengan desarrollada esta capacidad. Por ejemplo, Rusia, podría coaccionar a un país vecino, mediante la amenaza de ataques hipersónicos contra objetivos críticos, y conseguir objetivos políticos. Corea del Norte, por su parte, también podría utilizar esta capacidad para aislar a su régimen de cualquier presión extranjera y de Estados Unidos en particular.

China, debido a su política expansionista, también podría utilizar los misiles hipersónicos para mantener alejado a Estados Unidos del mar de la China y en breve espacio de tiempo conseguir objetivos que hasta hace unas décadas parecían inalcanzables; como la anexión de Taiwán o la soberanía de las multitudes de islas en disputa con Filipinas. Por ello, la proliferación de capacidades hipersónicas en los Estados regionales también podría ser desestabilizadora, alterando los equilibrios de poder regional.

Debido a la aparición en escena de estos misiles, los distintos actores internacionales tendrán que desarrollar un sistema de defensa anti misiles suficientemente robusto como para poder contrarrestar la amenaza que supone esta nueva capacidad. La OTAN, por ejemplo, ha desarrollado una estructura muy sólida de defensa de misiles. Como se puede apreciar en la Ilustración 4, la defensa se basa en numerosos elementos, a saber: radares en tierra, satélites en el espacio, sistemas de alerta en buques de guerra, centros de control, etc. Para coordinar los elementos que suponen un sistema de defensa anti misiles, las comunicaciones serán claves, teniendo en cuenta el poco tiempo que se dispone debido a las altas velocidades de los misiles. Así, los satélites de comunicaciones serán todavía esenciales para la transmisión de información a la cadena de mando.

Ilustración 4: Sistema De Defensa Antimisiles De La OTAN.



Fuente: NORTH ATLANTIC TREATY ORGANIZATION, 2016.

6 LA CAPACIDAD ANTI SATÉLITE ASAT

La capacidad anti satélite viene definida por la posibilidad de incapacitar o destruir satélites con fines militares. Debido al desarrollo tecnológico y la inversión de numerosos países en misiles capaces de llegar al espacio ultraterrestre, esta capacidad es ya una realidad no sólo en el caso de Estados Unidos, que hizo su primer teste en 1985 o la URSS en 1973, sino que otros países como China o la India también han demostrado con sus respectivos ensayos poseer esta capacidad. Una capacidad que se ha desarrollado mediante el disparo desde tierra, pero que en un futuro muy cercano existirán satélites que puedan derribar o dejar fuera de servicio otros satélites utilizando energía dirigida.

Particularmente China ha invertido grandes sumas de dinero en desarrollar y mejorar sus capacidades anti satélites, apostando por la investigación y el posible desarrollo de armas de energía dirigida y de bloqueo de satélites y, probablemente, ha avanzado en el sistema de misiles anti satélite que ya probó en julio de 2014. Aunque China no ha reconocido públicamente la existencia de cualquier programa nuevo desde 2007, escritos del PLA enfatizan en la necesidad de "destruir, dañar, e interferir con el reconocimiento del enemigo y degradar sus satélites de comunicaciones ", lo que supone un giro de la estrategia espacial china basada en la exploración e investigación en el espacio hacia adquirir capacidades ofensivas espaciales.

Después de la caída del muro de Berlín, Rusia parecía haber "dado un paso atrás" en la carrera espacial tecnológica y militar. Sin embrago, el 15 de noviembre de 2021, Rusia probó un misil anti satélite de ascenso directo (DA-ASAT) que impactó contra un satélite ruso, el Cosmos 1408, creando un considerable número de desechos espaciales en la órbita terrestre baja. Según el U. S Space Command la prueba generó más de 1.500 piezas de desechos orbitales rastreables y probablemente generará cientos de miles de piezas más pequeñas (UNITED STATES, 2021). Como consecuencia de estas pruebas, el general del US. Space Command, James Dickinson, declaraba que "Rusia había demostrado un desprecio deliberado por la seguridad, la protección, la estabilidad y la sostenibilidad a largo plazo del dominio espacial para todas las naciones", afirmando además que la prueba realizada por Rusia suponía " una amenaza para las actividades en el espacio exterior durante los próximos años, poniendo en peligro los satélites y las misiones espaciales, además de obligar a realizar más maniobras para evitar colisiones" (UNITED STATES, 2021). Por otro lado, y como respuesta a las acusaciones vertidas por el general americano, Moscú se defendía afirmando que Estados Unidos, China e India también han demostrado capacidades parecidas en el pasado, realizando pruebas similares y que el gobierno de Estados Unidos se negaba a cooperar y avanzar en las propuestas de Rusia y China para los acuerdos de control de armas en el espacio.

El desarrollo tecnológico en el campo de la capacidad anti satélite, supondrá que los satélites del futuro puedan realizar maniobras de evasión ante cualquier amenaza, bien proveniente desde la tierra o desde el propio espacio que pudiera comprometer su seguridad. No sólo eso ofrecerán los satélites en el futuro, sino que, al igual que sucedió con la evolución de las capacidades de las aeronaves en décadas pasadas, existirán satélites de escolta o protección de otros satélites, así como la capacidad ofensiva de satélites que podrán dejar inútiles o directamente derribarán a otros satélites, bien sea mediante el uso de energía dirigida, el empleo del láser o una determinada carga explosiva. Además de esto, la guerra electrónica en el espacio tendrá que ser otro elemento clave para tener en cuenta si se quiere tener una cierta libertad de acción o superioridad espacial en el espacio. En resumen, para poder tener una cierta libertad de acción en el espacio, las capacidades espaciales deberán incluir defensa anti misil y también defensa contra otros satélites de capacidades ofensivas.

7 LA EXPLORACIÓN ESPACIAL

A pesar de las numerosas misiones Apolo del siglo XX que aterrizaron en la Luna, no hubo evidencia alguna de existencia de agua o de minerales raros hasta que, más de 30 años después, en 2008, la India lanzara su primera misión a la Luna que incluía una sonda de impacto lunar con el objetivo de analizar su suelo. Este experimento permitió que el Mapeador de Mineralogía Lunar de la NASA detectase señales claras de agua (LOVEGREN, 2019) y estableciese una estimación de más de 1.600 millones de toneladas almacenadas en los polos lunares. Este descubrimiento, unido a la presencia de tierras raras, supuso que la Luna sea uno de los mejores candidatos para la extracción de materias primas, minerales y recursos más allá de la Tierra.

Los metales de tierras raras, o simplemente “tierras raras”, son materiales esenciales e irremplazables que se utilizan en la mayor parte de la tecnología moderna; desde 1985, China ha ganado sistemáticamente un control casi completo sobre la cadena de suministro global de esas tierras. El futuro de la seguridad de muchos países occidentales y del mundo estará directamente ligado a la disponibilidad de los recursos que proporcionan las tierras raras. No asegurar los recursos necesarios para seguir el ritmo de la innovación tecnológica significa no seguir siendo competitivos a nivel mundial (DIZIAMA, Brendan P.; CHOMÓN PÉREZ, Juan Manuel; GANSER, Andreas, 2022). Aunque se utilizan en cantidades muy pequeñas, su importancia para el sector de defensa de Estados Unidos y para las tecnologías emergentes y potencialmente disruptivas, combinada con el control de China sobre la mayoría del mercado, ha dado a los elementos de tierras raras una relevancia geopolítica descomunal. Los elementos de tierras raras ya son críticos para el sector de defensa de los Estados Unidos y de numerosos países, pero las

capacidades de minería, procesamiento y fabricación de tierras raras influirán aún más fuertemente en la dinámica geopolítica en los próximos años a medida que el mundo experimente su naciente transición energética y evolución del transporte (THE GEOPOLITICS..., 2019).

Según numerosos expertos, existen aproximadamente 140 millones de toneladas de reservas globales de tierras raras; con 55 millones y 35 millones de toneladas respectivamente, China e India poseen más de dos tercios de las reservas mundiales, muy por delante de Estados Unidos con 13 millones de toneladas. Por ello, la búsqueda de estas tierras en el espacio es una alternativa muy valiosa para la seguridad nacional de Estados Unidos (GUEDIN, 2019). Para sorpresa de muchos, pero con una relevancia que podría afectar a la seguridad nacional, tanto en la Luna como en Marte existe una gran cantidad de tierras raras que hace que la exploración espacial afecte a la seguridad nacional de los países con más poder que busquen tener autonomía en la obtención de recursos que se utilizan en la tecnología. En resumen, la necesidad de determinados recursos y nuevos terrenos explotables está poniendo de manifiesto la imposibilidad futura de continuar con un modelo de vida que el planeta Tierra no podrá sustentar. En otras palabras, "la Tierra se nos está quedando pequeña" (DOMINGUEZ, 2021).

En 2013, China se convirtió en el primer país en aterrizar una misión en la superficie de la Luna desde que lo hiciera la Unión Soviética en 1976. Esta misión de exploración lunar podría tener consecuencias en el panorama geopolítico internacional, debido a que la Luna podría ser rica en tierras raras que no abundan en la Tierra; como ya se ha comentado, unas tierras ricas en minerales necesarios para la tecnología actual como los móviles y ordenadores. Numerosos expertos afirman que existe una elevada posibilidad de que la Luna almacene gran cantidad de minerales de tierras raras, escasos en la Tierra y esenciales para la electrónica, pero también para los sistemas de guía de misiles y para las plataformas militares; como aviones de caza y ataque, fragatas y submarinos. Además de esto, también se cree que la Luna podría poseer grandes cantidades de Helio-3[3], un mineral con una gran capacidad de generar energía limpia, lo que supondría el no depender de los fósiles (FERNÁNDEZ DE BOBADILLA, 2021). Esto supondría que la exploración lunar y también espacial en busca de minerales preciados adquiriera una especial relevancia en los próximos años. De hecho, durante el mes de noviembre de 2019, la nave Chang'e-5 convirtió a China en el primer país en más de cuatro décadas en traer de vuelta muestras de suelo y rocas lunares para su estudio.

Como es sabido, China es uno de los países que mayores índices de contaminación tiene en el planeta; su dependencia del gas y de energías fósiles ha supuesto que tenga numerosos problemas de contaminación a lo que la única

3 El He-3 es un isótopo estable del helio que podría emplearse para producir energía mediante fusión nuclear, un proceso más limpio y eficiente que el de la fisión.

solución es el consumo de energías limpias. Para ello, China ya ha trazado un mapa de la superficie de la Luna utilizando los datos recibidos de las sondas Change 1 y 2, y ha estimado que existe alrededor de un millón de toneladas de He-3 en ella. Teniendo en cuenta que la demanda anual de energía china es de unos 220 millones de toneladas de petróleo o alrededor de 1.000 millones de toneladas de carbón, solamente se necesitarían ocho toneladas de He-3 (LELE, 2012) para contrarrestar esa dependencia, lo que hace que la exploración lunar sea rentable desde el punto de vista energético y económico para China.

China planea convertirse en un líder internacional en investigación y exploración lunar con el objetivo de instalar una estación de investigación lunar a partir de 2025, realizar una misión tripulada con aterrizaje en la Luna en 2036, y establecer una Base de Investigación y Desarrollo Lunar alrededor en el año 2050. Referente a la exploración lunar, Estados Unidos no debería quedarse atrás, especialmente por haber sido el primer país en enviar un hombre a la Luna. Para contrarrestar la posición china, Estados Unidos está desarrollando la iniciativa Lunar Catalyst (Lunar Cargo Transportation and Landing by Soft Touchdown); un ambicioso proyecto adoptado tanto por la NASA como por el sector espacial privado de los Estados Unidos y financiado por las principales compañías mineras que se ven atraídas por las grandes reservas de tierras raras en la corteza lunar (GUEDIM, 2019). Este programa lunar busca desarrollar robots de prospección y nueva tecnología que se utilizará para extraer minerales en la Luna; también podrían abordar la demanda emergente del sector privado para llevar a cabo actividades en la Luna (NATIONAL AERONAUTICS AND SPACE ADMINISTRATION, 2022). Esta creciente inversión en tecnología, en parte arrastrado por el descubrimiento de tierras raras, ha supuesto que se disponga de la capacidad de explorar otros planetas, incluido Marte.

A pesar de que la luna es el satélite más cercano a la Tierra, en los últimos años ha despertado un interés notable en la exploración de Marte. En las dos últimas décadas, las misiones que ha llevado a cabo el Programa de Exploración de Marte de la NASA han mostrado que Marte fue una vez muy diferente del planeta frío y seco que es hoy. Las pruebas descubiertas por las misiones terrestres y orbitales apuntan a condiciones húmedas de hace miles de millones de años. Estas condiciones duraron lo suficiente como para que se desarrollase la vida microbiana, lo que hace que Marte sea un planeta de notable interés para tanto China como Estados Unidos.

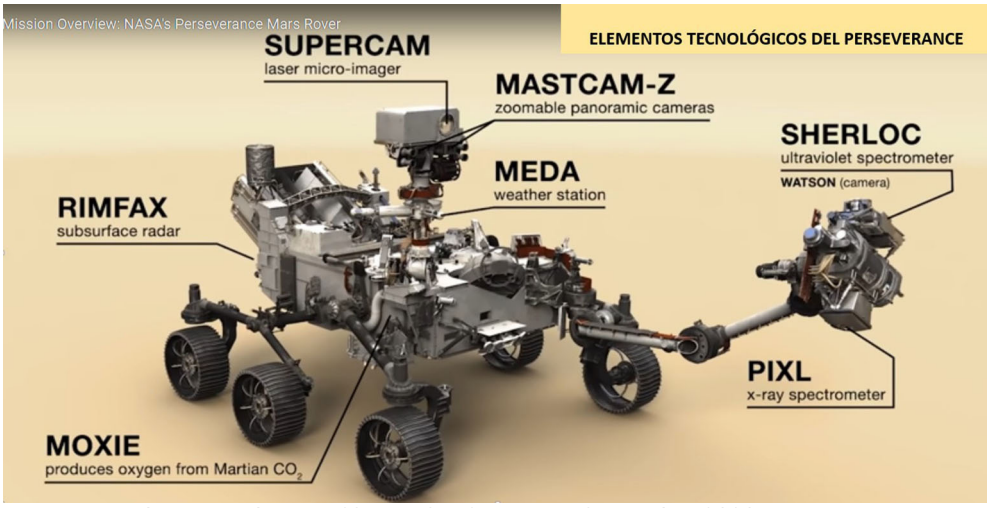
Con el objetivo de ser el primer país en llegar a Marte y también de explorar la corteza del planeta, Los Estados Unidos lanzaron el vehículo “Mars 2020/ Perseverance” en agosto de 2020 desde la estación de Cabo Cañaveral, en Florida. El aterrizaje en Marte tuvo lugar el 18 de febrero de 2021 en un antiguo delta fluvial de un lago que una vez llenaba el cráter Jezero. El Perseverance estará al menos un año marciano (dos años terrestres) explorando la región del lugar de aterrizaje, lo que proporcionará a Estados Unidos información geológica del terreno, testará la tecnología para futuras exploraciones en Marte u otros planetas y, especialmente,

almacenará piezas de rocas para posterior análisis en la Tierra en futuras misiones de la NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA).

El Perseverance posee unas capacidades tecnológicas que serán claves en la futura exploración espacial y que darán a Estados Unidos un elevado conocimiento del planeta rojo que, a su vez, podría ser clave en la exploración de otros planetas, además de la obtención de minerales raros al igual que lo ha sido la Luna. El Perseverance ofrece las siguientes posibilidades:

- Un avanzado sistema de cámaras con capacidad de imagen panorámica y estereoscópica con capacidad de zoom, para determinar la mineralogía de la superficie marciana y el análisis de la composición química.
- Un espectrómetro de fluorescencia de rayos X y un generador de imágenes de alta resolución para cartografiar la composición elemental de los materiales de la superficie marciana.
- Un espectrómetro que proporcionará imágenes a escala fina y utiliza un láser ultravioleta (UV) para cartografiar la mineralogía y los compuestos orgánicos.
- Un experimento que producirá oxígeno a partir del dióxido de carbono atmosférico marciano.
- Un radar de penetración terrestre que proporcionará resolución a escala centimétrica de la estructura geológica del de la sub superficie.

Ilustración 5: Elementos tecnológicos del Perseverance.



Fuente: NATIONAL AERONAUTICS AND SPACE ADMINISTRATION, 2020.

Al igual que hiciera Estados Unidos, China también ha llegado a Marte, con el objetivo de explorar el planeta en busca de posibles recursos y fuentes de energía.

Tianwen-1 (TW-es una misión interplanetaria de la Administración Nacional del Espacio de China (CNSA) que ha conseguido enviar una nave espacial robótica a Marte, que consta de 6 naves espaciales: un orbitador, dos cámaras desplegables, un módulo de aterrizaje, una cámara remota y el rover Zhurong (MYERS & CHANG, 2021). La nave, con una masa total de casi cinco toneladas, es una de las sondas más pesadas lanzadas a Marte y lleva una instrumentación científica de última tecnología. Es la primera de una serie de misiones previstas por la CNSA en el marco de su programa de Exploración Planetaria de China. Los objetivos científicos de la misión china incluyen los siguientes: la investigación de la geología de la superficie marciana y la estructura interna, la búsqueda de indicios de la presencia actual y pasada de agua, y la caracterización del entorno espacial y la atmósfera de Marte.

La misión fue lanzada desde el sitio de lanzamiento de naves espaciales de Wenchang el 23 de julio de 2020 en un vehículo de lanzamiento pesado Long March 5 (Jones, 2020). Tras siete meses de tránsito hacia Marte, la nave entró en la órbita marciana el 10 de febrero de 2021. Durante los tres meses siguientes, la sonda analizó los posibles emplazamientos de aterrizaje mediante una órbita de reconocimiento. Así, el 14 de mayo de 2021, el módulo Rover aterrizó con éxito en Marte, convirtiendo a China en la tercera nación en aterrizar en la superficie marciana y en establecer comunicación desde Marte, después de la Unión Soviética y los Estados Unidos.

Después del Rover Perseverance de Estados Unidos, Dianwen-1 es la segunda misión que capta grabaciones de audio en la superficie marciana. El "smallsat" desplegado por el rover Zhurong en la superficie marciana consiste en una cámara que fotografió tanto al propio rover como al módulo de aterrizaje de Tianwen-1. Con una masa inferior a 1 kg, la cámara remota de Tianwen-1 es el objeto artificial más ligero en Marte desde mayo de 2021. El 31 de diciembre de 2021, el orbitador Tianwen-1 desplegó una segunda cámara desplegable (TDC-2) en la órbita de Marte que capturó fotografías del Tianwen-1 en órbita para celebrar el fin de año.

Al igual que la misión americana, China tiene unos determinados objetivos científicos que pueden suponer una ventaja en recursos necesarios para la fabricación de tecnología o la obtención de materiales raros. En concreto, los objetivos científicos de Tianwen-1 incluyen: cartografiar la morfología y la estructura geológica, investigar las características del suelo de la superficie y la distribución del agua-hielo, analizar la composición del material de la superficie, medir la ionosfera y las características del clima y el entorno marciano en la superficie, y percibir los campos físicos (electromagnéticos, gravitatorios) y la estructura interna de Marte.

Sin duda, la exploración espacial es un claro ejemplo de la relevancia del espacio ultraterrestre. Un espacio geopolítico que ha tomado cada vez más relevancia en los últimos años. Debido a la evolución tecnológica, seguirá siendo clave no sólo para la seguridad nacional de los Estados, sino que también para las empresas comerciales que tengan intereses en la tecnología, las comunicaciones y la investigación espacial.

8 CONCLUSIONES

Aunque el espacio representa una posibilidad de cooperación internacional en el campo de la tecnología y la ciencia, su falta de legislación, su más que posible militarización y la existencia de recursos minerales tanto en Marte como en la Luna supondrá que exista una enorme competición entre las superpotencias por el dominio espacial que, eventualmente, supondrá el inicio de una nueva carrera espacial. Esta nueva carrera espacial, muy probablemente, tendrá consecuencias en el ámbito de la defensa; las posibilidades que ofrece el espacio en cuanto inteligencia y capacidades militares supondrá que los Estados tengan que invertir recursos para el desarrollo de capacidades que hoy en día no tienen. Al igual que sucediera durante la Guerra Fría, se avecina una competición en el espacio que, debido a su aceptable coste y a la multitud de actores, no solo estatales sino también civiles, será más compleja e impredecible que anteriormente.

Con motivo de esta carrera espacial y la militarización del espacio ultraterrestre, el gobierno americano decidió crear un nuevo servicio dentro de sus Fuerzas Armadas: el USSPACECOMMAND; con capacidades espaciales de vigilancia y control espacial encuadradas en el ámbito defensivo, pero también con capacidades ofensivas. Sin embargo, Estados Unidos no está sólo en la militarización del espacio, países como China, Rusia e Irán, entre otros muchos, han desarrollado capacidades militares espaciales de avanzada tecnología que, aunque todas parecen ser de ámbito defensivo, existen ciertas de ellas que son claramente ofensivas: como la discutidas ASAT y espionaje satelital.

La proliferación y la competición en el espacio también han supuesto que la "basura espacial" sea un fenómeno a tener en cuenta. Existen millones de piezas de desecho espacial volando en la órbita baja del espacio, por ejemplo: satélites inservibles, naves espaciales, pequeñas manchas de pintura de naves espaciales, partes de cohetes, objetos que son resultado de explosiones en el espacio debido a las pruebas anti satélites, etc. En los próximos años, el desafío de la congestión espacial será cada vez mayor y los Estados y también las empresas civiles necesitarán mejores capacidades para rastrear e identificar objetos y prevenir colisiones en el espacio. En definitiva, la tecnología tendrá cada vez más relevancia debido a la "basura espacial".

La basura espacial y la velocidad con que se están adquiriendo nuevas capacidades militares en el espacio, supondrá un problema de seguridad para todos los países en general, incluidos China y Estados Unidos. En el ámbito militar, las comunicaciones por satélite son esenciales en numerosas operaciones donde las comunicaciones no están aseguradas, o se necesitan comunicaciones vía satélite, especialmente por el ancho de banda que ofrece el espacio ultraterrestre. Está capacidad ha marcado la diferencia de los ejércitos más poderosos respecto a otros de menor tecnología militar que apenas tenían acceso a los satélites; sin embargo, con la actual reducción de costes y la proliferación satelital, cada vez más países

tendrán enlace a los satélites, lo que disminuirá la diferencia tecnológica entre la mayoría de las fuerzas armadas. Por lo tanto, las comunicaciones satélites serán una capacidad esencial y básica, pero no diferenciadora.

Al igual que los satélites de comunicaciones, los satélites de inteligencia han demostrado ser claves en la mayoría de las operaciones militares que se desarrollan en escenarios complejos y muy cambiantes, en los que poseer información del enemigo actualizada e inmediata es esencial. Existen una infinidad de operaciones militares en la que una información de inteligencia precisa y reciente ha sido la clave del éxito o fracaso. En la actualidad, la inteligencia se ha convertido en un requisito indispensable en el que los satélites de alta definición son cada vez más necesarios en el entorno VUCA.

Las armas hipersónicas diseñadas para romper el sistema de defensa antimisiles de los países que cuentan con estos sistemas es otro ejemplo que escenifica lo que está evolucionando la tecnología en el espacio ultraterrestre. El vehículo hipersónico de planeo HGV supone un cambio de paradigma en el tiempo de reacción de los sistemas de mando y control; el tiempo para tomar una decisión se reduce considerablemente y ya no hay "lugar para la duda" o el análisis minucioso. Ahora más que nunca, un fallo en las comunicaciones puede ser catastrófico con un misil HGV en el aire-espacio. Debido a su vuelo a velocidad ultra alta y a baja o alta altitud con una gran movilidad, los misiles HGV son casi imposibles de interceptar, por lo que se entra en un escenario de destrucción mutua asegurada, como ocurriera con las armas de destrucción masiva.

El desarrollo tecnológico en el campo de la capacidad anti satélite supondrá que los satélites del futuro evolucionarán para tener la capacidad de realizar maniobras de evasión ante cualquier amenaza que pudiera comprometer su seguridad, bien proveniente desde la tierra o desde el propio espacio. Además de la propia capacidad de evasión, en breve espacio de tiempo se desarrollarán satélites de escolta o protección de otros satélites, como así sucedió con la rápida evolución de la aviación de combate después de la Segunda Guerra Mundial y especialmente con la llegada del motor a reacción. Por lo tanto, los satélites con capacidad de lanzar energía dirigida para dejar inservible otro satélite será un requisito de las fuerzas espaciales no sólo para tener capacidad ofensiva, sino también como disuasión ante los satélites del enemigo. En definitiva, los satélites ya no solamente se usarán para la transmisión de datos y comunicaciones, sino que también tendrán capacidades ofensivas e incluso de escolta de otros satélites.

Debido a la evolución tecnológica, la cual ha supuesto un enorme abaratamiento de costes, la exploración espacial será una de las protagonistas indiscutibles en el espacio ultraterrestre. Los metales de tierras raras son cada vez más necesarios en la industria tecnológica y su escasez es uno de los motivos por lo que estos minerales están cada vez más presentes en las estrategias de los actores más relevantes. Para muchos expertos, el futuro de la seguridad de muchos países occidentales y del mundo estará directamente ligado a la disponibilidad de

los recursos que proporcionan estas tierras raras. La existencia de estos minerales tanto en la Luna como en Marte y su posibilidad de explotación es todavía una pregunta abierta, pero que pone de manifiesto la necesidad de invertir en la exploración espacial. El país que consiga controlar la explotación de tierras raras en otros planetas, debido a su escasez en la Tierra y su necesidad para la industria tecnológica, tendrá una posición de privilegio en un sector tan importante para la seguridad como lo es el tecnológico.

En resumen, debido a su relevancia para la seguridad, el espacio ultraterrestre se deberá considerar como un espacio geopolítico más, en el que las grandes potencias se disputarán su control y su explotación. Las posibilidades que ofrece el espacio ultraterrestre en cuanto a tecnología e inversión económica y mineral son casi infinitas, que además podría ser la respuesta en cuanto al agotamiento de recursos en la Tierra. La literatura espacial encabezada por Julio Verne hace casi un siglo empieza a ser una realidad, con todas las consecuencias que ello conlleva para la seguridad internacional. Aquel país que más invierta en el espacio ultraterrestre tendrá una ventaja sustancial en las próximas décadas que, en última instancia, supondrá una clara ventaja para el dominio de la geopolítica mundial aquí en la Tierra.

REFERENCIAS

AGENCY, D. I. *Challenges to Security in Space*. Washington: Disponible en: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf. Accedido en: 7 enero 2019.

BISBAL, F. *El Espacio Exterior*: un nuevo dominio de confrontación. [*S.l.: s.n*.], 2021.

BROAD, William J.; SANGER, David E. Flexing Muscle, China Destroys Satellite in Test. *New York Times*, New York, 19 Jan. 2007.

CHINA presenta una queja contra EE UU ante la ONU tras un incidente con la compañía de Elon Musk en el espacio. *El País*, Pekin, 28 dic. 2021. Disponible en: https://elpais.com/ciencia/2021-12-28/china-presenta-una-queja-contra-ee-uu-ante-la-onu-tras-un-incidente-con-la-compania-de-elon-musk-en-el-espacio.html Accedido en: 28 dic. 2021.

DEFENSE INTELLIGENCE AGENCY. *China Military Power*. Washington, DC: DIA, 2019.

DIZIAMA, Brendan P.; CHOMÓN PÉREZ, Juan Manuel; GANSER, Andreas. Rare earths: fighting for the fuel of the future. *The Diplomat*, 22 enero 2022. Disponible en: https://thediplomat.com/2022/01/rare-earths-fighting-for-the-fuel-of-the-future/. Accedido en: 7 enero 2022.

DOMINGUEZ, F. M. *Geopolítica espacial y búsqueda de recursos*. Madrid: Ministerio de Defensa, 2021.

ESPAÑA. Ministerio de Defensa. *Entorno Operativo 2035*. Madrid: Ministerio de Defensa, 2019.

ESPAÑA. Ministerio de Defensa. *Estrategia de seguridad Nacional*. Madrid: Secretaría Técnica del Ministerio de Defensa, 2017.

ESPAÑA. Ministerio de Defensa. *Estrategia Nacional de seguridad espacial*. Madrid, España: Secretaría Técnica del Ministerio de Defensa, 2019.

FERNÁNDEZ DE BOBADILLA, A. *La Carrera Espacial del siglo XXI*. Consecuencias de la llegada de China a la Luna. Trabajo Fin de Curso Estado Mayor, ESFAS. Madrid: Ministerio de Defensa. Accedido en: 17 mayo 2021.

FERNÁNDEZ, F. H. *Una carrera armamentística en el espacio*. ¿Déficit de Derecho Internacional Público? Madrid: Ministerio de Defensa, 2021.

FERNÁNDEZ-MONTESINOS, F. A. *El espacio exterior, una nueva dimensión de la Seguridad*. Madrid: Ministerio de Defensa, [2021]. Accedido en: 8 marzo 2021.

FORTEA, C. *De la Guerra*. Madrid: La esfera de los libros, 2014.

GARCÍA, C. G. *El arte de la Guerra*. [*S. l*.]: Letra Minúscula, 2021.

GUEDIM, Z. Mining in the moon and the ocean. *EDGY*, 2019. Disponible en: https://edgy.app/mining-the-moon-and-ocean-top-5-rare-earth-minerals-for-future-tech Accedido en: 15 diciembre 2021.

JONES, A. Tianwen-1 launches for Mars, marking dawn of Chinese interplanetary exploration. Disponible en: Space News: https://spacenews.com/tianwen-1-launches-for-mars-marking-dawn-of-chinese-interplanetary-exploration/ Accedido en: 23 julio. 2020.

LELE, A. y. *China's White Papers on Space: An Analysis*", Institute for Defence Studies and Analyses issue brief, 2012. Disponible en: Institute for Defence Studies and Analyses: https://idsa.in/issuebrief/ChinasWhitePapersonSpaceAnAnalysis. Accedido en: 14 junio 2021

LOVEGREN. Great Power Competition Feeds the Threat Posed by Anti-Satellite Technology., 2019. Disponible en: Worldview, Stratfor: https://worldview.stratfor.com/article/great-power-competition-feeds-threat-posed-anti-satellite-technology Accedido en: 28 junio 2021.

MACKINDER, H. J. *The geographical pivot of history*. Madrid: Planeta, 2020.

MAHAN, A. T. Influence of Sea Power Upon History, 1660-1783. Pantianos Classics, 2016.

MEARSHIMER, J. J. *The Tragedy of Great Power Politics*. Nueva York: W. W. Norton & Co, 2001.

MYERS, S. L.; CHANG, K. China's Mars Rover Mission Lands on the Red Planet. *New York Times*, New York, 2021 Disponible en: https://www.nytimes.com/2021/05/14/science/china-mars.html. Accedido en: 7 enero 2022

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION. Washington, DC: NASA, [202-?]. *Lunar catalyser*. Disponible en: https://www.nasa.gov/lunarcatalyst Accedido en: 7 enero 2022.

NORTH ATLANTIC TREATY ORGANIZATION. *NATO Ballistic Missile Defense Architecture as of 2019.* Washington, DC, 2016. Disponible en: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160711_160709-bmd-def-architecture.pdf. Accedido en: 9 sept. 2021.

ORGANIZAÇÃO DA AVIAÇÃO CIVIL INTERNACIONAL. *Convenção de Chicago*. [*S.l.*]: OACI, 1944.

PATEIRO, Laura Movilla. ¿Hacia un cambio de paradigma en el derecho del espacio ultraterrestre?: los acuerdos artemisa. *Revista Espãnola de Derecho Internacional*. v. 73, n. 2, p. 285-310, jul./dic. 2021.

RAND CORPORATION. *Tailoring Deterrence for China in space*. Washington, Estados Unidos: RAND Corporation, 2019.

THE EUROPEAN SPACE AGENCY. *ESA 2019 report on space debris - evolution in all orbits.* Paris, 2020. Disponible en: https://www.esa.int/ESA_Multimedia/Images/2020/05/ESA_2019_report_on_space_debris_-_evolution_in_all_orbits. Accedido en: 9 sept. 2021.

THE GEOPOLITICS of rare earth elements. The geopolitics of rare lands. *RANE*, 8 abr. 2019. Disponible en: https://worldview.stratfor.com/article/geopolitics-rare-earth-elements. Accedido en: 10 enero 2021.

UCS Satellite database: in-depth details on the 4,852 satellites currently orbiting Earth, including their country of origin, purpose, and other operational details. *Union of Concerned Scientists*, 8 Dec. 2005. Disponible en: https://www.ucsusa.org/resources/satellite-database. Accedido en: 9 sept. 2021.

URRUTIA, D. E. La prueba de misiles anti satélite de la India es un gran problema. He aquí por qué. *Space.com*, Washington, 30 Mar. 2019. Disponible en: https://www.space.com/india-anti-satellite-test-significance.html. Accedido en: 8 marzo 2019.

UNITED NATIONS. *Tratados y principios de la ONU sobre el espacio ultraterrestre*. Nueva York: ONU, 2002.

UNITED NATIONS OFFICE FOR OUTER SPACE AFFAIRS. *How many satellites are orbiting the Earth in 2020?* New York: UNOOSA, 2021.

UNITED STATES. Department of the Army. *Joint Publication 3-14*: Space Operations. Washington, DC: Ministry of Defense, 2020.

UNITED STATES. Departament of Defense. China's Capabilities Growth Shows Why U.S. Sees Nation as Pacing Challenge. Washington, DC: Department of Defence, 2021a.

UNITED STATES. Departament of State. *Estrategia Seguridad Nacional de los EE. UU*. Washington, DC: Department of State, 2017.

UNITED STATES. Space Command. Russian direct-ascent anti-satellite missile test creates significant, long-lasting space debris. Colorado: Department of Defense, 2021b. Disponible en: https://www.spacecom.mil/Newsroom/News/Article-Display/Article/2842957/russian-direct-ascent-anti-satellite-missile-test-creates-significant-long-last/. Accedido en: 15 nov. 2021

UNITED STATES. Space Command. *US Space Command mission*. Colorado: Department of Defense, 2019. Disponible en: https://www.spacecom.mil/Mission/ Accedido en: enero 2022.

WARDEN, J. *The Air Campaign: Planning for Combat*. New York: Tannenberg Publishing, 2002.

CIBERSEGURIDAD E INTELIGENCIA ARTIFICIAL EN EL ESCENARIO GLOBAL CONTEMPORÁNEO

Mariano Bartolomé*
Luis Souto**

RESUMEN
Este capítulo tiene como objetivo proporcionar una visión actualizada sobre la situación del recorte disciplinar conocido como ciberseguridad, a inicios de la tercera década del siglo 21. Para alcanzar esa meta, el trabajo se estructurará en tres partes: párrafos introductorios, un espacio de desarrollo y, por último, unas breves conclusiones. Específicamente en su desarrollo, se abordarán inicialmente los límites y contenidos de la mencionada ciberseguridad, describiendo sus diferentes aristas y algo de su terminología específica; luego se reflejará su estado de situación actual, subrayando la influencia ejercida por dos acontecimientos sucedidos en las postrimerías del decenio anterior; en tercer término, se explorará un impacto de la Cuarta Revolución Industrial – Big Data mediante – en la ciberseguridad: el que genera la Inteligencia Artificial (IA).
Palabras clave: Ciberseguridad; Ciberguerra; Inteligencia Artificial; Aprendizaje Automático.

CIBERSEGURANÇA E INTELIGÊNCIA ARTIFICIAL NO CENÁRIO GLOBAL CONTEMPORÂNEO

RESUMO
Este capítulo visa fornecer uma visão atualizada do estado da arte da disciplina conhecida como segurança cibernética no início da terceira década do século 21. Para atingir este objetivo, o trabalho será estruturado em três partes: parágrafos introdutórios, uma seção de desenvolvimento e, finalmente, algumas breves conclusões. Especificamente no desenvolvimento, serão abordados inicialmente os limites e conteúdos da segurança cibernética, descrevendo seus diferentes aspectos e algumas de suas terminologias específicas; em seguida, uma reflexão do sua situação atual, destacando a influência exercida por dois eventos que ocorreram no final da década anterior; em terceiro lugar, será explorado o impacto da Quarta Revolução Industrial – mediante o Big Data – sobre a segurança cibernética: aquele gerado pela Inteligência Artificial (IA).
Palavras-chave: segurança cibernética; guerra cibernética; inteligência artificial; aprendizagem de máquinas.

* Profesor, PhD, do Colegio Interamericano de Defesa (CID), Washington-DC Contato: mariano.bartolome@iadc.edu
** Profesor, PhD, do Colegio Interamericano de Defesa (CID), Washington-DC Contato: luis.souto@iadc.edu

1 INTRODUCCIÓN

Hace más de medio siglo, a fines de los años 60, tuvieron lugar dos importantes avances tecnológicos: la primera transmisión (entre las universidades de California y Stanford) de una red experimental de comunicaciones, basadas en computadoras, y la fabricación del primer chip de silicio por parte de la empresa Intel. Estos dos hechos se combinaron para producir una revolución en las Tecnologías de la Información y las Comunicaciones (TICs) que tuvo múltiples impactos en la vida de las personas, desde el nivel individual hasta el plano global. Los efectos sociales, económicos y políticos de ese avance fueron analizados y estudiados por numerosos especialistas como Alvin Toffler, Peter Drucker, Daniel Bell y Manuel Castells, entre los más conocidos. Y los conceptos "Sociedad de la Información" o "Sociedad del Conocimiento" fueron reiteradamente empleados para describir la nueva realidad.

Aquella red experimental de comunicación se convirtió en Internet, que en enero del año 2022 alcanzaba a casi 5 mil millones de usuarios, el 62,5% de la población mundial (KEMP, 2022)[1]. Estas cifras sugieren que antes de lo previsto quedarán superadas las estimaciones elaboradas hace casi una década sobre la evolución estimada de los usuarios de Internet a nivel global, en base a cifras del Banco Mundial; según esos cálculos, la totalidad de la población mundial estaría conectada a la red hacia el año 2050 (TROTMAN; ZHANG, 2013). Los flujos de datos en Internet, en el presente año 2022, ya superarían los 150 mil GB por segundo, configurando el basamento de una economía crecientemente digitalizada (UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, 2019).

La Internet constituye el basamento del ciberespacio, un concepto tomado de las novelas de ciencia ficción "Neuromancer" y "Burning Chrome" del autor William Gibson. El ciberespacio puede ser considerado, en forma simplificada, como un "entorno [predominantemente][2] virtual de información e interacciones entre personas" (KISSINGER, 2016). Este entorno es global y dinámico, y está sustentado en infraestructuras y sistemas de información y telecomunicaciones (QUINTANA, 2016). A pesar de su virtualidad, existe consenso en considerar al ciberespacio como una suerte de "lugar real" donde ocurren relaciones sociales (AIKEN, 2019; CORNEGLIAN, 2016), siendo posible entonces su análisis desde un punto de vista geopolítico. También se lo entiende como un "común global", en la

1 De acuerdo a la empresa especializada Statista Research Department (2022), a comienzos del presente año el país latinoamericano con el mayor número de usuarios era Brasil, con 165 millones, seguido por México con 96 millones. En esos momentos, la mayoría de los países de la región tenían un porcentaje de usuarios de Internet superior al 60%.

2 Decimos "predominantemente" porque el ciberespacio tiene un aspecto físico, sujeto a cuestiones territoriales. Lo integran, entre otras cosas, los cables submarinos de Internet; los centros de almacenamiento de datos; y los centros IXP, donde distintos actores del ecosistema digital establecen interconexiones para el intercambio de tráfico de Internet.

forma en que lo interpreta Stang (2013), es decir un dominio que no está bajo el control ni la jurisdicción de ningún Estado, pero su uso es materia de competencia por actores estatales y no estatales de todo el planeta. Pero esa idea de común global se limita a la infraestructura de Internet, a sus aspectos técnicos, mientras se observas competencias y pujas de poder en las acciones que allí se despliegan (BROEDERS, 2016).

Precisamente son esas pujas de poder y competencias, protagonizadas por heterogéneos actores, las que conforman la dimensión de seguridad del ciberespacio, comúnmente denominada "ciberseguridad". Como toda cuestión vinculada con la esfera cibernética, la ciberseguridad refleja un importante dinamismo, vinculado de manera directa con el vertiginoso ritmo de la evolución tecnológica. Así, es particularmente permeable a las innovaciones que propone la llamada Cuarta Revolución Industrial, que afectará todos los aspectos de la experiencia humana (SCHWAB, 2016). En especial, al llamado *Big Data*, que puede ser comprendida como "un conjunto de herramientas informáticas y estadísticas que permiten simplificar, administrar, coordinar y analizar grandes volúmenes de información" (MONLEÓN-GETINO, 2015, p. 436).

Con este marco, nuestro capítulo tiene como objetivo proporcionar una visión actualizada sobre la situación del recorte disciplinar conocido como ciberseguridad, a inicios de la tercera década del siglo 21. Para alcanzar esa meta, el trabajo se estructurará en tres partes: los presentes párrafos introductorios, un espacio de desarrollo y, por último, unas breves conclusiones. Específicamente en su desarrollo, se abordarán inicialmente los límites y contenidos de la mencionada ciberseguridad, describiendo sus diferentes aristas y algo de su terminología específica; luego se reflejará su estado de situación actual, subrayando la influencia ejercida por dos acontecimientos sucedidos en las postrimerías del decenio anterior; en tercer término, se explorará un impacto concreto de la Cuarta Revolución Industrial – Big Data mediante - en la ciberseguridad: el que genera la Inteligencia Artificial (IA).

2 CONTORNOS Y CONTENIDOS DEL CAMPO DE LA CIBERSEGURIDAD

En líneas generales puede entenderse que la ciberseguridad se enfoca en las amenazas y riesgos que surgen y se despliegan en el ciberespacio. Sin embargo, de manera más específica, este concepto tiene contenidos y límites variables, de acuerdo a la fuente. Maurer y Morgus (2014), por ejemplo, han recopilado medio centenar de definiciones diferentes sobre ciberseguridad. Para superar esta diversidad, aquí empleamos la definición amplia e inclusiva que propone la Organización de Naciones Unidas (ONU) a través de la Unión Internacional de Telecomunicaciones (UIT) [en inglés: International Telecommunications Union (ITU)]:

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. (INTERNATIONAL TELECOMMUNICATIONS UNION, 2018, p. 13).

Surge con toda claridad, de la definición de ITU, que el núcleo de la ciberseguridad es la protección de la disponibilidad, integridad y confidencialidad de los activos, frente a eventuales agresiones, o actividades maliciosas. Esas agresiones pueden ser ejecutadas por actores extremadamente heterogéneos, de jerarquía estatal o no estatal. La literatura especializada identifica, entre los actores no estatales más relevantes, a organizaciones terroristas, criminales, de espionaje, empresas privadas, hackers y los así llamados "*insiders*". Importantes y peligrosos fenómenos que tienen importancia prioritaria dentro de la esfera de la ciberseguridad están asociados a algunos de estos actores, como es el caso del ciberterrorismo, cibercriminalidad y ciberespionaje.

Es importante señalar que han incrementado su importancia, como actores, grupos no estatales dotados de importantes capacidades cibernéticas que realizan actividades de ciberespionaje de gran alcance, pero también de cibercrimen. Este tipo de actor, que frecuentemente opera como "*proxy*" de algunos Estados, es denominado Amenazas Persistentes Avanzadas (*Advanced Persistent Threat*, APT). Así, un APT es un grupo que "emplea técnicas de hackeo contínuas, clandestinas y sofisticadas para lograr acceso a sistemas y permanecer dentro de ellos por un prolongado período de tiempo, con consecuencias potencialmente destructivas" (KASPERSKY, S. P.).

Los Estados Naciones también pueden protagonizar este tipo de actividades, a través de organismos civiles o militares, utilizando de alguna manera su ciberpoder. El ciberpoder puede ser entendido, en forma amplia, como "la habilidad de usar el ciberespacio para crear ventajas e influenciar eventos en todos los ambientes y a través de los instrumentos de poder" (HATHAWAY; KLIMBURG, 2012). Con mayor precisión, indica Nye (2010), remite a "la habilidad de obtener resultados deseados a través del uso de recursos de información interconectada, del dominio cibernético" e involucra formatos de "poder duro" (*hard power*) y "blando" (*soft power*). Resulta conveniente señalar, en este punto del desarrollo, que a nivel global no existen criterios unificados en torno a las formas de mensurar el ciberpoder ni, cuantitativamente, las métricas que pueden emplearse a esos efectos. Solo a modo de ejemplo, algunos índices discriminan entre capacidades cibernéticas ofensivas y defensivas, para obtener finalmente

un ranking general en esta materia (VOO *et al*., 2020). Otros, en cambio, califican a los países analizados en diferentes categorías, para luego jerarquizarlos en tres niveles: potencias líderes en todas las categorías analizadas; potencias líderes en algunas de esas categorías; y naciones con fortalezas norias en algunas de esas categorías, pero deficiencias claras en otras (INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES, 2021).

Las actividades estatales en el ciberespacio que involucran a las instituciones militares suelen encuadrarse como "ciberdefensa". A su vez, la ciberdefensa suele vincularse con el concepto "ciberguerra", aparecido hace casi tres décadas (ARQUILLA; RONFELDT, 1993), que todavía hoy es objeto de controversias en cuanto a su significado y alcances. Al respecto, las perspectivas abarcan desde lecturas según las cuales la ciberguerra es un concepto de escasa utilidad, debido a su casi nula probabilidad de ocurrencia (RID, 2013), a planteos que vaticinan que esa será la fisonomía de los futuros conflictos (SANGER, 2018). Existe amplio consenso, en cambio, en que el hecho bélico incluirá distintas formas de combate cibernéticas que se combinarán con acciones ejecutadas en los otros dominios (STEVENS, 2018; BARTOLOMÉ, 2020a).

En esta perspectiva, destaca la iniciativa del Centro de Excelencia de Ciberdefensa (CCD COE), organismo vinculado a la Organización del Tratado del Atlántico Norte (OTAN), con sede en Tallin, Estonia. Fue a partir de él que surgieron los primeros intentos de interpretar el Derecho Internacional Humanitario (DIH) en el contexto de las ciberoperaciones y la ciberguerra. En 2009, el Centro reunió a un grupo internacional de académicos, profesionales del derecho y de la tecnología de la información para analizar este tema de manera exhaustiva y aportar cierto grado de claridad a las complejas cuestiones jurídicas relacionadas con él. Estos intentos tomaron la forma de manuales colectivos – Manual Tallinn (2013) y Tallinn 2.0 (2017), de carácter académico y no vinculante (SCHMITT, 2013; 2017). Como resultado del estudio, se comprobó que el DIH puede aplicarse al ciberespacio y, por tanto, a los ciberataques caracterizados como uso de la fuerza en el entorno virtual. Aun así, numerosos expertos señalaron varias cuestiones que siguen siendo inciertas, o generan dudas, en este campo (HATHAWAY; KLIMBURG, 2012). Entre ellas, las diferencias de empleo de ciberataques en tiempos de paz o guerra; cuándo es considerado un "uso de la fuerza" de acuerdo con el DIH; qué tipo de blancos son aceptables, o cómo ajustar estas acciones a los principios del *jus in bello – jus ad bellun*.

En relación a las acciones, las herramientas y técnicas empleadas en actividades cibernéticas maliciosas son variadas. Como hemos indicado en trabajos anteriores (BARTOLOME, 2020a), estas acciones suelen tener una serie de características que incrementan su peligrosidad. En un listado no exhaustivo, algunas de esas características son las siguientes:

- Carácter difuso. En el espacio virtual se diluyen las tradicionales diferencias entre las esferas pública y privada, interna y externa. Este carácter difuso plantea una importante dificultad desde el punto de vista de los marcos jurídicos vigentes.
- Difícil detección. Las acciones maliciosas en el ciberespacio pueden pasar inadvertidas, o ser confundidas con fallas de hardware/ software.
- Gran diversidad de blancos potenciales, incluyendo a aquellos adecuadamente protegidos desde el punto de vista físico
- Simultaneidad de blancos. Las acciones maliciosas pueden alcanzar en forma simultánea o concatenada a miles de computadoras y bases de datos interconectadas, en todo el planeta.
- Operación remota. La inexistencia del factor "distancia" en el ciberespacio permite la ejecución de acciones desde el otro extremo del planeta.
- Identificación y atribución. Suele ser extremadamente dificultoso identificar con certeza los autores intelectuales de la agresión, y poder atribuir esa responsabilidad con pruebas contundentes e irrefutables.

Además, las acciones maliciosas en el ciberespacio tienen un costo relativamente bajo, en comparación con otras formas de generación de daño. En este sentido, el "armamento" utilizado por el agresor puede consistir en computadoras de uso cotidiano y software de precio accesible, mientras el ejecutor no requiere conocimientos muy sofisticados. En forma sostenida a lo largo del tiempo, los conocimientos requeridos para realizar una acción maliciosa en el ciberespacio, y su sofisticación, han disminuido en forma constante, al tiempo que se incrementaron la eficacia del acto, y el daño generado (GAIDOSH, 2018; ROBINSON, 2016).

El abanico de herramientas y técnicas es enorme, precisamente por la amplitud de estos conceptos, y la evolución del desarrollo tecnológico. En este marco ocupa un lugar de relevancia el denominado *malware*, software malicioso especialmente diseñado para ser descargado en, o introducido a, una computadora, donde puede causar grandes daños o filtraciones de datos. Las formas más conocidas de malwares son virus (se diseminan a partir de las acciones de los usuarios), gusanos (se diseminan automáticamente), troyanos (mimetizados como software legítimo), *spyware* (monitorea la actividad de la computadora) y *ransomware* (bloquea el acceso a los archivos o computadoras). Habitualmente el malware ingresa a los equipos a través de técnicas de *phishing*, práctica de engaño a los usuarios a través de correos electrónicos o sitios web apócrifos, que muchas veces están respaldadas por complejas labores de ingeniería social[3]. No puede

3 Entendemos a la Ingeniería Social como un "acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas"

dejar de mencionarse la llamada Denegación Distribuida de Servicio (DDoS), que puede ser entendida como la parálisis intencional de una red de computadoras mediante el envío de estímulos enviados simultáneamente desde gran cantidad de procedencias. La ejecución de DDoS emplea miles de *botnets*, o sea, equipos conectados que un *malware* transforma en un *bot*.

No puede dejar de mencionarse el empleo en estas actividades de la *Deep Web*, es decir, la enorme porción de Internet cuyos sitios no están indexados en los motores de búsqueda tradicionales; en especial, la llamada "Web Oscura" (*Dark Web*), donde la privacidad es el elemento central, y en consecuencia la información se encuentra encriptada. Esta porción de Internet es aprovechada para la realización de prácticas y negocios fuera de la ley, abonados con criptomonedas de muy difícil rastreo. La *Dark Web* plantea el desafío de hallar un equilibrio entre la libertad de información y la privacidad, y las actividades cibermaliciosas (KUMAR; ROSENBACH, 2019).

Para finalizar los comentarios en torno al primer criterio seleccionado, para calificar las agresiones en el ciberespacio, debemos decir que, en materia de destino de esas acciones ocupan un lugar especial las llamadas infraestructuras críticas. Esa denominación refiere a la infraestructura y los activos de vital importancia para la seguridad, gobierno, salud pública y economía nacionales, y para la confianza ciudadana. Básicamente, la idea de infraestructuras críticas refiere a sistemas, máquinas, edificios o instalaciones relacionados con la prestación de servicios esenciales a la población (QUINTANA, 2016.p. 95). Esas infraestructuras incluyen los sistemas de procesamiento de información y telecomunicaciones, el software que permite operarlos, y el personal que maneja los sistemas y emplea el software.

Un segundo criterio para calificar las agresiones cibernéticas o actividades maliciosas en el ciberespacio evalúa su intensidad, diferenciando entre ciberincidentes y ciberataques. Los ciberincidentes son eventos de seguridad que comprometen la integridad, confiabilidad y disponibilidad de un activo de información (THE HAGUE CENTRE FOR STRATEGIC STUDIES, 2015). Se entiende que estos incidentes son de limitada gravedad y no siempre se comprueba una voluntad de generar daño, por parte del perpetrador. Los ciberataques, en cambio, apuntan a recolectar, interrumpir, denegar o destruir recursos de sistemas de información, o información en sí misma. Pueden causar lesiones o muerte a personas, además de daños o destrucción total a objetos (THE HAGUE CENTRE FOR STRATEGIC STUDIES, 2015). Debido a su intensidad y a sus efectos, los cibertaques pueden constituir una cuestión de Seguridad Nacional, y por esa razón la Estrategia Nacional de Ciberseguridad consiste en:

> La aplicación de medidas gubernamentales específicas y principios de aseguramiento de información a sistemas de TIC públicos, privados e internacionales relevantes, y a su contenido asociado, donde esos sistemas sean de afecten a la seguridad nacional (HATHAWAY; KLIMBURG, 2012, p. 43).

La Estrategia Nacional de Ciberseguridad tiene como objetivo lograr un ambiente seguro en el cual se puedan proteger a los ciudadanos de diversos ciberataques, y ataques no cibernéticos relacionados, tanto locales como extranjeros. Abarca las dimensiones gubernamental, nacional e internacional y puede ser interpretada desde diferentes perspectivas, cada una de ellas con diferentes prioridades. Hathaway & Klimburg, (2012) identifican por lo menos cinco perspectivas, que hacen énfasis en (i) el poder militar, (ii) la criminalidad, (iii) la inteligencia y contrainteligencia, (iv) la protección infraestructuras críticas, y (v) la ciberdiplomacia y gobernanza de Internet.

Precisamente la Seguridad Nacional constituye, en la visión de Newmeyer (2015), el núcleo de uno de los tres paradigmas que ayudan a comprender los problemas de ciberseguridad. En este paradigma el Estado mantiene su tradicional papel de protección de las fronteras, bienes y ciudadanos. La ciberdefensa y las infraestructuras críticas ocupan lugares centrales en este enfoque. Un paradigma con énfasis en la economía, por su parte, enfatiza en la importancia de Internet y la creciente digitalización para la riqueza y el bienestar de países y personas. Las TICs ocupan un lugar clave en este abordaje. Finalmente, la salud pública puede es el eje de un tercer paradigma que enfatiza en la ciberseguridad como un bien público portador de beneficios a los usuarios. La correcta implementación de eficaces medidas preventivas y de resiliencia, a modo de vacunas y medicinas, es clave en esta perspectiva.

3 LA SEGUNDA DÉCADA DEL SIGLO XXI

En el año 2010 se produjo una situación paradójica con relación al ciberespacio, que era el reflejo de dos lecturas opuestas sobre la situación en ese entorno. Desde una publicación científica italiana, Internet fue oficialmente propuesta para el Premio Nobel de la Paz, por ser un medio que incentiva el diálogo, el debate y el consenso a través de la comunicación. La idea fue respaldada por numerosos intelectuales, científicos y artistas, y fue aceptada por los organizadores del premio. Pero al mismo tiempo, desde prestigiosos medios periodísticos y académicos, de renombre mundial, se confirmó que ese entorno se había transformado en un nuevo “dominio” de la guerra. El

quinto dominio, que se sumaba a los tradicionales tierra, mar, aire y espacio. "La Guerra ha ingresado en el quinto dominio: el ciberespacio", indicó *The Economist* (2010), al tiempo que William Lynn, Subsecretario de Defensa de Estados Unidos, declaraba:

> En un sentido doctrinario, el Pentágono formalmente ha reconocido al ciberespacio como un nuevo dominio de combate. Si bien el ciberespacio es un dominio creado por el hombre, se ha tornado tan crítico para las operaciones militares como la tierra, el mar, el aire y el espacio. (LYNN, 2010).

En aquellos momentos, la comprensión de las capacidades y operaciones ofensivas en el ciberespacio, así como la posibilidad de apoyar acciones cinéticas, hicieron de ese nuevo dominio un componente esencial de mando y control en todas las demás áreas de operaciones. Este hecho llevó a la cibernética a dejar de ser un simple elemento de apoyo al combate para convertirse en un espacio operativo, a la altura de los dominios terrestre, marítimo, aéreo y espacial. Un año después, en 2011, la publicación de la Estrategia Internacional para el Ciberespacio (*International Strategy for Cyberspace*) estadounidense supuso un hito para el entorno cibernético global. Lo fue porque, además de ser el primer documento en este sentido, oficializó la lectura anticipada por Lynn respecto a la posición estratégica y operativa del principal actor en el mundo virtual. La Estrategia definió la importancia del ciberespacio al afirmar que "la infraestructura digital se ha convertido en la columna vertebral de economías prósperas, comunidades científicas, fuerzas armadas, gobiernos transparentes y sociedades libres" (UNITED STATES OF AMERICA, 2011).

La pública denominación del ciberespacio como quinto dominio reflejó la importancia que había alcanzado ese plano no sólo en materia militar, sino de seguridad en un sentido más amplio. Esa importancia se fundamentaba en diferentes hechos ocurridos en los años previos, especialmente en dos que tuvieron como protagonista a Rusia y ocurrieron en Estonia (2007) y Georgia (2008). Aunque ambos eventos reflejen algunas similitudes en términos de motivación política, tipos de objetivos y métodos utilizados, difieren entre sí en relación con las metas deseadas y los resultados obtenidos, como veremos más adelante.

Respecto al primero, entre los meses de abril y mayo de 2007, durante un período de dos semanas, Estonia fue víctima de un ciberataque masivo. Este

ataque, aunque no fue el único registrado hasta ese momento, ni el mayor, tuvo una enorme trascendencia, por diferentes razones. Por un lado, fue el primer ciberataque dirigido a la seguridad nacional de un país (DAVIS, 2009). Segundo, la mayoría de los blancos afectados constituían infraestructuras críticas, específicamente infraestructura de información. Por otra parte, constituía la primera agresión cibernética de tipo interestatal, aceptando la responsabilidad de Rusia (*vide infra*). Finalmente, mostraba las enormes dificultades de atribución de responsabilidad al atacante, tornando muy problemática la adopción de represalias, en términos legales y políticos (THEILER, 2011).

Los primeros ataques fueron dirigidos, casi en su totalidad, contra las instituciones políticas estonias. Alcanzaron con éxito a los sitios *web* de todos los ministerios gubernamentales, dos bancos importantes y varios partidos políticos. El primer ministro local, Andrus Ansip, y otros dirigentes fueron víctimas de DDoS. Los servicios de correo electrónico del Parlamento tuvieron que cerrarse temporalmente porque ya no podían manejar el volumen inusual de datos: los buzones de correo electrónico se saturaron con mensajes *spam* que redundaron en DDoS, además de *phishing* (FINN, 2007). La segunda fase de la agresión, iniciada el 30 de abril y prolongada hasta el 18 de mayo, fue considerada por el gobierno de Estonia como la etapa principal: los ataques se produjeron en cuatro oleadas de diferentes intensidades, enfocándose en distintos objetivos y usando variadas técnicas, todos con el objetivo de llegar a la infraestructura de TI de Estonia y provocar un apagado completo de sus sistemas (DAVIS, 2009). En esa ocasión, la coordinación de los ataques se delegó a los servidores de comando y control (C2) de las *botnets* (TIKK; KASKA, 2010).

A pesar de la sorpresa inicial, los estonios pudieron responder a los ciberataques de manera muy eficiente, mitigando sus efectos. Dicho en otras palabras, demostrando "ciberresiliencia". No hubo daño permanente a la infraestructura TI y las pérdidas financieras fueron mínimas. Según el entonces Subsecretario de Defensa de Estonia, la situación fue mitigada por el trabajo de un equipo de expertos, compuesto por especialistas de los departamentos de comercio y comunicaciones, las fuerzas armadas y la comunidad de inteligencia del país (KASH, 2008). Además, contribuyeron significativamente a la rápida restauración de las operaciones de la red de Estonia el apoyo de países aliados (entre ellos Alemania, Israel, Eslovenia y Finlandia), como así también del equipo de respuesta a emergencias informáticas de la Organización del Tratado del Atlántico Norte (OTAN) (COLLIER, 2007).

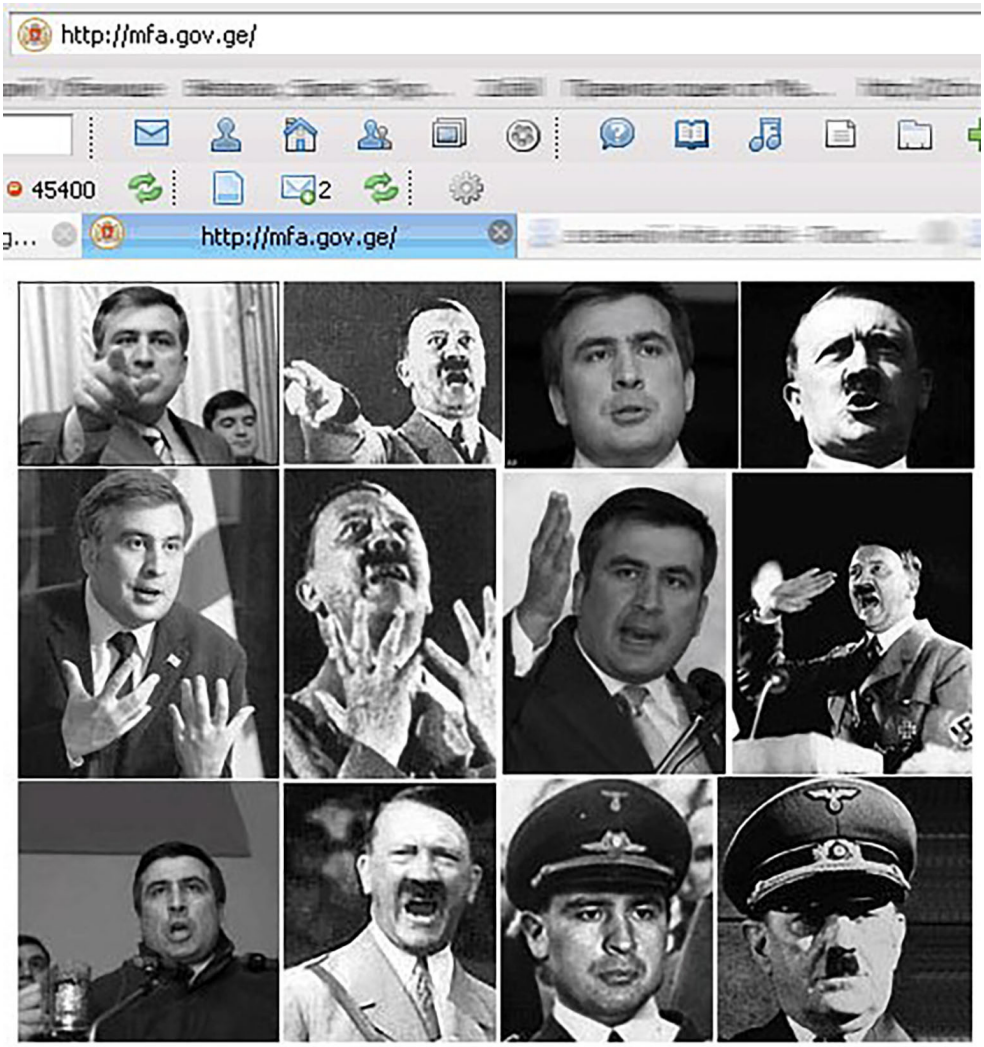
Existe consenso en que los ciberataques de Estonia fueron una represalia por algunas decisiones de Tallin percibidas como "antirrusas" en Moscú. Las investigaciones realizadas por el gobierno estonio con la asistencia de países

aliados indicaron que los ataques procedieron de Rusia y habrían sido ejecutados por grupos no estatales dirigidos desde el Kremlin. Una investigadora española (CARO BEJARANO, 2010) denominó "cibermilicias" a estos grupos, indicando que están formados por hackers patriotas que usan herramientas cibernéticas para participar en conflictos domésticos o internacionales. Precisamente debido a las mencionadas dificultades de atribución de responsabilidad, la participación rusa nunca ha sido comprobada; sin embargo, la certeza de su involucramiento continúa influyendo y afectando la relación bilateral.

Los acontecimientos de Estonia plantearon un importante dilema para la Organización del Tratado del Atlántico Norte, a la cual se había incorporado ese pequeño país, sobre el tipo de respuesta que debía adoptar. Como la institución no tenía una postura clara en materia de ciberseguridad, no quedaba claro si el ciberataque encuadraba en el mecanismo de defensa colectiva previsto por el Tratado del Atlántico Norte en su artículo 5, indicando que un ataque armado contra uno o varios aliados será considerado como un ataque dirigido contra todos los miembros. Para remediar este importante vacío, a comienzos de 2008 la Organización aprobó oficialmente su primera Política de Ciberdefensa (THEILER, 2011). Además, ese año inauguró en Tallin su nuevo Centro de Excelencia Cooperativo en Ciberdefensa (CCDCoE), mencionado en otro pasaje de este trabajo, que entre sus primeras tareas planteó la redacción de un texto referencial sobre el marco legal aplicable a ciberataques, respecto al uso de la fuerza. Ese texto es el Manual de Tallin, que ya lleva dos ediciones y constituye hasta el presente el documento más avanzado en esa materia (SCHMITT, 2013; 2017).

En 2008, exactamente un año después del incidente de Estonia, una ola continua de violencia en la región derivó en un breve conflicto armado entre Rusia y Georgia; se considera que fue la primera contienda que sumó el ciberespacio a los tradicionales dominios del aire, la tierra y el mar (KOZLOWSKI, 2014). A inicios del mes de agosto, en respuesta a los sucesivos ataques de los rebeldes separatistas osetios a las aldeas georgianas, las fuerzas militares gubernamentales bombardearon la capital de Osetia del Sur e invadieron su territorio (GEORGE, 2009). Esa acción provocó una rápida respuesta de Rusia, cuyo ejército expulsó al ejército georgiano de la zona, al tiempo que sus unidades cibernéticas realizaban ataques DDoS (Distributed Denial of Service Attack) contra servidores y páginas *web* del gobierno nacional, impidiendo sus comunicaciones y generando confusión y temor entre la población. El objetivo de esas acciones fue privar al oponente de la conciencia situacional general del conflicto (CLARKE, 2010). Simultáneamente, *hacktivistas* rusos se infiltraron en varios sitios web georgianos y los desconfiguraron con fines de propaganda rusa (HOLLINS, 2010).

Figura 01 - Collage de fotos en el sitio web del Ministerio de Asuntos Exteriores de Georgia en el que se compara al presidente georgiano con Adolf Hitler.



Fuente: MINISTERIO DE ASUNTOS EXTERIORES DE GEORGIA. Disponible en: http://georgiamfa.blogspot.com/. Accedido en: 13 abril 2022.

Durante el período crítico, en una ventana de operaciones de combate de menos de una semana, los georgianos no pudieron recuperar el control de su ciberespacio y realizar comunicaciones estratégicas a nivel nacional, siendo momentáneamente incapaces de comunicarse con la comunidad internacional

(FERNÁNDEZ, 2013). La mitigación de los ataques fue coordinada por el Grupo de Respuesta a Incidentes de Seguridad de Georgia que, después del colapso de los servidores locales, asumió el papel de *Computer Emergency Response Team* (CERT) nacional (TIKK, 2008). Durante el periodo en que estuvo bajo ciberataque, a semejanza de lo ocurrido en Estonia, Georgia también recibió un importante apoyo externo para mitigar las acciones de los hackers y restablecer la comunicación interna e internacional.

En definitiva, con el antecedente de Estonia y Georgia, durante la segunda década del siglo XXI, las cuestiones de ciberseguridad consolidaron su importancia, dentro del escenario de la Seguridad Internacional. Una confirmación de esa importancia se obtiene de algunas declaraciones realizadas sobre este tema, por influyentes académicos y funcionarios públicos. Por ejemplo, a comienzos de ese lapso Richard Clarke, encargado de la oficina antiterrorista de Estados Unidos durante los atentados del 9/11, indicó que el manejo de "bits and bytes" permitía destruir infraestructura física con la misma eficacia que un arma cinética (CLARKE; KNAKE, 2010). Joe Lieberman, presidente del Comité de Seguridad Interior del Senado de ese país, habló de los riesgos de un "Cyber 9/11", mientras Leon Panetta, Secretario de Defensa, indicó que la superpotencia enfrentaba la posibilidad de un "Cyber Pearl Harbor", tan destructivo como los ataques terroristas sufridos en las Torres Gemelas y el Pentágono (BUCHANAN, 2020). Este tipo de apreciaciones se mantuvieron a lo largo de los siguientes años y así David Sanger calificó a la cibernética como "el arma perfecta" debido a su adaptabilidad, su bajo costo y su anonimato, que permite negación total de parte de los responsables. Este ganador del Premio Pulitzer en tres oportunidades, agregó además que las ciberarmas permitían una amplia gama de operaciones ofensivas y habían desplazado al terrorismo y los ataques nucleares como la mayor amenaza (SANGER, 2018).

Algunos datos cuantitativos refuerzan la apreciación mencionada, en cuanto al posicionamiento prioritario de los temas de ciberseguridad en la década pasada. Entre ellos, que en ese lapso más del 60 % de las empresas de todo el mundo han experimentado algún tipo de incidente cibernético, mientras el 20% de las organizaciones globales consideran que el espionaje cibernético es su amenaza número uno (CVETICANIN, 2022). La importancia de las cuestiones cibernéticas en el campo de la Seguridad Internacional, en la segunda década del siglo, también se puede confirmar a través de la revisión de diez eventos de ese tipo que ocurrieron en ese lapso. En la zaga que desarrollamos en la Tabla 1 se puede confirmar las diferentes formas que pueden adoptar los ciberincidentes y ciberataques en la actualidad.

Tabla nº 1 – Ciberincidentes y ciberataques 2010-20

AÑO	EVENTO	INVOLUCRAMIENTO DE ESTADOS	ACTOR / PERPETRADOR	BLANCO	HERRAMIENTAS TECNICAS
2010	STUXNET	Supuesto (EEUU e Israel)	Agencia estatal	Estatal (Irán)	Malware (Virus)
2010	Wikileaks	---	Insiders	Estatal (EEUU)	Exfiltración datos
2012	Anonymous	---	Hacktivistas	Mixto	DDoS
2014	Sony Pictures	Supuesto (Corea del Norte)	APT	Privado	Phising Exfiltración datos
2015	Black Energy	Supuesto (Rusia)	Rusia	Estatal (Ucrania)	Phising Malware (Virus)
2016	Russiagate	Supuesto (Rusia)	Agencia estatal + APT	Sociedad Civil	Phising Redes Sociales
2017	Equifax	Supuesto (RPCh)	Agencia estatal	Privado	Exfiltración datos
2017	Wannacry / NotPetya	Supuesto (Corea del Norte / Rusia)	APT	Mixto	Malware (Ramsonware)
2018	Cambridge Analytica	---	---	Sociedad Civil	Redes Sociales
2020	Solar Winds	Supuesto (Rusia)	APT	Mixto	Malware (Back door)

Fuente: EL AUTOR, 2022.

Para cerrar este pasaje del capítulo, es necesario subrayar que no hay ningún indicio de disminución de la importancia de la ciberseguridad, en el decenio actual. Convalidando esta apreciación, en la reunión anual del Foro Económico Global celebrada en el año 2020, António Guterres, Secretario General de la ONU, incluyó al "lado oscuro" del mundo digital entre los cuatro "jinetes del Apocalipsis" que provocan incertidumbre e inestabilidad globales. En palabras de ese diplomático: "La nueva tecnología se utiliza para cometer delitos, atizar el odio, divulgar información falsa y explotar a las personas". Completaron la lista el cambio climático, la desconfianza de los ciudadanos en sus instituciones y las tensiones geopolíticas (BARTOLOMÉ, 2020b). Por su parte la más importante compañía aseguradora a nivel mundial, colocó en el primer lugar de su "Barómetro de Riesgos" a aquellos procedentes de, o vinculados a, el plano cibernético. Igual situación se registró en el año 2020, mientras en el ejercicio siguiente los riesgos cibernéticos quedaron

relegados a un tercer lugar, aunque en una vinculación sistémica con la interrupción de negocios (1˚) y – Covid mediante - el estallido de una pandemia global (2˚); dicho en otras palabras, un escenario en el cual una pandemia forzaba una migración súbita de actividades económicas *on-line*, vulnerables a agresiones cibernéticas (ALLIANZ GLOBAL CORPORATE; SPECIALTY, 2022).

4 EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL (IA) EN LA CIBERSEGURIDAD

Con el fin de la Segunda Guerra Mundial, el matemático británico y pionero de la informática Alan Mathison Turing, en su primera conferencia pública (CARPENTER; DORAN, 1977) sobre el tema de la inteligencia computacional, destacó: "Lo que queremos es una máquina que pueda aprender de la experiencia". En aquella época, Turing defendía la idea de que la Inteligencia Artificial (IA) se investigaría mejor programando ordenadores que construyendo máquinas inteligentes. Sin embargo, el término no se consolidó hasta 1956, tras una conferencia celebrada en el campus de la Universidad de Dartmouth, cuando el profesor local John McCarthy convenció a los participantes para que acepten ese concepto, iniciando la "edad de oro" de la IA (McCORDUCK, 2004).

Desde entonces, la IA se ha ido desarrollando de manera eficiente, convirtiéndose en un componente tecnológico cada vez más presente en el día a día de las personas. A pesar de ello, existe una falta de consenso en cuanto al concepto de inteligencia artificial, que no impiden el análisis de algunas definiciones ya ratificadas por la comunidad académica:

- Según el mencionado profesor McCarthy (2004), la inteligencia artificial se puede definir como "la ciencia y la ingeniería para fabricar máquinas inteligentes, especialmente programas informáticos inteligentes".
- La Fuerza Aérea de los Estados Unidos, en su "Anexo de Inteligencia Artificial" publicado en 2019, definió la IA como la capacidad de las máquinas para realizar tareas que normalmente requieren de la inteligencia humana, como reconocer patrones, aprender de la experiencia, entre otras, ya sea de forma digital o como el uso de software inteligente (USAF, 2019).
- En términos más generales, la Organización de Ciencia y Tecnología (STO), órgano dependiente de la OTAN, ha definido la IA como "la capacidad de las máquinas para realizar tareas que normalmente requieren inteligencia humana" (OTAN, 2020).

A partir de las definiciones presentadas, se puede deducir que la IA se refiere a sistemas o máquinas que imitan la inteligencia humana para realizar tareas específicas y que pueden mejorarse a sí mismas mediante la interacción mutua o en base a la información que recogen. El interés por la investigación y el

desarrollo de esta temática está directamente relacionado con la creciente cantidad de datos disponibles (el *Big Data* mencionado a inicios del presente trabajo) y la necesidad de sistemas informáticos capaces de procesarlos de forma más rápida y precisa de lo que sería capaz un ser humano (INTERNATIONAL BUSINESS MACHINES CORPORATION, 2020).

A lo largo del tiempo, la IA ha ido mejorando su método de aprendizaje mediante la incorporación de nuevas tecnologías. En este sentido, la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) de Estados Unidos ha discriminado a las innovaciones de la IA entre las que se sustentan en el conocimiento, y las basadas en los datos. La IA basada en el conocimiento integra varios sistemas modernos que se basan en reglas predefinidas, creadas por humanos, para la toma de decisiones; por lo tanto, no pueden razonar sobre nuevas situaciones ni aprender de sus experiencias (TRIPATHI, 2011). Los sistemas de IA basados en datos, por su parte, resuelven problemas específicos utilizando modelos estadísticos que se entrenan en grandes bases de datos, lo que garantiza una mayor autonomía en la toma de decisiones (TAMIR, 2020).

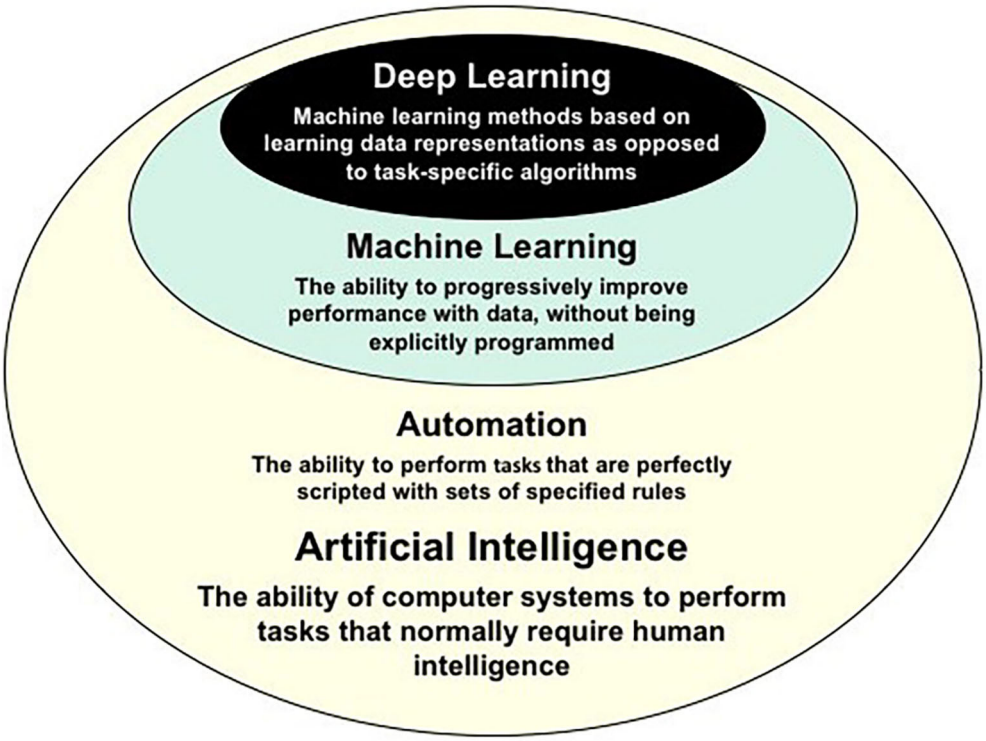
En el ámbito de la Defensa, la IA se considera una tecnología emergente que se ha incorporado a una amplia gama de aplicaciones, desde vehículos autónomos hasta herramientas de procesamiento de datos y logística (GRAY; ERTAN, 2021). En 2020, durante una simulación de realidad virtual financiada por el Pentágono, un avión de combate polivalente F-16 autónomo controlado por IA, venció a un piloto real en otra aeronave similar en varios combates aéreos (KNIGHT, 2020), consolidando aún más el alcance de este avance tecnológico.

En consecuencia, la IA se ha convertido en una tecnología atractiva para las fuerzas armadas, adquiriendo un papel cada vez más importante para la Defensa, ya que supera a los humanos en las tareas militares automatizadas. Además, permite un procesamiento más rápido de la información, actuando como multiplicador de fuerzas y contribuyendo en gran medida al proceso de toma de decisiones militares (HOROWITZ *et al.*, 2019).

Asimismo, gran parte de los Vehículos Autónomos No-Tripulados (VANTs), los sistemas de defensa aérea y los misiles autónomos que se utilizan actualmente emplean tecnología de IA basada en el conocimiento; es decir, no dependen del procesamiento de grandes cantidades de datos. Un ejemplo es el sistema de misiles *Patriot* de Estados Unidos, que utiliza el modo semiautónomo, que permite a los ordenadores identificar, apuntar y atacar a las amenazas entrantes sin interferencia humana (HAWLEY, 2017).

Recientemente se registró una importante mejora de los sistemas de IA basados en datos, conocida bajo los conceptos “Aprendizaje Automático” o “Aprendizaje de Máquina” (*Machine L*earning, ML), por un lado, y “Aprendizaje Profundo” *(Deep Learning*, DL), por otro. Los métodos de ML y DL son todavía relativamente nuevos y la mayoría de las fuerzas armadas carecen de sistemas capaces de absorber estas capacidades, confiando en cambio en sistemas autónomos más antiguos.

Figura 02 - Taxonomía de las tecnologías de inteligencia artificial



Fuente: MILITARY APPLICATIONS OF ARTIFICIAL INTELLIGENCE: ETHICAL CONCERNS IN AN UNCERTAIN WORLD (RAND CORPORATION, 2020).

El *Machine learning* (ML) utiliza un determinado tipo de algoritmos que permiten a los ordenadores analizar datos, aprender de experiencias pasadas y tomar decisiones, de forma similar al comportamiento humano. Aplicados a la ciberseguridad, estos algoritmos son capaces de detectar y analizar automáticamente los incidentes de seguridad, pudiendo responder de forma autónoma a una amenaza (SEGAL, 2020).

Por otro lado, se están desarrollando técnicas de ML para su uso en el ámbito cibernético, lo que permite analizar grandes cantidades de conjuntos de datos que incluyen códigos maliciosos, códigos de *malware* y flujos de red anormales, contribuyendo en gran medida al trabajo de los equipos de ciberseguridad en la identificación de nuevas amenazas (PALMER, 2020). Según un experto de la Universidad de Drexel, "uno de los principales problemas de la ciberseguridad es la cantidad de datos que los profesionales deben procesar para tomar decisiones críticas en materia de ciberseguridad" (DREXEL, 2021). Así, la ciberseguridad

combinada con la IA podrá revelar el *modus operandi* de un adversario, utilizando métodos de observación y recogiendo patrones para identificar los distintos tipos de ataques (NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, 2020).

Otro ámbito prometedor del uso de la IA, en lo que respecta a la ciberseguridad, es la creación y el despliegue de sistemas de software de defensa más fiables (NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, 2020). Se han desarrollado estudios con este tipo de tecnología para mejorar la capacidad de detectar errores en los programas, identificar vulnerabilidades de seguridad y facilitar a los ingenieros de software el diseño de sistemas más robustos y seguros. De lo anterior se deduce que, independientemente de la aplicación, la IA y el ML se están convirtiendo en actores principales en el escenario cibernético mundial. Esto se debe a que poseen la capacidad de mitigar las amenazas en tiempo real, pero sin comprometer la continuidad de las operaciones (STEFANINI, 2021), ya que combinados pueden rastrear datos y detectar anomalías que escapan al ojo humano.

Hacia el futuro, aunque la IA puede contribuir a mejorar los sistemas militares, ofreciendo la perspectiva de un aumento significativo de la potencia de combate, sus capacidades actuales distan mucho de ser perfectas y, sobre todo en este ámbito, los fallos pueden acarrear graves consecuencias (GRAY; ERTAN, 2021). En materia de ciberseguridad, esta cuestión es aún más preocupante, ya que del mismo modo que la IA puede emplearse para prevenir las ciberamenazas, esta misma tecnología también puede ser utilizada por los hackers con el objetivo de irrumpir en los sistemas militares (DREXEL, 2021). Algunos ejemplos de uso malicioso de la IA son:

- Corrupción y envenenamiento de datos (*Data Corruption & Poisoning*): esta técnica consiste en alterar los datos utilizados en el entrenamiento de la IA para engañar los patrones del programa. Un ejemplo es cuando los hackers introducen algoritmos en un determinado modelo de ML para que identifique datos maliciosos como benignos. Este método ataca la integridad del sistema incluso antes de entrar en funcionamiento (STARCK *et al.*, 2022).
- Evasión (*evasion*): este método pretende identificar cómo se aplica el aprendizaje de la IA. Para ello, el atacante debe ser capaz de controlar las entradas del sistema de IA durante su funcionamiento. Los ataques se dirigen a las aplicaciones de reconocimiento facial, detección de objetos y reconocimiento de objetivos (STARCK *et al.*, 2022)[4].
- Ingeniería inversa: En este caso, un adversario ataca un sistema de IA con el objetivo de extraer lo que ese sistema ha aprendido, permitiendo así

4 Por ejemplo, en un conflicto militar, una vez que se identifique que el sistema de defensa aérea basado en IA de mi oponente ha sido entrenado en aviones con camuflaje gris disruptivo, mis aviones podrían simplemente ser repintados con otro tipo de camuflaje para evitar ser detectados por los sistemas de la IA enemiga.

reconstruirlo. Para ello, el atacante necesita poder enviar estímulos (*inputs*) a un modelo y observar las respuestas (*outputs*) (STARCK *et al.*, 2022)[5].

- Redes Generativas Adversarias (*Generative Adversarial Network*, GAN): Implica la creación de un sistema de IA "en espejo" destinado a simular el comportamiento normal del flujo de la red, para desviar la atención de los ataques maliciosos y extraer datos sensibles (DREXEL, 2021).

5 CONCLUSIONES

Internet constituye el basamento del ciberespacio, entendido como un entorno virtual de información e interacciones entre personas, global y dinámico, sustentado en infraestructuras y sistemas de información y telecomunicaciones. El uso de este dominio es materia de competencia y pujas de poder por actores estatales y no estatales de todo el planeta, que le otorgan una dimensión de seguridad: la ciberseguridad. La ciberseguridad se centra en las amenazas y los riesgos que surgen y se desarrollan en el ciberespacio. Su núcleo se centra en la disponibilidad, integridad y confidencialidad de los activos, frente a posibles ataques o actividades maliciosas. Estas agresiones se pueden analizar según cuatro elementos: actores o perpetradores; objetivos; acciones e impactos.

Las ciberagresiones o actividades maliciosas en el ciberespacio pueden ser calificadas en ciberincidentes y ciberataques. Debido a su intensidad y a sus efectos, los cibertaques pueden constituir una cuestión de Seguridad Nacional.

Los actores que pueden ejecutar agresiones en el ciberespacio son extremadamente heterogéneos, y pueden ser estatales o no estatales. Se destacan organizaciones terroristas, criminales, de espionaje, empresas privadas, hackers y los así llamados *insiders*. Los Estados Naciones también pueden protagonizar este tipo de actividades, a través de organismos civiles o militares, utilizando de alguna manera su *cyber power*. También suelen involucrar a las instituciones militares, dando lugar al concepto de ciberdefensa y a los debates en torno a las formas de combate cibernéticas, que oficialmente se encuadran dentro del Derecho Internacional de los Conflictos Armados.

Las herramientas y técnicas utilizadas en actividades maliciosas en el ciberespacio también son variadas, tienen un costo relativamente bajo, en comparación con otras formas de generación de daño y no demandan conocimientos muy sofisticados. Se destaca en este campo el uso de la *Dark Web*. En materia de blancos las agresiones en el ciberespacio ocupan un lugar especial las infraestructuras críticas, que son de vital importancia para la seguridad, gobierno, salud pública y economía nacionales, y para la confianza ciudadana.

5 Por ejemplo, en el caso de un sistema de defensa aérea basado en la IA, este tipo de ataque podría llevarse a cabo mediante el envío por parte de un adversario de diferentes tipos de aviones (input) y la observación de aquellos que provocan una respuesta de la IA (output).

Con el antecedente de los ciberataques sufridos en el primer decenio de este siglo por Estonia y Georgia, durante la segunda década del siglo XXI, las cuestiones de ciberseguridad consolidaron su importancia, dentro del escenario de la Seguridad Internacional. Las características inherentes de las nuevas tecnologías se han convertido en impulsores de la evolución actual de la IA. Solo o combinado, definirá la ventaja tecnológica necesaria para la eficacia operativa de cualquier Fuerza Armada y será el gran catalizador responsable de dar forma al campo de batalla del siglo XXI, ya sea físico o virtual.

No hay duda de que la IA está haciendo que los sistemas de ciberseguridad sean más inteligentes, ya que se utiliza para la detección de amenazas y evita que los piratas informáticos se infiltren y manipulen los sistemas de defensa críticos. Sin embargo, el futuro de la IA seguirá estando condicionado por la capacidad de cada nación para equilibrar los beneficios y los desafíos de esa tecnología, particularmente en lo que respecta a la ciberseguridad.

No hay duda de que los sistemas basados en la IA harán que la guerra sea más rápida y eficaz. Por ello, resulta imperativo considerar el aspecto de la seguridad durante el desarrollo de cada fase del ciclo de vida de un sistema de IA militar, ya que cualquier fallo puede tener consecuencias catastróficas.

Con la tendencia al aumento de los ciberataques en los próximos años, el papel de la IA crecerá en importancia, dada la posibilidad de desarrollar nuevos algoritmos de detección de amenazas. Sin embargo, los riesgos potenciales derivados del empleo de sistemas basados en esta tecnología también aumentarán, ya que son susceptibles de fallar, como se ha demostrado anteriormente.

Por último, cabe señalar que los constantes avances tecnológicos y la interacción entre la ciberseguridad, la Inteligencia Artificial (IA) y el *Machine Learning* (ML) seguirán presentando nuevas oportunidades y desafíos, lo que implicará la necesidad de revisar la información aquí presentada.

REFERENCIA

AIKEN, Mary. *Life in Cyberspace*. European Investment Bank, 2019.

ALAS, Joe. *Reformists Pull Off Surprise Victory, consider dumping Centrists*. Baltic Times. March 7, 2007. Disponible en: https://www.baltictimes.com/news/articles/17446/. Accedido en: 13 abr. 2022.

ALLIANZ GLOBAL CORPORATE & SPECIALTY. *Allianz Risk Barometer*. *Identifying the Major Business Risks for 2022.* Munich: Allianz Global Corporate & Specialty, 2022.

AMNESTY INTERNATIONAL. *Surveillance Giants: how the Business Model of Google and Facebook threatens Human Rights*. POL 30/1404/2019. London: Amnesty International, 2019.

ARQUILLA, John; RONFELDT, David. *Cyberwar is Coming!* Comparative Strategy, 12(2), 1993, p. 141-165.

BANERJEA, Aparna. *NotPetya: How a Russian malware created the world's worst cyberattack ever*. *Business Standard*, August 27, 2018.

BARTOLOMÉ, Mariano. *Ciberseguridad: claves para entender su vigencia, dinámica y heterogeneidad en el mundo*. Buenos Aires: Infobae, 26 de septiembre de 2020b.

BARTOLOMÉ, Mariano. Las Ciberamenazas y su impacto en el campo de la Seguridad Internacional. Buenos Aires: *Revista de la Escuela Superior de Guerra*, 2020a, 602, p.151-163.

BRITISH BROADCASTING CORPORATION. *El ciberataque de escala mundial y "dimensión nunca antes vista" que afectó a instituciones y empresas de unos 150 países*. *BBC Mundo*, 12 de mayo de 2017.

BRITISH BROADCASTING CORPORATION. *Google Achieves AI "breakthrough" by Beating Go Champion*. London: BBC News, January 27, 2016. Disponible en: https://www.bbc.com/news/technology-35420579 . Accedido en: 14 abr. 2022.

BROEDERS, D. *The Public Core of Internet: An International Agenda for Internet Governance*. Delhi: CyFy Journal, 2016, v. 3, p. 24-30.

BUCHANAN, Ben. *Five Myths about Cyberwar*. Washington-DC: The Washington Post, February 2, 2020.

CARO BEJARANO, María José. *Alcance y ámbito de la Seguridad Nacional en el ciberespacio*. En Instituto Español de Estudios Estratégicos (editor) *Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el ciberespacio*. Cuaderno de Estrategia n.49. Madrid: Ministerio de Defensa, 2010.

CARPENTER, B. E.; DORAN R. W. *The other Turing machine*. London: The Computer Journal, 1977, Vol. 20 (3), p. 269–279. Disponible en: https://doi.org/10.1093/comjnl/20.3.269 Accedido en: 14 abr. 2022.

CCN-CERT. *Desinformación en el ciberespacio*, CCN-CERT BP/13, 2019.

CLARKE, Richard; KNAKE, Robert. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Harper Collins Publisher, 2010, 290 p.

COLLIER, Mike. *Estonia: Cyber Superpower*. Business Week. Dec 17, 2007. Disponible en: https://www.bloomberg.com/news/articles/2007-12-17/estonia-cyber-superpowerbusinessweek-business-news-stock-market-and-financial-advice . Accedido en: 13 abr. 2022.

CONFESSORE, Nicholas. *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*. New York: The New York Times, April 4, 2018.

COPELAND, B.J. *Alan Turing*. London: Encyclopedia Britannica, December 15, 2021. Disponible en: https://www.britannica.com/biography/Alan-Turing. Accedido en: 14 abr. 2022.

CORNEGLIAN, Flavio. O virtual como campo de estudo da geografía. *Caderno de Geografía*, 2016, 26 (46), p. 566-576.

CVETICANIN, Nikolina. *The Largest Battlefield in History - 30 Cyber Warfare Statistics*. *DataProt*, March 15, 2022. Disponible en: https://dataprot.net/statistics/cyber-warfare-statistics/ . Accedido en: 22 abr. 2022.

DAVIS, Joshua. *Hackers Take Down the Most Wired Country in Europe*. Wired Magazine. 15. ed., 2009. Disponible en: www.wired.com/2007/08/ff-estonia/ Accedido en: 11 abr. 2022.

DELOITTE. ¿*Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía*? Murphy Cyber Risk, 2017.

DEPARTMENT OF JUSTICE. *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax*. Office of Public Affairs, February 10, 2020.

DÍAZ-CARDIEL, Jorge. *¿Está perdiendo EE.UU. la guerra tecnológica y de ciberseguridad frente a Rusia y China?* Escudo Digital, 26 de febrero de 2021. Disponible en: https://escudodigital.com/expertos/opinion/el-hackeo-a-solarwinds-revela-importancia-ciberseguridad-eeuu-debe-tomarselo-en-serio/. Accedido en: 14 abr. 2022.

DREXEL University. *Role of Artificial Intelligence in Cybersecurity*. Philadelphia: Drexel University – College of Computing & Informatics, November 04, 2021. Disponible en: https://drexel.edu/cci/stories/role-of-AI-in-cybersecurity/. Accedido en: 14 abr. 2022.

FALLIERE, Nicolas; MURCHU, Liam; CHIEN, Eric. *W32.Stuxnet Dossier. Version 1.4.* Tempe, Arizona: Symantec Security Response, February 2011.

FERNÁNDEZ, Miguel A. Fernández. *Guerra Cibernética*. Portugal: Jornal de Defesa e Relações Internacionais, dezembro de 2013. Disponible en: https://atopo.depo.gal/Record/bib.495129. Accedido en: 09 abr. 2022.

FINN, Peter. *Cyber Assaults on Estonia Typify a New Battle Tactic*. Tallinn, Estonia: Washington Post Foreign Service. May 19, 2007. Disponible en: https://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html. Accedido en: 10 abr. 2022.

FIRE EYE. *APT28: At the Center of the Storm*. Special Report, January 2017.

GAIDOSH, Tamas. *The Industrialization of Cybercrime. Lone-wolf hackers yield to mature businesses*. Finance & Development, June 2018, p. 22-25.

GEORGE, Julia A. *The Politics of Ethnic Separatism in Russia and Georgia*. New York: Palgrave Macmillian, 2009. 260 p.

GRAY, Maggie; ERTAN, Amy. *Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States, Strategies and Deployment*. Tallin: NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), p. 34, 2021.

GUINNESS, Rob. *What is Artificial Intelligence? From Turing Machines to Checkers*. Toronto: Towards Data Science (TDS). Mar 20, 2018. Disponible: https://towardsdatascience.com/what-is-artificial-intelligence-part-2-bad0cb97e330 . Acceso en: 15 abr. 2022.

HATHAWAY, Melissa; KLIMBURG, Alexander. *Preliminary Considerations on National Cyber Security*. In Klimburg, Alexander (editor), National Cyber Security Framework Manual. Tallinn: NATO CCD COE, 2012, p.1-43.

HAWLEY, John K. *Patriot Wars*. Washington-DC: Center for a New American Security (CNAS), January 25, 2017. Disponible: https://www.cnas.org/publications/reports/patriot-wars Accedido en: 14 April 2022.

HOLLIS, David. *Cyberwar Case Study: Georgia 2008*. Small Wars Journal, January 6, 2011.

HOROWITZ, Michael C.; SCHARRE, Paul; VELEZ-GREEN, Alexander. *¿A stable nuclear future? The impact of autonomous systems and artificial intelligence.* New York: arXiv preprint arXiv:1912.05291, 2019. Disponible en: https://arxiv.org/abs/1912.05291. Accedido en: 15 abr. 2022.

INTERNATIONAL BUSINESS MACHINES CORPORATION. *¿O que é Inteligência Artificial (IA)?* New York: International Business Machines Corporation (IBM), June 3, 2020. Disponible en: https://www.ibm.com/br-pt/cloud/learn/what-is-artificial-intelligence. Accedido en: 15 abr. 2022.

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES (IISS). *Cyber Capabilities and National Power: A Net Assessment*. London: The International Institute for Strategic Sudies, 2021.

INTERNATIONAL TELECOMMUNICATIONS UNION (ITU). *Guide to Developing a National Cybersecurity Strategy. Strategic Engagement in Cybersecurity*. Geneve: ITU, 2018.

KASH, Wyatt. *Lessons from the Cyberattack on Estonia*. Entrevista con Lauri Allman, Subsecretario Permanente de Defensa de Estonia. Jun 13, 2008. Disponible en: https://gcn.com/cloud-infrastructure/2008/06/lessons-from-the-cyberattacks-on-estonia/278352/. Accedido en: 10 abr. 2022.

KEMP, Simon. *Digital 2022: Global Overview Report*. Singapore: Datareportal, 2022. Disponible en: https://datareportal.com/reports/digital-2022-global-overview-report . Accedido en: 22 abr. 2022.

KISSINGER, Henry. *Orden Mundial*. Barcelona: Debate, 2016.

KNIGHT, Will. *A Dogfight Renews Concerns About AI's Lethal Potential*. San Francisco-CA: Wired, Conde Nast, August 25, 2020. Disponible en:: https://www.wired.com/story/dogfight-renews-concerns-ai-lethal-potential/. Accedido en: 14 abr. 2022.

KOPERNA, Carol A. *Practical Issues for Expert Systems*. Bethlehem, PA: Lehigh University, January 1, 1986. Disponible en: https://preserve.lib.lehigh.edu/islandora/object/preserve:bp-13897820 . Accedido en: 15 abr. 2022.

KOZLOWSKI, Andrzej. *Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan*. European Scientific Journal (ESJ). Special Edition, v. 3, 2014.

KUMAR, Aqditi; ROSENBACH, Eric. *The Truth about the Dark Web*. Finance and Development, September 2019, p. 22-25.

LYNN, William. *Defending a New Domain. The Pentagon´s Cyberstrategy*. Washington-DC: Foreign Affairs, 2010, Vol. 89 No. 5, p. 97-108. Disponible: http://www.jstor.org/stable/20788647 Accedido en: 22 abr. 2022.

MAcFARQUHAR, Neil. *Inside the Russian Troll Factory: Zombies and a Breakneck Pace*. New York: The New York Times, February 18, 2018.

MANESS, Ryan; VALERIANO, Brandon. *International Cyber Conflct and National Security*. In: Reveron, Derek, Gvosdev, Nikolas & Cloud, John (editors), *The Oxford Handbook of US National Security*, Oxford Handbook Online, 2018, p. 403-419.

MAURER, Tim; MORGUS, Robert. *Compilation of Existing Cybersecurity and Information Security Related Definitions*. Switzerland: Federal Department of Foreign Affairs, 2014.

McCARTHY, John. *What is Artificial Intelligence?* Stanford-CA: Computer Science Department – Stanford University, 2004, p. 14. Disponible en: http://cse.unl.edu/~choueiry/S09-476-876/Documents/whatisai.pdf. Accedido en: 15 abr. 2022.

McCORDUCK, P. *Machines Who Think*. Natick-MA: A. K. Peters, 2004. Disponible en: https://monoskop.org/images/1/1e/McCorduck_Pamela_Machines_Who_Think_2nd_ed.pdf . Accedido en: 16 abr. 2022.

MONLEÓN-GETINO, Antonio. *El impacto del Big data en la Sociedad de la Información. Significado y utilidad*. Barcelona: Historia y Comunicación Social v. 20, n. 2, 2015, p. 427-445.

MORGAN, Forrest E., Boudreaux, Benjamin, LOHN, Andrew J., ASHBY, Mark, CURRIDEN, Christian, KLIMA, Kelly and GROSSMAN, Derek. *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*. Santa Monica, CA: RAND Corporation, 2020. Disponible en: https://www.rand.org/pubs/research_reports/RR3139-1.html . Accedido en: 14 abr. 2022.

MURPHY, Megan; SCANELL, Kara. *Sony Hack a US 'national security matter'.* New York: Financial Times, December 18, 2014.

NAKASHIMA, Ellen. *Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes*. Washington-DC: The Washington Post, January 12, 2018.

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL (NSTC). *AI and Cybersecurity: Opportunities and Challenges*. Washington-DC: Networking & Information Technology Research and Development Subcommittee: Technical Workshop Summary Report, March 2020.Disponible en: https://www.nitrd.gov/nitrdgroups/index.php?title=AI-CYBER-2019 . Accedido en: 15 abr. 2022.

NORTH ATLANTIC TREATY ORGANIZATION (NATO). *Science and Technology Trends 2020–2040: Exploring the S&T Edge*. Brussels, Belgium: NATO Science and Technology Organization, March 2020. Disponible en: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf . Accedido en: 14 abr. 2022.

NEWMEYER, Kevin. *Elements of National Cybersecurity Strategy for Developing Nations*. National Cybersecurity Institute Journal, v. 1 n. 3, 2015, p. 9-19.

NYE, Joseph. *Cyber Power*. Belfer Center for Science and International Affairs, May 2010.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. *Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence (ODNI)*. ODNI News Release No. 44-20, December 16, 2020. Disponible en: https://www.dni.gov/index.php/newsroom/press-releases/item/2175-joint-statement-by-the-federal-bureau-of-investigation-fbi-the-cybersecurity-and-infrastructure-security-agency-cisa-and-the-office-of-the-director-of-national-intelligence-odni . Accedido en: 22 abr. 2022.

PALMER, Danny. *Cybersecurity: Let's get tactical*. San Francisco-CA: ZDNet, March 2, 2020. Disponible:https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/ . Accedido en: 14 abr. 2022.

PARK, Donghui; WALSTROM, Michael. *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks*. University of Washington, The Henry M. Jackson School of International Studies, JSIS News, October 11, 2017.

QUINTANA, Yolanda. *Ciberguerra*, Madrid: Ediciones de la Catarata, 2016.

REDONDO, Mónica. *Publican los anuncios comprados por Rusia en Facebook*. Hipertextual, 2 de noviembre de 2017.

RID, Thomas. *Cyber War will not take place*. London, Hurst & Co, 2013.

ROBINSON, Neil. *NATO: Changing Gear on Cyber Defense*. NATO Review, 8 June, 2016.

SAMPEDRO OLIVER, Raúl. *Redes sociales: desinformación, adicción y seguridad*. Instituto Español de Estudios Estratégicos (IEEE), Documento de Opinión 30/2021, 9 de marzo de 2021.

SANGER, David. *The Perfect Weapon. War, Sabotage and Fear in the Cyber Age*. New York: Crown Publishing, 2018.

SCHMITT, Michael. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. 1.ed. Cambridge: Cambridge University Press, 2013.

SCHMITT, Michael. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*. 2.ed. Cambridge: Cambridge University Press, 2017.

SCHWAB, Klaus. *The Fourth Industrial Revolution: what it means, how to respond*. Cologny, Switzerland: World Economic Forum, 2016.

SEGAL, Eddie. *AI Applications in Cybersecurity with Real-Life Examples*. Carlsbad-CA: AltexSoft, June 02, 2020. Disponible: https://www.altexsoft.com/blog/ai-cybersecurity/ . Acceso en: 15 abr. 2022.

SIFRY, Micah. *Wikileaks and the Age of Transparency*. Yale: Yale University Press, 2011.

SIMON, David. *Raising the Consequences of Hacking American Companies*. Washington DC: Center for Strategic and International Studies (CSIS), 2017.

SMEETS, Max; LIN, Herbert. *Offensive Cyber Capabilities: to what Ends?* In Minarik, T., Jakschis, R. & Lindstrom, L. (editors), *10th International Conference on Cyber Conflicts: Maximizing Effects*. Tallinn: NATO CCD COE, 2018, p. 55-72.

STANG, Gerald. *Global Commons. Between Cooperation and Competition*. European Union Institute for Security Studies, Issue Brief n.17, April 2013.

STARCK, Nick, BIERBRAUER, David and MAXWELL, Paul. *Artificial Intelligence, Real Risks: Understanding – and mitigating – vulnerabilities in the Military use of AI*. West Point, New York: Modern War Institute at West Point, January 18, 2022. Disponible en: https://mwi.usma.edu/artificial-intelligence-real-risks-understanding-and-mitigating-vulnerabilities-in-the-military-use-of-ai/. Accedido en 16 abr. 2022.

STATISTA RESEARCH DEPARTMENT. *Número de usuarios de Internet por país en América Latina en enero de 2022*. *Statista,* 24 de febrero de 2022. Disponible en: https://es.statista.com/estadisticas/1073677/usuarios-internet-pais-america-latina/ . Accedido en: 22 abr. 2022.

STEFANINI. *The New Role of Artificial Intelligence in Cybersecurity: How Can It Protect Your Business?* Southfield-Michigan: Stefanini Group, April 23, 2021. Disponible en: https://stefanini.com/en/trends/news/role-of-artificial-intelligence-in-cybersecurity-to-protect-busi . Accedido en: 14 abr. 2022.

STEVENS, Tim. *Cyberweapons: Power and the Governance of the Invisible*. International Politics, 55, 2018, p. 482-502.

TAMIR, Michael. *What Is Machine Learning (ML)?* Berkley-CA: [UC] Berkeley School of Information, 26 June 2020. Disponible en: https://ischoolonline.berkeley.edu/blog/what-is-machine-learning/ . Accedido en: 14 abr. 2022.

THE ECONOMIST. War in the fifth domain. Are the mouse and keyboard the new weapons of conflict? *The Economist*, July 3, 2010, p. 9-10.

THE HAGUE CENTRE FOR STRATEGIC STUDIES. *Assessing Cyber Security. A Meta-Analysis of Threats, Trends, and Responses to Cyber Attacks*. The Hague: The Hague Centre for Strategic Studies, 2015.

THEILER, Olaf . *Nuevas amenazas: el ciberespacio*. Revista de la OTAN, 2011. Edición digital, 11 de septiembre de 2015.

TIKK, Eneken; KASKA, Kadri *et al*. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Cooperative Cyber Defence Centre of Excellence (CCDCOE), November 2008. Disponible en: http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf . Accedido en: 11 abr. 2022.

TIKK, Eneken; KASKA, Kadri; VIHUL, Liis. *Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons*. Thessaloniki, Greece: 9º European Conference on Information Warfare and Security, July 2010. Reading: Academic Publishing Limited, p. 288-294. Disponible en: https://scholar.google.com/scholar?cluster=11097321293520859072&hl=en&oi=scholarr. Accedido en: 11 abr. 2022.

TIMBERG, Craig; ROMM, Tony. *New Report on Russian Disinformation, prepared for the Senate, shows the operation's scale and sweep*. Washington-DC: The Washington Post, December 17, 2018.

TORRES SORIANO, Manuel. *Siete lecciones no aprendidas sobre Anonymous*. Madrid: Instituto Español de Estudios Estratégicos, Documento Opinión 122/2013, 10 de diciembre de 2013.

TRIPATHI, K. P. A review on knowledge-based expert system: concept and architecture. *International Journal of Computer Applications – Special Issue on Artificial Intelligence Techniques* – Novel Approaches & Practical Applications, v. 4, p. 19-23, 2011. Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.206.3352&rep=rep1&type=pdf . Accedido en: 14 abr. 2022.

TROTMAN, Andrew; ZHANG, Jinglan. *Future Web Growth and its Consequences for Web Search Architectures*. Computer Science, July 3, 2013.

TUCKER, Eric; BAJAK, Frank; O´BRIEN, Matt. *US agencies hacked in monthslong global cyberspying campaign*. AP News, December 13, 2020.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. *Informe sobre la Economía Digital*. Nueva York: UNCTAD, 2019.

UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE. *Data Protection. Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*. GAO-18-559, August 2018.

UNITED STATES OF AMERICA. *International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World*. Washington-DC: The White House, May 2011. Disponible en: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf . Accedido en: 14 abr. 2022.

THE UNITED STATES AIR FORCE. *USAF AI Annex to DoD AI Strategy*. Washington-DC: Tech. Rep., United States Air Force (2019). Disponible en: https://www.af.mil/Portals/1/documents/5/USAF-AI-Annex-to-DoD-AI-Strategy.pdf . Accedido en: 14 abr. 2022.

VERNON, David; METTA, Giorgio; SANDINI, Giulio. *A survey of artificial cognitive systems:* Implications for the autonomous development of mental capabilities in computational agents. Manhatan-NY: IEEE transactions on evolutionary computation, v. 11, n. 2, p. 151-180, 2007. Disponible en: https://ieeexplore.ieee.org/abstract/document/4141064/. Accedido en: 15 abr. 2022.

VOO, Julia *et.al.*. *National Cyber Power Index 2020.* Cambridge-MA: Belfer Center for Science and International Affairs, September 2020.

GUATEMALA: LA CIBERSEGURIDAD Y LA CIBERDEFENSA

Ronald Eduardo Morales Pérez*

RESUMEN
Los términos relativos a la protección digital pueden parecer confusos si no hay un contexto que no confirme sus intenciones: si la ciberseguridad intenta garantizar la protección de los datos de las personas y instituiciones en espacios digitales, la ciberdefensa, por proponer compararse con las fuerzas militares en ese espacio, abarca tareas más allá de las operaciones defensivas sino también exploratorias y de ataque. En tiempos en los que un ciberataque puede derivar de una acción encaminada a extraer dinero para generar inestabilidades estatales, se hace necesario un debate amplio y accesible a todos los internautas de la enorme importancia de valorar este tipo de protección. En este artículo se presentan aspectos generales, no profundos ni doctrinarios sobre los dos temas y enfoques que Guatemala comienza a desarrollar.
Palabras clave: Ciberseguridad; Ciberdefensa; Cibercrimen; Guatemala; Tecnología.

GUATEMALA: LA CIBERSEGURIDAD Y LA CIBERDEFENSA

RESUMO
Os termos referentes à proteção digital podem parecer confusos se não há um contexto que ratifique suas intenções: se a cibersegurança busca garantir a proteção de dados de indivíduos e instituições em ambientes online, a ciberdefesa, por se propor comparar com as forças militares no espaço digital, abrange tarefas além de operações defensivas, mas também exploratórias e de ataque. Em tempos que um ciberataque pode resultar desde a uma ação dirigida a extrair dinheiro até gerar instabilidades estatais, é necessário um debate amplo e acessível a todos os internautas da enorme importância da valorização dessa modalidade de proteção. No presente artigo, são apresentados aspectos gerais, nem profundos ou doutrinários sobre os temas e o enfoque que a Guatemala inicia a desenvolver.
Palavras-chave: Cibersegurança; Ciberdefesa; Cibercrime; Guatemala; Tecnologia;

1 INTRODUCCIÓN

El impulso de la tecnología ha transformado la sociedad, el uso intensivo de las tecnologías de la información y comunicaciones (TIC´s) y su ubicuidad,

* Maestría en Relaciones Internacionales en la Universidad Rafael Landívar de Guatemala; Maestría en Tecnología y Administración de Recursos en la Universidad Francisco Marroquín de Guatemala, licenciado en Administración de Sistemas de Información en la Universidad Francisco Marroquín de Guatemala; Comandante del Comando de Informática y Tecnología Superior de Estrategia Universidad Nacional de Defensa (China Taiwán). Contacto: remorales@mindef.mil.gt

influyen y seguirán influyendo en la manera que vive, se comunica y transforma el ser humano. Las empresas, como los estados, aprovechan este impulso para promover sus productos, establecer políticas y publicar acciones. Los ciudadanos, consumidores, son el objetivo perseguido por ellos, buscando causar un impacto en su pensamiento, induciéndole o intentando inducirlos hacia opciones que les sean ventajosas. Las personas de similar forma buscan satisfacer diferentes necesidades apoyándose en el uso de la TIC´s, para ello adquieren dispositivos llamados wearables[1], que usan en todo momento, para realizar deportes, para llevar el control de comidas, sueño, descanso, pasos dados, control de prisión, pulsaciones por minuto, para subir contenido en redes sociales, visitar sitios de interés, entre otras muchas que se pueden mencionar.

Si bien el uso, de todo lo anteriormente mencionado, le trae un mejor nivel de vida y comodidad a las personas, también lo expone a ser espiado o que delincuentes informáticos aprovechen las vulnerabilidades que estos puedan tener y se vean expuestos a extorsiones robos o peor aún, que sus datos personales sean negociados por estos en el ciberespacio. Pero no solo las personas se ven expuestas a estos delitos, los estados en su afán de llegar a los ciudadanos publican, crean aplicaciones para facilitar tramites o proveer información, se vuelven vulnerables y requieren de un esfuerzo superior para mantener, no solo sus propias infraestructuras protegidas y disponibles, sino por mandato constitucional, proteger a su población de este tipo de amenazas al igual que las no tecnológicas.

Existe una línea gris muy tenue que separa la Ciberseguridad de Ciberdefensa, cuando un ciberdelincuente ataque el sistema financiero de un país o una empresa multinacional, si bien en un primer análisis del ataque se puede pensar que se trata de una acción dirigida a extraer fondos o dinero de estos, esta acción también puede tener la intención de provocar caos o daños en uno de los elementos del poder nacional, como lo es la economía, esto provoque inestabilidad social y problemas profundos en la sociedad del Estado víctima.

En el presente artículo, se tocan aspectos generales, no profundos ni doctrinarios, sobre los dos temas y el enfoque que Guatemala está empezando a desarrollar.

2 CONCEPTOS Y DEFINICIONES

Para comprender mejor los desafíos a los que se enfrentan las distintas organizaciones en el ámbito de la ciberseguridad, es necesario comprender algunos

1 Wearable hace referencia al conjunto de aparatos y dispositivos electrónicos que se incorporan en alguna parte de nuestro cuerpo interactuando de forma continua con el usuario y con otros dispositivos con la finalidad de realizar alguna función concreta, relojes inteligentes o smartwatchs, zapatillas de deportes con GPS incorporado y pulseras que controlan nuestro estado de salud son ejemplos entre otros muchos de este género tecnológico que se halla poco a poco más presente en nuestras vidas.

conceptos y definiciones importantes, para lo cual se desarrollarán estos de manera general, tomando como marco de referencia distintas fuentes como EC-Council, que es el Consejo Internacional de Consultores de Comercio Electrónico, una entidad que agrupa a una serie de corporaciones que velan por implementar estándares de seguridad en sus respectivos campos.

También se han tomado algunos conceptos de NIST, que es el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, entidad encargada de crear estándares aplicables para el sector gubernamental, pero que ha sido ampliamente aceptado en la generalidad del ámbito de las Tecnologías de la Información; así mismo, existen corporaciones con gran trayectoria en el campo de la seguridad de la información como Cisco, quienes en base a sus investigaciones dentro del ámbito privado, han colaborado en la creación de estándares y buenas prácticas para el resguardo de nuestros datos.

Iniciaremos hablando de la relación entre seguridad de la información, seguridad informática y ciberseguridad. Aunque muchos la aceptan como sinónimos, algunos encuentran diferencias entre estos tres conceptos basados principalmente en su objetivo por lo que iniciaremos ahondando en su definición. Las primeras dos definiciones se alinean de mejor manera, al tratar la seguridad de manera proactiva, mientras que la ciberseguridad además se enfoca en la capacidad de dar respuesta a incidentes de seguridad de la información (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2012)

Seguidamente, debe considerarse también la conceptualización que gira en torno a los elementos de la seguridad de la Información, basándonos en la referencia de EC-COUNCIL, para ello se consideran la confidencialidad, integridad, disponibilidad, autenticidad y no repudio. En cuanto a las amenazas EC-COUNCIL define las amenazas como un evento no deseado que intenta acceder, filtrar, manipular o dañar la integridad, confidencialidad y disponibilidad de los activos, servicios o recursos de una organización, el impacto de una amenaza es potencialmente peligroso para los activos de una organización, una amenaza puede ser accidental, intencional o como reacción del impacto de alguna otra acción, las amenazas pueden tomar cualquier forma desde un atacante, un terrorista, hasta un desempleado o un empleado descontento con la organización (CERTIFIED SOC, 2019).

En su texto, Certified Soc Analyst, EC-COUNCIL clasifica las amenazas de la siguiente manera: *amenazas en la nube, amenazas a dispositivos móviles, amenazas persistentes avanzadas, virus y gusanos, ransomware, botnet, ataques internos y phishing*; esto para mencionar los más trascendentales en la actualidad. Sin embargo existen muchas más, lo realmente importante es que después de conocer los principales vectores de ataque, podemos hacer una concientización al personal de la organización sobre el uso de los datos en la red, como administrarlos, de qué manera podemos prevenir caer en estos tipos de ataques, como poder realizar

pruebas y el proceso de selección del personal que se unirá a nuestra organización, pero también es importante saber que categorías de amenazas existen para que por medio de la Ciberseguridad se le pueda dar una respuesta eficiente a los incidentes cibernéticos.

A su vez en ciberseguridad se deben identificar los tipos de atacantes que son las personas o los grupos que se enfocan en buscar o detectar vulnerabilidades para poder explotarlas y de esa manera generar una ganancia económica o personal. De acuerdo con Cisco, los atacantes pueden clasificarse de acuerdo con sus capacidades y motivaciones, por lo que se puede considerar agruparlos en las categorías de aficionados y Hackers. Estos últimos, según la finalidad de su actividad se han denominado Hackers de Sombrero Blanco, Gris y Negro (protegen la red, la vulneran para diseminar las posibilidades de intrusión a otros y los últimos buscan inutilizarla) (CISCO NETWORKING ACADEMY, 2022).

Es necesario remarcar que existen también los *hackers organizados*, quienes son personas con conocimientos avanzados que conforman organizaciones de ciberdelincuentes, efectúan acciones terroristas, conforman grupos de *hacktivistas* y en algunos casos buscan ser patrocinados por un estado para penetrar y obtener información de alto secreto y dañar los sistemas de información de otros gobiernos, los motivos de estos últimos son generalmente agendas políticas, económicas y militares con fines de espionaje (CISCO NETWORKING ACADEMY, 2022). En el ciberespacio las amenazas internas y externas continúan en aumento, esto hace necesario que las entidades responsables de la infraestructura de una organización continuamente procedan a identificar, evaluar y administrar el riesgo de la seguridad cibernética por medio de una estrategia que sea factible (CISCO NETWORKING ACADEMY, 2022).

Cuando se hace referencia a la estrategia que se tomará para la ciberseguridad de los activos de la información de la organización, existe una interrogante que es la que define el curso de acción de protección en un futuro y está es: ¿Qué marco de referencia se empleará para garantizar los controles de seguridad de forma óptima, escalable e íntegra? Existen varios marcos de referencia reconocidos como la ISO/27001; 2013, COBIT, NIST-SP800.

Según NIST, la identificación permite a la organización crear un control de activos, datos capacidades, personas, con el fin de determinar los posibles riesgos, que recursos son los que respaldaran las funciones críticas y de qué manera los riesgos en ciberseguridad permitan a la organización centrar y priorizar sus esfuerzos; un ejemplo de la identificación de activos puede ser listar los dispositivos y sistemas físicos de la organización, plataformas de software y aplicaciones, los sistemas de información externos, el hardware, datos, tiempo, personal priorizados en función de su criticidad y valor, los roles y responsabilidades de seguridad (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2019).

De acuerdo con la misma fuente, esta fase permite la creación de medidas y

contramedidas de seguridad, su implementación y desarrollo con el fin de limitar o contener el impacto que puede ocasionar un evento o incidente potencial de ciberseguridad, describe las medidas de seguridad que se utilizarán para que exista disponibilidad de los servicios de la infraestructura crítica, un ejemplo de esto puede ser la creación de auditorías a los dispositivos, usuarios y procesos autorizados, el acceso físico a los activos, los accesos remotos (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2019). La detección permite el desarrollo y la implementación de medidas y actividades apropiados con el fin de realizar el descubrimiento oportuno de un evento de ciberseguridad, por medio del monitoreo continuo de la red y los activos de la organización, por ejemplo, se monitorea la actividad del personal, se analizan los eventos detectados, se realizan escaneos de vulnerabilidades, se monitorea la red (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2019).

Para la respuesta de un incidente de ciberseguridad según NIST, se deben de tomar las medidas necesarias, incluyendo actividades para dar respuesta al incidente con el recurso necesario y tener la capacidad para reducir el impacto, un plan o actividad de respuesta puede ser ejecutado durante o después de un incidente (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2019). Esta actividad es muy importante tenerla bien definida y planificada, para que al momento de ser necesario se puedan implementar los planes creados en base a la necesidad de restaurar las capacidades o servicios que se hayan visto comprometidos o afectados durante un incidente de ciberseguridad, los planes pueden ser ejecutados durante o después de un incidente, estos planes normalmente incluyen lecciones aprendidas así como estrategias de recuperación con la finalidad de restaurar la reputación de la institución u organización (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2019).

Como se pudo observar, con la definición de los anteriores pasos, el marco de trabajo de National Institute of Standards and Technology permite en general crear un proceso ordenado y lógico a través de los distintos pasos para el aseguramiento de la información hasta el momento de la recuperación, en caso de que un incidente de seguridad sea consolidado, así como recuperación post-incidente. El futuro de la ciberseguridad se encamina a adoptar nuevas tecnologías, y también incursiona en nuevos paradigmas. Tecnologías como *Big Data, Machine Learning* y *Blockchain*, serán de vital importancia en la construcción de los sistemas de seguridad del futuro (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2019).

EC-COUNCIL define un CENTRO DE OPERACIONES DE SEGURIDAD (SOC) como *"una unidad centralizada que supervisa y analiza continuamente las actividades en curso en los sistemas de información de una organización, como redes, servidores, terminales, bases de datos, aplicaciones, sitios web, etc."* (CERTIFIED SOC, 2019).

Tomando la referencia anterior podemos entonces entender propiamente que el SOC es donde se centralizan todas las funciones y responsabilidades que buscan proteger la información de la organización como objetivo principal, en este

se realizan actividades de detección, gestión de incidencias y todo lo referente a la gestión y protección de información (CERTIFIED SOC, 2019).

Como dato importante se resalta que la inteligencia artificial de amenazas mejora el desempeño de un SOC y coadyuva al hombre en la eficacia y la sostenibilidad de la seguridad de puntos finales, pero las maquinas por si solas no son capaces de responder a todas las amenazas, necesitan de un ente externo, el hombre, para poder generar un análisis con más criterio, con los procedimientos e investigación realizada por la IA. Un analista inexperto puede realizar análisis de nivel superior acortando así el tiempo de respuesta de los incidentes (CERTIFIED SOC, 2019).

Podemos deducir entonces como objetivos principales de un centro de operaciones de seguridad el prevenir, detectar, reportar, priorizar y responder, un incidente de seguridad, cada uno de estos pasos los realiza mediante la utilización de herramientas que se dedican al estudio de los patrones que utiliza para su ataque, como por ejemplo la capacidad de prevención se refiere a la manera en la que evita que un ataque se lleve a cabo y tenga éxito, esto lo realiza por medio de la investigación de indicadores de compromisos (IOC) detectados anteriormente, y por medio de la implementación de reglas de detección. De manera general podemos decir entonces que un Centro de Operaciones de Seguridad trabaja de la siguiente manera:

> Recolecta, analiza y genera informes y reportes, recopila registros de indicadores de compromiso, mantiene informados a los analistas de seguridad de las actividades, alertas y riesgos que surgieron, crea registros y tiene almacenado el nivel de respuesta que se tuvo en el incidente, su flujo de trabajo se basa propiamente en la recolección de registros por medio de las herramientas y plataformas. (CERTIFIED SOC, 2019).

Además, se necesitan distintos criterios para determinar la estrategia apropiada, entre estos tenemos los daños potenciales a los recursos, la necesidad de preservar la evidencia, la disponibilidad del servicio, el tiempo y recurso necesario para la implementación de la estrategia, la eficacia en la estrategia ya sea por contención parcial o total del incidente, así como el tiempo de la solución del incidente. (CERTIFIED SOC, 2019).

3 EL CONTEXTO DE LA CIBERDEFENSA EN GUATEMALA

En el año 2004, la Organización de Estados Americanos publicó la Estrategia Integral Interamericana de Seguridad Cibernética, desde ese entonces ya en dicho documento se resaltaba que la arquitectura de seguridad para el ciberespacio requería de múltiples pasos y una vinculación entre el sector público y privado

con medidas que logren un adecuado consenso, planificación y aceptación (UNA ESTRATEGIA INTERAMERICANA, 2004).

En el Ejército de Guatemala se consideró dentro de la Política de Defensa Nacional lo concerniente a la Ciberdefensa en el año 2015, denotando también la visión y el interés dentro de la institución en la salvaguarda de la soberanía nacional en el dominio cibernético (GUATEMALA, 2015). Para el presente año, la Política Nacional de Defensa recién actualizada toma en cuenta las ciberamenazas como posibles violaciones a la soberanía nacional (GUATEMALA, 2021). En Guatemala, la Estrategia Nacional de Seguridad Cibernética, publicada por el Ministerio de Gobernación en el año 2018 demuestra la necesidad de integración al compromiso regional de proteger el ciberespacio de los guatemaltecos (GUATEMALA, 2018).

Para poder ahondar más en el tema, se delimitará que es la Ciberseguridad y que es la Ciberdefensa como tal, enfocando la atención, sobre todo, en la cooperación interinstitucional, estableciendo los campos de acción de los distintos actores de seguridad de la nación. Algo importante de conceptualizar, es el tener claro el propósito de la existencia de las fuerzas armadas en una nación determinada, como referencia tomaremos una cita de la Constitución Política de la República de Guatemala, considerando que, de manera similar, pueden definirse en otras naciones.

En el artículo 244 establece que: "*El Ejército de Guatemala, es una institución destinada a mantener la independencia, la soberanía y el honor de Guatemala, la integridad del territorio, la paz y la seguridad interior y exterior*" (GUATEMALA, 1985).

Por lo anteriormente citado, se puede deducir que las funciones del Ejército son las de utilizar los diferentes medios puestos a su disposición por el Estado, para que desarrollando operaciones militares cumpla su mandato. El mismo artículo continua "*Está integrado por fuerzas de tierra, aire y mar*". Esto da una idea clara que el Ejército de Guatemala, desarrolla su accionar en diferentes dominios, ya sea una fuerza de tierra o de superficie, fuerza de mar y fuerza de aire o fuerza aérea. En otras naciones donde cuentan con capacidades espaciales, además de los tres dominios descritos, se define un dominio adicional, la fuerza espacial.

Desde hace algunos años además de los dominios previamente descritos se ha considerado un nuevo dominio, el cual no es físico, ni dimensional: el ciberespacio, constituyendo el quinto dominio. Que puede ser definido, utilizando la Guía de Ciberdefensa de la Junta Interamericana de Defensa (JID), que el ciberespacio es el *"entorno conceptual en el que se produce la comunicación a través de redes informáticas"* (GUÍA DE CIBERDEFENSA, 2021).

Buscando una definición más precisa, se encuentra la de la Dra. Lani Kass, directora de la Air Force Cyberspace Task Force, USAF, indica que "el ciberespacio no es ni una misión ni una operación. Es un escenario estratégico, operacional y táctico" (CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL, 2012). Por

su parte, Héctor Gómez Arriagada informa que "las ciberoperaciones deberían entenderse como un instrumento más para la solución de problemas militares en su amplio espectro" (ARRIAGADA, 2013).

Con estos conceptos entonces, podemos definir que el ciberespacio debe ser considerado como un dominio más de actuación de las fuerzas armadas, con sus propias fuerzas, sus propios medios y misiones, pudiendo utilizarse en la consecución de los intereses nacionales de su respectiva nación como se emplea a otras fuerzas.

Para la consecución de sus misiones, una fuerza en el ciberespacio realiza ciberoperaciones, al respecto Gómez Arriagada indica:

> […] las Ciberoperaciones implican intencionalidad, voluntades contrapuestas y el enfrentamiento en el ciberespacio con fines militares, elementos claves que permiten distinguir las ciberoperaciones de otras actividades como la seguridad informática o las Operaciones de Información. (ARRIAGADA, 2013).

El concepto anteriormente citado permite inferir que: para el cumplimiento de su misión, principalmente de defensa, la fuerza militar realiza operaciones militares, que se adjetivan según su dominio de acción, en este caso el ciberespacio, estas se convierten en operaciones de ciberdefensa (ARRIAGADA, 2013).

Esto concuerda de manera muy adecuada con la definición dada por la Junta Interamericana de Defensa en su Guía de Ciberdefensa el cual indica que Ciberdefensa es la "Capacidad organizada y preparada para combatir en el ciberespacio. Comprende actividades defensivas, ofensivas y de inteligencia" (GUÍA DE CIBERDEFENSA, 2021).

La forma de enfrentar los distintos desafíos dentro del ámbito de la ciberdefensa, está íntimamente relacionado con la seguridad de la información y la ciberseguridad, pudiendo utilizar los mismos términos, protocolos, conexiones, hardware, software, con sus mismas vulnerabilidades, amenazas y por tanto la misma forma de tratar las amenazas y gestionar los incidentes de seguridad, teniendo la ventaja de contar con una enorme cantidad de marcos de referencia, dentro del ámbito cibernético casi todo está escrito, por lo que es posible aprovechar todas estas pautas de seguridad, dentro de las operaciones militares.

Las operaciones de ciberdefensa se diferencian de las operaciones de ciberseguridad o de seguridad informática, en la intencionalidad. Mientras que la ciberseguridad se aplica para el resguardo de la información de una organización, la ciberdefensa va más allá, utilizando la plataforma de la ciberseguridad y la seguridad informática, para la ejecución de operaciones militares, con el objeto de cumplir el propósito para el cual fueron creadas las fuerzas armadas, sean estas operaciones

ofensivas, defensivas o de otro tipo, de acuerdo con la doctrina militar y la nación donde sea aplicada.

Para el caso de Guatemala, como un punto de impulso para su accionar, se puede presentar una lección aprendida como axioma "El desarrollo de confianza, por medio del intercambio de conocimientos, mitiga los riesgos en el ámbito de la ciberdefensa". El riesgo principal se concentra en la falta de colaboración entre los sectores afectados, sin embargo, generando confianza entre ellos se pueden desarrollar estrategias conjuntas de mitigación a las amenazas cibernéticas.

En el mes de noviembre de 2010, la UIT publica su resolución 181 destinada a la confianza y seguridad en la utilización de las tecnologías de información. En este documento se establece que los proyectos deben encaminarse a una estrecha colaboración con todos los asociados (INTERNATIONAL TELECOMMUNICATION UNION, 2010). Tossi consideró varios aspectos referentes a las ciberamenazas que se ciernen sobre los países latinoamericanos en vías de desarrollo, al final de su exposición concluye que estas amenazas cibernéticas deben catalogarse en "explotación de redes, ciberespionaje, cibercrimen y ataques a redes informáticas y/o sistemas de control industrial" (TOSSI, 2015).

Vinculando los dos autores anteriores – UIT y Tossi – se obtiene una premisa nueva: confianza y colaboración frente a las amenazas cibernéticas. Una buena forma de crear vínculos de confianza entre sectores se lleva a cabo por medio de capacitaciones, conferencias y entrenamientos donde cada sector proponga, asista y colabore. Estos sectores a los que se hace referencia son inicialmente los sectores de Gobierno, Privado y Académico. Esta es la colaboración y los asociados a los que se refiere la UIT (INTERNATIONAL TELECOMMUNICATION UNION, 2020).

Abreviando el axioma, antes propuesto en "confianza y colaboración", y extrapolándolo a la región Centroamérica, se podría formular las siguientes preguntas para cada país: ¿Existe una política de ciberseguridad o ciberdefensa? ¿Existen unidades de respuesta a incidentes (CERT)? ¿Existen servicios de Gobierno a través de portales web o aplicaciones de telefonía? ¿Hay intercambio o acceso a capacitaciones, entrenamientos o certificaciones de ciberseguridad? Para el caso de Guatemala como muestra de la región, podrían responderse las interrogantes anteriores de esta manera: existe una Política de Seguridad Cibernética publicada en el año 2018, existe un CERT-GT que funciona a nivel gobierno, al cual la iniciativa privada y universidades aún no se encuentran integrados (GUATEMALA, 2019).

Continuando con la siguiente interrogante, Guatemala cuenta con portales de e-gobierno, banca, universidades y empresariales (ITNOW, 2016). Finalmente, también hay entrenamientos y capacitaciones proporcionados por gobierno (COMANDO SUPERIOR DE EDUCACIÓN DEL EJÉRCITO DE GUATEMALA, 2019), la iniciativa privada y universidades, pero los presupuestos han sido limitados, para acceder a estos, o no se han incluido en los proyectos anuales de compra de una forma adecuada para su ejecución (ESPINA, 2018).

Lo cual permite establecer que cada actor hace el esfuerzo por mejorar sus condiciones, según sus recursos, en el ámbito de la ciberseguridad. Cada uno tiene conocimiento de la problemática, afortunadamente, no han tenido que enfrentar un incidente de magnitud severa, que dañara significativamente los activos cibernéticos institucionales, que los lleve a considerar la necesidad de contar con un mayor presupuesto, que les dé una mayor protección.

Siempre haciendo un recuento dentro de la región centroamericana, encontramos que, como medida de fomento de confianza y colaboración entre fuerzas armadas, se encuentra la Conferencia de Fuerzas Armadas Centroamericanas (CFAC).

Este organismo (CFAC) desarrolla actividades especializadas en Logística, Inteligencia, Ayuda Humanitaria, Misiones de Paz, así como entrenamientos tácticos y técnicos. En el ámbito académico existe un programa de intercambio de docentes y alumnos en los centros de profesionalización y de formación de oficiales. Es adecuado entonces preguntar ¿Podrían incorporarse las actividades de capacitación e intercambios de conocimientos en materia de ciberseguridad y ciberdefensa en la CFAC?

Derivado de lo anterior, la respuesta podría positiva, si pueden incorporarse las actividades de capacitación de ciberseguridad y ciberdefensa para los miembros de la CFAC. Una opción estratégica y operacionalmente viable para capacitación en esta materia (ciberseguridad) para la CFAC puede ser propuesta por Guatemala, que forma sus cuadros de oficiales con especialidad de Informática desde 1977 y que ha conformado su batallón de ciberdefensa recientemente.

En años pasados (2000 al 2008) ha invitado a los miembros de CFAC a enviar oficiales a Guatemala para recibir capacitación durante periodos de 8 meses en materia de informática y tecnología, esto puede funcionar nuevamente. Durante ese período, oficiales de las fuerzas armadas de El Salvador, Honduras, Nicaragua y República Dominicana obtuvieron la Especialidad de Informática Militar.

Integrando al tema tratado, la dinámica con la sociedad civil, siempre en aspectos de Ciberdefensa y Ciberseguridad, se comenzará abordando concepciones generales sobre estas relaciones. Primeramente, Samuel Huntington, plantea que las relaciones civiles-militares más exitosas en la actualidad, se basan en lo que él denomina “control civil objetivo”. El autor desarrolla su definición fundamentándola en cuatro aspectos. El primero es el profesionalismo de los militares, el segundo la subordinación militar al poder civil, el tercero el reconocimiento de los civiles a la capacidad profesional militar, finalmente el cuarto aspecto es el resultado de los tres anteriores y consiste en la minimización de la intervención militar en lo civil y viceversa (HUNTINGTON, 1996).

Felipe Agüero, establece su concepto de “supremacía del poder civil” en las democracias en cuatro aspectos fundamentales: el primero conducir el gobierno sin intervención de los militares, el segundo definir los objetivos de la organización

encargada de la defensa nacional, el tercero formular y conducir la política de defensa y el cuarto monitorear la implementación de la política militar (AGÜERO, 1997).

La efectividad de ambos conceptos se hace patente en lo escrito por Michael C. Desch quien dice que cuando el cambio político genera conflicto, éste se ha tratado con profesionalismo, carácter y honorabilidad (DESCH, 2007). Esta frase que se extrae de este documento titulado "Busch y los Generales" permite dar cabida a una reflexión preliminar combinando los tres textos citados, y es que, para que realmente funcione lo que expone Huntington y Agüero debe haber más que "voluntad", debe trascender a "política de Estado".

4 CONCLUSIÓN

Es necesario incorporar en este escrito lo recomendado por el embajador Charles Ray quien al respecto expresa que estas relaciones (civil-militar) deben practicarse con el objeto de crear la cultura de entendimiento, ya que, al vencer las barreras de los estereotipos, se genera un clima de confianza entre ambas partes dando paso a buenas relaciones interpersonales (RAY, 2019). Efectivamente, la recomendación del embajador Ray permite incorporar ahora el concepto de Bruneau acerca de la "efectividad militar". Este concepto tiene que ver primariamente con la capacidad de la organización militar de alcanzar objetivos, estos objetivos son impuestos por la política. El éxito de alcanzar los objetivos radica en mucha preparación militar para crear poder a partir de los recursos básicos del Estado: riqueza, tecnología, tamaño de la población y el capital humano (BRUNEAU; CROISSANT, 2019)

Ahora bien, el Dr. David Pión-Berlin describe que parte de la problemática radica en que los civiles no pueden liderar a sus pares militares debido al desconocimiento de los asuntos de defensa y seguridad (PION-BERLIN, 2005). Sin embargo, en el campo de la Ciberseguridad, esta brecha se ha reducido, y existe en el ecosistema cibernético guatemalteco, mucha capacidad tanto en el ámbito civil público como privado.

Debemos remarcar que en Guatemala existe una base de procedimientos para el establecimiento de una relación civil-militar ideal, la cual desarrollada por la Dirección General de Política de Defensa y el Comando Superior de Educación del Ejército, en los cuales se imparten cursos que siempre incluyen la parte de Ciberdefensa. Muy probablemente, en el futuro inmediato, se concretice la Ley sobre Cibercrimen para Guatemala que permitirá un desarrollo de infraestructura y marcos legales adecuados, pero también abra la posibilidad de una mayor interacción cívico-militar en este campo, que permita robustecer las medidas de Ciberdefensa.

La Ciberdefensa y la Ciberseguridad, van de la mano, no puede ser una

fuerte si la otra es débil, la interacción cívico-militar se debe fortalecer en el ámbito nacional, la existencia de un marco legal adecuado puede ser el inicio de una integración más completa y armoniosa. Y en el ámbito regional, Guatemala ha dado los pasos adecuados en el establecimiento de medidas de fomento de confianza y colaboración entre fuerzas armadas, como lo establece la CFAC, en el ámbito de la Ciberdefensa, capacitando a más de 10 oficiales de los diferentes países de la región.

Si las cadenas ser rompen por el eslabón más débil, Guatemala ha desarrollado una serie de acciones para fortalecer el segmento que le corresponde y al mismo tiempo ensayado la cooperación y colaboración con otras fuerzas armadas y a lo interno con la sociedad civil de diferentes maneras. Por un ecosistema cibernético robusto y colaborativo, seguiremos trabajando.

REFERENCIAS

5 DATOS ACERCA DEL EGOVERNMENT EN GUATEMALA. Revista ITNow, August 22, 2016. Disponible en: https://revistaitnow.com/5-datos-acerca-del-egovernment-en-guatemala/. Accedido en: 16 feb. 2020.

AGÜERO, Felipe. Toward Civilian Supremacy in South America, Consolidating the Third Wave Democracies, Baltimore, The Johns Hopkins University Press, 1997.
ARRIAGADA, H. G. Cyberoperations. *Revista Marina*, Viña del Mar, v. 935, 2013.
BRUNEAU, Thomas C.; CROISSANT, Aurel. Civil-Military Relations: Why Control Is Not Enough, Civil Military Relations, 2019.

CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL. (España). *El Ciberespacio, nuevo escenario de confrontación*. Madrid: CESEDEN, 2012. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf. Accedido en: 14 nov. 2021

CERTIFIED SOC Analyst (CSA). *EC-Council*, Tampa, 2019.

CISCO NETWORKING ACADEMY. Introduction to Cybersecurity. [*S. l.*]: Cisco Network Academy, 2022. Disponible en: https://www.netacad.com/es/courses/cybersecurity. Accedido en: 16 nov. 2021

COMANDO SUPERIOR DE EDUCACIÓN DEL EJÉRCITO DE GUATEMALA. Clausura del Primer Curso de 'Oficial Director de Ciberseguridad. Ciudad de Guatemala, 2019. Disponible en: https://www.cosede.mil.gt/comando-superior-de-educacion-del-ejercito-guatemala/2019/02/01/clausura-del-primer-curso-de-oficial-director-de-ciberseguridad/. Accedido en: February 16, 2020.

DESCH, M. C. Bush and the Generals, *Foreign Affairs*, v. 86, n. 3, p. 97-108, 2007.

ESPINA, Cindy. Ejército Solicita Dinero Para Crear Centro de Ciberdefensa, *El Periódico (blog*), publicado en 14 jun 2018. Disponible en: https://elperiodico.com.gt/nacion/2018/06/14/ejercito-solicita-dinero-para-crear-centro-de-ciberdefensa/. Accedido en 16 feb 2020.

GUATEMALA. [Constitución (1985)]. *Constitución Política de la República de Guatemala*. Ciudad de Guatemala: [*S. n*.], 1985.

GUATEMALA. "Dependencias de Gobernación fortalecidas contra ataques cibernéticos," *Ministerio de Gobernación (blog)*, May 20, 2019, https://mingob.gob.gt/dependencias-de-gobernacion-fortalecidas-contra-ataques-ciberneticos/. Accedido en: 16 nov. 2021.

GUATEMALA. Estrategia Nacional de Seguridad Cibernética, *Ministerio de Gobernación (blog),* June 20, 2018, Disponible en: https://mingob.gob.gt/estrategia-nacional-de-seguridad-cibernetica/. Accedido en: 16 nov. 2021.

GUATEMALA. Política Nacional De Defensa 2021-2032. Ciudad de Guatemala*, Ministerio de la Defensa Nacional (blog)*, 11 de octubre de 2021. Disponible en: https://www.mindef.mil.gt/datos_abiertos/pdf/politica%20nac%20def%202021.pdf. Accedido en: 16 nov. 2021.

GUÍA DE CIBERDEFENSA: ORIENTACIONES PARA EL DISEÑO, PLANEAMIENTO, IMPLANTACIÓN Y DESARROLLO DE UMA CIBERDEFENSA MILITAR. Washington, DC*: Junta Interamericana de Defensa*, 2020. Disponible en: https://www.jid.org/wp-content/uploads/2022/01/Ciberdefensa10.pdf. Accedido en: 16 nov. 2021

HUNTINGTON, Samuel. Reforming Civil-Military Relations, Civil-Military Relations and Democracy, Baltimore, The Johns Hopkins University Press, 1996.
IBM. *Servicios gestionados de seguridad de infraestructura y de red*. La Molina: IBM, [202-]. Disponible en: https://www.ibm.com/pe-es/security/services/managed-security-services/infrastructure-and-endpoint. Accedido en: 14 nov. 2021.

INTERNATIONAL TELECOMMUNICATION UNION. Resolución 181 de Ciberseguridad, Guadalajara, Plenipotentiary Conference 2010, Disponible en: https://www.itu.int/en/council/Documents/basic-texts/RES-181-S.pdf Accedido en: 16 nov. 2021

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Glosario de términos clave de seguridad de la información*. Gaithersburg, MD: NIST, 2013.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Guía para la realización de evaluaciones de Riesgo - B-6*. Gaithersburg, MD: NIST, 2013.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Marco NIST Ciberseguridad - 5*. Gaithersburg, MD: NIST, 2019.

PION-BERLIN, David. Political Management of the Military in Latin America, Military Review, p.19–31, 2005.

RAY, Charles. La Realidad de Las Operaciones (Conferencia, October 28, 2019).

TOSSI, Alejandro Amigo. CONSIDERACIONES SOBRE LA CIBERAMENAZA A LA SEGURIDAD NACIONAL. Revista Política y Estrategia, no. 125: p. 83–96, 2015.

UNA ESTRATEGIA INTERAMERICANA INTEGRAL DE SEGURIDAD CIBERNÉTICA. *Boletín Electrónico,* n. 1, jul. 2004. Disponible en: http://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp. Acceso en: 16 nov, 2017.

CIBERSEGURIDAD, INTELIGENCIA ARTIFICIAL Y NUEVAS TECNOLOGÍAS EN EL ÁREA DE DEFENSA

Sergio Portillo Bustillo*
Juan Carlos Martínez Midence**
Rafael Antonio Maradiaga Molina***

RESUMEN
Este artículo pretende dirigir al lector breves consideraciones sobre el escenario actual de la seguridad cibernética desde una perspectiva diacrónica de seguridad nacional y presentando conceptos de términos recientes de Defensa digital, alineados con las obras de importantes experts en el tema. La intención es informar y envolver el ciudadano debates como la importancia del Estado valorar la defensa y la seguridad en ambientes en línea, el fenómeno de la "brecha digital" y sus implicaciones y el avance tecnológico en los países latinoamericanos en la era de los ciberataques.
Palabras clave: Ciberdefensa; ciberseguridad; Tecnologías de la Información y Comunicación (TIC's); Tecnología; Latinoamérica.

CIBERSEGURANÇA, INTELIGÊNCIA ARTIFICIAL E NOVAS TECNOLOGIAS NA ÁREA DE DEFESA

RESUMO
Esse artigo pretende dirigir ao leitor breves considerações sobre o atual panorama da segurança cibernética no mundo a partir de uma perspectiva diacrônica de segurança nacional e apresentando conceituações de recentes termos de Defesa digital, alinhadas com as obras de importantes experts do assunto. A intenção é informar e tornar próximas ao cidadão discussões como a importância da valorização do Estado pela defesa e segurança em ambientes online, o fenômeno da "brecha digital" e suas implicações e o avanço tecnológico em países da América Latina na era dos ataques cibernéticos.
Palavras-chave: Ciberdefesa; cibersegurança; Tecnologias da informação e Comunicação (TIC's); Tecnologias; América Latina

* Curso de Comando y Estado Mayor en la Escuela de Comando y Estado Mayor de Honduras, Curso de Altos Estudios Militares, Diplomado en Desarrollo Gerencial, actualmente Rector del Colegio de Defensa Nacional de Honduras. Contacto: sportillo65@yahoo.com

** Licenciado en Administración de Empresas y Ciencias Militares, Diplomado en Alta Gerencia, Finanzas y Administración Pública, actualmente Vicerrector del Colegio de Defensa Nacional de Honduras. Contacto: cdndrru@ffaa.mil.hn

*** Doctor en Ciencias de la Administración, Maestría en administración y finanzas, Ingeniero electricista Industrial, Ingeniero en telecomunicaciones, especialista en metodología de la investigación, estadística, tecnología de la información y comunicaciones; ciberdefensa y ciberseguridad. Actualmente docente del Colegio de Defensa Nacional de Honduras. Contacto: maradiagam@gmail.com

1 INTRODUCCIÓN

Desde el principio de los tiempos el hombre ha evolucionado gracias a su ingenio y espíritu emprendedor, ha estudiado a través del tiempo el que, como, donde, porque de las cosas usando herramientas sofisticadas, de acuerdo a su época, que facilitan su vida, la forma de hacer en negocios, educación, medicina, astronomía, seguridad y defensa en una serie de disciplinas y especialidades en los campos de la ciencia a través de la aplicación de la tecnología. Los sistemas de información utilizando las redes de telecomunicaciones y las tecnologías de la información y comunicación han evolucionado para favorecer y facilitar la toma de decisiones.

Las capacidades de Ciberdefensa es el término empleado para referirse a los recursos necesarios para asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los servicios proporcionados por los sistemas TIC en el entorno de operación, en respuesta a posibles inminentes acciones maliciosas originadas en el ciberespacio; esta se realiza para prever, planear, dirigir, organizar y emplear sus sistemas en todo tiempo y de manera efectiva.

La Inteligencia Artificial (IA), relacionada con la inteligencia humana establece la necesidad de producir máquinas útiles que procesan la conducta inteligente de humanos a través de procesos digitales. La ciberseguridad es el esfuerzo constante por proteger sistemas de red y los datos contra el uso no autorizado: a nivel personal, debe proteger la identidad, datos y dispositivos informáticos; a nivel corporativo, proteger la reputación, información y clientes de la organización y a nivel del estado, la seguridad nacional, y el bienestar de los ciudadanos.

2 CIBERSEGURIDAD

Los sistemas de información y comunicaciones frecuentemente son cada vez más atacados por nuevas y más complejas amenazas que implica, en lo que a Ciberdefensa se refiere, que los datos sobre nuevas vulnerabilidades y ataques deban ser analizados, fusionados, correlacionados y procesados, de forma automática o semiautomática con intervención de un operador, a una velocidad que permita tomar decisiones y ejecutar acciones en el momento oportuno (ESTRADA, 2017).

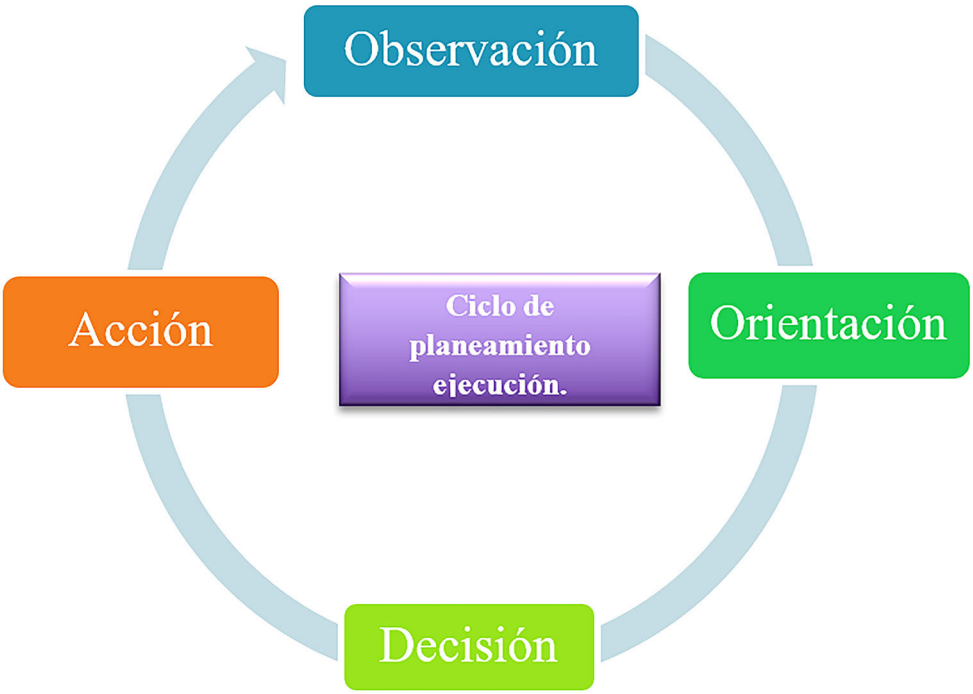
2.1 CICLO OBSERVAR-ORIENTAR-DECIDIR-ACTUAR (OODA)

En este contexto, tanto a nivel internacional como nacional, se está empezando a trabajar, como forma de garantizar la seguridad de los sistemas TIC, en un concepto de operación de Ciberdefensa que propone la aplicación de una ciclo de toma de decisiones basado en el estándar Observar-Orientar-Decidir-Actuar (OODA) desarrollado por el Coronel John Boyd, ex piloto de combate de la

USAF (Fuerza Aérea de EE.UU), en base a su intensa experiencia durante la Guerra Vietnam (ARNILLAS; SHAFFER; MANTILLA, 2013).

El ciclo de toma de decisiones es utilizado ampliamente en distintos campos que van desde el militar hasta el financiero y su propósito es el ofrecer una metodología para reaccionar rápidamente ante la incertidumbre sin certeza del desenlace, tomando ventaja sobre el adversario.

Figura 1. Fases del ciclo ODDA



Fuente: COLEGIO OFICIAL INGENIEROS DE TELECOMUNICACIÓN, [202-].

Su aplicación a Ciberdefensa consiste en desglosar sus actividades con respecto las cuatro fases del bucle Observar-Orientar-Decidir-Actuar, con el objetivo de obtener capacidades y proporcionar una capacidad reactiva para defender los sistemas TIC en su fase operativa. Se concentra en los aspectos que requieren la automatización para permitir una reacción en el momento oportuno ante ciberataques.

La aplicación del concepto ciclo OODA a ciberdefensa provee una manera simple e instintiva de estructurar servicios, componentes y funcionalidades a establecer en un sistema de Ciberdefensa. Actualmente, las herramientas disponibles para mitigar los ataques son cada vez menos eficaces contra los ataques,

ya que el número y el tipo y número de vulnerabilidades aumenta continuamente. Una forma de mejorar la disponibilidad y eficacia de los sistemas TIC es el uso del bucle de OODA, pues ayuda a identificar la necesidad automatizar las actividades de identificación y correlación de las actividades maliciosas, para saber en todo momento cual es la situación y poder responder apropiadamente y en el momento oportuno (BRUMLEY, 2014).

La aplicación del ciclo OODA comienza con la obtención de información proveniente de los sensores y datos de referencia como pueden ser las bases de datos de vulnerabilidades, listas negras, etc. realizando sobre ellos operaciones de transformación, normalización, fusión y agregación al objeto de obtener un delta de información útil. Seguidamente estos datos procesados se correlacionan contras reglas que describen patrones ataque para calcular todas las posibles vías de penetración en la red. Los posibles ataques se encadenan y se almacenan en una estructura de datos y se exponen a los operadores para su evaluación o se desencadenan capacidades de respuesta automática.

Figura 2. Entorno de operación del ciclo Observar-Orientar-Decidir-Actuar (OODA)

Fuente: COLEGIO OFICIAL INGENIEROS DE TELECOMUNICACIÓN, [202-].

El siguiente paso es el generar diferentes cursos de acción priorizados en función de su coste operativo en relación a impacto conseguido versus recursos necesarios. Cada curso de acción se compone de una combinación de acciones que en conjunto reducen las capacidades de los atacantes.

Cursos de acción incluyen una o varias acciones específicas, entre ellas puede ser la aplicación de un parche o una actualización, la reconfiguración

de una conexión, la activación o desactivación de un servicio, la alteración de la configuración del host específico o el desencadenamiento de una capacidad de respuesta (JOHAN SILVANDERA, 2019).

Los efectos de estas acciones son monitoreados y cualquier cambio en la red se detecta en el módulo de recogida de datos y el proceso se repite. En la figura siguiente se muestra el entorno de operación de aplicación del ciclo. Se definen dos tipos de operaciones básicas a realizar en cada una de las fases del ciclo:

- *Acciones Preventivas*: tienen como misión principal la prevención de los ataques antes de que ocurran y abarcan el despliegue de recursos de manera óptima para mejorar la seguridad de la red y la implementación de planes de mitigación (parches, actualizaciones, etc.).
- *Acciones Reactivas*: son las acciones en tiempo real a realizar como respuesta a incidentes de seguridad. Los cursos de acción generados podrán ser de una manera totalmente automática, sin intervención del operador, o de una manera semiautomatizada, donde opciones se presentan para la selección y aprobación del operador.

2.2 ESTRATEGIA DE DEFENSA Y SEGURIDAD NACIONAL

La Estrategia de Defensa y Seguridad Nacional es el marco de referencia para la política de sobre el tema referido, generando las políticas de Estado que parte de una concepción amplia de la cual se ha de desarrollar en el ámbito nacional, en complemento al internacional.

2.3 RETOS DE LA DEFENSA Y SEGURIDAD NACIONAL

Los retos que presentan un sistema global altamente interdependiente, tanto en el plano físico como en el digital, donde se desencadenan crisis en cadena que tienen impacto sobre varios ámbitos simultáneamente, requieren una reflexión estratégica que vaya acompañada del necesario ajuste o desarrollo de nuestro Sistema de Defensa y Seguridad Nacional. La naturaleza global de las amenazas junto con la velocidad del cambio hace necesario:

- Evaluar los ámbitos definidos en la Defensa y Seguridad Nacional y las relaciones entre ellos para establecer líneas de acción mucho más transversales e integradas que permitan la debida planificación y preparación para hacer frente a cualquier eventual crisis;
- Establecer un sistema de alerta temprana para cada ámbito de la Defensa y Seguridad Nacional, basado en indicadores y aprovechando la tecnología disponible, que permita la detección de crisis potenciales y

la activación temprana del sistema de gestión de crisis para una óptima administración de todos los recursos disponibles;
- Utilizar la tecnología, aprovechando la inteligencia artificial y la mecanización de procesos, para lograr una mayor velocidad de reacción, mayor integración, compartición de datos y digitalización de procesos.

2.4 OBJETIVOS DE LA DEFENSA Y SEGURIDAD

Lograr que los Sistemas de Información del Estado se utilicen de manera eficaz, para el fortaleciendo las capacidades de prevención, defensa, detección, y respuesta a las amenazas.

2.4.1 Objetivos Generales

- Garantizar que los Sistemas de Información que utiliza la administración pública posea el adecuado nivel de Defensa y Seguridad y resiliencia.
- Impulsar la Defensa y Seguridad y resiliencia de los Sistemas de Información utilizados por el sector institucional en general y los operadores de infraestructuras esenciales en particular.
- Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia.
- Sensibilizar al sector público, privado y la ciudadanía en general sobre los riesgos derivados por el acceso a la información.
- Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita El Estado para sustentar todos los objetivos de Defensa y Seguridad.
- Contribuir a la mejora de la Defensa y Seguridad nacional en el ámbito internacional.

2.5 LÍNEAS DE ACCIÓN DE LA DEFENSA Y SEGURIDAD NACIONAL

LÍNEA DE ACCIÓN 1: Desarrollar la capacidad de prevención, detección, respuesta y recuperación ante las amenazas.

LÍNEA DE ACCIÓN 2: Establecer la Defensa y Seguridad de los Sistemas de Información, de Energía y de Telecomunicaciones que soportan la administración pública.

LÍNEA DE ACCIÓN 3: Establecer Defensa y Seguridad de los Sistemas de Información, de Energía y de Telecomunicaciones que soportan las infraestructuras críticas.

LÍNEA DE ACCIÓN 4: Establecer la capacidad de investigación y persecución

del terrorismo y la delincuencia.

LÍNEA DE ACCIÓN 5: Impulsar la Defensa y Seguridad y resiliencia de las TIC en el sector público y privado.

LÍNEA DE ACCIÓN 6: Generar conocimientos, competencias e I+D+i.

LÍNEA DE ACCIÓN 7: Promover la sensibilización y Cultura de Defensa y Seguridad.

LÍNEA DE ACCIÓN 8: Promover el compromiso internacional.

LÍNEA DE ACCIÓN 9: Promover la coordinación nacional.

LÍNEA DE ACCIÓN 10: Adecuar las normas jurídicas vigentes.

2.6 LA NECESIDAD DE UNA ESTRATEGIA NACIONAL

El ciberespacio es un dominio único, ya que no ocupa espacio físico en sí. Pero sin embargo lo hace, depende de nodos físicos, servidores y terminales que se encuentran en las naciones que ejercen el control y a veces la propiedad. El bien público que viaja por la autopista de la información es artificial y difícil de categorizar o localizar. Se debe contar que el ciberespacio es un lugar sin límites o fronteras llenos de un bien común atrapado en datos, constituyendo información de todos los actores del mundo desde los Estados a las compañías hasta sin fin de información personal. Sin embargo, hay una geopolítica inmersa referente a los meridianos de nuestro planeta por los cuales se tiene acceso.

Hasta hace poco, la mayoría de los hackers estaban después de la información que constituye la carga útil del espacio, en lugar de su infraestructura. Esto, sin embargo, está cambiando. La base de la infraestructura y la información del espacio son casi en su totalidad en manos de las instituciones privadas y comerciales, en lugar de los gobiernos o de los militares. Para complicar aún más las cosas, a diferencia de los otros dominios, el ciberespacio no depende principalmente del poder del Estado para la Defensa y Seguridad; la gran mayoría de las redes son privadas y competitivas en su naturaleza. En este entorno, los proveedores han sido bastante resistentes a la regulación y la Defensa y Seguridad, y prefieren la autorregulación y menos Defensa y Seguridad en lugar de aceptar las limitaciones y los mayores costos que aumentan la Defensa y Seguridad y fiabilidad.

En este sentido, las regulaciones para optimizar los recursos que inciden en la Defensa y Seguridad que el Estado ha de dictar, se consideran:

- A los gobiernos incumbe la función de dirigir la formulación y aplicación de estrategias nacionales exhaustivas, orientadas al futuro y sostenibles. El sector privado y la sociedad civil, en diálogo con los gobiernos, tienen una importante función consultiva en la formulación de esas estrategias nacionales.

- La aportación del sector privado es importante para el desarrollo y la difusión de las Tecnologías de la Información y las Comunicaciones (TIC) en ámbitos como infraestructura, contenido y aplicaciones. El sector privado no es sólo un actor del mercado, sino que desempeña un papel en el contexto más amplio de desarrollo sostenible.
- El compromiso y la participación de la sociedad civil es igualmente importante en la creación de una Sociedad de la Información equitativa y en la instrumentación de las iniciativas para el desarrollo relacionadas con las TIC.
- Las instituciones internacionales y regionales, incluidas las instituciones financieras, desempeñan un papel clave a la hora de integrar la utilización de las TIC en el proceso de desarrollo y proporcionar los recursos necesarios para construir la Sociedad de la Información y evaluar los progresos alcanzados.

2.7 INICIATIVA PARA LA ESTRATEGIA

Las iniciativas que se han de considerar en la Estrategia Nacional se basan en cuatro principios fundamentales:

- Aprovechamiento de las tecnologías: fomentar el desarrollo de la utilización de una amplia gama de tecnologías, desde modernas infraestructuras hasta nuevas aplicaciones en esferas como comercio, salud, educación, agricultura, gobierno y Defensa y Seguridad en línea.
- Creación de capacidad: dar a la población local los medios para crear y administrar sus propios proyectos gracias al desarrollo efectivo de los recursos humanos.
- Políticas y estrategias: ayudar a los gobiernos a elaborar y poner en práctica políticas y leyes que favorezcan la instalación y utilización de las TIC.
- Asociaciones/alianzas: reunir a los socios del sector público y el sector privado para elaborar proyectos que beneficien a todos los interesados, incluida la comunidad entera.
- Sólo un enfoque integral, que conciba la Defensa y Seguridad de manera amplia e interdisciplinaria a nivel nacional, regional e internacional, puede responder a los complejos retos a los que nos enfrentamos. La política de Defensa y Seguridad se basa en seis conceptos básicos:
- Enfoque integral de las diversas dimensiones de la Defensa y Seguridad,
- Coordinación entre las administraciones públicas y con la sociedad,
- Eficiencia en el uso de los recursos,
- Anticipación y prevención de las amenazas y riesgos,

- Resistencia y recuperación de sistemas e instrumentos e,
- Interdependencia responsable con nuestros socios y aliados.

Dentro de la estrategia de Defensa y Seguridad del Estado, se analizan los fenómenos globales que propician la propagación o transformación de los riesgos y amenazas que nos afectan; entre los fenómenos se encuentran disfunciones de la globalización, desequilibrios demográficos, pobreza y desigualdad, cambio climático, peligros tecnológicos e ideologías radicales y no democráticas, todos éstos considerados como potenciadores de los riesgos y amenazas.

La estrategia de Defensa y Seguridad del Estado destaca que es necesaria una coordinación entre en la administración pública y el sector privado en materia de infraestructuras críticas, dado que parte de las infraestructuras críticas y esenciales, en alguna proporción, está en manos de este sector privado, lo que hace necesaria una comunicación, coordinación constante y eficaz.

Para reforzar la resistencia y capacidad de recuperación de los activos fundamentales, la estrategia de Defensa y Seguridad del Estado considera indispensable seguir avanzando en aspectos como la consolidación de los instrumentos para la protección de las instalaciones, la mejora del marco regulador de los sectores críticos, el establecimiento de medidas que aumenten su fortaleza, incrementen su resistencia y refuercen sus capacidades de adaptación ante condiciones adversas, el diálogo y cooperación permanente entre las administraciones públicas y los operadores de infraestructuras y servicios.

La estrategia de Defensa y Seguridad del Estado, destaca por encima de las demás la necesidad de impulsar cambios orgánicos al máximo nivel del Estado, que garanticen la articulación de esta nueva concepción integrada de la Defensa y Seguridad, su gestión y su seguimiento.

2.8 COMPETENCIA POLÍTICA

Son retos como la competencia geopolítica, la polarización social o la transformación tecnológica que las estrategias denominan como “dinámicas de transformación de la Defensa y Seguridad Global” y que, a diferencia de los retos directos y tangibles que reconocen las estrategias (terrorismo, crimen organizado o conflictos armados, entre muchos otros), no cuentan con líneas de acción transversales para afrontarlas y permanecen en los ‘silos’ ministeriales de turno.

Las dinámicas que se retroalimentan retos como la dependencia, la disrupción tecnológica, la desinformación, la deslocalización o el talento, cuyos efectos no son tan inmediatos o tangibles sobre la Defensa y Seguridad Nacional como para entrar en su agenda con personalidad propia. Sin embargo, sus efectos son sistémicos porque ponen en peligro el modo de vida habitual de los ciudadanos y generan inseguridad ontológica en la sociedad. Mientras no se reconozcan como riesgos,

el Sistema de Defensa y Seguridad Nacional no podrá habilitar sus instrumentos y capacidades de coordinación para asegurar una atención transversal e integral a los mismos.

Cuadro 1: Dinámicas de transformación de la Defensa y Seguridad Global

Dimensiones	Descripción
Competencia geopolítica	Crece la competición entre actores que tienen distinta visión de la Defensa y Seguridad y de las instituciones multilaterales
Proteccionismo económico	Auge del proteccionismo en una economía globalizada
Polarización social	Crece la influencia de movimientos exclusivistas que pueden afectar a la cohesión social y la estabilidad política
Aceleración tecnológica	Las nuevas tecnologías tendrán un impacto en la Defensa y Seguridad
Cambio climático	Tiene graves repercusiones políticas, económicas y sociales, a corto y largo plazo

Fuente: COLEGIO OFICIAL INGENIEROS DE TELECOMUNICACIÓN, [202-].

La postergación de las "dinámicas" frente a las "amenazas y desafíos" a la hora de tomar medidas en las estrategias se explica por varias razones. En primer lugar, y dada la naturaleza intergubernamental del procedimiento, es lógico que entren antes en la agenda de la Defensa y Seguridad Nacional las preferencias y preocupaciones de cada uno de los Ministerios. Las dinámicas transversales carecen de mentor y sus efectos son intangibles y a largo plazo, por lo que es difícil de justificar su inclusión en la agenda. No se subestima su importancia, pero en las agendas particulares siempre hay retos más urgentes y lo que es importante para todos acaba sin entrar en la agenda de nadie.

En segundo lugar, las estrategias abordan estas dinámicas como algo que transforma la Defensa y Seguridad global, por lo que las propuestas de acción se remiten a la gobernanza y la cooperación internacional. Se alerta sobre su posible impacto sobre las amenazas y desafíos habituales para la Defensa y Seguridad, pero no se determinan medidas internas que puedan mitigar impactos sobre la prosperidad económica o la estabilidad política y social. Se consideran dinámicas que vienen de fuera y a las que hay que estar atentos, pero que no precisan medidas

preventivas, de respuesta o de resiliencia transversales, al menos hasta que se manifiesten de forma notoria.

La presencia de amenazas no tradicionales en Honduras y la utilización de estos factores que tienden a generar el desbalance de la Defensa y Seguridad Nacional, por la participación activa de entes, individuos y organizaciones estructuradas de ciudadanos nacionales proclives a la comisión de ilícitos, hace necesario que las autoridades al más alto nivel del Estado tomen las decisiones oportunas, adecuadas e inteligentes para proteger a la sociedad y sostenimiento continuo de la Defensa y Defensa y Seguridad Nacional y, consecuentemente, el orden público. Para lo cual el Estado tiene la obligación de hacer uso de la fuerza necesaria considerando el respeto a las leyes y Derechos Humanos.

En tal virtud, es procedente e imprescindible el empleo de la fuerza a través de Las Fuerzas Armadas y otras instituciones afines, para impedir el apoyo a los delincuentes y disminuir la violencia a través de una estructura organizacional interagencial sostenida donde se involucren los operadores de justicia y otras instituciones como parte de los instrumentos del poder nacional para garantizar a la sociedad la tranquilidad y la paz. Para lo cual se deben seguir procedimientos doctrinarios, valores institucionales y las experiencias en el empleo de recursos para lograr la asimetría en la ejecución y conducción de tareas como parte de operaciones bajo el concepto de Defensa y Seguridad pública.

2.9 LOS INTANGIBLES DE LA DEFENSA Y SEGURIDAD NACIONAL

La pandemia puso en evidencia la dependencia y vulnerabilidad de las cadenas de suministros que satisfacen necesidades críticas de los servicios públicos, la actividad económica y la vida diaria de las personas. Al riesgo de que los desequilibrios medioambientales al alza interrumpan los suministros vitales se añade ahora el riesgo de que la confrontación geopolítica y geoeconómica se instale en las cadenas de suministro. Este riesgo se restringía, hasta ahora, a los suministros energéticos, pero es de esperar que la nueva Estrategia se ocupe de asegurar el suministro o almacenaje, al menos de los productos sanitarios que se han echado en falta durante la pandemia. La relocalización de las partes críticas de las cadenas de suministro en territorio nacional para reducir la dependencia podría ampliarse a otros elementos críticos, pero incluso si se restringe a la salud, el incremento de autonomía depende más de los recursos disponibles que de la voluntad para hacerlo.

En el contexto geoeconómico actual, donde las grandes potencias e instituciones combinan todos sus instrumentos de poder, duro o blando, para favorecer su expansión, la Defensa y Seguridad económica no pueden depender de que las organizaciones multilaterales vuelvan a funcionar eficazmente.

Sin embargo, el mayor riesgo para la Defensa y Seguridad nacional no es el de que los países se vean excluidos de las cadenas de suministro, sino que sus instituciones se vean desplazadas hacia los tramos de menor valor añadido de ellas por su obsolescencia o desfase tecnológico. Para evitar deslizarse por esa pendiente hacia la irrelevancia económica.

En buena lógica, esta dinámica debería incluirse entre las amenazas y desafíos de la nueva Estrategia porque su impacto sobre la prosperidad y la Defensa y Seguridad nacional es superior en probabilidad y efecto que la de cualquiera de los anteriores. Es un riesgo sistémico para la prosperidad porque la obsolescencia tecnológica reduce los ingresos públicos y privados, destruye el tejido industrial, económico y social y aumenta el desempleo y la desigualdad. Es también sistémico para la Defensa y Seguridad porque a medida que disminuye el crecimiento, aumenta la pobreza, la exclusión y la polarización, con el consiguiente incremento de la radicalización y las tensiones sociales que conducen a la violencia política y al extremismo violento.

2.10 DESCRIPCIÓN DE LA GESTIÓN DE LA SEGURIDAD EN OPERADORES CRÍTICOS

La información, junto a los procesos, personas y sistemas que hacen uso de ella, son activos muy importantes dentro de una entidad u organización. Las entidades y sus sistemas de información están expuestos a un número cada vez elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a los mismos a diversas formas de fraude, espionaje, sabotaje o vandalismo, entre otros.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de la entidad para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades, son algunos de los aspectos fundamentales en los que el Plan de Seguridad es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones y entidades.

Con un Plan de Seguridad, las entidades conocen los riesgos a los que está sometida su información y activos y los asume, minimiza, transfiere o controla mediante una metodología definida, documentada y conocida por todos, que se revisa y mejora constantemente.

Además, será importante que en la entidad se establezca y facilite el acceso a una fuente especializada de consulta en seguridad de la información. Deberán desarrollarse contactos con especialistas externos en seguridad, que incluyan a las administraciones pertinentes, con objeto de mantenerse actualizado en las tendencias, la evolución de las normas y los métodos de evaluación, así como proporcionar enlaces adecuados para el tratamiento de las incidencias de seguridad.

3 INTELIGENCIA ARTIFICIAL

Bajo este dimensionamiento de seguridad, se han identificado varias herramientas que permitan alcanzar los objetivos que garanticen la seguridad de las naciones, entre estos instrumentos tenemos la Inteligencia Artificial y la Ciencia de Datos que por sus siglas en inglés (DS Data Science), son en la actualidad los modelos y algoritmos que establecen los patrones de comportamiento no solo del terrorismo, sino de la diversidad de actividades que desarrolla la humanidad en los tiempos actuales (GAMBOA, 2014).

3.1 RECUPERACIÓN FRENTE A CIBERATAQUES

Proporcionaría a los usuarios la capacidad de reinstalar plataformas y aplicaciones, restaurar copias de seguridad, procesar las transacciones eficaces, y alertar sobre qué información ha sido comprometida para eficazmente y eficientemente recuperarse de los ciberataques restaurando el sistema completo a un estado seguridad inicial no comprometido.

- *Restauración de la integridad del sistema*. Capacidad de restaurar el sistema a un estado anterior, a un estado de seguridad no comprometido.
- *Restauración de la integridad de la información*. Capacidad para restaurar la información almacenada o procesada por el sistema a un estado anterior de nivel de seguridad no comprometido, de forma que se pueda verificar su integridad y confidencialidad.
- *Trazabilidad de la información comprometida. C*apacidad de mantener un registro de toda la información cuya confidencialidad haya sido comprometida para poder informar convenientemente a todas a las partes interesadas.

3.2 CENTRO DE DATOS (DATA CENTER)

Un Centro de Datos es un espacio exclusivo donde las instituciones mantienen y operan las infraestructuras TIC que utilizan para gestionar su actividad institucional. Es el espacio donde alojar los servidores y equipos de almacenamiento donde se ejecutan las aplicaciones, se procesan y almacenan los datos y el contenido. Para algunas instituciones se trata de una simple jaula o bastidor, mientras para otras puede ser una sala privada donde alojar un determinado número de bastidores, dependiendo del tamaño de la institución.

Los Centros de Datos ofrecen alimentación eléctrica garantizada, alimentación de reserva, refrigeración, cableado, sistemas de detección y extinción de incendios, inundaciones y controles de seguridad.

3.3 CENTRO DE DATOS INDEPENDIENTE

Un Centro de Datos independiente ofrece mucho más que mero espacio e instalaciones para alojar las infraestructuras TIC, las aplicaciones o los contenidos. También proporciona acceso a la conectividad de amplísimo número de operadores fijos y móviles proveedores de Internet (ISP), puntos neutros y otros proveedores de servicios de red, con el fin de crear redes de comunicaciones que ofrezcan la máxima satisfacción al usuario final.

Un proveedor de centros de datos totalmente independiente y neutral es aquel que no depende de ningún proveedor de redes, hardware o software. Al no estar vinculado a ningún proveedor en particular, todos los proveedores de conectividad ofrecen sus servicios de modo directo. Esto significa que el usuario final tiene la posibilidad real de elegir entre toda una serie de proveedores que compiten por ofrecerle las mejores prestaciones, servicios y precios para sus aplicaciones y contenidos. Los operadores de telecomunicaciones ya tienen sus routers y puntos de presencia físicos (PoP) activos en el centro de datos, de modo que el usuario puede conectarse rápida y fácilmente.

Además de una excelente conectividad, un centro de datos independiente garantiza disponer de un espacio sostenible y de calidad con sistemas avanzados de alimentación eléctrica, refrigeración, seguridad y cableado. También puede ofrecer servicios adicionales, como el soporte técnico.

4 NUEVAS TECNOLOGÍAS EN EL ÁREA DE LA DEFENSA

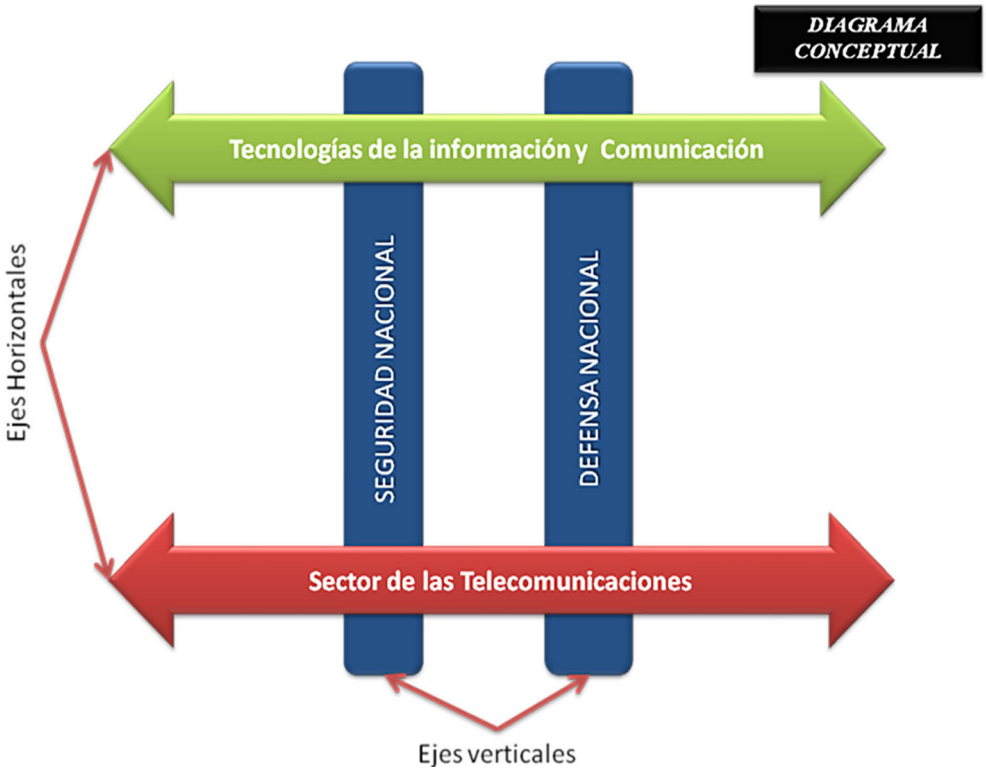
La tecnología a través de la historia, ha cambiado nuestra forma de vida, costumbres y forma de pensar. En el futuro su influencia será mayor. Las tecnologías de información son uno de los componentes claves para alcanzar cada una de las etapas involucradas en la creación del conocimiento.

Se expone una temática teórica para plantear los antecedentes de la investigación, cuyo fin último es establecer la "incidencia del sector de telecomunicaciones y las tecnologías de la información y comunicaciones en la Seguridad y Defensa nacional" (ESPAÑA, 2020).

4.1 INCIDENCIA DE LOS EJES TRANSVERSALES Y VERTICALES

Básicamente se plantea relaciones entre: -el sector de las telecomunicaciones y -las tecnologías de la información y comunicaciones como ejes transversales vinculadas al mejoramiento de: -la seguridad y –Defensa, como ejes transversales, tratando de esbozar la interacción entre ambos ejes y cómo se llevan a cabo dentro de una política de Estado (Diagrama 1).

Diagrama 1: Diagrama conceptual



Fuente: EL AUTOR, 2022.

Es básico, fundamental y decisorio el aprovechamiento de las herramientas que proporcionan el sector de las telecomunicaciones, así como las Tecnologías de la Información y Comunicación, bajo un enfoque que permita en el corto y mediano plazo, optimizar los recursos del país aprovechando la red de telecomunicaciones en beneficio del Estado.

La evolución de las tecnologías de la informática altera la naturaleza y el curso futuro de la economía, y el Estado debe responder a estas nuevas formas de comunicación estimulando una supercarretera que nos lleve a la globalización de la información y que las personas evolucionen por el nuevo conocimiento que adquieren a una mejor forma de vida.

4.2 NUEVA TRANSFORMACIÓN EN EL ENTORNO

En la última década se han experimentado grandes cambios en la forma de adquirir conocimientos, por medio del uso compartido de tecnologías de

información hasta la convergencia de servicio a través de redes interconectadas cada vez con mayor velocidad para cursar señales.

Es difícil estar actualizado en esta era tecnológica, los cambios son tan rápidos que continuamente hay que aprender, adaptar e improvisar. Instituciones usan la tecnología para competir y alcanzar sus objetivos y, desafortunadamente, descubren que la tecnología no garantiza el éxito y comprender cómo y dónde la tecnología trabajará en su beneficio.

Las tecnologías nos ofrecen herramientas para establecer estrategias, no las definen. La naturaleza siempre cambiante de la tecnología de información representa nuevas demandas de estrategias que deben estudiarse por los expertos en la materia con equipos de trabajos multidisciplinarios para plantear un nuevo entorno y procuren alinear la estrategia con la capacidad tecnológica. Facilitará la interacción humana, proponiendo técnicas que ayuden a las personas a trabajar en proyecto el tiempo necesario, sin importar su situación geográfica, requiriendo un adecuado conocimiento en informática, ligando su trabajo por sus conocimientos, más que por sus títulos o rangos.

El líder de una organización y su relación con la tecnología tienen un marcado impacto en el éxito de sus objetivos y meta, debe conocer la tecnología y saber utilizarla educándose continuamente, caso contrario se convertirán en un problema social.

4.3 INNOVACIÓN TECNOLÓGICA

Al surgir una nueva tecnología, la disponibilidad está limitada a algunas organizaciones que tienen acceso a esta, teniendo ventaja sobre los que no la usan. Si esta tecnología demuestra ser exitosa, se expande en disponibilidad y se convierte en la nueva forma dominante de información; mientras se expande ofrece ventajas competitivas hasta que más de la mitad de los usuarios potenciales la adoptan, después de esto ya no ofrece ventaja competitiva y se convierte en un problema para los que no la tienen.

En la etapa de madurez, cuando esa tecnología es la norma ya no ofrece un valor significativo, hasta que es actualizada.

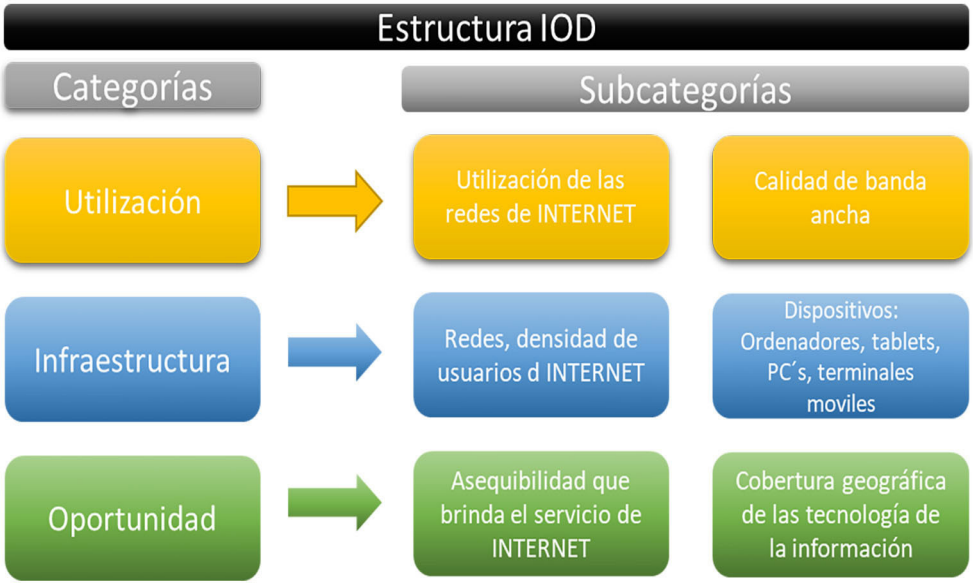
4.4 BRECHA E INCLUSIÓN DIGITAL

La brecha digital es producto de la evolución natural de la sociedad y la tecnología, y no de la casualidad. No se define en términos de falta de acceso a los servicios telefónicos, sino en la falta de acceso a las TIC. Generalmente, la brecha

digital no se refiere sólo al acceso a la tecnología, ni que sea necesariamente algo sobre costos elevados, sino que encierra un componente socioeconómico (UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, 2002). Es de carácter multidimensional ya que responde a factores como el ingreso, la instrucción, la cultura y la tecnología en términos de acceso y habilidades de uso (INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, 2004).

En esta realidad no es difícil admitir que, en esta era del conocimiento, las diferencias no se establecerán entre ricos y pobres, sino entre alfabetos -los conectados a la red- y los que no lo están, las analfabetas. No hay competitividad sin conectividad. La conectividad por sí sola no es suficiente. La expansión rápida de la sociedad de la información puede también tener efectos negativos. Puede agravar las disparidades económicas existentes a nivel internacional, regional y local. El acceso a las TIC y su disponibilidad, así como la capacidad de utilizarlas pueden ser consideradas como una amenaza por aquellos que no las poseen (INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, 2004).

Diagrama 2: Estructura de IOD



Fuente: CHO, [202-]. (Adaptado)

El principio de acceso sin discriminación a los servicios modernos de telecomunicación es importante para colmar la brecha. El diagrama 2 propone la diversidad digital, establecida por el "índice de oportunidad digital" (IOD), creado

por la UIT que contiene indicadores aprobados a escala internacional y sirve para evaluar la situación de las TIC en cada país, evalúa éxito o fracaso de sus iniciativas tecnológica con respecto a otros países y, por consiguiente, mide el acceso a la sociedad de la información.[1]

La inclusión digital sostiene este sector de la sociedad civil y hay que pensarla como un asunto colectivo, no individual, donde los beneficios sociales hay que verlos en relación a los que se generan para las comunidades, organizaciones, familias y grupos que sacan provecho de las tecnologías, aunque no tengan acceso a éstas.

4.5 CAMBIOS SOCIALES Y TECNOLÓGICOS

El procesado de información se ha vuelto cada vez más visible e importante en la vida económica, social y política. Una prueba es el crecimiento estadístico de las ocupaciones especializadas en actividades de la información suponiendo una mayor cuota de empleo en muchas sociedades industrializadas.

Las nuevas TI, basadas en la microelectrónica, junto con otras innovaciones, como los discos ópticos o la fibra óptica, permiten enormes aumentos de potencia y reducciones de costo en el procesado de información[2]. La informática y las telecomunicaciones en el pasado implicaban tecnologías distintas. En la actualidad, han convergido alrededor de actividades clave, como el uso de Internet (ÁLVAREZ, 2002).

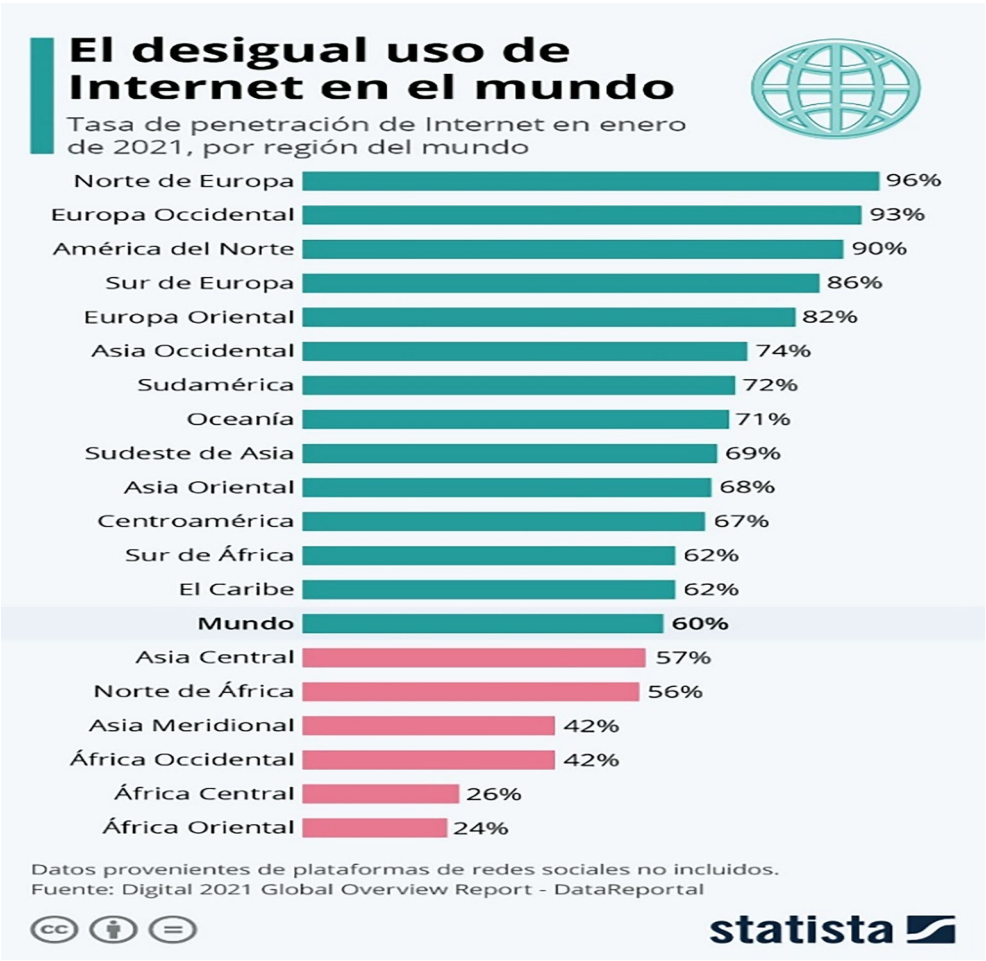
4.6 LA INTRODUCCIÓN DE NUEVAS TECNOLOGÍAS EN PAÍSES EN VÍAS DE DESARROLLO

A pesar que la introducción de nuevas tecnologías de información beneficia a países de más bajo perfil tecnológico e infraestructura en las redes de telecomunicaciones en comparación con a países con la globalización de la información, los perjuicios que conllevan son mucho mayores. Este fenómeno es particularmente notable en el ámbito informativo y económico con la introducción de Internet de los países industrializados hacia los que están en vías de industrialización, ya que estos se han convertido en consumidores de discursos creados por primermundistas, y han tenido que adaptarse a las transacciones de comercio electrónico diseñadas y operadas por los países con la infraestructura para manejar la economía mundial.

1 EL IOD se compone de tres categorías principales: oportunidad, infraestructura y utilización.

2 Cambio Tecnológico: Cubre la generación, almacenamiento, transmisión, manipulación y visualización de información, que incluye datos numéricos, de texto, de sonido o de vídeo.

Diagrama 3: Desigualdad acceso a Internet en el mundo



Fuente: STATISTA, 2020.

Con la inmediatez de la televisión y la profundidad de la prensa escrita, además de otras herramientas útiles y atractivas para el usuario[3], el periódico electrónico ha nacido como un medio más para ofrecer la satisfacción de necesidades de los usuarios. El desarrollo de Internet ha transformado muchos hábitos de relación y de trabajo, y desde luego el modo de acceso a la información, así como el modo en que se produce y procesa la información.

El desarrollo de la tecnología se abordó como una gran oportunidad para romper desigualdades y para facilitar el acceso total a la información por parte de todo el mundo

3 Hipervínculos, motores de búsqueda, menú interactivo, foto galerías, capacidad de reproducir audio y video, entre otros.

sin censura; además se ha tomado en cuenta como un espacio para la sociedad civil en una oportunidad de favorecer a la democracia total, directa y participativa. (VIRILIO, 1997)

4.7 INFLUENCIA DE LAS NUEVAS TECNOLOGÍAS EN LA VIDA DEL ESTADO

Las TIC no pueden resolver por sí solas los problemas del mundo, revisten esencial importancia para responder al creciente número de desafíos que se plantea en el mundo en el siglo XXI. Reducir la brecha digital e invertir en nuevas autopistas cibernéticas para poder lograr rápidamente las metas de desarrollo mundial, brindará, en un momento en que los mercados desarrollados están saturándose, nuevas y viables oportunidades comerciales.

La incorporación de las nuevas tecnologías potencia la productividad, y el sector de las telecomunicaciones fortalece la economía. Las TIC que crean la base tecnológica para la Sociedad de la Información, son por su naturaleza independientes de cualquier principio de valor. Una sociedad puede perseguir el deseo de mejorar la equidad social y la participación democrática de los ciudadanos a través del uso masivo de las nuevas herramientas tecnológicas, así como fortalecer el desarrollo de sus sectores.

4.8 LA CREACIÓN DEL CONOCIMIENTO Y LA VENTAJA COMPETITIVA

La creación del conocimiento es un arduo proceso que implica un compromiso a todos los niveles, así como una participación activa y responsable de los diversos actores de la sociedad[4].Las tecnologías de información son uno de los componentes claves para alcanzar cada una de las etapas involucradas en la creación del conocimiento.

Diagrama 4: Creación del conocimiento

Fuente: EL AUTOR, 2022.

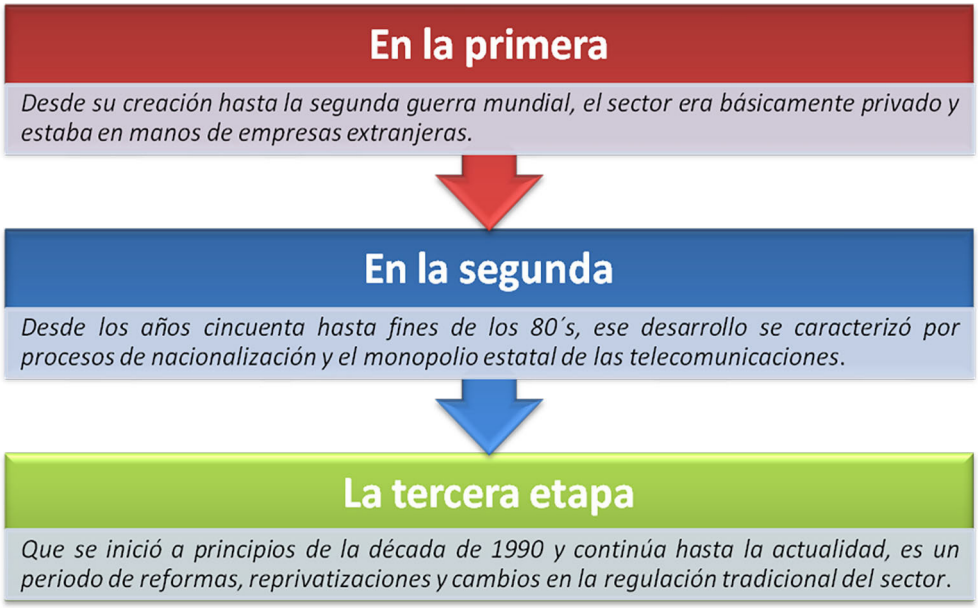
4 David Smith postula cuatro niveles de desarrollo organizacional en la creación del conocimiento, Cada uno de estos niveles otorga facilidades y ventajas, brindando la capacidad de avanzar a la etapa siguiente para alcanzar nuevas capacidades, mismas que le otorgan grandes ventajas e involucra tres elementos convergentes

La tecnología, —aún la más moderna, la más sofisticada o la más costosa— no es nunca por sí misma una solución mágica. Las TIC por sí mismas sólo se consideraban como una herramienta para facilitar la comunicación y la coordinación, y, al utilizarse con propósitos de administración del conocimiento dentro de las instituciones, se tendía más a su abuso que a su efectiva explotación (NONAKA, 1995). Los procesos de creación de conocimiento nunca deben iniciar ni terminar con la implementación de algún sistema de TI y de ningún modo debe verse éste como el punto focal del proceso.

4.9 EVOLUCIÓN DEL SECTOR EN AMÉRICA LATINA

El desarrollo del sector telecomunicaciones en la región atravesó tres (3) etapas:

Diagrama 5: Evolución en Latinoamérica



Fuente: EL AUTOR, 2022.

4.10 SOBRE DEFENSA Y SEGURIDAD NACIONAL

Seguridad nacional es un concepto que encuentra sus raíces en la teoría de la Geopolítica del siglo XIX en Alemania e Inglaterra (BETANCUR-DÍAZ, 2020). Se asumió que la seguridad nacional de los países dependía fundamentalmente de la integridad territorial y de la defensa militar de la soberanía y sufrió diversas influencias, principalmente del pensamiento militar francés y del español de la era

franquista y, poco después, del pensamiento militar norteamericano, el cual se convirtió en padre de la doctrina moderna de la seguridad nacional.

4.11 SERVICIOS DE SEGURIDAD

Comprenden aquellos órganos del Estado encargados de la recopilación de informaciones políticas, militares y económicas sobre otros Estados, especialmente sobre los Estados actual o potencialmente adversarios (actividad de espionaje). Tienen la tarea de impedir la actividad de espionaje extranjera en el territorio nacional y donde sea posible, llevar a cabo todas las acciones que puedan disminuir la fuerza política, militar y económica de los otros Estados –actividad de penetración ideológica, de derrotismo, de sabotaje, entre otros (BOVA, 1991).

Según Sergio Bova (1991), en el siglo XX y hasta la segunda guerra mundial, tanto el Estado como su contraparte se enfocaron en las siguientes características:

Cuadro 2: Enfoques

SERVICIOS SECRETOS (ESTADO)	EL ESPIONAJE
- Espionaje; - Sabotaje y agitación política, y - Contraespionaje y seguridad.	- Espionaje estratégico; - Espionaje bélico, y - Espionaje operativo.

Fuente: BOVA, 1991.

Los órganos de seguridad del Estado se dedican a espiar y analizar los movimientos de grupos guerrilleros o terroristas, partidos políticos, sindicatos, asociaciones y otros grupos que puedan quitarle el poder al grupo que atentan o que, de otra manera, puedan atentar contra la estabilidad del régimen, orden público e incluso la paz social. Se dedican a disminuir, contrarrestar, anular o erradicar su actividad y los efectos de ésta.

4.12 SERVICIOS POLÍTICOS DE SEGURIDAD

El aspecto más amplio se compone de instrumentos y mecanismos para mantener la gobernabilidad. Son instancias del Estado para prevenir, buscar, localizar, detectar, controlar y resolver posibles conflictos, o en el caso de que éstos ya se encuentren en pleno para: disminuir, contrarrestar, anular y erradicar su acción y los efectos para mantener las relaciones:

- entre instituciones del Estado.
- gobierno y población civil.
- exteriores.
- entre Estado y grupos de presión, partidos políticos y movimientos sociales.

4.13 ELEMENTOS DE LA SEGURIDAD NACIONAL

Algunos autores determinan que la seguridad nacional se divide en dos (2) partes, de acuerdo a:

Cuadro 3: Elemento de seguridad

SEGURIDAD		
PRIORIDADES ESTADO	ÁMBITO **ACCIÓN TERRITORIAL**	**ESFERA APLICACIÓN SOCIAL**
- Positiva	- Interior.	- del Estado.
- Negativa.	- Exterior.	- de la ciudadanía

Fuente: BOVA, 1991.

Cuando los líderes políticos hablan de la seguridad nacional, es posible que se refieran a la seguridad de la élite política dirigente. Es importante diferenciar entre la *seguridad del Estado*, preservación del aparato de gobierno, y la *seguridad de la sociedad* de la sociedad civil (RENATO ZERBINI RIBEIRO LEÃO, 2014).

La seguridad del Estado y la seguridad de la ciudadanía (seguridad pública o protección civil o seguridad de la sociedad civil) hacen el objetivo de la seguridad nacional junto con la integridad del territorio y de la soberanía, así como de la independencia política y económica respecto de otros estados.

La seguridad interior como exterior se enfocan a mantener, garantizar y preservar tanto la seguridad del Estado como la seguridad de la ciudadanía, lo cual nos ilustra cuán íntimamente ligadas se encuentran el ámbito de acción territorial y la esfera de aplicación social. El Estado tiene enemigos naturales y coyunturales que pueden atentar contra su estabilidad, funcionamiento y seguridad. Asimismo, hay grupos y factores que atentan contra la estabilidad, convivencia armónica, integridad, tranquilidad y seguridad de la ciudadanía.

Tanto para el Estado como para la ciudadanía, los grupos de riesgo –sus enemigos, pues- pueden provenir del interior del país o bien, del extranjero –tal sería el caso de una guerrilla o de una delincuencia organizada financiada desde otros países. Otros factores de riesgo que pueden atentar contra la seguridad del Estado y de la ciudadanía serían desastres naturales provocados intencional o accidentalmente, y lo que importa es prevenir desgracias y salir bien librados del problema. Seguridad del Estado es la legitimidad de éste y la obediencia y respeto que le guarda la sociedad. (MARTHA LAURA BOLÍVAR MEZA, 2019).

Condiciones de estabilidad, legitimidad y legalidad con la que las instancias del Estado operan y ejercen la función gubernativa, de conformidad con sus misiones, fines y objetivos generales y particulares. La seguridad ciudadana o seguridad pública y protección civil, es la condición de libertad, tranquilidad, armonía, orden y paz social en que vive la población del país. Con respecto a su temporalidad o actualidad cronológica los asuntos relativos a la seguridad nacional pueden ser:

Cuadro 4: Aspectos coyunturales y permanentes

	CARACTERISTICAS
Coyunturales o temporales	– Contingencias y desastres naturales ó provocados. – Acuerdos comerciales. – Acontecimientos sociales, culturales o deportivos.
Permanentes	– Soberanía. – Integridad territorial. – Seguridad pública y la protección civil. – Bienestar de la población. – Equilibrio y mantenimiento del orden público y la paz social.

Tienden a fortalecerla o lesionarla:

Cuadro 5: Factores

	FACTORES DE FORTALECOMIENTO Y LESION
Fortalecen la seguridad nacional	– Correcta interpretación y aplicación de la ley. – Equitativa distribución de la riqueza del país. – Crecimiento y estabilidad económica, desarrollo y justicia social y mejoramiento de calidad de vida de la población. – Respeto irrestricto a los derechos humanos, políticos, sociales. – Administración clara y transparente de los recursos nacionales. – Manejo transparente y claro de los procesos y recursos propios de la administración e impartición de justicia. – Honestidad, decencia e incorruptibilidad del sistema. – Respeto a los procesos y resultados electorales. – Disminución de la delincuencia menor y crimen organizado. – Planeación de los sistemas de defensa nacional. – Planeación de los sistemas de prevención y atención de desastres naturales. – Formación de una conciencia nacional y cultural. – Desarrollo tecnológico y científico. – Adecuación de procesos legislativos y administrativos gubernamental.

FACTORES DE FORTALECOMIENTO Y LESION	
Lesionan de la seguridad nacional	– Existencia de impunidad e ineficiencia en la interpretación y aplicación de la ley – Indiferencia y violación a las garantías y equilibrios propios del Estado democrático de derecho. – Injusta e inequitativa distribución de la riqueza. – Pobreza y rezago económico. – Violación flagrante y continua a los derechos humanos, políticos, sociales. – Administración viciada de los recursos nacionales por parte de los titulares de los poderes. – Deshonestidad, inmoralidad pública y corrupción. – Manipulación e imposición en los procesos y resultados electorales. – Aumento de la delincuencia menor y del crimen organizado con el consecuente incremento de inseguridad pública y alteración de la paz y orden público. – Represión política. – Presencia de apatía, desconfianza, incertidumbre e inseguridad en la población civil. – Deficiente planeación de sistemas de defensa nacional a posibles agresiones. – Deficiente planeación de sistemas de prevención y atención de desastres naturales. – Ausencia de una conciencia nacional entre la población civil. – Falta de bases ideológicas, principios cívicos y valores humanos. – Rezago y atraso tecnológico y científico. – Analfabetismo e ignorancia. – Rezago en los procesos legislativos y administrativos de la función gubernamental. – Anarquía. – Migración. – Presencia de grupos subversivos, ya sean de tipo político (anarquistas) o armados (guerrilleros, terroristas).

Fuente: EL AUTOR, 2022.

La Seguridad del Estado se considera como el primer elemento clave de la seguridad nacional, porque el gobierno debe gozar de estabilidad. Sólo en situación de seguridad el Estado será capaz de garantizar la seguridad y la tranquilidad del pueblo. El Estado tiene dos tipos de enemigos:

Tabla 6: Aspectos coyunturales y temporales

TIPO	FORMA	OBSERVACIONES
Coyunturales o temporales	**Internos**	– Partidos políticos reconocidos por la autoridad, contrarios u opositores a ésta y al partido o grupo que atenta su titularidad. – Grupos políticos o armados interior/exterior que operan en la clandestinidad que aprovechan cualquier desequilibrio social. – Delincuencia menor y organizada, que amenazan la seguridad ciudadana: lucha para disminuirlas, anularlas, contrarrestarlas y erradicarlas directa o indirectamente. – Corrupción como enemigo natural del Estado: es un fenómeno en que los grupos de poder pueden caer, cegados por la enfermedad de poder, la ambición u otros vicios igualmente nocivos para la salud e imagen del gobierno.
	Externos	– Potencias o grupos de poder –políticos y/o armados- provenientes del extranjero que pretenden lograr algún beneficio a través de: o Penetración ideológica. o Actividades subversivas, agitación pública, choque o sabotaje. o Hostilización. o Boicot o bloqueo económico o diplomático. o Agresión bélica.

Fuente: EL AUTOR, 2022.

Ante los desastres naturales, el Estado no puede evitarlos, pero sí prevenir situaciones que puedan perjudicar la población, o bien, aliviar o subsanar desgracias que la colectividad sufra. Respecto a sus enemigos, el Estado siempre los tendrá, aun cuando lleve una administración transparente y la nación cuente con desarrollo económico, político y social. La diferencia es que sí puede ejercer mayor control sobre éstos últimos.

Cuadro 7: Ejes verticales y transversales

EJES	VERTICALES		
	Variables de estudio	Defensa	Seguridad
TRANSVERSALES	Sector de Telecomunicaciones	**- Aprovechamiento de redes de - Telecomunicaciones.** **- Conectividad.** **- Interconexión.** **- Convergencia de servicios.** **- Integridad territorial.**	**- Desastres Naturales.** **- Estabilidad Económica.** **- Soberanía nacional.** **- Integridad territorial.** **- Ampliación de Banda Ancha.** **- Políticas de Estado.** **- Migración a nuevas redes.** **- Seguridad del Estado.** **- Relación entre poderes del Estado.**
	Tecnologías de la Información y Comunicación	- **Capacitación en nuevas tendencias.** **- Ciberterrorismo.** **- Contra narcotráfico.** **- Protección civil.** **- Jurídica interna.**	- **Ciberseguridad.** **- Bienestar poblacional.** **- Generación de contenidos.** **- Políticas de Estado.** **- Justicia social.** **- Aprovechamiento de nuevos conceptos de TI.** **- Reducción de la brecha digital.** **- Relaciones exteriores.** **- Procesos de transparencias.** **- Equidad social.** **- Blindaje económico.**

Fuente: EL AUTOR, 2022.

4.14 SERVICIOS ECONÓMICOS DE SEGURIDAD[5]

Estos recursos son las reservas monetarias que constituyen el denominado blindaje financiero, así como todas aquellas reservas de energéticos y alimentos.

4.15 SERVICIOS JURÍDICOS DE SEGURIDAD

Surge cuando algún problema surge en el interior del país, ejecutados por autoridades competentes del Estado en materia judicial, en niveles de acción gubernativa para resolver conflictos. Su principal característica es el manejo, la interpretación y aplicación de la ley para impartir justicia, y cuando se trata de aplicar estos mecanismos hacia el exterior, se maneja por la vía política.

4.16 DESCRIPCIÓN DE LA "GUERRA ELECTRÓNICA"

La "Guerra Electrónica" de las comunicaciones o *EW* por sus siglas en inglés "*Electronic Warfare*" es el nombre que se le da a todas aquellas acciones que tienen por objetivo bloquear, interceptar o negar la comunicación de un punto transmisor a otro receptor. Esta llamada "guerra" tiene tres elementos principales (PEDRO JARPA MARTÍNEZ, 2013):

- El ataque electrónico (*EA, Electronic Attack*)
- El apoyo electrónico (*ES, Electronic Support*)
- La protección electrónica (*EP, Electronic Protect*)

4.17 ATAQUE ELECTRÓNICO

El AE (ataque electrónico) se puede realizar por medio de tres tipos de acciones o técnicas (SUNDARAM, 1976):

- Técnica de jamming: El término jamming no posee una traducción acertada que englobe todo el concepto. En su más puro significado, jamming se define como aquella actividad que afecta la línea de tiempo en alguna comunicación. Es decir, logra que la información no llegue al receptor en el momento que debía de hacerlo. Al afectar esto, se afecta también la relevancia de la información. Esto se debe a que la información solamente es útil en determinado instante. No es útil si se recibe antes o después del tiempo establecido.

5 Son recursos del Estado para prevenir o resolver contingencias derivadas de crisis o conflictos internos o externos.

- Técnica de engaño: La técnica de engaño tiene como objetivo formar una nueva ruta de comunicación. Es así que en lugar de que la información llegue al receptor deseado, ésta sufre un cambio de ruta y es recibida por otro sistema receptor. De igual forma, el engaño puede consistir en la sustitución del sistema transmisor. En este caso el receptor original está recibiendo una señal que proviene de un segundo sistema transmisor. Cuando el receptor está ocupado no puede recibir la señal emitida por el transmisor original.
- Técnica de radiación directa de energía: La radiación directa de energía es la manera más fácil de atacar a un sistema de comunicación. Sin embargo, es la más fácil de detectar y poder evitar. Consiste en enviar una determinada señal con determinada potencia para dañar o destruir completamente la comunicación entre transmisor y receptor. La potencia emitida debe ser mayor a la que emplea el transmisor del sistema que está sobre ataque.

Un dispositivo capaz de emplear cualquiera de las tres técnicas o una combinación de ellas para interferir, dañar o destruir la transmisión de información dentro de un sistema electrónico de comunicaciones es llamado *jammer*.

4.17.1 Apoyo electrónico

El apoyo electrónico funciona como auxiliar del AE. Su función es la medición de parámetros de interés en el sistema de comunicación. Una de las razones principales de hacer esto radica en que si no hay señal que interferir no tiene caso gastar la potencia del *jammer* implementado. Sin embargo, dependiendo de la aplicación será el tipo de *jammer* que se emplee. Es así que se puede mantener en operación un *jammer* por tiempo indefinido o se puede encender siempre y cuando se detecte una comunicación. Todo esto se verá más adelante cuando se analicen los distintos tipos de *jammers* que existen. Entre los parámetros que se encarga de medir el apoyo electrónico se encuentran (PEDRO JARPA MARTÍNEZ, 2013):

- SNR (*Signal-to-Noise Ratio*): Determina la calidad con la que llega la señal al receptor después de recorrer la ruta del sistema de comunicación e ir contaminándose por ruido.
- JSR (*Jam-to-Signal Ratio*): Determina si la potencia con que transmite el jammer es mayor o menor que aquella que emplea el transmisor original del sistema.
- PSR (*PacketSend Ratio*): Relaciona los paquetes que fueron enviados correctamente por una ruta de tráfico con los paquetes que trataron de ser enviados fuera de la capa MAC.

- PDR (*PacketDelivery Ratio*): Compara los paquetes que llegaron al receptor con los que fueron enviados.
- BER (*Bit Error Rate*): Indica la fracción de bits que contiene o pudiera contener errores. Es decir, es la probabilidad de que un bit sea incorrecto. El BER se puede escribir también como Pe.
- SER *(Symbol Error Rate*): Es la probabilidad de que un símbolo sea incorrecto y se llega a escribir como Ps.
- SIR (*Signal-to-Interference Ratio):* Relaciona la potencia de la señal deseada con la potencia de la suma de las señales no deseadas.

4.17.2 Protección electrónica

La PE (protección electrónica) consiste en el uso de estrategias para evitar los dos primeros elementos de la llamada "Guerra Electrónica", es decir, el ataque y el apoyo. La codificación y la modulación entran dentro de este elemento. Con la unión de modulación y codificación nacieron las comunicaciones *AJ* por sus siglas en inglés, *antijam*. Este tipo de comunicaciones tienen como objetivo evitar que un sistema externo pueda dañar, bloquear o interceptar la comunicación de otro sistema.

4.17.3 Tipos de señales AJ (antijam)

A pesar de existir varios tipos de señales *AJ*; no es parte de este trabajo mencionar todas. Es por eso que se discutirán las dos principales. Los dos tipos de señales *AJ* a tratar tienen que ver con la telefonía móvil. El primero consiste en la secuencia directa de amplio especto o DSSS (*Direct Sequence Spread Spectrum).* Este tipo de señal es empleado en el estándar de segunda generación de telefonía móvil IS-95A conocida común y erróneamente como CDMA. Se debe recordar que CDMA (*Code Division Multiple Access*) es una técnica de acceso múltiple y no un estándar. De igual forma, se emplea en el estándar de 2.5G IS-95B y en el de 3G Cdma2000 (TERO OJANPERÄ, 1998).

El segundo tipo de señal AJ es el salto de frecuencia o FHSS (*Frequency Hopping Spread Spectrum*). El estándar de segunda generación de telefonía móvil GSM emplea esta técnica para lograr la diversidad de frecuencia.

Para que una señal pueda ser considerada como AJ es necesario que el sistema que la transmita sea un sistema LPD (*Low Probability of Detection*) y/o LPI (*Low Probability of Intercept*). En un sistema *LPD* el objetivo es lograr que la señal permanezca tan oculta como sea posible. *DSSS* es un ejemplo de sistema *LPD*. En *DSSS* esto se logra al distribuir la señal por todo el espectro disponible, lo que hace que la potencia sea muy baja y parezca ruido. Es así que se vuelve complicado detectar si la señal es de información, o es simplemente ruido.

En un sistema *LPI* (*Low Probability of Intercept*) puede ser que se haya detectado la señal, pero mientras no se intercepte la información, ésta estará protegida. Un ejemplo de estos sistemas es *FHSS*. En *FHSS* la protección se logra cambiando de frecuencia constantemente. Contrario a *DSSS*, donde el ancho de banda requerido es grande, en los sistemas que emplean *FH* la señal ocupa generalmente un ancho de banda angosto que depende del propio sistema, de la aplicación y de la técnica de modulación.

Existen dos tipos de salto de frecuencia. *FFH* (*Fast Frequency Hopping*) y *SFH* (*Slow Frequency Hopping*). La diferencia radica en el número de bits de datos que "saltan". Cuando el salto es rápido, *FFH*, existen muchos cambios de frecuencia, pero se encuentran involucrados pocos bits de datos. En cambio, en *SFH* es mayor la cantidad de datos, pero los cambios de frecuencia no son tan numerosos.

REFERENCIAS

ÁLVAREZ, Fermín B. Innovación Tecnológica y Cambio Social. *Las encrucijadas del cambio social:* homenaje al profesor José Luis Sequeiros Tizón, Vigo, Universidade de Vigo, 2002, p. 85-97.

ARNILLAS, Carlos de Izcue; MANTILLA, Yuri T; SHAFFER, Andrés A. El ciclo O.O.D.A. y la guerra de maniobras. *Apuntes de Estrategia Operacional*. La Punta, Escuela Superior de Guerra Naval, 2013, p. 71-74.

BETANCUR-DÍAZ, Ana M. De la geopolítica clásica a la geopolítica crítica: perspectivas de análisis para fenómenos del espacio y del poder en América Latina. *FORUM*, n. 17, p. 126 -149, enero - junio 2020. Disponível en: https://doi.org/10.15446/frdcp.n17.79687. Accedida en: 9 feb.2021.

BRUMLEY, Lachlan; KOPP, Carlo; KORB, Kevin. *The orientation step of the OODA loop and information warfare,* Australia, Monash University, 2014.

BOVA, Sergio. Servicios de seguridad. *Diccionario de Política de Norberto Bobbio,* tomo II, Ciudad de México, Siglo XXI, 1991, p. 1442-1446.

COLEGIO OFICIAL INGENIEROS DE TELECOMUNICACIÓN (España). Introducción a la Ciberdefensa. *In-Nova*, Toledo, [202-]. Disponible en: https://www.in-nova.org/es/soluciones-y-servicios/formacion-y-entrenamiento/proximas-acciones/introduccion-ciberdefensa. Accedido en: 15 ene. 2022.

ESPAÑA. *Estrategia de Tecnología e Innovación para la Defensa ETID*. Madrid: Ministerio de Defensa de España 2020.

ESTRADA, Alejandro C*. Ciberseguridad, una estrategia informática/militar*. Madrid, Darfe, 2017.

GAMBOA, Hugo A. B. *Inteligencia artificial,principios y aplicaciones*. Quito, Escuela Politécnica Nacional, 2014.

INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA.*Indicadores de la Brecha Digital*. México, 2004.

JOHAN SILVANDERA, Lars A. Introducing intents to the OODA-loop. In: *23RD INTERNATIONAL CONFERENCE ON KNOWLEDGE-BASED AND INTELLIGENT INFORMATION & ENGINEERING SYSTEMS*. Karlskrona, Sweden: [s.n.]. 2019. p. 6.

MEZA, Martha Laura Bolívar. Crisis de legitimidad del estado contemporáneo. *POLIS*, v. 15, n. I México, p. 33-63, 2019.

MARTÍNEZ, Pedro J. *Guerra electronica*. Santiago: Academia Politecnica Militar, 2013.

NONAKA, Ikujiro. The Knowledge-Creating Company. Oxford: Oxford University Press, 1995.
OJANPERÄ,Tero; PRASAD, Ramjee.*Wideband CDMA for Third Generation Mobile Communications*. Massachusetts: Artech House Publishers, 2001.

RENATO ZERBINI RIBEIRO LEÃO. *El rol de la sociedad civil organizada para el fortalecimiento de la protección de los derechos humanos en el siglo XXI*: un enfoque especial sobre los DESC. IIDH, Madrid, p. 30, 2014.

SUNDARAM, Ginebra G. S. Aplicaciones de la guerra electrónica en las fuerzas terrestres. *Boletín de Información*, n. 104, Madrid, Centro Superior de Estudios de la Defensa Nacional, 1976.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. Conferencia Mundial de desarrollo de las Telecomunicaciones. UIT. Estambul, Turquía. 2002.

VIRILIO, Paul. *El Cibermundo y La Política de lo Peor*. Madrid: Catedra Ediciones, 2004.

CIBERSEGURIDAD, INTELIGENCIA ARTIFICIAL Y NUEVAS TECNOLOGÍAS, EL CIBERPODER EN EL ÁMBITO DE LA DEFENSA NACIONAL

Xavier Rodríguez Cerano*

RESUMEN

La ciberseguridad es materia presente en múltiples actividades cotidianas, el ciberespacio es cada día más empleado y los sistemas de misión crítica basados en él crecen a cada momento proporcionando diversos beneficios a la población mundial, pero también exponiéndola a nuevos riesgos, las organizaciones internacionales como la OEA han sugerido la cooperación internacional para contrarrestar las nuevas amenazas e impulsan esfuerzos conjuntos para desarrollar una estrategia integral para su atención. Los Estados que cuentan con mejores servicios en Internet y que cuentan con planes de protección de su infraestructura crítica de información, tienen un mayor ciberpoder y con ello incrementan su capacidad de influir en otros actores, otros países como los de la región latinoamericana deben incrementar su cobertura de Internet, impulsar la preparación académica principalmente en el ámbito de la ciberseguridad e invertir en infraestructura.

Palabras clave: Ciberpoder; ciberseguridad; Defensa Nacional; Infraestructura Crítica de Información.

CIBERSEGURANÇA, INTELIGÊNCIA ARTIFICIAL E NOVAS TECNOLOGIAS, O CIBERPODER NO ÂMBITO DA DEFESA NACIONAL

RESUMO

A cibersegurança é um tema presente em múltiplas atividades cotidianas, o ciberespaço é cada vez mais utilizado e os sistemas de missão crítica baseados nele crescem a cada momento, proporcionando diversos benefícios à população mundial, mas também expondo-a a novos riscos, organizações internacionais como a OEA sugeriram a cooperação internacional para combater as novas ameaças e promover esforços conjuntos para desenvolver uma estratégia abrangente para lidar com elas. Os Estados que contam com melhores serviços de Internet e que contam com planos de proteção para sua infraestrutura crítica de informação têm maior poder cibernético e, portanto, aumentam sua capacidade de influenciar outros atores; outros países, como os da região latino-americana, devem aumentar sua cobertura de Internet, promover a preparação acadêmica principalmente no campo da cibersegurança e investir em infraestrutura.

* Coronel Ingeniero en Computación e Informática, Maestro en Seguridad Nacional por el Colegio de Defensa Nacional y en Administración de Tecnologías de la Información por el Instituto Tecnológico de Estudios Superiores de Monterrey, cursando el Doctorado en Desarrollo y Seguridad Nacional en el Instituto Mexicano de Estudios Estratégicos en Seguridad y Defensa Nacionales, Subdirector de la Escuela Militar de Ingenieros. Email: xrodriguezc@sedena.gob.mx.

Palavras-chave: Ciberpoder; cibersegurança; Defesa Nacional; Infraestrutura; Crítica de Informação.

1 INTRODUCCIÓN

En el siglo XX, la informática y las ciencias computacionales cambiaron para siempre la forma de ver el mundo, lo mismo para tareas cotidianas, que para estudios e investigaciones científicas e incluso para sistemas de información que apoyan los esfuerzos de guerra o de defensa nacional. A partir de la segunda guerra mundial y en los conflictos armados de la segunda mitad del siglo pasado, se emplearon con éxito sistemas computacionales para el almacenamiento de información, para facilitar la administración y el control de los recursos humanos, financieros y materiales y se emplearon novedosas técnicas de encripción y descifrado de información para los sistemas de comunicaciones militares. Con la creación de la red de Internet, las distancias se acortaron, los investigadores pudieron intercambiar avances científicos y tecnológicos y se dieron diversos cambios en la comunicación de las personas que hasta la fecha son aprovechadas.

El presente trabajo tiene por objeto mostrar un panorama de la ciberseguridad, la inteligencia artificial y las nuevas tecnologías en un contexto de defensa nacional en América Latina, mostrando de forma general los avances en cuanto a la unificación de criterios alcanzados con el apoyo de la Organización de Estados Americanos (OEA) para la definición del concepto de seguridad, así como para identificación de las principales amenazas a que se enfrenta la región.

Posteriormente se resaltan las características favorables del ciberespacio y como la pandemia del COVID-19 resultó en un incremento en su uso y agregó variantes para hacer más llevadero el confinamiento, logrando un mayor crecimiento. Se habla del concepto del ciberpoder en el que los Estados pueden influir en eventos sobre otros actores con este tipo de capacidades y sobre el problema de que las fronteras son ahora más difusas en el ciberespacio.

A continuación se muestra que a pesar de que ha habido avances para reducir las distancias entre los países desarrollados y aquellos en vías de desarrollo, en el ciberespacio existen esas brechas y eso deja fuera de sus beneficios a los países con menores recursos, pero también hay actores no estatales con un gran poder acumulado que han demostrado en los últimos tiempos que pueden ejercerlo sobre entes que antes se consideraban prácticamente imbatibles y que ello puede convertirse en una amenaza.

En seguida se señala: la existencia de los hackers de nuestros tiempos que han sido capaces de vulnerar con alto grado de éxito a los sistemas financieros de diversos países y con una forma de operación que reúne características comunes; y de la *Deep Web* que tiene proporciones muy superiores a la red superficial y un mayor acceso a contenidos de todo tipo, con la diferencia de que no es accesible empleando los motores de búsqueda tradicionales.

En el ámbito de la seguridad se toca el tema de la ciberguerra y el cibercrimen a través de los cuales se puede vulnerar a los ciudadanos de un país directamente o dañar a la infraestructura crítica de información que afecta a la seguridad nacional y a la seguridad hemisférica, pero también hay muchos avances gracias a la cooperación internacional y al respaldo de las organizaciones regionales como la OEA y la CEPAL.

Posteriormente se describen algunas de las capacidades de la inteligencia artificial: de sus posibilidades al recabar una gran cantidad de datos a través de distintos tipos de sensores y procesarlos y de que una de sus grandes cualidades se da cuando se presenta la interacción entre elementos para retroalimentarse mutuamente y que será útil para el resto, particularmente en situaciones como las que se presentan en un campo de batalla.

Para continuar, se explica el panorama general de la legislación relacionada con la ciberseguridad y las nuevas tecnologías, donde hay áreas de oportunidad, pero también se ha hecho un esfuerzo notable de carácter regional latinoamericano, que ha permitido avanzar en temas como la protección de la propiedad industrial y de los datos personales.

Por último, se exploran algunas de las nuevas tecnologías emergentes que se han posicionado como las opciones en las que se está invirtiendo y desarrollando como el Internet de las Cosas, el *Business Intelligence* y el Cómputo en la Nube, para cerrar con las conclusiones respecto a esta gran gama de tecnologías que sirven para incrementar el poder nacional de los Estados, pero también si son descuidados se convierten en vulnerabilidades que atacantes estatales y no estatales podrían explotar.

2 CIBERSEGURIDAD

Para la década de los 60s del siglo pasado, cuando los programadores de computadoras escribían códigos para ejecutar diversas tareas en microchips y sistemas de información, aprovecharon la técnica de emplear solo dos dígitos para representar los años del calendario, para ahorrar espacio de almacenamiento, que para la época era costoso y reducido, lo cual resultó sumamente funcional y eficiente. Sin embargo, este método representó un problema cuando hubo que pensar en el cambio de milenio, es decir, cuando el 99 de 1999 se convertiría en el 00 del año 2000, dado ese caso las computadoras no tendrían manera de identificar que 00 correspondía a 2000, por lo que se preveía que se generaran datos corruptos y problemas en los sistemas informáticos de misión crítica, desde aquellos relacionados con la seguridad social, pasando por sistemas de armas automatizados, hasta los que se emplean para la aviación, lo que se convirtió en un tema de atención por parte del congreso norteamericano por los grandes riesgos que se enfrentaban (HOUSE OF REPRESENTATIVES, 1998).

Esto representó en aquel momento que la industria de los servicios públicos, el sistema financiero internacional, las telecomunicaciones y los sistemas de transporte, se enfrentaran a altos riesgos que obligaron a la comunidad internacional a organizarse

para atender la contingencia, se emitieron leyes, regulaciones, resoluciones y se crearon comisiones nacionales para atender la problemática (LEDO, 2005), el error Y2K, como se le conoció, amenazaba en términos de la triada de la seguridad de la información a dos de sus tres componentes: la integridad y la disponibilidad de los datos en los sistemas informáticos de misión crítica, lo que fue una de las primeras amenazas globales de ciberseguridad de que se tiene noticia.

La necesidad de pensar en la seguridad, para evitar que errores de diseño como el Y2K ocasionaran fallos en la infraestructura crítica de información, se trasladó a todos los ámbitos de la vida, lo mismo en negocios, que en la educación y las comunicaciones por lo que gradualmente la cultura primeramente de la protección de la información y posteriormente de la ciberseguridad ha permeado y en la mayor parte del mundo se emplean servicios públicos a los que se accede empleando usuarios y contraseñas y existen leyes y mecanismos para proteger la integridad y confidencialidad de la información de los ciudadanos.

3 CONFERENCIA ESPECIAL SOBRE SEGURIDAD DE LA ORGANIZACIÓN DE ESTADOS AMERICANOS

En la conferencia especial sobre seguridad, celebrada en la Ciudad de México el 28 de octubre de 2003, se emitió la Declaración sobre Seguridad en las Américas, afirmando en ella que la nueva concepción de la seguridad en el Hemisferio es multidimensional, ya que hay nuevos desafíos a la seguridad de los Estados del Hemisferio y la consolidación de la paz se basa entre otros aspectos en la cooperación y el respeto a la soberanía nacional (ORGANIZACIÓN DE ESTADOS AMERICANOS, 2003).

Entre las amenazas a enfrentar mediante la cooperación y los valores compartidos de los países integrantes del Hemisferio, están las tradicionales y las siguientes nuevas amenazas, preocupaciones y otros desafíos de naturaleza diversa (ORGANIZACIÓN DE ESTADOS AMERICANOS, 2003):

- El terrorismo, la delincuencia organizada transnacional, el problema mundial de las drogas, la corrupción, el lavado de activos y el tráfico ilícito de armas.
- La pobreza extrema y la exclusión social.
- Los desastres naturales y los de origen humano.
- Las pandemias.
- La trata de personas.
- Los ataques a la seguridad cibernética.
- Daños por accidentes marítimos.
- Armas de destrucción en masa.

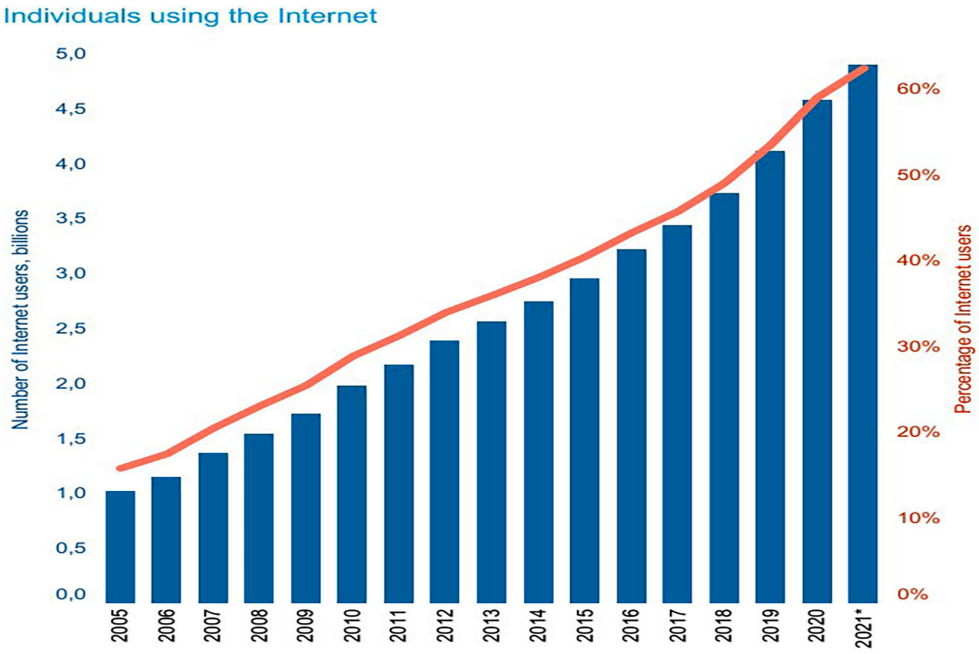
Por ello en el mismo documento se establecen compromisos y acciones de cooperación, como el desarrollo conjunto de la cultura de seguridad cibernética para prever, tratar y responder ataques cibernéticos, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes

de los sistemas, buscando crear una estrategia integral de la OEA sobre seguridad cibernética (ORGANIZACIÓN DE ESTADOS AMERICANOS, 2003).

4 EL CIBERESPACIO

La ubicuidad y riqueza en el contenido de la red Internet han cambiado en el siglo XXI la forma de vida, de comunicación y la manera de hacer negocios de las personas, ello ha implicado amplios beneficios para organizaciones públicas y privadas. Con la pandemia de la COVID-19 y la necesidad de que las personas se aislaran y confinaran para reducir los contagios, su uso se intensificó y se agregaron modalidades al estilo de vida: se incrementó el uso de las redes sociales para las relaciones interpersonales, se empleó el home office para el trabajo, los maestros y estudiantes aprendieron a mantener su actividad desarrollándola en línea, se incrementó el comercio electrónico con nuevos servicios como la compra del supermercado y se incrementaron los servicios públicos proporcionados a través de plataformas digitales. Según la Unión Internacional de Telecomunicaciones para 2019, 4,100 millones de personas utilizaba ya la red Internet, aumentando en 800 millones para llegar a 4,900 millones de personas para el 2021, pasando del 54% al 63% de la población mundial, ver gráfica 1 (INTERNATIONAL TELECOMMUNICATION UNION, 2021):

Gráfica 1 - Usuarios de Internet en el mundo para finales de 2021.



Fuente: INTERNATIONAL TELECOMMUNICATION UNION, 2021.

5 CIBERPODER

De forma análoga a los poderes empleados en otras dimensiones de operaciones, como el poder marítimo en el mar o el poder aéreo en el espacio aéreo, el ciberpoder es la capacidad de emplear al ciberespacio para crear ventajas e influir en eventos en todos los entornos operativos y a través de los instrumentos de poder. Para ello, el elemento clave es la información, lo mismo en el campo del poder económico como factor que vincula a todos los actores en su toma de decisiones, que en los campos político y diplomático a través de su ubicuidad y por ende de su capacidad de enviar mensajes que buscan influencia e incluso en el campo militar al revolucionar técnicamente a las fuerzas armadas con nuevos conceptos y doctrinas, convirtiéndose en un elemento indispensable de la guerra moderna (KUEHL, 2009).

Cuadro 1 - Dimensiones físicas y virtuales del ciberpoder

	Intra ciberespacio	**Extra ciberespacio**
Instrumentos de información	**Tangibles**: Ataques de denegación de servicios. **Intangibles**: Conjunto de normas y estándares.	**Tangible**: Ataques a sistemas SCADA. **Intangible**:Campañas de difusión para influir en la opinión pública
Instrumentos físicos	**Tangibles**:Control gubernamental sobre las compañías. **Intangible**: Infraestructura para apoyar activistas de derechos humanos.	**Tangible**: Destrucción física de enrutadores o cortes de cableado. **Intangible**:Protestas para denunciar y evidenciar a compañías proveedoras.

Fuente: NYE, 2010.

El ciberpoder ya se ejerce y es clave para el desarrollo de los países, mediante distintas estrategias se busca incrementar las capacidades de acceso a estas herramientas y proporcionar servicios que hace menos de una década eran impensables, es difícil pensar en una tecnología novedosa que no se vea afectada por el componente cibernético, las computadoras y sistemas de información en los automóviles, las nuevas posibilidades en el sistema financiero y la velocidad y ubicuidad de las comunicaciones son ejemplo de ello, el ciberpoder está creando sinergia entre otros elementos de poder para mejorarlos y lo hace transformando cada día la forma de crear datos, en formatos de imagen, sonido, y muchos otros e intercambiando ese contenido se transforma la forma en que se ejerce influencia,

lo mismo en una reunión del cuadro 1: tanto los instrumentos físicos como los instrumentos de información del ciberpoder pueden proporcionar efectos tangibles e intangibles.

Pero al igual que en otras ramas de la economía, las empresas con tal poder logran imponer normas y políticas favorables a sus propósitos, lo que ha ocasionado que algunos países busquen gradualmente tener su propia versión de Internet, buscando control y soberanía, pero afectando la autorregulación que permitiría gradualmente la gobernanza global, estos actores con gran poder desarrollan gradualmente nuevas capacidades que son susceptibles de ser empleadas como ciberarmamento con posibilidades ofensivas y defensivas, en ocasiones convencen a los Estados de patrocinarlos para transferir parte de ese poder o por lo menos reducir la posibilidad de ser víctima de ellos. Ello hace que la cooperación internacional sea necesaria, pero la diferencia de horarios, idiomas, tecnología y sobre todo la heterogeneidad de la legislación aplicable ocasiona retrasos en la solución de conflictos que en el ciberespacio parecen aún mayores.

El ciberespacio es muchas veces confundido con un bien público, pero un bien público es aquel del que todos se benefician sin exclusión, lo que es cierto cuando se describen protocolos de comunicaciones en Internet, pero no cuando se trata de la infraestructura física, que generalmente es un recurso escaso ubicado dentro de los límites de Estados soberanos, lo que deja en el aire el concepto de cibersoberanía y la dificultad inherente para definirlo (NYE, 2010).

De hecho, el concepto de soberanía se ha modificado por los múltiples tratados internacionales que los países tienen entre ellos para atender temas como reducción de aranceles y facilidades comerciales para sus empresas y ello implica ceder parte de esa soberanía en aras de mantener a mediano plazo la certeza jurídica que permita que inversionistas nacionales e internacionales accedan a buenos negocios y con ello se mejoren las condiciones de vida de la población, en el ciberespacio se hace aún más complejo porque sin que se tengan este tipo de instrumentos para acordar las reglas del juego, las facilidades que permite la tecnología ocasionan que en muchos casos se presenten situaciones en donde un servidor de un sistema informático provee sus servicios a poblaciones de muchos países desde un país que no siempre es beneficiario del mismo y a su vez el equipo de personas que administran el servicio no siempre se encuentra en su totalidad en el país en que se encuentra el servidor ni en alguno de los países usuarios de sus servicios.

Pero estas cualidades presentan su propio riesgo para los cibernautas que todos los días estudian, investigan, se entretienen o simplemente se comunican en el ciberespacio, en el informe de riesgos globales 2022 del Foro Económico Mundial se señala que los ataques de *ransomware*, es decir los que impiden el acceso a la información propia mediante el "secuestro de datos", se incrementaron en un 450% durante 2020, existe además la necesidad de contar con al menos 3 millones de ciberespecialistas, el crecimiento del mercado de comercio digital crecerá para 2024

hasta los 800,000 millones de dólares y el mismo reporte asegura que el 95% de las fallas de ciberseguridad corresponden a errores humanos (WORLD ECONOMIC FORUM, 2022).

5.1 EQUIDAD DIGITAL

La dependencia de los sistemas de información de misión crítica es cada día mayor para el acceso a servicios públicos, negocios e incluso, para realizar compras rutinarias, empleando para ello diferentes herramientas conectadas a Internet, lo que implica riesgos de comisión de ciberdelitos como los ciberfraudes con altos costos para las organizaciones y para los individuos que los han padecido. Además de ello, el salto en la digitalización que implicó la pandemia no tuvo un incremento homogéneo hacía la hiperconectividad, por lo que los países latinoamericanos y africanos están en riesgo de padecer de la inequidad digital en el corto plazo, así como requerirán probablemente mayor tiempo en adoptar las medidas y controles de seguridad informática necesarios para contrarrestar los riesgos cibernéticos a que se enfrentará su población (WORLD ECONOMIC FORUM, 2022).

5.2 CONCENTRACIÓN DE PODER DIGITAL

Cuando un individuo u organización logra acceder a una gran cantidad de medios electrónicos, o a conocimientos digitales de nivel crítico, se ocasiona una suerte de monopolio que impide una adecuada competitividad y puede provocar no solo el establecimiento de precios discrecionales en los productos que comercializa, sino deficiencias en la imparcialidad para la toma de diversas decisiones gubernamentales y legales. Cuando Donald Trump se negó a reconocer su derrota en la contienda para elegir al nuevo presidente de los Estados Unidos de América, su discurso en redes sociales culminó en un motín al Capitolio, lo que llevó a Twitter y otras plataformas a suspender las cuentas del que aún era presidente de ese país y considerado uno de los hombres más poderosos del planeta (CHEN *et al.*, 2021) No obstante, lo anterior, si a esa circunstancia se le agrega la consideración de que muchas de las grandes empresas de medios tecnológicos no tienen su sede principal en Latinoamérica y por lo tanto su dependencia de los gobiernos locales es mucho menor, la concentración de poder digital en los países del área se traduce en un mayor impacto.

5.3 AMENAZAS PERSISTENTES AVANZADAS (APT)

Pero tener un gran ciberpoder no es una garantía, cuando hace algunos años se leía sobre hackers que robaban información, se creía que se trataba de jóvenes solitarios que en la oscuridad de su habitación se dedicaban a buscar acceder a sistemas de información de instituciones como la CIA o la KGB, la generalidad es que

los sistemas de información serios cada vez cuentan con mayores recursos para su protección, por lo que este tipo de casos son cada vez menos probables y en su lugar encontramos grupos bien organizados con presupuesto para vulnerar paso a paso, sin prisas pero sin pausa, infraestructura crítica de información de sus países objetivo y de forma específica al sistema financiero para patrocinar sus esfuerzos.

Por sus siglas en inglés son conocidas como *Advanced Persistant Threat* o Amenazas Persistentes Avanzadas, nombre que toman de su forma de operación, existen más de 100 APTs con origen en Corea del Norte, pero hay decenas de ellas de Rusia, China, Vietnam, Irán, India y Estados Unidos, las víctimas se encuentran principalmente en Estados Unidos y Europa, pero la mayor parte de los países del mundo ya han sufrido de sus ataques. Tal es el caso de Lazarus, APT norcoreana responsable del virus Wanna Cry, del ataque a la multinacional Sony para evitar que estrenara una película en la que se ridiculizaba al mandatario de su país, pero principalmente de los ataques al sistema financiero de más de 30 países incluyendo a Ecuador, Rusia, Filipinas, Bangladesh, Polonia y México, robando grandes cantidades de dinero en cada caso (OFFICE OF PUBLIC AFFAIRS, 2021).

6 DEEP WEB

Pero no todas las amenazas son grupos de profesionales, a veces el propio usuario de Internet encuentra los peligros por sí mismo, buscar en Internet hoy en día puede no tener el resultado que pensamos, hay una gran cantidad de información que se pierde debido a que se hospeda en sitios generados dinámicamente y los motores de búsqueda estándar no la encontrarán porque no es estática y no tiene vinculación con otras páginas, puede que estás páginas tengan información valiosa y serán descubiertas hasta que se haga una búsqueda específica, por ello una gran cantidad de contenido de Internet se mantiene oculto en lo que se conoce como la Deep Web, en donde se estima se almacena alrededor de 400 o 500 veces más información que la que se puede consultar en la Web de la superficie como se conoce a la que se encuentra indexada en los motores de búsqueda.

Aunque se estima que la Deep Web crece de forma más rápida que la Web de superficie, dentro de ella crece aún más velozmente la Dark Web, que tiene la diferencia de que a sus sitios solo se puede acceder de forma anónima, diversas tecnologías como la computación distribuida, cómputo en la nube, cómputo móvil y redes de sensores han contribuido a su expansión, el alojamiento seguro y anónimo, el empleo de criptomonedas como Bitcoin, Darkcoin o Peercoin y diverso software para fines ilícitos aun la hacen más deseable para un sector de usuarios de Internet que buscan estas características. Entre los usos que se le han dado, están los de periodistas, disidentes políticos, denunciantes y defensores de los derechos humanos, como los casos de Bradley Manning, Julián Assange y Edward Snowden en que aprovecharon sus características para sus actividades (SUI *et al.*, 2015).

7 CIBERGUERRA

Peligros más serios se encuentran cuando se vulnera la infraestructura critica de un Estado: en 2010, el software Stuxnet logró lo que ya se preveía, paralizar el hardware ocasionando daños a reactores nucleares en Irán; en 2021, un hacker se introdujo en un sistema de control de tratamiento de agua municipal e intentó aumentar la lejía en el agua a niveles dañinos en el estado de Florida, en los Estados Unidos. Este tipo de instalaciones que proporcionan bienes o servicios de carácter esencial en diversos ámbitos y que son controlados mediante sistemas de información son lo que se conoce como Infraestructura Crítica de Información, su inhabilitación o fallo podría dañar a grandes poblaciones civiles (GUTTIERRI, 2022).

Se ha desarrollado ciberarmamento basado en software con la intención de contener ciberataques de organizaciones antagónicas, pero en más de una ocasión ha resultado en un efecto bumerang, como en el caso de EternalBlue, una herramienta de penetración diseñada por la Agencia de Seguridad Nacional norteamericana que fue robada y empleada en 2017 por piratas informáticos de Corea del Norte que la emplearon como parte del ataque de *ransomware* Wanna Cry que afectó computadoras de más de 150 países y paralizó el sistema nacional de salud del Reino Unido durante varios días, o el ataque NotPetya originalmente dirigido a Ucrania por hackers militares rusos que causó miles de millones de dólares en daños en todo el mundo, impactando incluso a Rosneft, la compañía petrolera estatal rusa. China es el líder mundial en tecnología de vigilancia y censura, su gobierno evita que la tecnología pueda emplearse para la movilización social y ha forzado concesiones de corporaciones como Apple, Disney, Facebook, Google y Microsoft ejerciendo una variante autoritaria del poder blando (GUTTIERRI, 2022).

8 CIBERCRIMEN

Como se observa, hay una gran variedad de delitos que se comenten en el ciberespacio, entre los más comunes están la piratería de software y contenido multimedia, estafas en línea, acoso y pornografía infantil para lo que se emplean técnicas de *phising*, mediante la que se simula ser una fuente confiable para robar datos y contraseñas, troyanos que una vez que son ejecutados por el equipo atacado pueden realizar múltiples tareas en beneficio del atacante, virus que infectan y generalmente dañan la información de las computadoras, puertas traseras que son códigos que dan acceso a un sistema para el que no se tiene autorización y el spyware que envía información principalmente bancaria, pero también toda aquella susceptible de explotación por parte del atacante. En Latinoamérica, el cibercrimen cuesta a los países de la región 90,000 millones de dólares al año, encontrando que su mayor dificultad es la carencia de entidades especializadas en la materia que tengan la facultad para investigar y perseguir la comisión de este delito y la falta de

capacitación suficiente para una labor exhaustiva y coordinada (ORGANIZACIÓN DE ESTADOS AMERICANOS, 2016).

9 MODELO DE MADUREZ DE LA CAPACIDAD DE CIBERSEGURIDAD.

Ante los antagonismos expresados, la Organización de Estados Americanos en colaboración con el Banco Interamericano de Desarrollo y el Centro de Capacidad de Seguridad Cibernética Global de la Universidad de Oxford, primero en 2016 y posteriormente en 2020 analizó la capacidad de seguridad cibernética de los Estados miembros de la OEA, empleando para ello las cinco dimensiones identificadas en el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones: política y estrategia de ciberseguridad; cibercultura y sociedad; habilidades de educación, capacitación y ciberseguridad; marcos legales y regulatorios; normas, organizaciones y tecnologías.

Entre las dos mediciones ha habido un progreso evidente, en 2016 cuatro de cada cinco países carecían de estrategias de ciberseguridad o de un plan de protección de infraestructura crítica, para la revisión realizada en 2020, 12 países habían aprobado estrategias nacionales de ciberseguridad, incluidos Colombia en 2011 y en 2016, Panamá en 2013, Trinidad y Tobago en 2013, Jamaica en 2015, Paraguay en 2017, Chile en 2017, Costa Rica en 2017, México en 2017, Guatemala en 2018, República Dominicana en 2018, Argentina en 2019 y Brasil para el 2020 (INTER-AMERICAN DEVELOPMENT BANK, 2020).

10 INTELIGENCIA ARTIFICIAL

En este contexto de antagonismos y esfuerzos por contenerlos, el ciberespacio esuna fuente inagotable de beneficios para las personas en nuestros días, la propia red de Internet ha tenido que renovarse de forma constante para ser atractiva y útil cada día. Con la COVID-19, el software para videoconferencia y el destinado al trabajo colaborativo fue empleado como se ofertaba, con el tiempo se descubrieron algunas vulnerabilidades que han tenido que irse corrigiendo para evitar espectadores no deseados o fugas de información corporativa. También hubo un crecimiento en las aplicaciones desarrolladas para hacer la vida más sencilla, como las compras en línea, incluso el supermercado o prácticamente cualquier producto de los lugares más alejados del mundo se puede adquirir en línea cumpliendo las normatividades propias de los países implicados, la industria del entretenimiento cambió, cada vez hay una mayor cantidad de plataformas informáticas con distribución de contenido de video en *streaming*, de podcast, de radio en línea, de música, de libros y videojuegos.

La tecnología subyacente en estos avances es la inteligencia artificial, empleando para ello el poder computacional de computadoras y sistemas de información que tienen algoritmos capaces de aprender y tomar decisiones, por lo que de forma incremental y exponencial acceden a tareas antes destinadas a seres humanos, lo

cual es motivo también de atención para la prevención de posibles desventajas que de forma directa o indirecta pueda generar su empleo masivo, entre otras áreas en que se emplea de forma cotidiana la Inteligencia Artificial (CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL, 2020) están:

- Reconocimiento de imagen es estáticas.
- Mejoras del desempeño de la estrategia algorítmica comercial, principalmente en el sector financiero.
- Procesamiento eficiente y escalable de datos de pacientes facilitando la mejor atención médica.
- Mantenimiento predictivo, ampliamente empleado en diferentes industrias.
- Detección y clasificación de objetos, materializado principalmente en vehículos autónomos, con potencial para muchos otros campos.
- Distribución de contenido en redes sociales, empleado para marketing, para concientizar sin fines de lucro y como servicio público.
- Protección contra amenazas de ciberseguridad para organizaciones que cuentan con infraestructura crítica de información.
- Predicciones sobre salud, educación, trabajo, relaciones interpersonales y negocios.

Latinoamérica tienela capacidad para aprovechar el potencial de la Inteligencia Artificial, tiene limitaciones sociales y económicas y en general hay poca inversión entre gobierno, industria e investigación, lo que es una debilidad porque por su naturaleza multipropósito podría expandir sus capacidades y aprovechar su cualidad de predicción para fungir como una herramienta importante para abordar diversos desafíos que afectan el desarrollo de la región.

En el sector militar la tecnología de la Inteligencia Artificial tiene amplias aplicaciones que están siendo empleadas en mayor y menor medida por diversas fuerzas armadas en el mundo, como: el análisis de grandes volúmenes de información para la toma de decisiones, la autonomía de vehículos terrestres y aéreos para realizar operaciones sin tripulación, misiles o bombas capaces de funcionar de forma conjunta, obteniendo datos unas de otras y aprendiendo a partir de ello, reaccionando en tiempo real, lo cual incide directamente en el incremento del poder militar.

El máximo potencial que se puede dar a un sistema al que se le agrega Inteligencia Artificial se obtiene mediante la interconexión de los elementos que puedan captar información, de forma tal que el entrenamiento de una red neuronal contenga información no solo individual sino colectiva de los componentes que interactúan para lograr captar la mayor parte de información en el menor tiempo posible, logrando mediante este intercambio continuo, mejores reacciones que les permitan alcanzar sus objetivos y reaccionar mejor ante amenazas, evitando pérdida de componentes y de información.

En el campo de batalla, dependiendo el tipo de combate, es posible colocar sensores al soldado para conocer su estado físico y mental, su ubicación y los patrones relacionados a sus movimientos, en los vehículos se logra no solo su ubicación, sino las condiciones mecánicas, necesidades de combustible y mantenimiento, incluso obteniendo datos meteorológicos y otro tipo de información mediante sensores fijos o móviles que capten todo tipo de información que pueda ser procesada y sea útil para la toma de decisiones, toda esta información puede ser compartida con otros compañeros a través de gafas inteligentes que informen sobre el estado de sus compañeros y vehículos para retroalimentar al grupo que combate (CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL, 2020).

Pero la Inteligencia Artificial aplicada a las fuerzas armadas no termina en los sensores que se pueden emplear, se requieren también del manejo de la gran cantidad de información que se obtiene mediante estos sensores, procesarla rápidamente y regresarla a los usuarios que la explotarán, para lo cual se emplean principalmente la minería de datos que es la generación de conocimiento mediante el procesamiento de grandes cantidades de datos y el *big data* que se refiere a la obtención, manejo, almacenamiento y búsqueda de patrones en los datos y el *machine learning* o aprendizaje automatizado, que emplea algoritmos que siguen modelos de comportamientos usuales, para lo que se requiere una gran cantidad de datos con suficiente granularidad sin sesgo ni manipulación (CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL, 2020).

11 NORMAS Y LEYES

Para atender las necesidades en materia de ciberseguridad, se debe promover y fomentar la armonización de la normatividad a nivel regional para contar con un marco legislativo que incentive la confianza en las transacciones en línea, tanto a nivel nacional como a nivel regional, enfocándose en la protección de la privacidad y datos personales, delitos informáticos y delitos por medio de las tecnologías de la información y comunicaciones, spam, firma electrónica o digital y contratos electrónicos, como marco para el desarrollo de la sociedad de la información (UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, 2015).

Respecto a las transacciones electrónicas, firmas electrónicas y autenticación, así como impuestos y aduanas, hay esfuerzos destacados como la adaptación de las normativas de Argentina, Chile, Colombia, Ecuador, México, Perú y Venezuela a la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) y la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (CNUCE) de 2005 que ha sido firmada por Colombia y Paraguay (UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, 2009).

En cuanto a la Protección de Datos Personales, a nivel constitucional, la protección a la vida privada ha sido reconocida por Argentina, Chile, Colombia, Ecuador y México, las Constituciones de Paraguay, Perú y Venezuela, reconocen de manera expresa el derecho del Habeas Data (o derecho a la autodeterminación informativa), algunos países han regulado el tema de la protección de datos a través de una ley especial, como Argentina, Chile, Colombia, Uruguay, Bolivia, Cuba, Ecuador, México, Paraguay, Perú y Venezuela han regulado el tema mediante distintas leyes de diversa índole (UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, 2015).

Para el combate a los Delitos Informáticos, Chile y Venezuela han emitido leyes especiales en materia de delitos informáticos, Argentina, Ecuador, México, Paraguay y Perú, han incorporado en sus respectivos códigos penales y en algunas otras leyes a los delitos informáticos (UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, 2015).

En el ámbito de la propiedad intelectual existe mayor nivel de armonización normativa por los países que han suscrito tanto el Convenio de París como el Convenio de Berna el Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre el Derecho de Autor (WCT) ha sido suscrito y se encuentra en vigor en Argentina, Chile, Colombia, Ecuador, México, Paraguay y Perú. Mientras que Bolivia, Uruguay y Venezuela también lo han suscrito, sin que todavía se encuentre en vigor. Por lo que se refiere al Tratado de la OMPI sobre la Interpretación o Ejecución y Fonogramas (WPPT), es preciso señalar que dicho instrumento ha sido suscrito y se encuentra en vigor en Argentina, Chile, Colombia, Ecuador, México, Paraguay, Perú y Uruguay. Tanto Bolivia como Venezuela ya firmaron el Tratado, sin embargo, aún no ha entrado en vigor. En cuanto al ADPIC de la OMC, es importante mencionar que tanto Argentina, como Chile, Colombia, Ecuador, México y Perú se han adherido al mismo (UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, 2015).

En materia de nombres de dominio, tanto Argentina, como Chile, México, Perú y Venezuela han adoptado dentro de sus políticas de resolución de controversias la Política Uniforme de Resolución de Controversias sobre Nombres de Dominio de ICANN, y reconocen el procedimiento arbitral del Centro de Arbitraje y Mediación de la OMPI, Perú reconoce como instancia arbitral al Cibertribunal Peruano, Paraguay dirime sus controversias sobre nombres de dominio mediante mecanismos extrajudiciales de Arbitraje y Mediación.

12 NUEVAS TECNOLOGÍAS

Gracias a los esfuerzos de armonización el siguiente paso es la innovación. El poder tecnológico de un país, generalmente está alineado con su proclividad a la visión de Estado, será fuerte cuando se tenga la capacidad de pensar en proyectos que tengan resultados y mejoras para las siguientes generaciones y no solo para ganar votos para la siguiente elección, lo que se percibe en obras de gran magnitud y

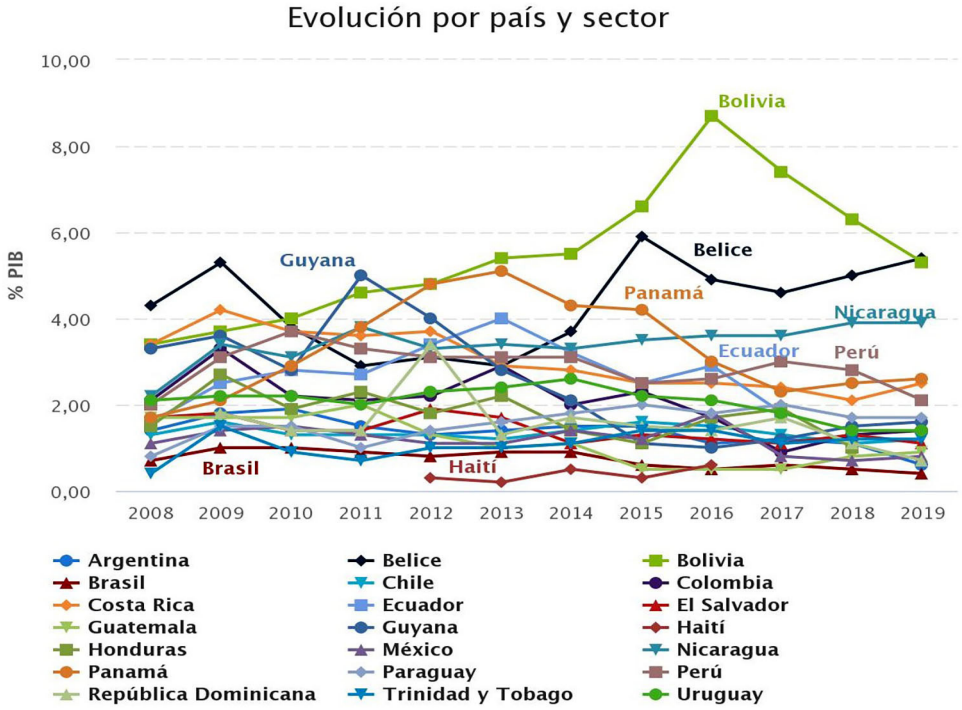
proyectos de investigación y desarrollo de largo plazo, en la gráfica 2: observamos la evolución de la inversión pública en infraestructura económica en Latinoamérica de acuerdo a lo identificado por (INFRALATAM, 2019).

13 INTERNET DE LAS COSAS Y BLOCKCHAIN

En ese contexto, entre las tecnologías de vanguardia que dan un gran impulso a la digitalización, está la Internet de las cosas: su impacto es transversal tanto en el desarrollo de bienes y servicios como para usos productivos, para 2017 había casi 8.000 millones de unidades instaladas de la Internet de las cosas a nivel mundial, de las cuales el 63% correspondía a soluciones de consumo, como domótica, tecnologías punibles o autos conectados, en tanto que el restante 37% se repartía en soluciones para sectores específicos.

Al mismo tiempo, la adopción de las cadenas de bloques o *blockchain* muestra un aumento exponencial. Una vez que de forma gradual se alcanzaron los 2 millones de usuarios de monederos (*blockchain wallets*) entre 2011 y 2014, su crecimiento se aceleró, superando los 21,5 millones a finales de 2017.

Gráfica 2: Inversión Pública en Infraestructura Económica.



Fuente: INFRALATAM, 2019.

Data Science es un paradigma científico, mediante el que los procesos y sistemas de búsqueda del conocimiento es diametralmente opuesto a los anteriores, la forma en que los científicos de datos se organizan y trabajan es diferente ya que obtienen asistencia inteligente para manejar una gran cantidad de datos, una gran selección de ecuaciones y modelos, una gran selección de algoritmos de estimación y una complicada evaluación y explicación de los resultados.

14 INNOVACIÓN

En los primeros 20 años del presente siglo, los países de Latinoamérica han realizado modificaciones a sus políticas internas para fomentar la innovación, incrementando de esta forma el número de patentes solicitadas, la región sigue siendo principalmente usuaria de la tecnología desarrollada en países avanzados, pero en algunos campos como en el caso de Brasil y los biocombustibles se adquieren gradualmente posiciones de liderazgo. Esta innovación proviene principalmente de las universidades que por medio de patrocinios empresariales llevan nuevas ideas a los mercados y fortalecen la investigación pública y su vínculo con la aplicación industrial (RUIZ, 2017).

Tabla 1: Solicitudes de Patentes, Residentes.

Nombre del país	Año Más Reciente	Valor Más Reciente	
América Latina y el Caribe	2019	8.391	
América del Norte	2019	289.351	
Asia meridional	2019	20.191	
Asia oriental y el Pacífico (excluido altos ingresos)	2019	1.249.860	
Europa y Asia central	2019	138.074	

Fuente: ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL, 2020.

Las estadísticas de la Organización Mundial de Propiedad Intelectual (OMPI) indican que la innovación en Latinoamérica y el Caribe sigue rezagada frente a otras regiones en lo que respecta a las patentes, que es uno de los indicadores más comúnmente empleados para determinar la cantidad de invenciones y nuevos

productos que se generan en un país, según el BID (Inter-American Development Bank, en inglés) existe una alta correlación entre la inversión en Investigación y Desarrollo y el número de patentes que se registran (ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL, 2020).

El fortalecimiento de la defensa nacional tiene vinculación directa con el desarrollo científico y tecnológico, en Latinoamérica, algunos países como México y Brasil en los últimos 15 años, han evolucionado en muchos aspectos y logrado la estabilidad multidimensional por lo que implementan políticas públicas que promueven el desarrollo de la investigación y desarrollo de Defensa. Un primer signo favorables e observa en su Política Exterior, que materializa alianzas estratégicas internacionales, sin haber generado ninguna crisis grave que hubiere producido desconfianza a nivel hemisférico o global. En la actualidad la independencia en la industria militar e sinal canzable para la mayoría de los países, es por ello que la confianza mutua es una condición básica para el desarrollo sectorial. Durante el periodo 2007-2020, ambos países estimularon la ciencia, tecnología e innovación con fondos públicos, en busca de la madurez tecnológica en sectores estratégicos, incorporándose a las cadenas de valor global es que incluyen al sector Defensa considerando la dualidad militar y civil para la producción y oferta de servicios, impulsando la formación y especialización de investigadores a través de becas y fondos para proyectos de investigación para el desarrollo del capital humano y la innovación (CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS, 2020).

Tabla 2: Top Ten Gartner Hype Cycles, 2018-2020.

2018 ↓	2019 ↓	2020 ↓
Emerging Technologies	Emerging Technologies	Emerging Technologies
Artificial Intelligence	Artificial Intelligence	Artificial Intelligence
Data Science and Machine Learning	Digital Workplace	Analytics and Business Intelligence
Cloud Computing	Cloud Computing	Digital Workplace
Internet of Things	Analytics and Business Intelligence	Enterprise Architecture
Analytics and Business Intelligence	Internet of Things	Security Operations
Blockchain Business	Data Science and Machine Learning	Cloud Security
Digital Workplace	Data Management	Endpoint Security
Cloud Security	Cloud Security	Data Science and Machine Learning
Threat-Facing Technologies	Identity and Access Management Technologies	Cloud Computing

Fuente: DAWSON, 2021

Estas innovaciones dirigen hacia las tendencias internacionales, como las que se observan en la tabla 3, en donde diversas tecnologías emergentes, pronosticadas

por la consultora de investigación en tecnologías de la información Gartner, que tendrán su auge entre los siguientes 2 y 10 años y que en los años 2018, 2019 y 2020 se han repetido, como: Inteligencia Artificial, *Data Science and Machine Learning, Cloud Computing, Analytics and Business Intelligence, Digital Workplace y Cloud Security* (DAWSON, 2021).

15 DATA SCIENCE

La ciencia de datos es un campo interdisciplinar que extraeconocimiento a partir de conjuntos de datos, ya sea desde bases de datos o desde textos, audios o vídeos, aplicando para ello técnicas que ayudan a resolver problemas que no se podrían resolver fácilmente a través de otros métodos. La ciencia de datos combina métodos y tecnologías matemáticos, estadísticos e informáticos como el análisis exploratorio, el *machine learning*, el *deeplearning*, el procesamiento del lenguaje natural, la visualización de datos y el diseño experimental(MINECO, 2018). La construcción de sistemas capaces de aprender a resolver problemas sin la intervención de humana y que vemos en sistemas de predicción ortográfica o traducción automática hasta coches autónomos o sistemas de visión artificial.

16 CÓMPUTO EN LA NUBE

El cómputo en la nube es un esquema de acceso ubicuo bajo demanda a través de internet, a diversos recursos de cómputo a través de los cuales pueden ser rápidamente asignados y provistos con un mínimo de gestión administrativa e interacción es un modelo que promueve la disponibilidad mediante el autoservicio bajo demanda, con acceso de red de amplio ancho de banda, conmutación de recursos, elasticidad y servicio medido, empleando para ello el software como servicio, la plataforma como servicio y/o la infraestructura como servicio (BARNARD, 2016).

Los modelos de despliegue del cómputo en la nube son: la nube privada que es operada por una sola organización, que puede ser la usuaria o un tercero; la nube comunitaria en donde varias organizaciones comparten el apoyo a una comunidad puede ser administrada por las organizaciones o por un tercero; la nube pública que pertenece a una organización que comercia servicios en la nube, poniéndolos disponibles al público en general o a industrias; y la nube híbrida en donde se combinan dos o más tipos de nubes que son entidades únicas unidas por la tecnología y la portabilidad de datos y aplicaciones (BARNARD, 2016)

Entre las características del cómputo en la nube son la reducción de costos - ya que no se requiere contar con especialistas e infraestructura de vanguardia - haciendo flexibles los cambios y actualizaciones, sin curvas de aprendizaje prolongadas, no obstante en contra tiene la dependencia de proveedores y

la obligatoriedad de contar con acceso permanente a Internet para el buen funcionamiento de la infraestructura soportada, lo que no siempre es factible ni esperable, otro punto delicado es la seguridad de la información ya que se deposita en un tercero la confianza en la protección física y lógica de la infraestructura.

17 BUSINESS INTELLIGENCE

Se refiere a la recopilación, organización y análisis de datos para transformarlos en información que pueda ser empleada para la mejora de procesos y la estructuración de la toma de decisiones, anticipando riesgos y proporcionando predicciones para el crecimiento del negocio de que se trate, tomando la palabra negocio como el giro de una organización sea gubernamental, privada o de cualquierotro tipo, por medio del *business intelligence* se identifican oportunamente tendencias en el mercado y se está en condiciones de realizar comparativos con organizaciones similares, dar seguimiento de las metas institucionales e incluso optimizar procesos de la organización.

Se complementa con *Business Analytics* que en lugar de realizar el análisis descriptivo de la información lo hace conjuntando datos históricos y presentes para complementándolo con estadísticas e información diversa definir claramente el momento del negocio y de esta forma detectar patrones negativos que inciden en los procesos de negocio, por lo que se genera información para coordinación y evaluación interna y se convierte en decisiones estratégicas.

18 CONCLUSIÓN

Cuando se habla del poder nacional de los Estados, se identifica entre sus componentes al poder militar, al poder político o al poder económico, en algunos casos se habla también del poder tecnológico y en los últimos años encontramos en la literatura al poder cibernético o ciberpoder que tiene sus propias características.

Entre las cualidades que el ciberpoder comparte con la tecnología están que son la base de la infraestructura crítica y que por lo tanto su dominio es parte de la seguridad nacional, es decir que a menor dependencia tecnológica o cibernética se tendrán mayores posibilidades de preservar las condiciones para que un Estado prevalezca y se desarrolle.

Latinoamérica tiene aún muchas áreas de oportunidad, es una zona del mundo que enfrenta múltiples riesgos y amenazas y que antes de buscar el desarrollo tecnológico de vanguardia necesita cubrir necesidades básicas de su población y reducir el impacto que tiene de los antagonismos tradicionales que laceran sus instituciones y a su población.

Pero los múltiples avances tecnológicos que se han dado en parte por la pandemia del COVID-19 revolucionaron los mercados y a la propia sociedad de los

países latinoamericanos, por lo que es necesario agilizar la integración a la sociedad de la información para evitar que la brecha tecnológica se abra y los pueblos de la región sufran una mayor inequidad digital.

El PIB de Latinoamérica como en gran parte del mundo tuvo una contracción cercana al 8%, una de las más altas del presente siglo, repercutiendo en pérdida de empleos e incremento proporcional en otro de los antagonismos tradicionales de la región, la pobreza. Por ello se vuelve primordial mantener e incrementar el ímpetu por proporcionar internet a la mayor parte de la población como se hace en buena parte de la región.

El crecimiento en el acceso a servicios digitales para prolongar el empuje que se ha dado a la educación a distancia, a las transferencias de recursos electrónicas en el sistema bancario, la telemedicina y los servicios públicos en línea entre muchos otros beneficios que permite el empleo del ciberespacio, son base de las políticas públicas que han mejorado la competitividad de la región, pero son necesarias inversiones adicionales en infraestructura y la expansión de la tecnología 4G e incorporación a la 5G.

Pero la consolidación de estas tecnologías ocasionará la intensificación de las ciberamenazas sobre todo si no se toman las previsiones con controles de seguridad, sistemas de gestión de seguridad de la información, una base creciente de profesionales dedicados a la protección de los activos de información y la incorporación en las legislaciones locales y regionales de los nuevos delitos inherentes a su empleo.

El esfuerzo, entonces, por la búsqueda de la equidad digital no termina en agregar conectividad o dar acceso a mayor número de personas o mejorar los anchos de banda de la población vulnerable, se requiere adicionalmente del impulso de la capacitación especializada para las áreas relacionadas con la ciberseguridad, la inteligencia artificial y las nuevas tecnologías relacionadas con el ciberespacio y de forma adicional incorporar a la población adulta mayor con menor preparación a esquemas en que puedan acceder a servicios digitales de forma amigable y segura.

Probablemente el esfuerzo que se requiere para que la región compita con los grandes productores de hardware y software en las empresas multinacionales de mayor tamaño en los países de alto nivel de desarrollo sea poco factible por los costos en recursos humanos, materiales, financieros y temporales que se deben desembolsar, pero por otro lado formar expertos en uso de software especializado, con conocimientos matemáticos, de administración de grandes bases de datos e implementación de tecnologías de importación parece una tarea alcanzable y que podría dar dividendos en un menor tiempo.

A nivel Estado, se requieren nuevos esfuerzos para fortalecer la ciberseguridad en la región, no se tienen planes de ciberseguridad para la protección de su infraestructura crítica de información, también se necesitan capacidades de respuesta a los incidentes de ciberseguridad y contar con organismos centrales que coordinen las actividades de seguridad informática. Del otro lado, la mayor parte de los países latinoamericanos cuentan con equipos de respuesta a incidentes.

La ciberseguridad es una necesidad global de interés fundamental, es un conocimiento básico en el que se debe saber que hacer en caso de emergencia como en el mundo físico, el mundo está lleno de ciberestafas, ciberamenazas y cibercriminales, los que no saben de principios y fundamentos de seguridad, son las primeras víctimas, gobiernos, iniciativa privada y las fuerzas armadas deben entrenarse para familiarizarse con los ciberataques más comunes, aquellos que parecen tener el mínimo nivel de complejidad pero que igualmente ocasionan impactos severos.

Las ciberamenazas de las nuevas tecnologías están en constante evolución y se hacen gradualmente más complejas, por ello se requiere de la capacitación especializada para atender las emergencias y para que los expertos auxilien en la preparación de ejercicios simulados con ciberataques controlados y se identifiquen los riesgos, recordando que más del 90% de los ciberataques que tuvieron éxito, requirieron de la vulnerabilidad de una persona.

Finalmente, en el ámbito de la seguridad nacional, las áreas de protección de infraestructura crítica de información deben tener entrenamientos intensos para conocer procedimientos, enlaces con otras entidades con las que se requerirá coordinar acciones y cuando así lo requiera la emergencia con otros países, de manera tal que se cuente con profesionales que tengan la posibilidad de identificar y contrarrestar las amenazas, recordando la frase de los entrenamientos militares que dice que vale más un torrente de sudor en el campo de instrucción que una gota de sangre en el campo de batalla.

REFERENCIAS

CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL (España). *Usos militares de la inteligencia artificial, la automatización y la robótica.* España, Instituto Español de Estudios Estratégicos, 2020. Disponible en: https://emad.defensa.gob.es/Galerias/CCDC/files/USOS_MILITARES_DE_LA_INTELIGENCIA_ARTIFICIALx_LA_AUTOMATIZACION_Y_LA_ROBOTICA_xIAAxRx.-_VV.AA.pdf. Accedido en: 5 mar. 2022.

CHEN, Emily; DEB, Ashok; FERRARA, Emilio. Election 2020: the first public Twitter dataset on the 2020 US Presidential election, *Journal of Computational Social Science*, 2021. Disponible en: https://link.springer.com/content/pdf/10.1007/s42001-021-00117-9.pdf. Accedido en: 5 mar. 2022.

CENTRO DE INVESTIGACIOINES Y ESTUDIOS ESTRATÉGICOS. Ciencia, tecnología e innovación en la Defensa: los casos de Brasil y México (2007-2020). *Cuaderno de Trabajo*, v.7, 2020. Disponible en: https://www.publicacionesanepe.cl/index.php/cdt/article/view/858/529. Accedido en: 2 abr. 2022.

DAWSON, P. *Hype Cycles*: Innovating Delivery Through Trust, Growth and Change. Gartner, 12 agosto 2021. Disponible en: https://emtemp.gcom.cloud/ngw/globalassets/intl-mx/information-technology/documents/2021-hype-cycles-innovating-delivery-through-trust-growth-and-change-mx.pdf. Accedido en: 2 abr. 2022.

ESPAÑA. Ministerio de Assuntos Económicos y Transformación Digital. *Iniciativa de datos abiertos del Gobierno de España*. Reutiliza la información pública. Madrid: MAETD, 2018. Disponible en: https://datos.gob.es/es. Accedido en: 4 abr. 2022.

GUTTIERRI, K. Accelerate change or lose the information war. Æther*: a journal of strategic airpower & spacepower*, Alabama, Air University, v. 1, n. 1, 2022.

HOUSE OF REPRESENTATIVES. The Year 2000 Problem. *105th Congress*, Washington, DC., Congress, 1998. Disponible en: https://www.congress.gov/105/crpt/hrpt827/CRPT-105hrpt827.pdf. Accedido en: 5 mar. 2022.

INTER-AMERICAN DEVELOPMENT BANK. Improving Lives, Washington, 2020. Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf. Accedido en: 2 abr. 2022.

INTERNATIONAL TELECOMMUNICATION UNION. *Measuring digital development*. Geneva, ITU Publications, 2021. Disponible en: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf. Accedido en: 3 mar. 2022.

INTRODUCCIÓN al cómputo en la nube. Traducción Alicia Barnard, Alejandro Delgado y Juan Voltssás. *Cuadernos digitales de archivística*, v.8, 2016. Disponible en: https://iibi.unam.mx/voutssasmt/documentos/InterPARES_8_020617.pdf. Accedido en: 4 abr. 2022.

KUEHL, D. From Cyberspace to Cyberpower: Defining the Problem, *Cyberpower and National Security.* Washington DC*.,* National Defense University Press, 2009. Disponible en: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210. Accedido en: 3 mar. 2022.

LEDO, M. E. A. Alerta Mundial y Tratamiento del Y2K en el Sistema de Salud Cubano, *Revista Habanera de Ciencias Médicas*, La Habana, Cuba, v. 4, n. 4, p. 1-23, 2005.

NYE, J. *Cyber Power.* Cambridge, Harvard Kennedy School, 2010. Disponible en: https://apps.dtic.mil/sti/pdfs/ADA522626.pdf. Accedido en: 4 mar. 2022.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Conferencia Especial sobre Seguridad In: *Declaración Sobre Seguridad En Las Américas*, México, 2003. Disponible en: https://www.oas.org/36ag/espanol/doc_referencia/DeclaracionMexico_Seguridad.pdf. Accedido en: 4 abr. 2022.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. *Más derechos más gente*. Organización de Estados Americanos, 2016. Disponible en: https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/16. Accedido en: 4 abr. 2022.

OFFICE OF PUBLIC AFFAIRS. *Justice News*. Washington DC: The United States Department of Justice, 2021. Disponible en: https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and. Accedido en: 3 mar. 2022.

ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL, *Solicitudes de patentes, residentes – Latin America &Caribbean, East Asia &Pacific, South Asia, Europe & Central Asia, North America*. Banco Mundial Datos, 2020. Disponible en: https://datos.bancomundial.org/indicador/IP.PAT.RESD?end=2019&locations=ZJ-Z4-8S-Z7-XU&start=2000. Accedido en: 2 abr. 2022.

PUBLIC investment in economic infrastructure: evolution by country and sector. *INFRALATAM*, [*S. l.*], 2021. Disponible en: http://infralatam.info. Accedido en: 3 mar. 2022.

RUIZ, S. Las patentes en Latinoamérica: excepciones a derechos conferidos, materia patentable y mercados potenciales. Madrid, *Blog sobre Marcas, Patentes y Derecho de las TIC*., 2017. Disponible en: https://www.hyaip.com/es/espacio/las-patentes-en-latinoamerica-excepciones-a-derechos-conferidos-materia-patentable-y-mercados-potenciales/#:~:text=Según%20la%20OMP%2C%20en%20el,registrada%20en%20el%20mismo%20año. Accedido en: 2 abr. 2022.

SUI, D.; CAVERLEE. J.; RUDESILL. D. The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box, Washington, DC*, Wilson International Center for Scholars*, 21 Octubre 2015. Disponible en: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2676615_code1468587.pdf. Accedido en: 3 mar. 2022.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. Estudio sobre las perspectivas de la armonización de la ciberlegislación en América Latina, *Conferencia de las Naciones Unidas Sobre Comercio y Desarrollo*. Genebra, 2009. Disponible en: https://unctad.org/es/system/files/official-document/dtlstict20091_sp.pdf. Accedido en: 4 abr. 2022.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. Examen de la armonización de la ciberlegislación en América, In: Accedido en*: Conferencia de las Naciones Unidas Sobre Comercio y Desarrollo*, Genebra, 2015. Disponible en: https://www.casede.org/index.php/biblioteca-casede-2-0/seguridad/ciberseguridad/545-examen-de-la-armonizacion-de-la-ciberlegislacion-en-america-latina/file. Accedido en: 4 abr. 2022.

WORLD ECONOMIC FORUM. *Global Risk Report 2022*. 17ed.,2022. Disponible en: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf. Accedido en: 3 mar. 2022.

CONECTIVIDAD DIGITAL EN LA SITUACIÓN DE EMERGENCIA POR COVID-19

Rodrigo Guillén*

RESUMEN

Las Tecnologías de la Información y la Comunicación (TIC) han tenido un desarrollo explosivo en la última parte del siglo XX y el comienzo del siglo XXI. Prácticamente no hay un solo ámbito de la vida humana que no se haya visto impactada por este desarrollo: la salud, las finanzas. El conocimiento se multiplica exponencialmente y se distribuye de manera prácticamente instantánea, pero también sin equidad. Organismos internacionales como el Unesco, Banco Mundial, BID y la CAF sostienen que, si bien Internet, los teléfonos móviles y otras tecnologías digitales se están extendiendo rápidamente en todo el mundo en desarrollo, los dividendos digitales esperados, mayor crecimiento, más empleo y mejores servicios públicos están por debajo de las expectativas, y el 60% de la población mundial sigue sin poder participar en la economía digital en constante expansión, a la que se le denomina brecha digital, con múltiples consecuencias en la vida de los países, entre ella el Perú donde indicadores de accesibilidad y asequibilidad a los servicios de las TIC afectará la estrategia de contención y restablecimiento a la normalidad como consecuencia de la epidemia del coronavirus COVID 19. El restablecimiento a la normalidad del sector productivo, en la etapa post pandemia COVID-19, requerirá elevar los indicadores digitales del sector empresarial mediante una estrategia nacional para cerrar la brecha digital en el país, por su impacto socio económico y convertir a las TIC en una herramienta fundamental para el restablecimiento de la normalidad que el país exige.

Palabras clave: Conectividad digital; TIC; Internet; Emergencia por COVID-19; Brecha digital.

CONECTIVIDADE DIGITAL EM SITUAÇÃO DE EMERGÊNCIA POR COVID-19

RESUMO

As tecnologias de informação e comunicação (TIC) tem obtido um explosivo desenvolvimento nessa última virada de século. Praticamente não há uma esfera da vida humana que não tenha sido impactada por esse desenvolvimento: a saúde, as financas. O conhecimento se multiplica exponencialmente e se distribui praticamente de maneira instantânea, no entanto sem equidade. Órgãos internacionais como a UNESCO, o Banco Mundial, o BID e a CAF defendem que, embora a Internet, os

* Maestro en Gobernabilidad, con estudios de Maestría en Ingeniería de Telecomunicaciones, Maestría en Economía, Doctorado en Economía en el Centro de Altos Estudios Nacionales-Escuela de Posgrado – Perú. Contacto: rodrigoguillenq123@gmail.com

celulares e outras tecnologias digitais estejam se espalhando rapidamente em todo o mundo em desenvolvimento, os dividendos digitais esperados - maior crescimento, mais empregos e melhores serviços públicos – estão abaixo das expectativas, além de 60% da população mundial segue sem poder particar da crescente economia digital, situação denominada de "exclusão digital", com muitas consequências nas vidas dos países entre eles o Peru, onde indicadores de acessibilidade e viabilidade aos serviços das TICs irão afetar a estratégia de contenção e restabelecimento à normalidade como consequência da pandemia do coronavírus. O restabelecimento à normalidade do setor produtivo na etapa pós-COVID demandará elevar os indicadores digitais do setor empresarial mediante a uma estratégia nacional para acabar com a exclusão digital no país pelo seu impacto socioeconômico e converter as TICs em ferramentas fundamentais para a restauração da normalidade que o país exige.
Palavras-chave: Conectividade digital; TIC; Internet; Emergência por COVID-19;, Exclusão digital.

1 PLANTEAMIENTO DEL PROBLEMA

Las Tecnologías de la Información y la Comunicación (TIC) han tenido un desarrollo explosivo en la última parte del siglo XX y el comienzo del siglo XXI, al punto de que han dado forma a lo que se denomina "Sociedad del Conocimiento" como también "Sociedad de la Información". Prácticamente no hay un solo ámbito de la vida humana que no se haya visto impactada por este desarrollo: la salud, las finanzas, la educación, los mercados laborales, las comunicaciones, el gobierno, la productividad industrial, etc. El conocimiento se multiplica exponencialmente y se distribuye de manera prácticamente instantánea.

Vivimos tiempos de grandes transformaciones tecnológicas que modifican de manera profunda las relaciones humanas. El acceso y generación de conocimiento pasan a ser los motores del desarrollo. Las nuevas formas de conectividad están en el corazón de procesos de cambio en las esferas económicas, políticas y culturales que han dado lugar a lo que se denomina "globalización".

El desarrollo de las Tecnologías de Información y Comunicación (TIC) es importante para los países por sus efectos positivos en varios aspectos de la sociedad. Al respecto las Naciones Unidas (2011) en base a una revisión de diferentes estudios concluyó que el desarrollo de las TIC tiene un efecto sobre la economía, el empleo, las innovaciones, la seguridad, la educación entre otros.

Las Tecnologías de la Información y Comunicación son herramientas que representan un conjunto de tecnologías que tienen como denominador común el uso del código binario (bit) para representar y trabajar información de forma digital. Desde su aparición han provocado un cambio significativo en la organización

productiva y social sobre las que se consolidan las bases de las llamadas Sociedades de la Información y provocando también cambios en la vida de las personas comunes y corrientes.

En el marco de la sociedad de la información, el nivel de penetración de los bienes y servicios ligados a las TIC en los hogares es, sin duda, el punto de partida para impulsar políticas públicas que fomenten la conectividad digital. Sin embargo, aún son grandes las brechas que existen tanto en acceso, calidad del acceso y uso del servicio. Al diseñar las políticas públicas se presentan varios desafíos tales como mejorar la infraestructura y así mejorar la accesibilidad territorial y asegurar la eficiencia para fortalecer la calidad de los servicios al menor precio posible, mejorar el capital humano y así garantizar la equidad en el acceso. Para el diseño, implementación y la evaluación de las políticas públicas es indispensable contar con un perfil de los hogares y usuarios que permita, por una parte, distinguir y asociar grupos a acciones de política particulares y, por otra, medir y valorar brechas o disparidades asociadas a condiciones económicas, territoriales, generacionales, de género. Si bien existe información sobre disponibilidad, acceso y uso de las TIC, esta no siempre es plenamente representativa ni actual, pues o proviene de encuestas que, por lo general, no abarcan a toda la población o provienen de los censos de población y vivienda que a veces entregan información desactualizada. Esto hace que, en algunos países como en el Perú, no sea posible contar con perfiles socioeconómicos de los hogares y usuarios y que no siempre se puedan realizar comparaciones entre los países a partir de los datos disponibles.

Las Tecnologías de la Información y la Comunicación (TIC) son un conjunto de servicios, redes, software y dispositivos de hardware que se integran en sistemas de información interconectados y complementarios, con la finalidad de gestionar datos e información de manera efectiva, mejorando la productividad de los ciudadanos, gobierno y empresas, dando como resultado una mejora en la calidad de vida de la población en general. Ellas se encuentran intrínsecamente ligadas con la rutina y acciones diarias de un porcentaje significativo de los ciudadanos del mundo, siendo hoy el mayor medio de conectividad e interacción y desarrollo que tenemos a nuestro alcance. Por otro lado, nos encontramos inmersos en un proceso de globalización económica que genera una creciente interdependencia entre los países, y donde las TIC han permitido la dinamización de los procesos económicos, sociales y hasta culturales.

Sin embargo, a pesar de la importancia de la información de las TIC en las sociedades, en países de América Latina existen rezagos en la adopción de los servicios de telecomunicaciones. Es así que en la actualidad los indicadores de penetración de los servicios de telefonía fija e internet fija de banda ancha se encuentra por debajo de la media de los países desarrollados; esto es debido a una

serie de características que comparten países de América Latina, tales como contar con una población de bajo poder adquisitivo, déficit de infraestructura, falta de una cultura digital, altas tasas de ruralidad, difícil geografía, entre otros.

Por otro lado, de la gran variedad de los servicios de telecomunicaciones es el servicio de telefonía móvil el que ha logrado avanzar en el cumplimiento de las metas del servicio universal, principalmente a través de las fuerzas del mercado, al crecer de manera sostenida en los países de América Latina como a nivel mundial.

En la actualidad, la penetración del servicio de telefonía móvil ha logrado superar el 100% de la población en gran parte de los países de América latina, permitiendo a la población acceder a los beneficios que esta tecnología conlleva, e inclusive en algunos países de la región la penetración del servicio de banda ancha móvil supera el 80%. En efecto, en 2019, casi el 87% de las personas en países desarrollados utilizaban internet en comparación con el 47% de los países en desarrollo.

También se observan brechas digitales dentro de los países. A Internet se conectan más hombres, residentes de ciudades y jóvenes que habitantes de zonas rurales y personas mayores. Una infraestructura y unos servicios de TIC eficientes y asequibles dentro de entornos normativos y reglamentarios propicios permiten a las empresas y a los gobiernos participar en la economía digital y a los países aumentar su bienestar económico general y su competitividad. Unos 20 países han convertido el acceso a Internet en un derecho fundamental o un derecho de los ciudadanos.

El Banco Mundial (BM) sostuvo que, si bien Internet, los teléfonos móviles y otras tecnologías digitales se están extendiendo rápidamente en todo el mundo en desarrollo, los dividendos digitales esperados, mayor crecimiento, más empleo y mejores servicios públicos están por debajo de las expectativas, y el 60% de la población mundial sigue sin poder participar en la economía digital en constante expansión.

Según el *Informe sobre el desarrollo mundial: dividendos digitales*; los beneficios de la acelerada expansión de las tecnologías digitales han favorecido a las personas adineradas, cualificadas e influyentes del mundo, que están en mejores condiciones de sacar provecho de las nuevas tecnologías. Además, si bien el total de usuarios de Internet se ha triplicado con creces desde 2005, hay 4,000 millones de personas que todavía no tienen acceso a Internet (WORLD BANK GROUP, 2016).

El Informe afirma que, si bien hay muchos casos individuales de éxito, hasta ahora el efecto de la tecnología en la productividad mundial, en la ampliación de las oportunidades para los pobres y la clase media, y en la propagación de la gobernanza responsable, ha sido mucho menor que el esperado. Las tecnologías digitales se están expandiendo rápidamente, pero los dividendos digitales crecimiento, empleo y servicios han quedado a la zaga (WORLD BANK GROUP, 2016).

Kaushik Basu, primer economista del Banco Mundial, manifestó que el hecho de que en la actualidad el 40% de la población mundial esté conectada a través de Internet es una transformación impresionante.

> Si bien estos logros deben celebrarse, también debemos ser conscientes de no crear una nueva subclase social. Dado que casi el 20 % de la población mundial no sabe leer ni escribir, es improbable que la expansión de las tecnologías digitales por si sola signifique el fin a la brecha de conocimientos que existe en el mundo. (BANCO MUNDIAL EN VIVO, 2016).

Para que se pueda cumplir plenamente la promesa de desarrollo que encierra una nueva era digital, el Banco Mundial recomienda dos cursos de acción principales: acortar la brecha digital haciendo que Internet sea universal, accesible, abierta y segura; y reforzar las regulaciones que garantizan la competencia entre empresas, adaptar las habilidades de los trabajadores a las exigencias de la nueva economía, y promover instituciones responsables medidas que en el informe se denominan complementos analógicos de las inversiones digitales.

Las estrategias de desarrollo digital deben ser más amplias que las estrategias del sector de las TIC. Para obtener el máximo provecho, los países deben crear las condiciones adecuadas para la tecnología: regulaciones que faciliten la competencia y el ingreso en el mercado, habilidades que permitan a los trabajadores aprovechar las oportunidades que ofrece la economía digital, e instituciones que rindan cuentas a las personas. Las tecnologías digitales pueden, a su vez, acelerar el ritmo de desarrollo.

Invertir en infraestructura básica, rebajar el costo de hacer negocios, reducir los obstáculos al comercio, facilitar el ingreso de las empresas incipientes en el mercado, robustecer las autoridades en materia de competencia, y facilitar la competencia en las plataformas digitales son algunas de las medidas recomendadas en el Informe sobre el desarrollo mundial que pueden contribuir a que las empresas sean más productivas e innovadoras. Además, si bien un nivel básico de alfabetización sigue siendo esencial para los niños, la enseñanza de habilidades cognitivas y de pensamiento crítico avanzadas y la formación fundacional en sistemas técnicos avanzados de TIC serán fundamentales a medida que Internet se siga extendiendo.

Sin embargo, a pesar de la importancia de la información de las TIC en las sociedades, en países de América Latina y el Caribe entre ellos el Perú; existen muchos rezagos en la priorización y estrategia en la adopción de estas tecnologías. Las Tecnologías de la Información y comunicación pueden ser de banda angosta o banda ancha. La Banda Ancha es entendida como acceso a Internet de alta velocidad, que combina la capacidad de conexión (ancho de banda) y la velocidad

del tráfico de datos (expresada en Mbps), permitiendo a los usuarios acceder a diferentes contenidos, aplicaciones y servicios. Según el Banco Mundial en el estudio *Información y Comunicación para el desarrollo 2009* indicó "la Banda Ancha aumenta la productividad y contribuye al crecimiento económico, y por lo tanto merece un rol central en las estrategias de desarrollo" (WORLD BANK. 2009)

2 DEFINICIONES DE LA BRECHA DIGITAL EN PERÚ

El concepto de ¨brecha digital¨ es amplio y complejo. Organizaciones de la industria, gobiernos, académicos, consultoras y otros actores han realizado profundos estudios para ordenar los múltiples aspectos, sus causas, sus impactos y recomendar acciones para reducirla todo lo posible. Gobiernos, operadores, proveedores de equipamiento y la industria en general ya han puesto manos a la obra en este proceso. Convergencia *Research* considera que el análisis de la ¨brecha digital¨, comprende, al menos, los siguientes aspectos:

- Brecha de infraestructura o cobertura (Accesibilidad): Las redes de comunicaciones tienen que lograr una cobertura total de la población, abarcando las urbes, pero también el plano rural.
- Brecha de adopción (asequibilidad): Es la que existe entre los que están alcanzados por los servicios de una red y los que contratan los servicios. Esta brecha es consecuencia de la brecha socio-económica. La reducción de esta brecha, a su vez, podría contribuir a generar más desarrollo económico y social y, eventualmente, menor desigualdad. La cobertura de redes es una condición necesaria para que no exista brecha de adopción o acceso. Dentro de esta brecha hay, al menos, dos problemáticas adicionales clave: la asequibilidad en el servicio y el dispositivo (brecha en la capacidad de pago) y la motivación, que está relacionada con aspectos culturales y educativos, como encontrarle el sentido o provecho al hecho de estar conectado.
- Brecha de uso: Una vez conectada, la brecha de uso es la diferencia entre las aplicaciones disponibles y las que se utilizan. Comprende también barreras culturales. Las aplicaciones (*software*) tienen que ser conocidas, pero también deben representar una utilidad y estar disponibles a precios razonables. En el caso particular de Internet, suelen aparecer usos disruptivos como las redes sociales, u otros generados a partir de los mismos usuarios de la red. Parte de las limitaciones en el uso de aplicaciones disponibles están relacionadas con la velocidad y robustez de las redes, por ejemplo, las aplicaciones en la nube, en la medida en que sigan expandiéndose demandarán soluciones más veloces, de menos latencia y de mayor seguridad. Es-

tos aspectos de la ¨brecha digital¨ son interdependientes y categorizarlos es sólo una simplificación para analizarlos y ordenar el punto de partida de este estudio.

2.1 INDICADORES

El Índice de Adopción Digital (IAD) fue construido como un indicador para medir la brecha mundial de las tecnologías digitales. Es el esfuerzo del BM y de Microsoft para proveer al mundo entero de información comprensible sobre la tecnología en tres segmentos de la economía: negocios, personas y gobiernos.

El IAD muestra un rango de puntaje de 0 a 1, donde 0 es la mayor brecha digital y 1, la menor. Perú obtiene un índice de 0.51, uno de los niveles más altos de América Latina en cuanto a la brecha digital, solo superando a Paraguay y Bolivia. En las variables evaluadas, el sector gubernamental muestra una mayor adopción digital con un índice de 0.65, seguido por los ciudadanos con 0.49 y, al final, los negocios con solo 0.39. Por ejemplo, se menciona que el 56% de los negocios en Perú cuentan con un *website*, mientras que el acceso a Internet en los hogares es de 30%. (PERÚ, 2018).

En América Latina, Uruguay alcanza el mayor puntaje con 0.72, seguido por Chile con 0.70, Brasil con 0.64, Colombia con 0.62, Argentina con 0.60, Panamá con 0.55, Venezuela y Ecuador con 0.54, México con 0.52, Paraguay y Bolivia con 0.48 (PALMA, 2016).

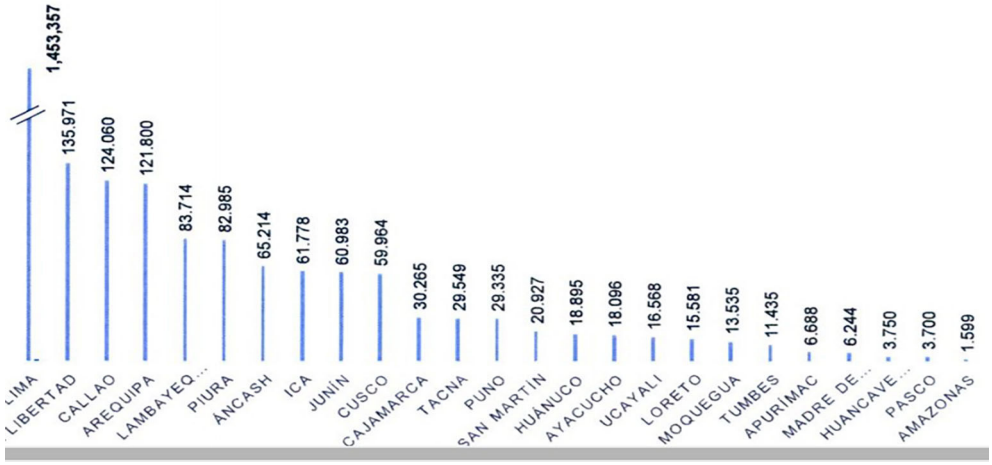
3 PENETRACIÓN DE INTERNET

3.1 PENETRACIÓN DE INTERNET FIJO

Es así que en la actualidad los indicadores de penetración de los servicios de telefonía fija e internet fija de banda ancha en América latina se encuentra por debajo de la media de los países desarrollados; esto es debido a una serie de características que comparten países de América Latina, tales como contar con una población de bajo poder adquisitivo, déficit de infraestructura, falta de una cultura digital, altas tasas de ruralidad, difícil geografía, entre otros.

En el caso del Perú según el Informe del INEI de setiembre 2019; solo 21.9 % de los hogares peruanos tienen acceso a telefonía fija las mismas que acceden a través de 2´475,995 de conexiones. En Lima acceden el 45.2%, y en las áreas rurales solo el 0.7% de hogares. Asimismo, el 39.2 de hogares acceden a internet y el 33.7 Lo hacen a una computadora. En las áreas rurales el 4.8% de los hogares. Acceden a internet y el 2.8% a una computadora. Además, a nivel de desagregado de líneas fijas a nivel nacional, Lima concentra la mayor cantidad de líneas, seguido por la Libertad y Arequipa.

Figura 1: Conexiones a internet fijo por provincia - 2018



Fuente: WORLD BANK, 2018, p.12**.**

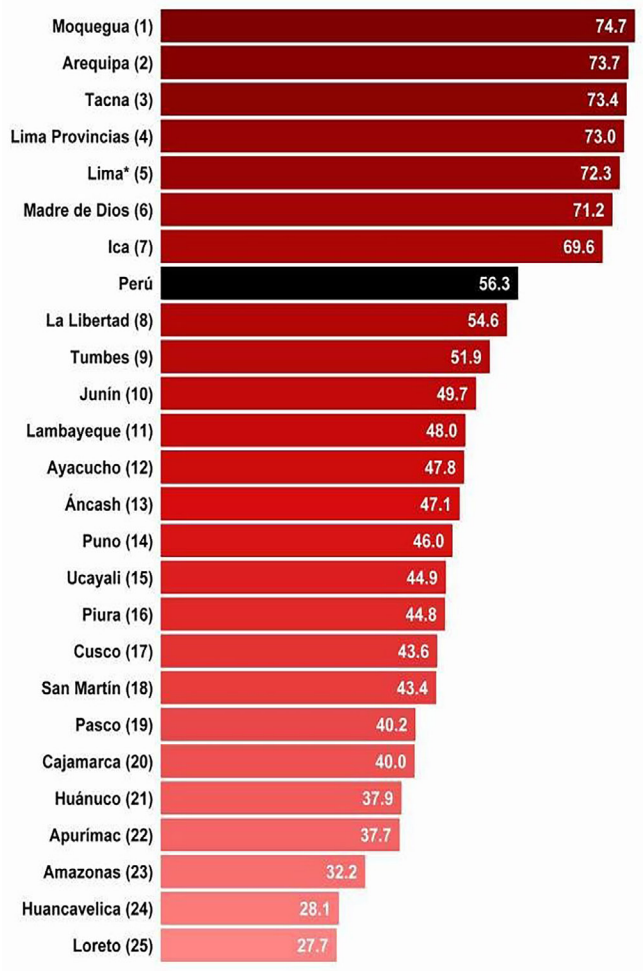
3.2 PENETRACIÓN DE INTERNET MÓVIL

En el informe ejecutivo sobre el estado de internet en materia de conectividad de 2017 realizado por Akamai (Plataforma de distribución en la nube) se estima que 69 de cada 100 habitantes accedieron al servicio de Internet móvil. El acceso a internet móvil presento un crecimiento del 85% desde el primer trimestre de 2014, cuando se reportaron un total de 11. 4 millones de líneas móviles que accedieron a Internet.

Figura 02: Penetración del acceso a internet -Dic 17

Fuente: WORLD BANK, 2018, p.14**.**

Figura 03: Penetración de Telefonía Móvil con Internet a nivel regional (2014-2018 en % de población)



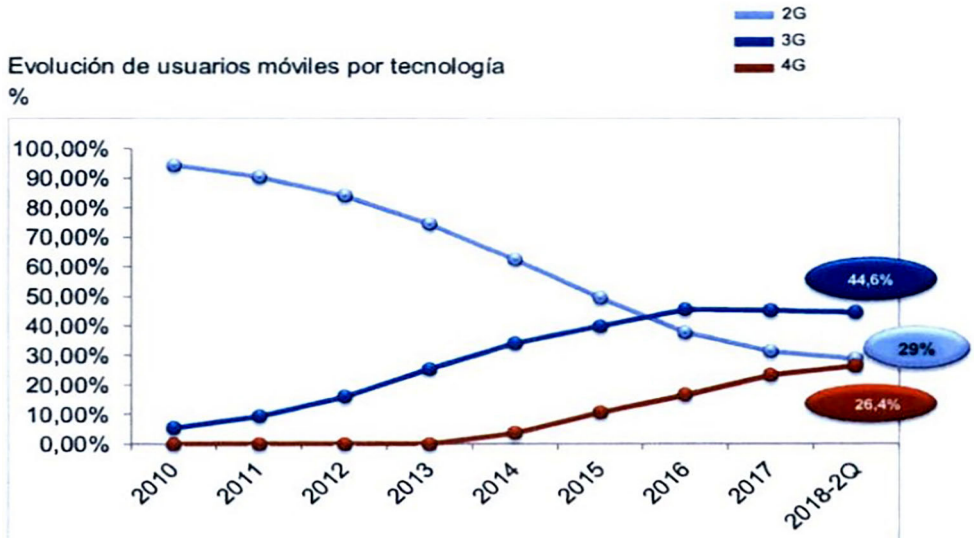
Fuente: WORLD BANK, 2018.

Las regiones que tienen en el orden del 40% o menos de penetración son Loreto, Huancavelica, Amazonas, Cajamarca y Huanuco.

3.3 TRAFICO DE INTERNET MÓVIL

El tráfico de Internet Móvil ha mostrado un crecimiento exponencial entre 2014 y 2017. Entre el primer trimestre de 2014 y el cuarto de 2017, el tráfico de Internet cursado por las redes móviles se multiplico por 27 veces, como se muestra en la siguiente figura:

Figura 04: Trafico de Internet Móvil y Consumo Promedio

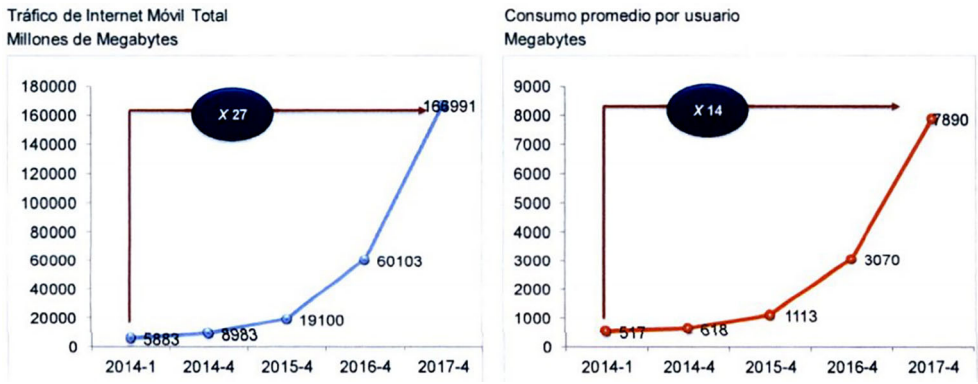


Fuente: WORLD BANK, 2018, p.15.

3.4 PENETRACIÓN MÓVIL POR TECNOLOGÍA

Según reporte del Ministerio de Transportes y Comunicaciones (PERÚ, 2019), el 59% de las líneas móviles que acceden a Internet lo hacen a través de redes 3G y 2G. Con base a las estadísticas del Banco Mundial, en el segundo trimestre de 2018, solo el 26,4% de las conexiones móviles en el Perú correspondían a usuarios 4G, conforme se muestra en la siguiente figura.

Figura 05: Evolución de usuarios móviles por tecnología



Fuente: WORLD BANK, 2018, p.16**.**

4 ROL DE LAS TIC EN LA ACTUAL SITUACIÓN DE EMERGENCIA NACIONAL

El 15 de marzo de 2020, el gobierno peruano emitió el Decreto Supremo Nº 044-2020-PCM (PERÚ, 2020), declarando Estado de Emergencia Nacional por 15 días y el aislamiento social obligatorio (cuarentena) por las graves circunstancias que afectan la vida de la nación a consecuencia del brote de la enfermedad Covid-19. El periodo de cuarentena, posteriormente, fue ampliado por el Decreto Supremo Nº 051-2020-PCM (PERÚ, 2020a), luego por el Decreto Supremo Nº 064 -2020-PCM hasta el 26 de abril de 2020 (PERÚ, 2020b).

El 1 de abril pasado, el organismo regulador de las telecomunicaciones en el Perú, el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) , manifestó que el incremento de los servicios se disparó hasta cerca de 42 por ciento en las redes fijas de Internet y hasta 20 por ciento en las redes móviles, luego de 17 días de la declaración de Estado de Emergencia Nacional y el aislamiento social obligatorio (cuarentena) dispuesto por el gobierno peruano el 15 de marzo, a consecuencia del brote de la Covid-19, enfermedad más conocida como coronavirus. (PERÚ, 2021).

Una evaluación rápida del rol y su impacto en la situación de emergencia nacional en el Perú; tienen que realizarse en tres situaciones; antes, durante y post emergencia. En ella la Brecha Digital existente en nuestro país se convierte en una barrera con características estratégicas; no solo es como cubrir el déficit de infraestructura en corto plazo, sino también como cerrar la pobreza en el país. Y por otro lado es de suma importancia acelerar la culminación de los proyectos de Gobierno Electrónico y trasversalmente a estos objetivos es de suma importancia trascendente diseñar un Plan de recursos logísticos , tecnológicos y de RRHH para hacer frente a estos retos y para ello es de urgente importancia la sensibilización de los líderes de toma de decisiones de gobierno al más alto nivel para que las TIC y la brecha digital se conviertan en las prioridades de políticas de gobierno a todos los niveles.

El Perú es un país que tiene un poco más de 32 millones de habitantes, el séptimo país más poblado de América y, según el INEI, se estima que hacia 2021, año del Bicentenario de la Independencia, la población superará los 33 millones· De la población actual, 79 por ciento es urbana y 21 por ciento se encuentra en áreas rurales· Por otro lado, cerca de 35 por ciento de la población se encuentra en la capital, Lima, mientras que en el segundo departamento que le sigue se encuentra un poco más de 6 por ciento de la población total· (EN EL 2020 POBLACIÓN, 2020)

En este contexto, en el país hay una población muy concentrada en la capital, por lo que las telecomunicaciones con sus redes y las TIC juegan un rol muy importante en esta coyuntura.

4.1 SITUACIÓN ANTES DE LA EMERGENCIA

Como se indicó la brecha digital en el país está relacionado directamente a la pobreza ya que la oferta y la demanda de bienes y servicios TIC del mercado no tiene alcance en las poblaciones incomunicadas y pobres del país. Las variables a considerar en la brecha digital son la Accesibilidad (Acceso a Infraestructura), Asequibilidad (Acceso por precios) y de uso.

Desde el punto de vista Normativo, la atención de las emergencias obedece a un marco que involucra a todos los actores; pero sin embargo para el caso de la Epidemia del Coronavirus requerían de ciertas precisiones para la atención de los ciudadanos afectados por la brecha digital. El marco general existente es la siguiente en Constitución Política del Perú: Art. 137°.

> El Presidente de la Republica, con acuerdo del Consejo de Ministros, puede decretar, por plazo determinado, en todo el territorio nacional, o en parte de él, y dando cuenta al Congreso o a la Comisión Permanente, los estados de excepción que en este artículo se contemplan:
> 1. Estado de emergencia, en caso de perturbación de la paz o del orden interno, de catástrofe o de graves circunstancias que afecten la vida de la Nación. En esta eventualidad, puede restringirse o suspenderse el ejercicio de los derechos constitucionales relativos a la libertad y la seguridad personales, la inviolabilidad del domicilio, y la libertad de reunión y de tránsito en el territorio comprendidos en los incisos 9, 11 y 12 del artículo 2° y en el inciso 24, apartado f del mismo artículo. En ninguna circunstancia se puede desterrar a nadie. El plazo del estado de emergencia no excede de sesenta días. Su prorroga requiere nuevo decreto. En estado de emergencia las Fuerzas Armadas asumen el control del orden interno si así lo dispone el Presidente de la Republica.
> 2. Estado de sitio, en caso de invasión, guerra exterior, guerra civil, o peligro inminente de que se produzcan, con mención de los derechos fundamentales cuyo ejercicio no se restringe o suspende. El plazo correspondiente no excede de cuarenta y cinco días. Al decretarse el estado de sitio, el Congreso se reúne de pleno derecho. La prórroga requiere aprobación del congreso. (PERÚ, 1993, p. 33-34).

El Poder ejecutivo luego de evaluar el estado de excepción requerida y al amparo de éste artículo dicta el Decreto Supremo N° 044-2020-PCM (PERÚ, 2020) que declara Estado de Emergencia Nacional por las graves circunstancias que afectan la vida de la Nación a consecuencia del brote del COVID-19.

Otro Decreto Supremo N° 020-2007-MTC: Texto Único del Reglamento General de la Ley de Telecomunicaciones Artículo 18.- Obligaciones en casos de estados de excepción:

> En los estados de excepción contemplados en la Constitución y declarados conforme a ley, todos los operadores de servicios portadores y teleservicios o servicios finales deben otorgar prioridad a la transmisión de voz y data, necesaria para los medios de comunicación de los Sistemas de Defensa Nacional y Defensa Civil. En caso de guerra exterior, declarada conforme a ley, el Consejo de Defensa Nacional a través del Comando Conjunto de las Fuerzas Armadas, podrá asumir el control directo de los servicios de telecomunicaciones, así como dictar disposiciones de tipo operativo.
> Para atender dichos requerimientos, el operador del servicio de telecomunicaciones podrá suspender o restringir parte de los servicios autorizados, en coordinación previa con el Ministerio y los Sistemas de Defensa Nacional y Civil.
> Para dichos fines, el Ministerio comunicará a los órganos competentes de los Sistemas de Defensa precitados, las concesiones, autorizaciones, permisos y licencias que otorga, así como sus cancelaciones. (PERÚ, p.7).

En el Artículo 19.- Obligaciones en casos de emergencia del mismo Decreto:

> En caso de producirse una situación de emergencia o crisis local, regional o nacional, tales como terremotos, inundaciones u otros hechos análogos, que requieran de atención especial por parte de los operadores de los servicios de telecomunicaciones, éstos brindarán los servicios de telecomunicaciones que sean necesarios dando prioridad a las acciones de apoyo conducentes a la solución de la situación de emergencia. Para tal efecto, los titulares de concesiones y autorizaciones seguirán las disposiciones del Ministerio. (PERÚ, 2007).

En el Decreto Supremo N°051-2010-MTC –Oct-2010 "Marco Normativo General del Sistema de Comunicaciones de Emergencia" establece:_Red Especial terrestre de Comunicaciones en Emergencia; Red Especial satelital de Comunicaciones de Emergencia; Servicio de Emergencia por mensajería de voz 119; Servicio de llamadas gratuitas y mensajería corta en zonas afectadas. (PERÚ, 2010).

Estas disposiciones se dictaron en el escenario que las emergencias se producen como consecuencia de fenómenos naturales como terremotos, inundaciones, alud u otros hechos generados por el hombre que generen una situación de peligro inminente o daño a la vida ; la cual es aplicable para el caso de la Epidemia del Coronavirus pero siendo necesario ampliar y precisar las disposiciones su alcance nacional y la atención inmediata a las redes de emergencia de salud y atención inmediata a los incomunicados producto de la brecha. (PERÚ, 2020).

En el Contratos de Concesión de Servicios de Telecomunicaciones (En algunos). Obligaciones en casos de Emergencia, Crisis o Estados de Excepción. Estados de Excepción contemplados en la constitución y declarados conforme a Ley:

> La sociedad concesionaria otorgará prioridad a la transmisión de voz y data para los medios de comunicación del Sistema de defensa nacional y Sistema de defensa Civil. En casos de guerra exterior, el consejo de Seguridad y Defensa Nacional a través del Comando Conjunto de las Fuerzas Armadas podrá asumir el control directo de los servicios de telecomunicaciones, así como dictar disposiciones de tipo operativo. Para atender dichos requerimientos la Sociedad Concesionaria podrá suspender o restringir parte de los Servicios Registrados, en coordinación previa con el Ministerio de Transportes y Comunicaciones y los referidos sistemas de Defensa Nacional y Civil. (PERÚ, 2020).

Las empresas operadoras se encuentran obligadas en el periodo de Emergencia Declarada a cumplir con el otorgamiento de prioridad a la transmisión de voz y de data a los medios de comunicación que esté definida por el Sistema de Defensa Nacional y Sistema de Defensa Civil.

4.2 SITUACIÓN DURANTE LA SITUACIÓN DE EMERGENCIA NACIONAL

Al amparo de la resolución N°044-2020-CD/ OSIPTEL se aplicaron una serie de medidas en la línea de las disposiciones emitidas por el Poder Ejecutivo mediante el Decreto Supremo. (PERÚ, 2020c).

Las medidas dictadas por OSIPTEL no consideraron la importancia estratégica de los servicios de telefonía e internet en condiciones de convertirse en el único medio de conectividad masiva de la población; toda vez que las medidas no estuvieron en la dirección de fortalecer las debilidades existentes

antes de la emergencia; sino orientar a las disposiciones sanitarias del personal de las empresas de Internet.

Las medidas dispuestas carecieron de medidas de carácter operativo para la explotación de las redes por parte de los operadores; ya que el incremento del tráfico durante el periodo de cuarentena se incrementó como el propio OSIPTEL el primero de abril, indicando que el tráfico se incrementó hasta cerca de 42 por ciento en las redes fijas de y hasta 20 por ciento en las redes móviles, luego de 17 días de la declaración de Estado de Emergencia Nacional (PERÚ, 2020c)

De igual modo el consumo de la Televisión abierta y TV Cable se ha incrementado considerablemente. El diario Gestión dio cuenta que durante el primer día de cuarentena la audiencia televisiva se incrementó 49 por ciento, entre las 6 y 24 horas. OSIPTEL también emitió la Resolución N°0035-2020-PD/OSIPTEL; disponiendo medidas para que las empresas operadoras cumplan durante el Estado de Emergencia:

> - No podrán suspender o dar de baja el servicio público de telecomunicaciones por falta de pago.
> - Suspender la atención presencial en oficinas o centros de atención a usuarios y puntos de venta a nivel nacional.
> - Los problemas de calidad e interrupción que registren los servicios públicos de telecomunicaciones serían atendidos únicamente a través de los canales de atención telefónica o canales virtuales. Asimismo, podrá disponerse el desplazamiento del personal en los casos en los que, debido a la naturaleza del problema, se requiera acercarse al domicilio del usuario.
> - Los operadores realizarán la gestión de tráfico que sea necesaria para priorizar el funcionamiento de las aplicaciones orientadas a teletrabajo o trabajo remoto, teleeducación y telesalud, durante el horario de 08:00 a 18:00 horas de lunes a viernes, tal como se dispone en el Reglamento de Neutralidad de Red para el caso de situaciones de emergencia. (PERÚ, 2020d).

Asimismo, el 31 de marzo se emitió una segunda norma, la Resolución Nº 00045-2020-CD/OSIPTEL (PERÚ, 2020c), que dispuso medidas temporales adicionales para la prestación de servicios públicos de telecomunicaciones durante el aislamiento social, las cuales se detallan en la siguiente figura 6:

Figura 6: Atención De Principales Solicitudes De Servicios Públicos De Telecomunicaciones Durante El Aislamiento Social

TIPO DE ABONADO: PERSONA NATURAL O JURÍDICA QUE NO DESARROLLA SERVICIOS PÚBLICOS O ACTIVIDADES ESENCIALES			
TRÁMITE	**SERVICIO**	**CANAL DE ATENCIÓN**	**DESPLAZAMIENTO A LA CASA DEL ABONADO**
ALTA	Ninguno	No procede	No procede
MIGRACIÓN	Todos	Telefónico	Permitido, solo para el caso de cambio de equipo con autoinstalación para el servicio de acceso a Internet fijo.
SUSPENSIÓN	Todos	Telefónico	No procede
BAJA	Todos	Telefónico	No procede
REPORTE POR SUSTRACCIÓN O PÉRDIDA DE EQUIPO.	Servicio móvil	Telefónico	No procede
REPOSICIÓN DE SIM CARD	No procede	No procede	No procede
COMPRA DE PAQUETES Y RECARGAS	Todos	Telefónico y virtual	No procede
TIPO DE ABONADO: ENTIDAD PÚBLICA O PRIVADA QUE DESARROLLA TELEDUCACIÓN, TELESALUD Y TELETRABAJO DE SERVICIOS PÚBLICOS O ACTIVIDADES ESENCIALES			
TRÁMITE	**SERVICIO**	**CANAL DE ATENCIÓN**	**DESPLAZAMIENTO A OFICINAS DEL ABONADO**
ALTA	Acceso a Internet fijo, servicio de telefonía fija para call center y prestaciones relacionadas.	Telefónico y virtual.	Permitido
MIGRACIÓN	Todos	Telefónico	Permitido
SUSPENSIÓN	Todos	Telefónico	No procede
BAJA	Todos	Telefónico	No procede
REPORTE POR SUSTRACCIÓN O PÉRDIDA DE EQUIPO.	Servicio Móvil	Telefónico	No procede
REPOSICIÓN DE SIM CARD	No procede	No procede	No procede
COMPRA DE PAQUETES Y RECARGAS	Todos	Telefónico y virtual	No procede

Fuente: PERÚ, 2020c.

Tal como se aprecia de las medidas dictadas por el OSIPTEL; las Altas, y la reposición de SIM CARD no proceden; es decir aquellos pobladores sin servicio; aún con cualquier esfuerzo de adquisición estuvieron imposibilitados de incorporarse a la conectividad digital, manteniendo su aislamiento total en plena emergencia.

Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) OSIPTEL o el Ministerio de Transportes y Comunicaciones en el ámbito de sus competencias para atender sectorialmente las emergencias y estados de Excepción; deberían dictar medidas para que se mejore los índices de calidad del servicio y velocidad en las redes de acceso móvil del país ya que solo en el orden del 26% de usuarios tienen facilidades 4G.

Desde el punto de vista de Brecha Digital no se pudo incentivar la ampliación de nuevos accesos ya que OSIPTEL mantuvo las disposiciones del Decreto Legislativo 1338 (PERÚ, 2017) que señala que las gestiones de altas o activaciones del SIM CARD deben realizar de manera presencial, inclusive para las contrataciones de los servicios móviles las operadoras de telecomunicaciones deben efectuar la verificación biométrica de la huella dactilar. Mientras dure la declaratoria de emergencia y la posible mantención de la distancia social OSIPTEL debería de emitir disposiciones transitorias de excepción para promover el acceso a los incomunicados.

Por otro lado, el Ministerio de Educación mediante Resolución Ministerial N° 160-2020-MINEDU disponen el inicio del año escolar a través de la implementación de la estrategia denominada "Aprendo en casa", a partir del 6 de abril de 2020; mediante su prestación a distancia en las instituciones educativas públicas de Educación Básica, a nivel nacional, en el marco de la emergencia sanitaria para la prevención y control del COVID-19. (PERÚ, 2020e p.10).

Posteriormente el 18 de abril se emite el Decreto Legislativo N° 1465 (PERÚ, 2020f), mediante el cual se establece medidas para garantizar la continuidad del servicio educativo en el marco de las acciones preventivas del gobierno ante riesgo propagación del Covid-19. Y se asigna los presupuestos para garantizar la continuidad del servicio educativo.

Luego, el 4 de mayo el Ministerio de Educación emitió la Resolución Ministerial N° 184-2020-MINEDU (PERÚ, 2020g) que Disponen que el inicio de la prestación presencial del servicio educativo a nivel nacional en las instituciones educativas públicas y de gestión privada de Educación Básica, se encuentra suspendido mientras esté vigente el estado de emergencia nacional y la emergencia sanitaria para la prevención y control del COVID-19.

Como se puede concluir de las disposiciones emitidas la prestación del servicio educativo a nivel nacional por las instituciones públicas y privadas tendrán que realizarse mediante la modalidad no presencial utilizando herramientas de teleeducación y educación virtual.

Si bien, es cierto la opción no presencial es una opción educativa novedosa para la mayoría de los peruanos y necesaria para su introducción en el país, ella trae consigo también el reconocimiento del impacto de la tecnología TIC en dicha brecha ya que solo un porcentaje del sistema educativo tendrá el acceso.

Independiente de la evaluación de los contenidos educativos el acceso a la educación virtual se encuentra sujeto a dos instrumentos tecnológicos, el servicio de televisión y el servicio de internet, y como ya lo hemos manifestado anteriormente en nuestro país existen no solo brecha, sino también problemas de calidad de velocidad y barreras de asequibilidad. Se puede identificar algunos aspectos de esta problemática:

> - Un gran porcentaje de padres de familia poseedoras de los servicios de telefonía móvil e internet de banda angosta; no se encuentran en posibilidades adquisitivas adquirir equipos y servicios de banda ancha. Entre ellos acceder a los aplicativos de internet, herramientas que el personal docente ha generalizado en su relación con los estudiantes, mediante el aplicativo; esta barrera dificulta la conectividad docente-alumno
> - Como se indicó anteriormente el 70 de la población que accede a los servicios de telefonía móvil e internet móvil se encuentran en la modalidad contractual pre-pago, encontrándose entre ellos un gran porcentaje de padres de familia que atien-

den la educación de sus hijos; en esta modalidad de acceso a los servicios no se encuentran garantizado plenamente la continuidad del servicio por las interrupciones en la recarga afectando la conectividad docente-alumno.

- OSIPTEL en su informe del desarrollo de los servicios de telecomunicaciones durante los meses de marzo y abril manifestó un crecimiento considerable del tráfico de algunas aplicaciones como Netflix (98%), WhatsApp (52%) y TikTok (49%).
- De igual manera, el consumo de los servicios en redes fijas fue en el orden del 40% por ciento en las redes fijas, esto debido al incremento de las aplicaciones, Netflix (102%) y Tiktok (95%), hecho que respondería al alto uso de dispositivos móviles conectados mediante Wi-Fi.
- La inaplicación del Reglamento General de Calidad de los Servicios Públicos de Telecomunicaciones por situaciones producidas durante el estado de emergencia, las cuales, además, no darán lugar a la aplicación de sanciones. (INVERSIONES..., 2021).

5 SITUACIÓN DESPUÉS DE LA EMERGENCIA NACIONAL

La pandemia del COVID-19 plantea un desafío al sistema socio-económico mundial. A partir de la aplicación de las primeras medidas sanitarias, sumadas al temor por el contagio, comenzaron a acumularse las evidencias anecdóticas que daban cuenta de la importancia de las tecnologías digitales para contrarrestar el aislamiento, difundir medidas profilácticas, y facilitar el funcionamiento de sistemas económicos. La previsión del impacto económico en los países y las medidas que se deberán priorizar como estrategia de restablecimiento es preocupación de los organismos internacionales.

La Comisión Económica para América Latina (CEPAL) en su informe *América Latina y el Caribe ante la pandemia del COVID-19: Efectos económicos y sociales*, publicado el 03 de abril efectúa un análisis económico-social de la región indicando que América Latina y el Caribe enfrenta la pandemia desde una posición más débil que la del resto del mundo (NACIONES UNIDAS, 2020). Antes de la pandemia, la CEPAL preveía que la región crecería un máximo del 1,3% en 2020. Sin embargo, los efectos de la crisis han llevado a cambiar esa previsión y pronosticar una caída del PIB de al menos un 1,8%. Sin embargo, no es de descartar que el desarrollo que la pandemia lleve a previsiones de contracciones de entre un 3% y un 4%, o incluso más (NACIONES UNIDAS, 2020). El impacto económico final dependerá de las medidas que se tomen a nivel nacional, regional y mundial.

Los sectores más afectados por las medidas de distanciamiento social y cuarentena son los de servicios, que, en gran medida, dependen de contactos

interpersonales. En la región, los sectores que podrían sufrir las mayores contracciones son comercio, transporte, servicios empresariales y servicios sociales las cuales proveen el 64% del empleo formal. Además, el 53% del empleo de la región se da en actividades informales, que serán significativamente afectadas por basarse principalmente en contactos interpersonales (NACIONES UNIDAS, 2020).

Con respecto al uso y acceso del Internet, CEPAL indica en su informe:

> Las medidas para detener la propagación de coronavirus han acelerado el ritmo al que el trabajo y la educación pasan al ámbito digital. Las tecnologías digitales han disminuido el impacto de la pandemia en algunas profesiones y en la educación, al tiempo que han permitido sostener comunicaciones personales y actividades de entretenimiento en los hogares. Aunque más del 67% de los habitantes de la región usaron internet en 2019 y la penetración de la banda ancha ha aumentado marcadamente, el aumento del uso de las tecnologías digitales puede exacerbar las desigualdades. (NACIONES UNIDAS, 2020, p.8).

Otro organismo internacional que se encuentra involucrado del seguimiento del impacto de la pandemia del COVID-19 es la CAF (Corporación Andina de Fomento) que publico el estudio *El estado de la digitalización de América Latina la frente a pandemia del COVID-19*, en abril de 2020. En la presentación del estudio, el reconocido profesor investigador autor del estudio Raúl Katz e outros indicarón aspectos resaltantes:

- Las redes troncales y de distribución de banda ancha fija tienen la capacidad de adaptarse a los picos sistemáticos de tráfico", aunque "es importante considerar la asignación de espectro adicional" y apuntó a que "la brecha de adopción indica que una porción de la población no puede beneficiarse de Internet para mitigar la cuarentena";
- Región necesita un "plan de resiliencia digital";
- Todos los actores que participan en una cadena de aprovisionamiento deben presentar un grado avanzado de digitalización;
- Acelerar el despliegue de mayor cantidad de radio bases para banda ancha móvil, asignar a operadores móviles espectro adicional de manera temporaria;
- Aumentar la porción de espectro no licenciado en las bandas superiores de 5 ghz y 6 ghz para resolver los cuellos de botella en los enrutadores Wi-Fi;
- Promover innovación en el desarrollo de plataformas que permitan superar las falencias en las cadenas de aprovisionamiento;

- Estimular al sector productivo para que innove;
- Enfatizar la capacitación de los sectores sociales más vulnerables. (KATZ *et al,* 2020).

Como antecedentes al impacto del COVID 19, la CAF efectúo estudios para evaluar el impacto en la producción debido a los cambios en los procesos que se tuvo que adoptar como consecuencia del incremento del teletrabajo en tiempos de confinamiento como consecuencia de la epidemia SARs-CoV expandida en China en el año 2013.

Los resultados de la estimación sugieren que aquellos países con mayor dotación de infraestructura de banda ancha fueron capaces de contrarrestar, al menos parcialmente, los efectos de la pandemia. En un estudio realizado en abril del 2020 en plena pandemia del COVID-19 ratifica la estimación del año 2003; determinando la importancia de la digitalización como factor mitigante de la disrupción de la pandemia.

En la evaluación que realiza de la situación de los países de América Latina para enfrentar el COVID-19 llega a las siguientes conclusiones:

- Como ya está ocurriendo a escala mundial, las redes latinoamericanas están siendo afectadas por el aumento exponencial del tráfico. En particular, durante el mes de marzo se identifica una disminución de velocidad de banda ancha fija en Chile (-3%) y Ecuador (-19,6%), combinado esto con un incremento de la latencia de la misma tecnología en Brasil (11,7%), Chile (19,0%), Ecuador (11,8%) y México (7,4%) (fuente: Ookla/Speedtest). Considerando, de acuerdo con los modelos de Telecom Advisory Services, que la velocidad de banda ancha fija tiene un impacto en el PIB de 0,73% cuando la velocidad se incrementa en 100%, si la disminución de la velocidad registrada en marzo se perpetúa, el impacto económico negativo podría llegar a ser significativo.
- La migración masiva al teletrabajo está saturando la capacidad de enrutadores Wi-Fi en el hogar, motivado esto por un aumento de trabajo en la nube (incremento del 80% del tráfico de subida de datos) y el uso de videoconferencia. Este factor también contribuye a la disminución de velocidad de las redes.
- La digitalización de los hogares latinoamericanos indica una creciente conectividad y uso de Internet, proyectada en el 2020 al 78,78%, pese a que en algunos países la penetración es mucho menor (Bolivia: 58,34%, El Salvador: 45,02%; Honduras: 39,33%); adicionalmente, la dicotomía rural/urbana indica un nivel importante de marginalización digital. Esto indica que la brecha digital representa un obstáculo para sectores importan-

tes de la población que dependerían del acceso a Internet para recibir información sanitaria, descargar contenidos educativos para atender la educación virtual, o adquirir bienes de manera electrónica.

- Adicionalmente, la brecha digital se agrava dado que el uso de Internet en gran parte de los hogares latinoamericanos que han adoptado Internet se limita a herramientas de comunicación y redes sociales.
- La resiliencia del aparato productivo también indica falencias no en términos de adopción tecnológica sino en la asimilación de tecnología en procesos productivos, en particular en las cadenas de aprovisionamiento. Si bien el porcentaje de empresas con acceso a Internet excede en todos los países el 85%, el porcentaje de las mismas que usan banca electrónica varía en un rango de entre 34,20% en Perú y 95,39% en Colombia, mientras que el porcentaje de aquellas que adquieren insumos mediante Internet oscila entre 15,20% en Perú y 66,00% en Brasil. Las falencias en la cadena de aprovisionamiento se agravan cuando se analiza las debilidades de diferentes actores de la cadena logística (por ejemplo, baja digitalización del transporte terrestre, falta de estándares comunes para la comunicación entre las organizaciones). Esto resulta en una debilidad importante para afrontar las disrupciones en la cadena de aprovisionamiento ocasionadas por la pandemia.
- La resiliencia en el aparato del Estado frente a la pandemia está basada en su capacidad para seguir funcionando en términos de procesos administrativos, así como para continuar entregando servicios públicos. El cálculo de un índice compuesto de resiliencia del aparato del Estado indica que, debido al trabajo de años en el desarrollo de gobierno electrónico, ciertas naciones de la región parecen estar mejor posicionados para afrontar la disrupción: en particular, Chile, Uruguay, México, Brasil y Argentina.

En resumen, reconociendo que la digitalización puede jugar un papel fundamental en mitigar los efectos de la pandemia, es importante que los gobiernos, el sector privado, y la sociedad civil latinoamericana conformen un acuerdo de colaboración y trabajo conjunto que permita en el muy corto plazo identificar aquellas áreas de trabajo para mejorar el desempeño de ciertos componentes del ecosistema digital. Entre algunas de las iniciativas a tomar, se recomienda:

- Acelerar el despliegue de mayor cantidad de EEBB para banda ancha móvil, eliminando cualquier requerimiento de permisos para el despliegue de antenas.
- Asignar a operadores móviles espectro adicional de manera temporaria.

- Requerir a los proveedores de servicios de video streaming la reducción en el volumen de tráfico que estos generan a partir de la disminución de estándares en la definición técnica de contenidos.
- Examinar la necesidad de aumentar la porción de espectro no licenciado en las bandas superiores de 5 GHz y 6 GHz para resolver los cuellos de botella en los enrutadores Wi-Fi.
- Promover innovación en el desarrollo de plataformas que permitan superar las falencias en las cadenas de aprovisionamiento. Por ejemplo, estimular el desarrollo empresas tecnológicas para que provean una relación más eficiente entre proveedores logísticos y servicios de transporte.
- Estimular al sector productivo para que innove alrededor en la restructuración de procesos para permitir incrementar el porcentaje de la población que pueda trabajar remotamente.
- Enfatizar la capacitación de los sectores sociales más vulnerables para poder enfrentar la desocupación. (USO DE WHATSAPP…, 2020).

El estudio de la CAF *El estado de la Digitalización d América latina frente a la pandemia del COVID-19*, desarrolla una evaluación de la capacidad de los países de América Latina para superar el impacto de la pandemia del COVID-19 en todos los aspectos de la vida socioeconómica de la población, para tal efecto utiliza líneas de actuación del impacto de la digitalización; entre ellos los aspectos socioeconómicos, infraestructura digital, uso del servicio den los hogares, impacto en la producción y en el gobierno, identificando la capacidad de los países para volver a la normalidad. En el estudio el profesor Raúl Katz y otros utilizan el termino resiliencia para evaluar la capacidad de los países; entendiéndose el termino resiliencia; como la capacidad de un sistema para recuperar su estado inicial cuando haya cesado la perturbación a la que ha estado sometido como es el caso del COVID-19 (KATZ *et al*, 2020).

6 IMPACTO DE LA DIGITALIZACIÓN

6.1 IMPACTO DE LA DIGITALIZACIÓN EN LA CAPACIDAD (RESILIENCIA) SOCIOECONÓMICA

Los organismos internacionales que se encuentran monitoreando la economía mundial le han otorgado un rol estratégico a la innovación digital y a las Tecnologías de la Información y Comunicaciones (TIC) por su impacto en los indicadores de la economía mundial, ya que estudios a nivel internacional evidencian una correlación altamente positiva, entre la banda ancha móvil y el PBI per cápita .El incremento del 10% de la banda ancha móvil induce un incremento del 1.38% del PBI nacional per cápita.

El Banco Mundial en una publicación de 2019 (WORLD BANK, 2019) resalto la magnitud del impacto de la economía digital en el mundo indicando que la innovación digital está en vías de transformar casi todos los sectores de la economía introduciendo nuevos modelos comerciales, productos, servicios y, en última instancia, nuevas formas de crear valor y empleos. Los resultados de esta transición ya son evidentes: la economía digital mundial en 2016 representaba un valor de USD 11,5 billones, o sea 15,5 % del producto interno bruto (PIB) mundial. Se espera que esta cifra llegue a 25 % en menos de una década.

De igual modo resalta en dicha publicación el drama de la brecha digital indicando que no todos se han beneficiado de la misma manera: aunque la revolución digital es un fenómeno mundial, todavía existen enormes desigualdades entre los países y dentro de ellos en lo que respecta a penetración, asequibilidad y desempeño de los servicios digitales. Si bien casi la mitad de la población mundial tenía acceso a internet en 2016, la tasa de penetración en los países menos adelantados (PMA) era solo del 15 %, o sea 1 de cada 7 personas; asimismo resalta el costo prohibitivo del acceso a internet de banda ancha móvil o fija en los países menos adelantados (PMA) donde la falta de infraestructura digital y los obstáculos regulatorios entorpecen el desarrollo de la banda ancha. El Banco Mundial indica con información a diciembre del 2015, que el costo de los servicios móviles de banda ancha era de alrededor del 17 % del ingreso nacional bruto (INB) medio mensual per cápita en los países menos adelantados (PMA), en comparación con tan solo el 5% a nivel mundial.

Concordando con estas referencias el estudio publicado por la CAF en abril de 2020, identifica a la velocidad de Internet de banda ancha como un variable con efectos en el PBI. Para efectos de utilizar las evaluaciones del estudio de la CAF no se tomará en cuenta el factor de brecha digital, y centraremos la evaluación en las poblaciones con servicio afectado por la pandemia COVID-19.

Estudios realizados anteriormente muestran evidencia empírica del impacto que la velocidad de banda ancha en el desarrollo económico. A este fenómeno lo han denominado “retorno de la velocidad” cuantificando cual es el impacto en el producto bruto y la productividad. Estudios realizados anteriormente del impacto de la velocidad de banda ancha en 159 países del mundo por el profesor Raúl Katz otros autores (2020), con información del 2008 al 2019 determinan que en países impacto variable en el PBI.

La disminución de la velocidad de descarga como resultado de la pandemia del COVID-19 registrado en marzo y abril en el Perú debe ser considerado para su evaluación para los siguientes meses ya que si ésta se perpetua, el impacto económico negativo podría materializarse.

6.2 CAPACIDAD (RESILIENCIA) DE LA INFRAESTRUCTURA DIGITAL

Las medidas sanitarias dispuestas por los gobiernos en todos los países de América Latina entre ellas el Perú para enfrentar el COVID-19 entre ellas la

inmovilización laboral y la cuarentena domiciliaria ha ocasionado un incremento rápido en el uso por parte de la población de redes y servicios de telecomunicaciones para resolver temas de aprovisionamiento de bienes, conectividad social, y acceso a información. Ya existe numerosa evidencia del aumento en la utilización de las redes de telecomunicaciones a partir del desencadenamiento de la pandemia, y como consecuencia una erosión natural de los índices de calidad.

Otros de los aspectos que se toma en cuenta en el estudio del CAF es el impacto negativo en la calidad de la prestación de los servicios, del incremento del tráfico como consecuencia de la nueva actitud de la población en su uso escenario no previsto en magnitud en el diseño de las redes principalmente de acceso en el caso la infraestructura móvil. Por consiguiente, las medidas de corrección y/o reformulación de la ingeniería de tráfico implicará incremento de infraestructura en el despliegue adicional que permitirá acomodar el pico en el tráfico, En condiciones de despliegue normal requieren un lapso relativamente prolongado, por lo que será necesario priorizar y optimizar tiempos para atender este escenario. El estudio de la CAF recomienda tres iniciativas, que pueden ser tomadas en cuenta con impacto relativamente corto.

Primero, despliegue de mayor cantidad de Estaciones Bases (EEBB) para banda ancha móvil. Este esfuerzo es una iniciativa que todo operador toma en cuenta normalmente para enfrentar saltos circunstanciales en tráfico. Para acelerar el proceso es necesario emitir disposiciones excepcionales para acelerar la emisión permisos para el despliegue de antenas. Actualmente esta gestión se constituye como barrera en algunos países de América Latina entre ellos el Perú constituido actualmente en algunos países como barrera

Segunda iniciativa es asignar a operadores móviles espectro adicional de manera temporaria. Esto es lo que ha hecho la FCC, el regulador estadounidense, otorgando a operadores móviles el uso temporario de ciertas bandas de espectro en regiones predeterminadas.

La tercera es requerir a los proveedores de servicios de video *streaming* la reducción en el volumen de tráfico que estos generan. Como ya ha sido documentado, video *streaming* consume una parte importante del tráfico de las redes. Ciertos operadores ya han respondido en muchos casos: Google anunció la reducción en la calidad de definición de YouTube, Disney demoró el lanzamiento de su servicio de *streaming* Disney+ en Francia, Microsoft limitó el ritmo de actualización de sus plataformas de juegos en Xbox.

Otro aspecto resaltante a considerar como producto de las medidas de inmovilización social y cuarentena ha sido el aumento dramático del teletrabajo. Más allá del impacto en las redes de telecomunicaciones, el teletrabajo ha generado impactos en aplicaciones de videoconferencia (para facilitar la comunicación laboral) y el tráfico de datos dentro del hogar con base a la tecnología de Wi-Fi. El aumento natural en el número de dispositivos conectados en el hogar utilizando plataformas de videoconferencia y trabajo en la nube ha creado un cuello de

botella en los enrutadores Wi-Fi que operan sobre espectro no-licenciado. De acuerdo con las estadísticas de medición de tráfico, esta tecnología está sometida a picos relacionados con el teletrabajo. En el caso del Perú se deberá de examinar el comportamiento de las bandas no licenciadas donde trabaja los enrutadores Wi Fi.

En conclusión, la infraestructura digital es un componente fundamental en el mantenimiento de la resiliencia económica. La capacidad de las redes para acomodar las necesidades de comunicación resultantes de COVID-19 solamente puede ser garantizada mediante la acción conjunta de operadores, reguladores, y plataformas de Internet.

6.3 CAPACIDAD DE CONSUMO (RESILIENCIA) DE LOS HOGARES DIGITALES

Las medidas dispuestas para afrontar la pandemia del COVID-19 están orientadas principalmente a la persona, por lo que la penetración de Internet en hogares es la palanca fundamental para hacerle frente y contribuir a la eficiencia y eficacia de las medidas sanitarias. La digitalización de hogares permite a la población continuar realizando una cantidad de tareas cotidianas que anteriormente requerían el contacto físico. De acuerdo con las últimas estadísticas disponibles, la penetración de Internet en América Latina es 68,66%. Este valor revela de por si el primer obstáculo para afrontar el COVID-19 mediante el uso de tecnologías digitales. La marginalización de 32% de la población en el uso de Internet excluye una porción importante de los habitantes de la posibilidad de acceder a servicios que pueden reemplazar algunas actividades que requieren habitualmente el contacto físico. Esta marginalización varía por países.

El promedio ponderado para la región indica el progreso que ha realizado América Latina en los últimos años en términos de adopción de Internet. Conviene recordar, sin embargo, que los promedios nacionales esconden diferencias significativas al interior de cada país, como es el caso del Perú.

Otro aspecto para considerar además de la penetración de internet es el número de dispositivos de acceso en el hogar. Si bien la tenencia de computadoras en América Latina alcanza 44,89%, en gran parte de los hogares esto no sería suficiente para acomodar el acceso simultáneo de varios miembros de la familia, como es el caso de educación a distancia y el teletrabajo (KATZ *et al,* 2020).

Si bien la adopción de Internet a nivel agregado muestra un grado importante de avance, el análisis de su utilización revela un comportamiento de uso que reduce la contribución de la misma a la resiliencia del hogar digital para enfrentar la pandemia. En términos generales, la banda ancha es usada como medio de comunicación y de vinculación social.

Más allá de la comunicación resultante del uso de redes sociales mediante WhatsApp, o Facebook Messenger, es necesario medir la capacidad para adoptar

servicios que permitan "virtualizar" actividades físicas. Para medir la capacidad de hogares digitales para encarar actividades por medio de Internet, es estudio de la CAF creado un "índice de resiliencia digital del hogar" que combina cuatro indicadores.

6.4 CAPACIDAD (RESILIENCIA) DE LA CADENA DE PRODUCCIÓN

La digitalización de la producción representa el factor fundamental para mantener la economía operando a pesar de las disrupciones que implican el COVID-19, ya sea durante y post emergencia. Durante el periodo de emergencia se requiere incrementar volumen y velocidad de producción de bienes y servicios requeridos para la emergencia sanitaria, aislamiento y cuarentena. Post emergencia se requiere procesos eficientes y eficaces de producción para el restablecimiento de la normalidad. Para analizar el grado de capacidad productiva o "resiliencia productiva", se considera dos dimensiones.

La digitalización de procesos productivos, evaluando hasta qué punto el sistema productivo puede seguir operando bajo las condiciones actuales de pandemia, considerando especialmente a las cadenas de aprovisionamiento, el procesamiento y los canales de distribución. En el estudio de la CAF se evalúa la cadena de aprovisionamiento de las empresas de los países de América latina, del cuadro siguiente se puede observar que Perú tiene el indicador de solo el 34% de empresas usan banca electrónica, siendo este indicador el más bajo de la muestra de 8 países de América latina. De igual modo Perú es el país con uno de los más bajos índices porcentuales de empresas que usan internet para la adquisición de insumos, solo el 15% lo hace (CENTRO DE ALTOS ESTUDIOS NACIONALES, 2020).

6.5 CAPACIDAD (RESILIENCIA) DEL ESTADO

La resiliencia en el aparato del Estado frente a la pandemia está basada en su capacidad para seguir funcionando en términos de procesos administrativos, así como para continuar entregando servicios públicos. Como es obvio, en esta última categoría, existen servicios no prescindibles cuya continuidad está menos condicionada por el nivel de digitalización (por ejemplo, la seguridad y la salud pública). Por otra parte, la digitalización de otros servicios puede aumentar su capacidad de afrontar el COVID-19. La digitalización de las acciones de gobierno son una herramienta de eficacia y eficiencia la prestación de los servicios públicos que le corresponden al estado en todos los niveles local, regional y nacional. En el caso del Perú se han realizado avances en esa dirección, pero requiere necesariamente una transformación digital en todos los procesos burocráticos del estado que permitan gestionar el estado con indicadores digitales.

Por último, en la publicación del Banco Mundial *La COVID-19 (coronavirus) refuerza la necesidad de conectividad,* de 29 de abril del 2020 indica lo siguiente: "En este momento debemos trabajar todos juntos para lograr cumplir la promesa de que las nuevas tecnologías lleguen a todos y para mantener al mundo conectado, incluso en épocas de distanciamiento social" (DIOP, 2020). Posteriormente recomienda acciones que se necesitará para lograr una banda ancha universal, accesible y de buena calidad en esta etapa de pandemia. (WORLD BANK, 2020).

En primer lugar, y a corto plazo, urge aumentar el ancho de banda, controlar el congestionamiento y evitar que Internet colapse, y conectar a quienes aún no cuenten con conexión. Para ello, debe modificarse la configuración de la red, la gestión del tráfico y el acceso a la capacidad ociosa en la infraestructura a fin de brindar conectividad a instituciones, hogares y pequeñas y medianas empresas. Los servicios públicos tienen activos valiosos, como ductos y postes, edificios, derechos de propiedad sobre tierras e incluso redes de fibra que podrían aprovecharse para instalar de manera económica nueva infraestructura de banda ancha. En el caso de los operadores de telecomunicaciones, pueden compartir infraestructura para ampliar la cobertura y reducir los costos de instalación de redes.

En segundo lugar, debemos impulsar la transformación digital en algunos de los países más pobres del mundo aumentando masivamente los recursos destinados a establecer los cimientos de una economía digital próspera. Dolorosamente, esta crisis pone de manifiesto que los beneficios y las oportunidades que genera la tecnología no están distribuidos de manera equitativa. En la economía informal, no existe el teletrabajo. En los países pobres, incluso la mayoría de las empresas más establecidas, carecen de la capacidad de pasar a trabajar en línea. Docentes, estudiantes y funcionarios gubernamentales necesitan tener conectividad, pero también habilidades para poder utilizar las herramientas digitales de forma efectiva. Las economías dependen cada vez más de las finanzas digitales (*fintech*) para mantenerse a flote, y la demanda de servicios como pagos móviles, entregas de alimentos a domicilio y comercio electrónico experimentará un crecimiento exponencial.

En este momento debemos trabajar todos juntos para lograr cumplir la promesa de que las nuevas tecnologías lleguen a todos y para mantener al mundo conectado, incluso en épocas de distanciamiento social.

6.6 DIGITALIZACIÓN DE CANALES DE DISTRIBUCIÓN

Las barreras a la digitalización en la cadena de aprovisionamiento de la región se extienden a los canales de distribución en el cuadro siguiente se presenta una compilación de estadísticas sobre el porcentaje de empresas latinoamericanas que han desplegados canales de venta digitales o han desarrollado sitios.

7 CONCLUSIONES Y RECOMENDACIONES

7.1 PRINCIPALES CONCLUSIONES

Los principales desafíos que plantea conseguir un incremento del acceso y uso del Internet para reducir la brecha digital en el Perú están vinculados a cuestiones de inversión en infraestructura la misma que debe ser visualizada desde el escenario del Mercado con la oferta de servicios de TIC y de la demanda como capacidades, emprendimiento, contenido local y protección del consumidor y desde el Estado en su rol de buscar el bienestar de la población.

El grado de competencia en los mercados de comunicación de los servicios de telecomunicaciones y en especial de los servicios de internet de banda ancha del país tiende a ser intensa en poblaciones urbanas con alto PBI per cápita; mientras que la competencia se diluye o desaparece en poblaciones o regiones con niveles de pobreza por encima del 30% siendo necesario reforzar una regulación asimétrica para alcanzar los objetivos de inclusión digital en el país.

La concepción del servicio público para la prestación de los servicios de internet de banda ancha ha sido entendida como responsabilidad del mercado y no del Estado; por lo que se deduce que la existencia de la brecha digital del país es una consecuencia de las fallas del mercado y fallas del estado en asumir la responsabilidad del servicio público de internet de banda ancha del país. Está demostrado la relación directa entre penetración de banda ancha y PBI, así como velocidad de internet y PBI per cápita.

La evaluación del rol de los servicios de Telecomunicaciones en la situación de emergencia del coronavirus ha mostrado las deficiencias en la prestación del servicio y también la carencia del mismo por una parte importante del país producto de la brecha digital ya que solo el 73% de la población tienen acceso a internet y que solo. Por otro lado, en el orden del 50% de los CCPP están incomunicados en el país; a pesar del esfuerzo y el despliegue realizado durante los 25 años que lleva desarrollándose el mercado de las telecomunicaciones en el país. Esta debilidad en la importancia de las telecomunicaciones en el desarrollo y la defensa del país ha sido testificada en el Plan Nacional de Infraestructura para la competitividad aprobado mediante Decreto Supremo N°238-2019-EF, el 28 de Julio del 2019 (PERÚ, 2019); donde se indica que esta brecha de infraestructura de los servicios de telecomunicaciones, representa a corto plazo en el orden de S/.28 mil millones y a largo plazo en el orden de S/.106 mil millones.

A pesar de los esfuerzos aislados de algunos sectores como el de Transportes y Comunicaciones y la Secretaría de Gobierno Digital; no ha sido posible conceptualizar la prioridad estratégica de la conectividad digital en el país; siendo incipiente la prioridad e importancia de parte de las autoridades de los gobiernos locales, regionales y nacionales la ejecución de inversión en infraestructura para

la transformación digital de los procesos gubernamentales. Aún con medidas de gestión rutinaria como las autorizaciones para la instalación de antenas.

La brecha digital está completamente correlacionada con los niveles de pobreza del país y niveles de brecha educativa; evidenciándose el lento avance en promover en cerrar la brecha digital y la introducción de internet de banda ancha en escuelas, PYMES (pequeñas y medianas empresas) y gestión de gobierno. Esto se evidencia en barreras burocráticas para el despliegue de infraestructura de fibra óptica e instalación de antenas de telefonía móvil, cuando el país tiene un déficit de 17 mil 500 antenas para atender la demanda al 2021 según información de OSIPTEL. (INVERSIONES…, 2021)

Las estrategias de contingencia implementadas en el Perú para afrontar la agresión del coronavirus tuvo entre sus ejes acciones y medidas sanitarias, de seguridad, de otorgamiento de bonos, aprovisionamiento de bienes y servicios básicos y de tipo educativo; todas estas ejes soportados en el único medio de conectividad masiva de la población como son las TIC, utilizando masivamente los servicios de televisión e internet; estos servicios se han convertido en los instrumentos imprescindibles para la prestación al usuario de los servicios de teleducación, educación virtual, telemedicina, gobierno electrónico, comercio electrónico, banca electrónica, principalmente para interactuar en la implementación de las acciones de gobierno con la población; convirtiéndose éste medio en una necesidad de importancia estratégica de contingencia, para lo cual requiere garantía operativa, confiabilidad de alta calidad en las redes de transporte y de acceso y de urgencia se dicte las medidas regulatorias de contingencia para garantizar la continuidad del servicio de buena calidad.

A pesar del esfuerzo del Ministerio de educación para implementar los de teleeducación y educación y virtual utilizando el soporte de la televisión e internet con sus aplicaciones, en el periodo de emergencia nacional y previsible para la etapa post emergencia, no se asegura el logro del objetivo educativo aun solo en los pobladores que poseen el acceso, sino se garantiza la continuidad de las redes de transporte y acceso principalmente del internet móvil y sus aplicaciones que soportan estos servicios a nivel nacional, teniendo en cuenta inclusive la incomunicación de gran parte de la población que no se encuentra en acceso a estos servicios producto de la brecha digital.

Adicional al problema de la brecha digital del país, los indicadores que influyen en procesos de producción nacional, y procesos de gobierno son débiles comparados con otros países de la región. De las empresas del país solo el 34% utiliza banca electrónica, solo el 15% utiliza el internet en la adquisición de insumos, de igual modo solo el 1.8% de la población utiliza el comercio electrónico; estos indicadores evidencian las barreras para afrontar las estrategias de aislamiento, cuarentena y se convertirá en un obstáculo para el proceso de retorno a la normalidad en todos los aspectos de la vida nacional. (CENTRO DE ALTOS ESTUDIOS NACIONALES, 2020).

La participación del Ministerio de Transportes y Comunicaciones y FITEL (ahora PRONATEL); han testificado las barreras y eficiencia en gestionar proyectos como el de la Red Dorsal Nacional de fibra óptica, que a lo largo de más de 7 años no ha podido concretar el proyecto evidenciado deficiencias no solo conceptuales de mercado sino también en el planeamiento, asignación y ejecución de los proyectos que utilizaron los fondos FITEL. Es necesario una reformular las políticas de acceso universal asignando dichos proyectos a los operadores existentes en el mercado para ejecutar proyectos a una velocidad máxima de dos años, utilizando los recursos del Fondo FITEL y Canon.

La implementación y seguimiento a las medidas de salubridad dispuestas por el poder ejecutivo utilizando los medios electrónicos disponibles ha trastocado algunos derechos como el de la privacidad o el uso de datos personales. Por lo que se requiere precisiones y excepciones en la regulación correspondiente. En necesario considerar que la tecnología no es el enemigo, pero para lograr una mejor convivencia en este nuevo mundo digital conviene mantener el respeto a las libertades personales de todos los individuos.

7.2 PRINCIPALES RECOMENDACIONES

Es necesario que los responsables de políticas del más alto nivel del país consideren de urgente necesidad estratégica cerrar la brecha digital en el Perú por sus impactos en el desarrollo socio-económico del mismo, y más aún haberse convertido en la herramienta fundamental para afrontar los efectos del coronavirus durante y post la Emergencia Nacional. El estado es el responsable de la prestación del servicio público, mientras que el concesionario privado ejecuta la prestación del servicio de internet por encargo del Estado.

Las estrategias digitales deben tener una concepción nacional para que exista el despliegue de infraestructura de redes en base al impulso del mercado y complementado con acciones del estado en poblaciones donde exista debilidad del mercado o no exista mercado. Se recomienda la elaboración de un Plan Integral de corto plazo para cerrar la brecha digital del Perú asumiendo el Estado rol trascendente.

Establecer un marco normativo que incentive el despliegue de infraestructura de banda ancha donde exista debilidad del mercado. En este marco es de importancia y urgente la redefinición y restructuración de los ingresos provenientes de las tasas que pagan los concesionarios de los servicios de telecomunicaciones para orientarlos a la ejecución de cerrar la brecha digital del país.

La accesibilidad y la asequibilidad de la banda ancha a poblaciones rurales desfavorecidos producto de la brecha requiere de incentivos y reducción de barreras fiscales y burocráticas que impiden el despliegue de la banda ancha. De igual modo se hace necesario que el estado a través de sus diversas autoridades de gobierno,

financien o promuevan incentivos para el despliegue de redes cuando los mercados son débiles para atender la demanda o no exista mercado, pero exista población pobre. Ampliar el Plan de conectividad de internet de PRONATEL, para el 100% de Centros educativos, Centros de Salud, Centros Policiales, Cooperativas Agrarias y Desembarcaderos pesqueros.

Reformular las políticas y estrategia de acceso universal, que viene ejecutando FITEL, asignando los proyectos de despliegue para cerrar la brecha a los operadores existentes en el mercado para ejecutar dichos proyectos a una velocidad máxima de dos años. Utilizar los recursos del Fondo FITEL y Canon.

El Ministerio de Educación debe liderar, conjuntamente con la Asociación de Medios de Comunicación y los operadores de Telecomunicaciones. un plan de formación de habilidades digitales a corto plazo para la población en general y específicamente para la población estudiantil, las mismas que deberán de ser incorporadas en forma general en plan curricular nacional de Educación.

Promoverse un Plan de Transformación digital de los procesos de los gobiernos locales, regionales y nacional, incorporando a corto plazo procesos digitales para atender las necesidades de servicio público urgente post emergencia nacional, implementando infraestructura de internet e interoperabilidad con los centros nacionales de datos sectoriales.

El Ministerio de la Producción, Ministerio de Transportes y Comunicaciones, CONFIED y los organismos empresariales PYMES, conjuntamente deberán de elaborar un Plan de uso de la digitalización en los Procesos de Adquisiciones, banca electrónica y comercio electrónico en las empresas.

El Ministerio de Transportes y Comunicaciones y OSIPTEL deberán establecer lineamientos para mejorar la prestación de los servicios de internet móvil garantizando la velocidad y continuidad del servicio por el incremento de tráfico producto de la situación de emergencia del coronavirus, permitiendo que la conectividad digital garantice el proceso restablecimiento de la normalidad.

REFERENCIAS

AGÜERO, Joel Martín Visurraga. *Certificado Digital, Documento Nacional de Identidad Electrónico y Gobernabilidad Electrónica en Instituciones Públicas Peruanas*. Tesis (Doctor en Gestión Pública y Gobernabilidad). Facultad de Ciencias Empresariales, Universidade César Vallejo, 2016. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/4644/Visurraga_AJM.pdf?sequence=1&isAllowed=y Accedido en: 24 sept. 2021.

BANCO MUNDIAL EN VIVO. *Informe sobre el desarrollo mundial 2016: El dividendo digital,* 111min, 2016. Disponible en: https://envivo.bancomundial.org/informe-sobre-el-desarrollo-mundial-2016. Accedido en: 10 mar. 2021.

CALATAYUD, A; KATZ, R. R. *Cadena de Suministro 4.0:* Mejores prácticas intranacionales y Hoja de Ruta para América Latina. [S. l.]: Banco Interamericano de Desarrollo, 2019. Disponible en: https://books.google.es/books?hl=es&lr=lang_es&id=CuW3DwAAQBAJ&oi=fnd&pg=PA107&dq=Calatayud,+A.+y+Katz,+R.+(2019).+Cadena+de+Suministro+4.0:+Mejores+pr%C3%A1cticas+intranacionales+y+Hoja+de+Ruta+para+Am%C3%A9rica+Latina.+Banco+Interamericano+de+Desarrollo&ots=FOW5KgIKd8&sig=iGrn0ru9aXAcYvS18mSdmEb-kks#v=onepage&q&f=false .Accedido en: 4 nov. 2021.

CAREW, D.; MARTIN, N.; BLUMENTHAL, M.; ARMOUR, P.; LASTUNEN, J. *The potential economic value of unlicensed spectrum in the 5.9 GHz Frequency band: insights for allocation policy. [S. l.]* RAND Corporation, 2018.

CENTRO DE ALTOS ESTUDIOS NACIONALES (Perú). El COVID-19 como amenaza a la Seguridad Nacional: La conectividad digital, durante la emergencia y post emergencia nacional. *Cuadernos de Trabajo*, n. 4 Extraordinário, Lima, 2020. Disponível em: https://cdn.www.gob.pe/uploads/document/file/1224822/REVISTA_CAEN_2020_-_4.pdf. Accedido en: 24 sept. 2021.

DE BOGOTÁ, Cámara de Comercio, *et al*. *Observatorio de la economía digital de Colombia*. Bogotá: CIEB 2018.

DIOP, Makhtar. *La COVID-19 (coronavirus) refuerza la necesidad de conectividad*. Banco Mundial - Voces, 2020. Disponible en: https://blogs.worldbank.org/es/voices/la-covid-19-coronavirus-refuerza-la-necesidad-de-conectividad Accedido en: 10 mar. 2021.

EN EL 2020 POBLACIÓN peruana alcanza 32,6 millones de habitantes. *Instituto Nacional de Estatística e Informática (INEI)*, Lima [2020]. Disponible em: https://m.inei.gob.pe/prensa/noticias/en-el-2020-poblacion-peruana-alcanza-326-millones-de-habitantes-12302/#:~:text=En%20medio%20de%20los%20problemas,poblaci%C3%B3n%20supere%20los%2033%20millones. Accedido em: 20 mar. 2021.

GARCÍA GÓMEZ, Francisco Javier. *Brecha Digital, Brecha Social, Brecha Económica, Brecha Cultural:* La biblioteca pública ante las cuatro caras de una misma moneda. Ayuntamiento de San Javier Murcia- España: Universidad de Murcia-Biblioteca Pública Municipal, 2019.

INVERSIONES en el sector telecomunicaciones crecieron 14.6% en el 2021. *OSIPTEL*, Lima, 2022. Disponible en: https://www.osiptel.gob.pe/portal-del-usuario/noticias/inversiones-en-el-sector-telecomunicaciones-crecieron-14-6-en-el-2021/ Accedido en: 8 abr. 2022.

KATZ, Raúl *et al*. *Estado de la Digitalización de América Latina frente a la Pandemia del COVID 19.* Caracas, Observatorio CAF del Ecosistema Digital, 2020. Disponible en: https://scioteca.caf.com/bitstream/handle/123456789/1540/El_estado_de_la_digitalizacion_de_America_Latina_frente_a_la_pandemia_del_COVID-19.pdf Accedido en: 09 mayo 2021

NACIONES UNIDAS. América Latina y el Caribe ante la pandemia del COVID-19: efectos económicos y sociales. *Informe Especial N° 1*, Santiago, Comisión Económica para América Latina y el Caribe, 2020. Disponible en: https://repositorio.cepal.org/handle/11362/45337 Accedido en: 9 jun. 2021

NACIONES UNIDAS. La UIT publica las cifras más recientes sobre desarrollo de tecnologías a escala mundial. *Noticias*. Vitacura, Santiago de Chile, 9 jun. 2011. Disponible en: https://www.cepal.org/es/noticias/la-uit-publica-cifras-mas-recientes-desarrollo-tecnologias-escala-mundial. Accedido en: 5 jul. 2011.

NACIONES UNIDAS. *Horizontes 2030*: la igualdad en el centro del desarrollo sostenible. [S. l.] CEPAL, jul. 2016. Disponible en: https://www.cepal.org/es/publicaciones/40159-horizontes-2030-la-igualdad-centro-desarrollo-sostenible. Accedido en: 09 jun. 2021

PALMA, Rudy Eric. Brecha digital en Perú es una de las más altas de América Latina, según el Banco Mundial. Tecnología, *Revista Gana Más*. Santiago de surco Lima, Perú, 8 ene 2016. Disponible en: https://revistaganamas.com.pe/brecha-digital-en-peru-es-una-de-las-mas-altas-de-america-latina-segun-el-banco-mundial/. Accedido en: 15 feb. 2020

PERÚ. Constitución Política Del Perú (1993). Lima, 1993. Disponible en: https://cdn.www.gob.pe/uploads/document/file/198518/Constitucion_Politica_del_Peru_1993.pdf Accedido en: feb. 2021

PERÚ. *Decreto Supremo N° 020-2007-MTC*, Normas Legales, Lima, 2007. Disponible en: https://www.gob.pe/institucion/mtc/normas-legales/10005-020-2007-mtc. Accedido en: 9 jun. 2021

PERÚ. *Decreto Supremo N° 051-2010-MTC*. *¡Aprueba el "Marco Normativo General del Sistema! Modifica el Plan Técnico Fundamental de Numeración, aprobado por Resolución Suprema No. 022-2022-MTC. Lima: Presidencia del Perú, 2010. Disponible en:* https://cdn.www.gob.pe/uploads/document/file/19107/DS_051-2010-MTC.pdf Accedido en: 9 jun. 2021

PERÚ. Decreto Supremo N° 051-2020-PCM, Normas Legales, Lima, 2020a. Disponible en: https://www.gob.pe/institucion/pcm/normas-legales/462808-051-2020-pcm. Accedido en: 9 jun. 2021

PERÚ. Decreto Supremo N° 044-2020-PCM, Normas Legales, Lima, 2020. Disponible en: https://www.gob.pe/institucion/pcm/normas-legales/460472-044-2020-pcm. Accedido en: 9 jun. 2021

PERÚ. Decreto Supremo N° 064-2021-PCM, Normas Legales, Lima, 2021b. Disponible en: https://www.gob.pe/institucion/pcm/normas-legales/2670566-064-2021-pcm. Accedido en: 9 jun. 2021

PERÚ. Decreto Supremo nº 044 de 15 de marzo de 2020. Decreto Supremo que declara Estado de Emergencia Nacional por las graves circunstancias que afectan la vida de la Nación a consecuencia del brote del COVID-19. Normas Legales. *El Peruano*. Lima, 15 mar. 2020c. Disponible en: https://cdn.www.gob.pe/uploads/document/file/566448/DS044-PCM_1864948-2.pdf Accedido en: 15 dic. 2021.

PERÚ. Decreto Supremo N° 238-2019-EF de 28 de julio de 2019 Plan Nacional de Infraestructura para la Competitividad. Ministerio de Economía y Finanzas, Normas Legales. *El Peruano*. Lima, 2019.

Disponible en: https://cdn.www.gob.pe/uploads/document/file/348761/DS238_2019EF.pdf Accedido en: 21 sept. 2021.

PERÚ. Decreto legislativo nº 1338. Presidencia Del Perú. Normas Legales. *El Peruano*. Lima, 6 de enero de 2017. Disponible en: https://cdn.www.gob.pe/uploads/document/file/160612/1_0_3824.pdf
Accedido en: 28 oct. 2021.

PERÚ. Decreto legislativo que establece medidas para garantizar la continuidad del servicio educativo en el marco de las acciones preventivas del gobierno ante el riesgo de propagación del Covid-19. De 19 de abril de 2020.Normas Legales. *El Peruano.* Lima, 1 abr. 2020f. Disponible en: https://cdn.www.gob.pe/uploads/document/file/605862/DL_1465.pdf Accedido en: 15 sept. 2021.

PERÚ. Informe N° 0410-2019-MTC/26 de la Dirección General de Políticas y Regulación en Comunicaciones. *Ministerio de Transportes y Comunicaciones*., Lima, Ministerio de Transportes y Comunicaciones. 2019. Disponible en: https://portal.mtc.gob.pe/comunicaciones/regulacion_internacional/regulacion/proy%20normativos/2019/informe_N_0410-2019-MTC-26.pdf. Accedido en: 1 ene. 2021.

PERÚ, Plataforma *Digital única del Estado Peruano. Instituto Nacional de Estatística e Informática.* Censo 2017. Lima, 2018. Disponible en: http://censo2017.inei.gob.pe/resultados-definitivos-de-los-censos-nacionales-2017/ Accedido en: 18 ene. 2020.

PERÚ. Resolución e Presidencia Nº 00035-2020. Aprueban Norma que establece disposiciones para garantizar la Continuidad de los Servicios Públicos de Telecomunicaciones, en el Marco del D.S. Nº 044-2020-PCM. Normas Legales. *El Peruano*. Lima, 16 mar. 2020c. Disponible en: https://busquedas.elperuano.pe/normaslegales/aprueban-norma-que-establece-disposiciones-para-garantizar-l-resolucion-n-00035-2020-pdosiptel-1865029-1/ Accedido en: 15 abr. 2022.

PERÚ. Resolución Ministerial N° 160-2020-MINEDU de 1 de abril de 2020. Disponen el inicio del año escolar el 6 de abril de 2020, a través de la implementación de la estrategia denominada "Aprendo en casa", y aprueban otras disposiciones. Normas Legales. E*l Peruano*. Lima, 1 abr. 2020e. Disponible en: https://busquedas.elperuano.pe/normaslegales/aprueban-norma-que-establece-disposiciones-para-garantizar-l-resolucion-n-00035-2020-pdosiptel-1865029-1/ Accedido en: 15 sept. 2021.

PERÚ*. Resolución Ministerial N° 184-2020-MINEDU de 4 de mayo de 2020*. Disponer que el inicio de la prestación presencial del servicio educativo a nivel nacional en las instituciones educativas públicas y de gestión privada de Educación Básica, se encuentra suspendido mientras esté vigente el estado de emergencia nacional y la emergencia sanitaria para la prevención y control del COVID-19. Lima: Ministerio da Educação, 2020g. Disponible en: https://cdn.www.gob.pe/uploads/document/file/671906/RESOLUCION_MINISTERIAL-00184-2020-MINEDU.pdf Accedido en: 15 sept. 2021.

PERÚ. Ministerio de Transportes y Comunicaciones. Plan Nacional para el Desarrollo de la Banda Ancha en el Perú: 2011-2016. Raúl Pérez-Reyes Espejo Viceministro de Comunicaciones. Lima, dic. 2011

SAGASTI, F. R. (2002). Agenda: Perú; la propuesta más completa para el siglo XXI. Canada: IDRC, CRI, 2002. Disponible en: https://idl-bnc-idrc.dspacedirect.org/handle/10625/28979 Accedido en: 17 ago. 2021.

TELECOM ADVISORY SERVICES IIS; KATZS, R.; JUNG, Juan; CALLORTA, Fernando. El estado de la digitalización de América Latina frente a la pandemia del Covid-19: [S.l.]: CAF, 2020. Disponible en: https://scioteca.caf.com/bitstream/handle/123456789/1540/El_estado_de_la_digitalizacion_de_America_Latina_frente_a_la_pandemia_del_COVID-19.pdf Accedido en: 20 mar. 2021.

TELECOMUNICACIONES DE AMÉRICA LATINA*.* AHCIET comienza el año lanzando el estudio de "Desafío 2020. Inversiones para reducir la brecha digital**"** *ACHIET (ASIET). Desafíos 2020 Inversiones para reducir la Brecha Digital, 2018.*

USO DE WHATSAPP, Facebook y Tiktok crece sostenidamente en las redes fijas de internet durante la cuarentena. *OSIPTEL*, Lima, 5 mayo 2020. Disponível en: https://www.osiptel.gob.pe/portal-del-usuario/noticias/uso-de-whatsapp-facebook-y-tiktok-crece-sostenidamente-en-las-redes-fijas-de-internet-durante-la-cuarentena/ Accedido en: 15 sept. 2021. Disponible em: https://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/F60EC7FFA954DEC805257C7D004E4C04/$FILE/Plan_Desarrollo_BandaAncha_Dic2011.pdf Accedido en: 8 mar. 2021.

VEGA, Patcy Jesús Arce. *Impacto de la Inversión Pública en el crecimiento de la región Cajamarca periodo 2008-2017*. Disertación (Maestría en Gestión Pública) Instituto De Gobierno y de Gestión Pública. Cajamarca, Perú, 2019.

WORLD BANK. *Acuerdo de Cooperación Técnica Reforma para la expansión de Servicios e Infraestructura de Banda Ancha a Zonas Remotas y Rurales.* Washington, DC, 2018*.* Disponible en: https://portal.mtc.gob.pe/comunicaciones/regulacion_internacional/regulacion/proy%20normativos/2019/Informe_DiagnosticoBancoMundial.pdf. Accedido en: 09 jun. 2021

WORLD BANK. *Information and Communications for Development: Extending Reach and Increasing Impact.* Washington, DC, 2009. Disponible en: https://openknowledge.worldbank.org/handle/10986/2636 Accedido en: 09 jun. 2021.

WORLD BANK GROUP*.* Dividendos Digitales*. Informe sobre el desarrollo mundial 2016,* Washington DC, World Bank, 2016. Disponible en: https://documents1.worldbank.org/curated/en/658821468186546535/pdf/102724-WDR-WDR2016Overview-SPANISH-WebResBox-394840B-OUO-9.pdf> DOI: 10.1596/978-1-4648-0671-1 Accedido en: 09 jul. 2021

CIBERSEGURANÇA, TECNOLOGIAS DISRUPTIVAS E CIBERDEFESA NACIONAL: UMA VISÃO ESTRATÉGICA PARA A RESILIÊNCIA DIGITAL

Paulo Fernando Viegas Nunes*

RESUMO

Fruto da revolução tecnológica e da transformação digital, as modernas sociedades tornaram-se dependentes da internet e do ciberespaço. Num mundo hiperconectado, a afirmação de uma agenda digital, catalisadora da geração de riqueza e progresso social, depende, cada vez mais, de uma utilização livre, fiável e segura do ciberespaço. Num ambiente de segurança internacional dissimétrico, dinâmico e complexo, assistimos a uma profunda alteração politico-estratégica na forma como os Estados têm vindo a lidar com os riscos e as ameaças emergentes do ciberespaço, muitas vezes de natureza híbrida e transnacional. Neste espaço global, surgem tecnologias disruptivas, descontinuidades estratégicas e sinais de fragmentação digital, originando novos desafios à segurança e defesa nacional. Essencialmente ao longo da última década, Portugal tem vindo a amadurecer a sua visão estratégica para o ciberespaço e a consolidar a edificação de uma capacidade nacional de cibersegurança e ciberdefesa. Atendendo ao contexto nacional e internacional, caracterizando os fundamentos que enformaram as políticas de defesa e a consequente formulação de um pensamento estratégico para o ciberespaço, realiza-se uma síntese analítica do percurso nacional. Neste contexto, apresenta-se também um conjunto de contributos destinados a reforçar a resiliência digital neste domínio de cidadania, salvaguarda de interesses nacionais, afirmação de valores e defesa de soberania.

Palavras-chave: Ciberespaço; tecnologias disruptivas; cibersegurança; ciberdefesa; resiliência digital; estratégia nacional para o ciberespaço.

RESUMEN

Como resultado de la revolución tecnológica y transformación digital, las modernas sociedades se tornaron dependientes de la internet y el ciberespacio. En un mundo hiperconectado, la afirmación de una agenda digital, catalizadora de la generación

* Brigadeiro-General do Exército, licenciado e mestre em Engenharia Eletrotécnica e Computadores pelo Instituto Superior Técnico da Universidade de Lisboa (IST); Doutor em Ciências da Informação pela Universidade Complutense de Madrid. Possui o Curso de Estado-Maior e o Curso de Promoção a Oficial General. Exerceu funções de comando, estado-maior e ensino em unidades e estabelecimentos das Forças Armadas. Participou em diversas missões internacionais no âmbito da ONU (Sahara Ocidental), União Europeia e North Atlantic Treaty Organization (NATO). Foi Comandante da NATO Comunications anda Information School (NCI-Latina), Acting Director da NCI Academy (Oeiras), Coordenador Científico do Mestrado em Guerra de Informação (AM). Atualmente é Presidente do Conselho de Administração da Sistema Integrado de Redes de Emergência e Segurança de Portugal (SIRESP S.A).

de riqueza y progreso social, depende cada vez más, del uso libre, confiable y segura del ciberespacio. En un entorno/ambientación/alrededor de seguridad internacional disimétrico, dinámico y complejo, asistimos a un profundo cambio político-estratégico en la forma como los Estados han venido afrontando con los riesgos y las amenazas emergentes del ciberespacio, muchas veces de naturaleza/carácter híbrido y transnacional. En esto espacio global surgen tecnologías disruptivas, discontinuidades estratégicas y señales de fragmentación digital, emergiendo nuevos desafíos a la seguridad y defensa nacional. Esencialmente durante la última década, Portugal ha estado madurando su visión estratégica para el ciberespacio y consolidando la construcción de una capacidad nacional de ciberseguridad y ciberdefensa. Teniendo en cuenta el contexto nacional e internacional, caracterizando los fundamentos que dieron forma a las políticas de defensa y la consecuente formulación de un pensamiento estratégico para el ciberespacio, se realiza una síntesis analítica del camino nacional. En este contexto, también presentamos un conjunto de aportes encaminados a fortalecer la resiliencia digital en este ámbito de la ciudadanía, salvaguarda de los intereses nacionales, la afirmación de valores y la defensa de la soberanía.
Palabras clave: Ciberespacio; tecnologías disruptivas; ciberseguridad; ciberdefensa; resiliencia digital; estrategias nacionales en el ciberespacio.

1 INTRODUÇÃO

A revolução tecnológica acelerou as dinâmicas associadas aos processos de globalização, desencadeando um conjunto de alterações económicas e sociais sem precedentes. Os últimos 40 anos, coincidindo com a disseminação da utilização da Internet à escala planetária, foram marcados pela transformação digital e pela crescente centricidade assumida por esta rede global.

Aumentando a importância do funcionamento em rede e dos fluxos de informação que aí circulam, a digitalização favoreceu o trabalho cooperativo e tornou mais eficiente a execução de múltiplas tarefas, permitindo sincronizar o ciclo de inovação com os requisitos operacionais das organizações, melhorando a estrutura de enquadramento e as condições de desenvolvimento das modernas sociedades.

A hiperconetividade daí decorrente, reforçada pela adoção das comunicações de 5.ª Geração (5G), por sistemas de apoio à decisão suportados por ambientes de realidade virtual, pela supercomputação (quântica) e pela Inteligência Artificial (IA), alteraram os padrões de utilização do ciberespaço e são hoje uma realidade, influenciando, cada vez mais, os decisores humanos, disponibilizando recomendações, influenciando o presente e o futuro das organizações e dos Estados. O *World Economic Forum* (WEF), num relatório recente , estima que, em 2025, 85 milhões de empregos sofrerão o impacto de uma alteração na divisão do trabalho entre seres humanos e máquinas. Uma parte significativa

dos novos empregos terá uma relação direta com a área tecnológica e será criada em áreas ainda não existentes ou que já se encontram em transformação ao nível dos seus requisitos de competências. Neste "admirável mundo novo", complexo e interdependente, assistimos à adoção de modelos organizacionais híbridos onde a presença no mundo físico se estende para o ciberespaço, para uma interação virtual, intangível, onde a informação e o conhecimento se afirmam como os ativos mais críticos e valiosos.

A pandemia COVID-19, impondo o isolamento social, impulsionou a adoção de processos de teletrabalho e de ensino à distância, acelerando as iniciativas de transformação digital já em curso. No entanto, biliões de pessoas encontram-se neste momento em risco de falhar este "salto tecnológico", nomeadamente, porque à escala global as disparidades verificadas ao nível da literacia digital desafiam a própria construção social em rede. Com a flexibilização do local de trabalho e o aumento da interação remota, tornou-se cada vez mais importante proteger a informação dentro e fora das organizações. A informação dirige a vida das sociedades e das pessoas e estas vivem em rede.

Neste contexto, para além dos constrangimentos associados aos diferentes níveis de literacia, importa reconhecer que a existência de diferentes ritmos de transformação digital gera fortes assimetrias, afetando a cooperação, competição e até o conflito entre Estados. As dinâmicas de poder geradas numa sociedade de natureza conectiva e cognitiva estendem-se a todos os domínios da atividade humana, de natureza física ou virtual, seguindo frequentemente princípios comuns, mas necessariamente adaptados às especificidades dos meios utilizados e à sua área de aplicação.

Através do ciberespaço e a partir dele, atores mal-intencionados podem lançar ataques tanto no domínio social, político, económico como militar. Neste contexto, constata-se que a dimensão "ciberespaço" entrou definitivamente na sua fase de utilização instrumental como vetor de projeção de poder à escala global, ao serviço da consecução dos objetivos estratégicos de atores Estado e não-Estado. Os novos modelos de interação oferecidos pelo ciberespaço terão, cada vez mais, um forte e inegável impacto tanto na sociedade civil como no domínio militar, nomeadamente, porque o ciberespaço, enquanto espaço global comum, não é limitado pela esfera pública ou privada, interna ou externa, civil ou militar.

2 TECNOLOGIAS DISRUPTIVAS E GUERRA HÍBRIDA: IMPACTO MILITAR

A evolução do ciberespaço, observada ao longo dos últimos anos, não pode ser dissociada da necessidade de ajustamento permanente às suas dinâmicas operacionais e tecnológicas, reforçando a necessidade de novos processos de cibersegurança e ciberdefesa. Tecnologias como a IA, sistemas de armas autónomos, *big data*, biotecnologia e tecnologias *quantum* estão já a transformar

o mundo, na área da segurança e defesa, e até a forma como as Forças Armadas operam.

Face ao seu atual quadro de empenhamento e às características do ambiente operacional, existe um claro desajuste entre as capacidades e meios militares que equipavam as Forças Armadas da era industrial, predominantemente cinéticas, e as requeridas pelos conflitos da era moderna. A tipologia da moderna conflitualidade requer, cada vez mais, a mobilização de capacidades de natureza não-cinética para a sua resolução, onde o desenvolvimento de operações no ciberespaço, funcionando como um multiplicador de força, permite projetar poder no e a partir do ciberespaço, afetando outros domínios operacionais, muitas vezes sem a utilização de meios cinéticos (NUNES, 2020). A última década, marcada por uma utilização crescente do ciberespaço nas operações militares, acentuou esta tendência. Também em áreas como a criminalidade e o terrorismo, o Ciberespaço ocupa uma posição central. Os beligerantes aprenderam todos a utilizar, alguns deles com um nível de sofisticação muito elevado, as capacidades oferecidas por este espaço global.

A tecnologia está também a transformar os conflitos de múltiplas e diversas formas. A associação ao ciberespaço, da IA, da robótica, da supercomputação, dos novos modelos de interação oferecidos pela área da realidade virtual e aumentada, terão inevitáveis e fortes consequências no domínio militar. A integração destas novas tecnologias no corpo humano, até muito recentemente considerada ficção científica, faz agora parte de uma nova realidade. Num futuro próximo, os avanços em neuro-tecnologia permitirão assegurar o desenvolvimento de aplicações homem-máquina, melhorando as capacidades dos soldados no campo de batalha.

A integração e fusão de novas tecnologias, nos atuais e futuros sistemas militares, podem também criar sistemas de armas de grande letalidade e precisão. A utilização crescente de drones e sistemas de armas autónomos alterou os custos humanos, políticos e económicos da guerra. Em 2020, o conflito em Nagorno-Karabakh demonstrou a eficácia de drones suicidas semiautónomos lançados contra um adversário que assenta a sua atuação em táticas convencionais de combate. Mais recentemente, a guerra na Ucrânia, que começou em fevereiro de 2022, também confirmou a eficácia de drones utilizados contra uma potência militar de grande dimensão. Infelizmente, o progresso registado na elaboração de acordos internacionais, relativos à utilização de armas letais de natureza autónoma, suscetíveis de controlar este fenómeno, tem sido relativamente lento.

Muitas das tecnologias emergentes e disruptivas surgem a partir da investigação e desenvolvimento civil, tornando-se essencial garantir a existência de parcerias e uma efetiva cooperação civil-militar. Em última instância, a tecnologia pode ajudar a conter o conflito. Uma precisão analítica superior obtida a partir da IA, nomeadamente, graças à *big data* e à utilização de algoritmos

avançados de *machine learning*, poderá por exemplo convencer os beligerantes de um conflito que os custos da guerra vão muito provavelmente exceder quaisquer potenciais ganhos.

Estas e outras tecnologias emergentes e disruptivas apresentam assim tanto riscos como oportunidades para as sociedades. É por esta razão que muitos países e organizações internacionais como a NATO têm vindo a trabalhar em direta cooperação com o sector público e privado, com a academia e com a sociedade civil, para desenvolver e adotar novas tecnologias, fortalecer a base industrial de defesa e garantir a sua vantagem tecnológica (NORTH ATLANTIC TREATY ORGANIZATION, 2019). Para se manter na vanguarda do desenvolvimento tecnológico, fazer face aos desafios colocados pelas tecnologias emergentes e disruptivas, a NATO (2022) está neste momento também a envolver-se com outras organizações internacionais, incluindo a União Europeia (UE) e a Organização das Nações Unidas (ONU), nomeadamente, para assegurar a defesa dos Aliados e o sucesso das suas operações.

Um mundo mais interligado significa também a existência de um espetro mais alargado de ameaças e riscos. Os métodos tradicionais de conduzir a guerra, quando combinados com as novas tecnologias disruptivas e com novos elementos adjuntos como a desinformação online e os ciberataques resultam em "guerra híbrida". Este fenómeno, explora a ambiguidade utilizada por atores Estados e não-Estado para infligir dano, pulverizar a linha entre a guerra e a paz, introduzir a dúvida e desestabilizar as sociedades. Estas zonas cinzentas, não lineares, têm vindo a ser promovidas pelas principais potencias mundiais de forma a minar os esforços dos seus adversários ao mesmo tempo que paradoxalmente se procura evitar uma declaração formal de guerra.

A crescente prevalência da guerra híbrida reflete uma ordem global em mudança. Conflitos que se podem negar e de natureza indireta, incluindo a guerra cibernética (onde a distância física e o poder militar perdem relevância) podem ser combinados com sanções económicas e comerciais.

3 CIBERESPAÇO: UM DOMÍNIO ESTRATÉGICO PARA PORTUGAL

A designada "era da informação", permitiu atingir patamares de progresso e bem-estar social sem precedentes. Fruto da adoção de novos modelos de interação assentes num espaço global comum (ciberespaço) o mundo passou a estar permanentemente *online*, aprofundando uma cultura de partilha e cooperação.

Abraçando as vantagens oferecidas pela transformação digital e afirmando o desígnio político de aumento da competitividade nacional num contexto europeu e mundial, a economia nacional, passou a estar cada vez mais centrada em rede. Sobretudo a partir do princípio da década de 1990 e no início deste

século, Portugal investiu fortemente na melhoria das suas infraestruturas de comunicações, apresentando uma elevada taxa de penetração na adoção de novas aplicações e serviços digitais. Em consequência desta aposta, enquanto economia de serviços e de base terciária, a geração de riqueza nacional tornou-se cada vez mais dependente da internet, passando a estar mais exposta e vulnerável a um leque alargado de novos riscos de segurança.

Assumindo uma natureza híbrida, tanto na geração de valor como no exercício do poder, o ciberespaço tem vindo a ser utilizado como elemento de desinformação, de manipulação de ideias e de influência política. Acontecimentos recentes como a "primavera árabe", as eleições norte-americanas, o "Brexit", ou até a própria pandemia COVID-19 e o atual conflito na Ucrânia, evidenciam bem o poder das redes sociais e o impacto da (des)informação na geopolítica mundial.

O ciberespaço, sem limitações geográficas, facilita assim o lançamento de ataques a partir de qualquer local, tornando difícil distinguir todos os atores envolvidos e clarificar o que é interno e externo. Os hackers que, nos anos de 1990, se concentravam essencialmente na penetração de redes e na produção de software malicioso, já não configuram hoje a única ameaça. Ao longo das últimas décadas, também em áreas como o ativismo social, o crime organizado e o terrorismo, alguns atores têm vindo a utilizar o ciberespaço como vetor de ataque. Estas novas ameaças, incluindo ações desenvolvidas por atores Estado e não-Estado, devido à sua natureza assimétrica e efeitos potencialmente disruptivos e destrutivos, levaram a que este espaço global seja hoje assumido como um novo domínio das operações militares.

O nível de inovação e sofisticação tecnológica, que caracteriza os vários vetores de ataque, com uma forte ligação à interação em rede e aos dispositivos ligados à Internet, fazem crescer exponencialmente o nível da ameaça e os riscos sociais, colocando em risco as infraestruturas críticas, os processos de administração e governação eletrónica do Estado e, de uma forma geral, a própria resiliência nacional.

Com a adoção das comunicações 5G, exemplo ilustrativo do que aqui se refere, cresceu o receio de que as infraestruturas de telecomunicações nacionais possam vir a ser espiadas por grandes potencias mundiais ou que, em caso de conflito, possam vir a ser "desligadas" por outra nação. Uma outra questão, indissociável destas, levanta-se também ao nível da "soberania digital", nomeadamente, porque, a materializar-se esta situação, um Estado já não conseguiria, por si só, refazer/reajustar a sua infraestrutura de comunicações nacional sem a ajuda dos grandes fabricantes de equipamentos que, inevitavelmente, se encontram associados aos seus países de origem.

Dificilmente será possível explorar todo o valor que o ambiente de informação e o ciberespaço oferecem às modernas sociedades sem garantir a sua segurança e defesa. Por essa razão, este constitui reconhecidamente um

domínio estratégico para Portugal, necessitando de ser pensado como uma área prioritária de afirmação de soberania, de defesa de valores e interesses nacionais.

De forma a melhor definir os fundamentos da visão político-estratégica nacional associada à segurança e defesa do ciberespaço, importa assim, contextualizar e enquadrar a sua perspetiva nacional e internacional, identificando os esforços já realizados, em curso e a desenvolver neste domínio.

4 ENQUADRAMENTO DA VISÃO ESTRATÉGICA NACIONAL

Refletindo a evolução das políticas de defesa nacional, tanto no domínio da cibersegurança como da ciberdefesa, Portugal tem vindo, essencialmente desde 2010, a desenvolver um conjunto de iniciativas destinadas a garantir uma utilização mais livre, fiável e segura do ciberespaço. Para esse efeito, em 2012, na sequência da aprovação do plano global estratégico de racionalização de custos com as Tecnologias de Informação e Comunicação (TIC) na Administração Pública, Resolução do Conselho de Ministros n.º 12/2012, de 07 de fevereiro, sob a coordenação do Gabinete Nacional de Segurança (GNS) e com a colaboração de todas as entidades relevantes nesta matéria, foi prevista a definição de uma Estratégia Nacional de Segurança da Informação (ENSI), que compreendia a criação, instalação e operacionalização de um Centro Nacional de Cibersegurança (CNCS). Para esse efeito, através da Resolução do Conselho de Ministros n.º 42/2012, de 05 de abril, foi constituída uma Comissão Instaladora do CNCS, colocada, devido à transversalidade dos seus objetivos, na dependência do Primeiro-Ministro. Esta Comissão, no contexto dos seus trabalhos, apresentou uma primeira proposta de estratégia nacional de cibersegurança.

Em linha com a visão política e com a proposta formulada, o Conceito Estratégico de Defesa Nacional (PORTUGAL, 2013), estabelecendo um conjunto de prioridades estratégicas, reconheceu também a "informação e a segurança do ciberespaço" como um dos seus pilares estratégicos. Atendendo às questões emergentes da segurança do ciberespaço, o CEDN determinou, entre outras medidas, a criação de uma estrutura nacional de cibersegurança e, ao nível das Forças Armadas, a edificação de uma capacidade de ciberdefesa. Neste âmbito, prevendo-se uma resposta articulada e sinérgica destes elementos, importa reconhecer que, à luz da Constituição da República Portuguesa, Resolução da Assembleia da República n.º 15/2005, de 07 de abril, enquanto os riscos para a segurança do País são geridos no âmbito da cibersegurança, os riscos para a defesa do Estado se enquadram no domínio da ciberdefesa, exigindo uma participação ativa das Forças Armadas.

Ainda em 2013, no quadro da reforma "Defesa 2020", o Ministro da Defesa Nacional (MDN), determinou a criação de um Centro de Ciberdefesa (CCD) no

âmbito do Estado-Maior-General das Forças Armadas (EMGFA) e definiu a sua orientação política para a ciberdefesa. Despacho n.º 13692/2013, de 28 junho. Materializando a visão política formulada, o Chefe do Estado-Maior-General das Forças Armadas (CEMGFA) apresentou um plano de desenvolvimento da capacidade de ciberdefesa (PORTUGAL, 2019).

Seguindo as indicações da UE, que recomendou a operacionalização deste tipo de estruturas em todos os Estados-Membros (EM) até dezembro de 2012, o levantamento do CNCS concretizou-se em 2014, ficando este integrado no GNS. Na sequência deste passo, foi também aprovada uma Estratégia Nacional de Segurança do Ciberespaço (PORTUGAL, 2015). Acompanhando a evolução tecnológica e a dinâmica das ciberameaças, esta estratégia foi objeto de revisão e atualizada para o período 2019-2023 (PORTUGAL, 2019) tendo, neste contexto, sido também identificada a necessidade de reforçar a edificação da capacidade nacional de ciberdefesa (PORTUGAL, 2018). Neste processo, procurou-se garantir a articulação com os esforços cooperativos já lançados por outros países e pelas organizações internacionais de que Portugal faz parte integrante (NORTH ATLANTIC TREATY ORGANIZATION, 2020).

Na sequência da aprovação da ENSC, foi também criado o Conselho Superior para a Segurança do Ciberespaço (PORTUGAL, 2017), que assumiu a responsabilidade de coordenação política e estratégica da cibersegurança nacional, consolidada através do Art.º 5.º da Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço.

Tendo em vista o desenvolvimento de uma visão política para a ciberdefesa e a consequente criação de uma Estratégia Nacional de Ciberdefesa (ENCD), foram desenvolvidos diversos estudos e documentos de trabalho, tanto ao nível do MDN e do EMGFA (PORTUGAL, 2019), como do Instituto da Defesa Nacional (FREIRE, NUNES & ACOSTA, 2013; NUNES, 2018). Neste contexto, importa ainda assinalar que, na última revisão do Conceito Estratégico Militar (PORTUGAL, 2014), foram já identificados vários cenários de emprego das Forças Armadas tanto no contexto da ciberdefesa como na área da cibersegurança nacional.

Reforçando esta visão, através do seu Despacho n.º 52/2019, de 23 de outubro, o MDN aprovou as Linhas Orientadoras para a Estratégia Nacional de Ciberdefesa (PORTUGAL, 2019b), determinando o desenvolvimento de uma "Estratégia Nacional de Ciberdefesa e a edificação da capacidade de condução de operações no, e através do, ciberespaço [...] de forma a garantir o alinhamento com a Estratégia Nacional de Segurança do Ciberespaço" (PORTUGAL, 2019b). Atendendo ao quadro de alianças e aos esforços já em curso, em linha com a ENCS, o CEMGFA identificou, na sua diretiva para o triénio 2018-2021, a necessidade de atualizar o plano de desenvolvimento desta capacidade (PORTUGAL, 2019), contribuindo assim para dinamizar a edificação da capacidade nacional de

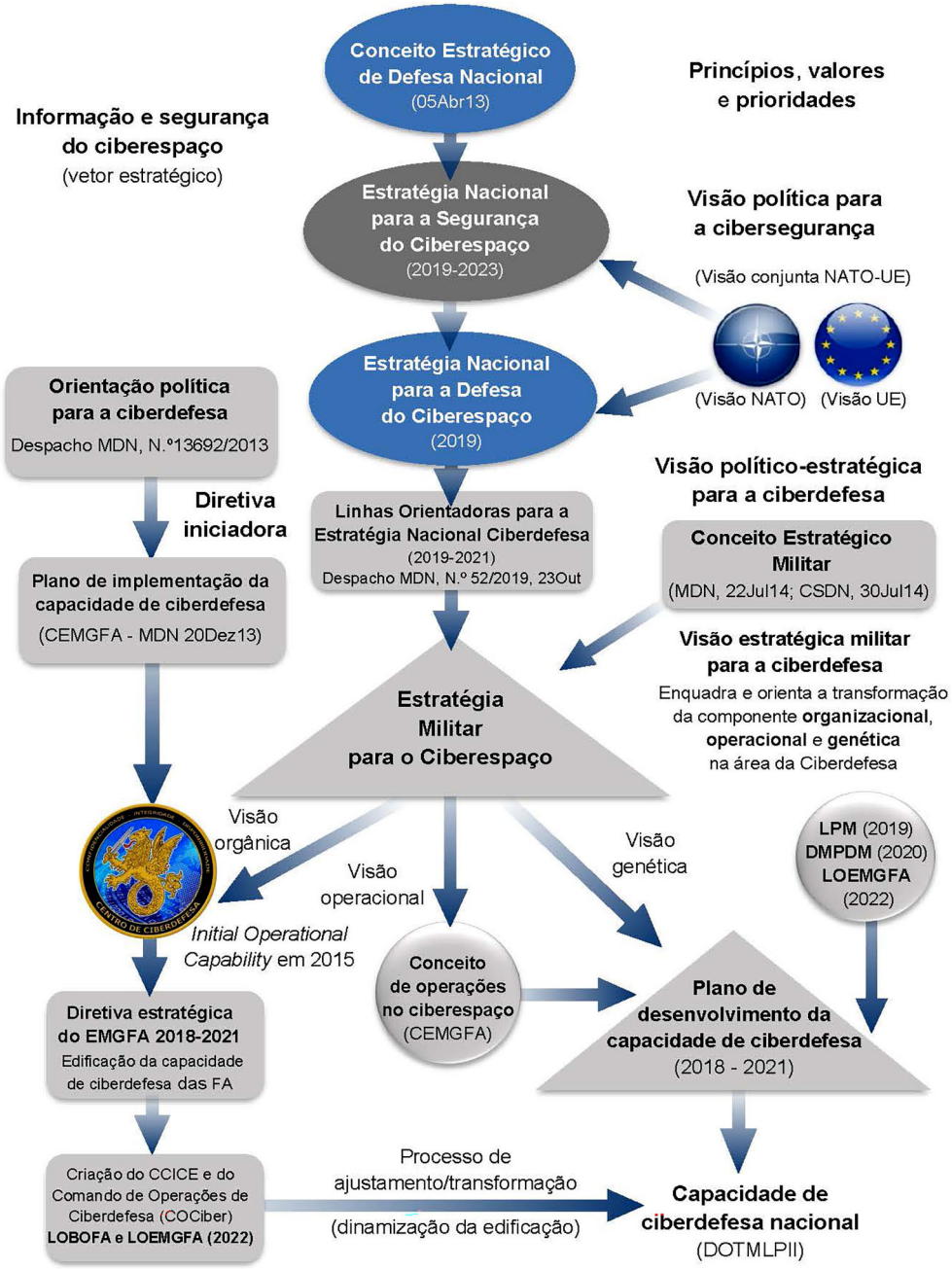
ciberdefesa. A revisão da Lei de Programação Militar (PORTUGAL, 2019) e a Diretiva Ministerial de Planeamento de Defesa Militar (PORTUGAL, 2020), vieram também reforçar o caráter prioritário desta capacidade no planeamento de Defesa Militar.

Mais recentemente, através do seu Despacho n.º 15/2020, de 06 de fevereiro, o MDN criou um Comité de Monitorização da Ciberdefesa (CMCD) na sua direta dependência, cuja missão é o acompanhamento permanente de todos os assuntos relacionados com a ciberdefesa nacional, garantindo assim a necessária coerência e integração de esforços. Face às suas atribuições, o CMCD é responsável pelo "acompanhamento e monitorização do plano de desenvolvimento da capacidade de ciberdefesa para o período 2019-2023, em curso no EMGFA, assegurando a sua atualização nos próximos triénios" (PORTUGAL, 2020b, p.2). Entre outras atribuições, foi cometida ao CMCD a responsabilidade de apresentar uma proposta de ENCD, um enquadramento jurídico-constitucional da atuação das FA neste domínio e uma proposta de política de recursos humanos para a ciberdefesa. Na decorrência desta decisão, já em 2021, o MDN, através do seu Despacho n.º 04/2021, de 12 de fevereiro, determinou formalmente o início de uma campanha de recrutamento para a ciberdefesa, solicitando para esse efeito aos Ramos das Forças Armadas a elaboração de um plano, prevendo o recrutamento de efetivos para 2022 e tendo em consideração o plano de incorporações e admissões para 2021, incluindo a requalificação de pessoal para a ciberdefesa.

Na sequência da revisão da Lei Orgânica de Bases das Forças Armadas (LOBOFA), Lei Orgânica n.º 2/2021, de 9 de agosto, e da publicação do Decreto-Lei n.º 19/2022, de 24 de janeiro, que estabelece a Lei Orgânica do EMGFA e altera as Leis Orgânicas dos três ramos das Forças Armadas, atendendo aos dois novos domínios das operações militares, reconhecidos pela NATO (ciberespaço e espaço), foi criado o Centro de Comunicações e Informação, Ciberespaço e Espaço (CCICE), na direta dependência do CEMGFA. Neste âmbito, foi também criado o Comando de Operações de Ciberdefesa (COCiber), na dependência do CCICE.

Refletindo simultaneamente uma visão conceptual, cronológica e analítica, a figura 1 ilustra o enquadramento do desenvolvimento da política de defesa nacional neste domínio, perspetivando a forma como esta se articula ao nível estratégico e operacional e como orienta o processo de ajustamento/transformação do desenvolvimento da capacidade nacional de defesa do ciberespaço. Neste âmbito, atendendo ao quadro de alianças e organizações internacionais de que Portugal faz parte integrante, importa agora caracterizar o contexto internacional, os esforços cooperativos e analisar a forma como estes fatores contribuem para o alinhamento estratégico da política de defesa nacional.

Figura 1 – Enquadramento da política de defesa e da estratégia militar para o ciberespaço



Fonte: NUNES, 2020, p. 17; NUNES, 2018, p.94 (Adaptado).

4 CONTEXTO INTERNACIONAL E ALINHAMENTO ESTRATÉGICO

Face ao alinhamento político-estratégico nacional, antes caracterizado, releva-se a existência de um quadro evolutivo diferenciado, mas ainda assim articulado, entre a área da defesa e da segurança do ciberespaço. Enquanto o domínio da ciberdefesa, tem vindo a ser influenciado pelos passos dados pela NATO e pela forma como esta organização perspetiva o desenvolvimento de capacidades militares e a evolução da sua política de ciberdefesa, a área da cibersegurança é fortemente influenciada, por vezes até regulada/dirigida, pela UE, segundo uma perspetiva de reforço da segurança e da resiliência do ecossistema digital.

A Aliança Atlântica assumiu a ciberdefesa como uma preocupação prioritária na cimeira de Lisboa, onde foi aprovado o seu conceito estratégico (NORTH ATLANTIC TREATY ORGANIZATION, 2010). Face ao aumento das ameaças cibernéticas, identificando o ciberespaço como área de confrontação estratégica e a aplicabilidade do direito internacional, a Aliança aprovou a sua *Enhanced Policy on Cyber Defence* em 2014, durante a cimeira de Gales (NORTH ATLANTIC TREATY ORGANIZATION, 2014b), prevendo a adoção de uma resposta conjunta, face à ocorrência de ataques puramente cibernéticos ou de natureza cinética/ convencional. Na sequência desta decisão, consolidando a implementação de mecanismos de cooperação e assistência ao nível da partilha de informação, Portugal assinou em 2016 um memorando de entendimento e de partilha de informação na área da ciberdefesa.

Na cimeira de Varsóvia, marcada pelo reconhecimento do ciberespaço como novo domínio das operações militares, Portugal ratificou também o *Cyber Defence Pledge* (NORTH ATLANTIC TREATY ORGANIZATION, 2016a), assumindo o compromisso de reforçar a proteção de redes e infraestruturas, alocar recursos, robustecer as capacidades nacionais e a partilha de informação neste domínio, promovendo a formação e o treino. No âmbito da revisão da sua estrutura de comando, a Aliança decidiu, na cimeira de Bruxelas (NORTH ATLANTIC TREATY ORGANIZATION, 2018), criar um Comando para as Operações no Ciberespaço (*Cyberspace Operations Centre*), bem como a possibilidade de algumas das Nações Aliadas disponibilizarem voluntariamente a produção de efeitos operacionais (defensivos e ofensivos), no quadro das missões e operações NATO.

Atendendo ao impacto das tecnologias emergentes no domínio do ciberespaço e no âmbito mais alargado da defesa e segurança da Aliança, na cimeira de Londres (NATO, 2019), em dezembro de 2019, os líderes da NATO concordaram na definição de um roteiro para a implementação de uma política de desenvolvimento de Tecnologias Emergentes e Disruptivas (TED). Em fevereiro de 2021, os Ministros da Defesa da NATO endossaram uma estratégia para as TED, identificando áreas concretas a considerar pela Aliança à medida que se processa a sua adoção. Em 2021, na Cimeira de Bruxelas (NORTH ATLANTIC TREATY ORGANIZATION, 2021a), como parte integrante da Agenda Estratégica 2030 da Aliança (NORTH ATLANTIC

TREATY ORGANIZATION, 2021b), os líderes da NATO concordaram lançar o Defence Innovation Accelerator for the North Atlantic (DIANA), um acelerador de inovação no domínio da defesa, de natureza civil-militar, e estabelecer um Fundo de Inovação NATO (2022), destinado a financiar projetos de *start-ups*. Estima-se que ambas as iniciativas venham a estar plenamente implementadas por ocasião da próxima cimeira da NATO, a ter lugar em Madrid, durante o ano de 2022. Em Portugal, no âmbito da rede DIANA (NORTH ATLANTIC TREATY ORGANIZATION, 2022), ficarão localizados um acelerador de inovação (Arsenal do Alfeite) e um centro de testes (Centro de Experimentação Operacional da Marinha, em Tróia).

Consciente do impacto estratégico das ciberameaças, em 2009, a UE desenvolveu também um conceito de ciberdefesa (UNIÃO EUROPEIA, 2009), posteriormente ampliado e aprovado em 2012 (UNIÃO EUROPEIA, 2012). O primeiro quadro estratégico para a ciberdefesa foi aprovado pelo Conselho em 2014 (UNIÃO EUROPEIA, 2014), contribuindo para intensificar a cooperação europeia neste domínio.

Em junho de 2017, a UE (2017) estabeleceu a designada *Cyber Diplomacy Toolbox* (CDT), com o objetivo de criar as bases para a articulação de uma resposta diplomática conjunta contra o desenvolvimento de atividades cibernéticas maliciosas, desencorajando potenciais agressores e mitigando o impacto de ciberataques que ameacem os interesses políticos, económicos e a segurança da UE. Para esse efeito, foi desde logo prevista a imposição de medidas restritivas contra as entidades e indivíduos envolvidos, sendo estas proporcionais ao foco, escala, duração, intensidade, complexidade, sofisticação e efeito das mesmas (UNIÃO EUROPEIA, 2017).

Em linha com esta iniciativa, o Conselho da UE promoveu a atualização do quadro estratégico da ciberdefesa (UNIÃO EUROPEIA, 2018), identificando domínios prioritários de intervenção e clarificando o papel a desempenhar por todos os atores envolvidos. De forma a robustecer a sua capacidade para fazer face a ciberataques, a UE divulgou um conjunto de medidas destinadas a incentivar os EM a fortalecer as suas capacidades de ciberdefesa, oferecendo a possibilidade de estes submeterem projetos cooperativos no quadro da *Permanent Structured Cooperation* (PESCO) e do Fundo Europeu de Defesa (FED), incluindo o lançamento de uma plataforma de educação e treino, para fomentar as suas oportunidades de formação. Envolvendo os setores industriais e tecnológicos e as universidades, salienta-se a participação nacional em projetos europeus no domínio da ciberdefesa, nomeadamente, assumindo a coliderança conjuntamente com a França, da *Cyber Defence Discipline* do *EU Military Training Group* e liderando o Projeto PESCO *Cyber Academia and Innovation Hub* (CAIH), coordenado pelo MDN e a ser edificado nas instalações cedidas pelo Exército na Academia Militar, em Lisboa.

Em maio de 2019, foi aprovado o quadro regulatório da imposição das sanções previstas no CDT, sendo este adotado pelo Conselho da UE como um

instrumento da Política Externa e de Segurança Comum (UNIÃO EUROPEIA, 2019). Pela primeira vez, no dia 30 de julho de 2020, o Conselho da UE impôs um conjunto de medidas restritivas contra seis indivíduos e três entidades que foram consideradas responsáveis pelo envolvimento em vários ciberataques lançados contra diversos EM (UNIÃO EUROPEIA, 2020a). Estas sanções foram consideradas oportunas, nomeadamente porque o cibercrime tem vindo a explorar a pandemia COVID-19, conduzindo atividades ilícitas, tendo por alvo não apenas indivíduos, mas também as principais operadoras de telecomunicações da UE, infraestruturas críticas e, em particular, o sector da saúde.

A imposição de sanções, como resposta a ciberataques, constitui um sinal claro da alteração de uma estratégia política mais cautelosa, para uma resposta mais firme e afirmativa da UE, demonstrando que os EM estão preparados para atingir um maior nível de cooperação no domínio da ciberdissuação. Tal poderá também contribuir para incentivar um maior desenvolvimento da moldura penal e confirmar a tendência para a aplicação dos princípios da legislação internacional à utilização das TIC.

Refletindo a adoção de uma aproximação mais pragmática, a Estratégia de Segurança Europeia (EU, 2020b), publicada em 2020, prevê a criação de um centro de competências e de uma *Joint Cyber Unit* (EU, 2020b, p. 9) reforçando os esforços já em curso para o estabelecimento de regras comuns na área da cibersegurança em todas as instituições da UE. Tal poderá resultar numa maior consciência situacional e aumentar a cooperação entre as diversas agências e organizações da UE, como a *European Union Agency for Cybersecurity* (ENISA), o *European Cybercrime Centre* (EC3) da Europol e a rede de *Computer Security Incident Response Teams* (CSIRT) europeia.

A Comissão apresentou em 16 de dezembro de 2020 a nova Estratégia de Cibersegurança da UE (2020c), assumindo esta um papel determinante na construção de um futuro digital (UNIÃO EUROPEIA, 2020d), no plano de recuperação (UNIÃO EUROPEIA, 2020e) e na afirmação da Estratégia de Segurança Europeia. Esta estratégia, tendo como finalidade primária assegurar a resiliência coletiva da UE contra ciberataques, pretende garantir que todos os cidadãos e empresas podem beneficiar plenamente de ferramentas e serviços digitais fiáveis e confiáveis. Simultaneamente, a Comissão também desenvolveu um conjunto de iniciativas destinadas a aumentar a resiliência física e cibernética de entidades e redes críticas apresentando uma proposta de diretiva orientada para a adoção de um conjunto de medidas destinadas a reforçar o nível de cibersegurança da UE – revisão da Diretiva NIS (UNIÃO EUROPEIA, 2020f), e uma nova diretiva sobre a resiliência de entidades críticas (UNIÃO EUROPEIA, 2020g).

Em 21 de março de 2022, o Conselho aprovou formalmente a "Bússola Estratégica" (EU, 2022), oferecendo à UE um plano de ação ambicioso para reforçar a sua política de segurança e defesa até 2030. Entre outros aspetos, a EU

pretende assim criar um conjunto de instrumentos de combate à manipulação da informação e à ingerência estrangeiras, continuando a desenvolver instrumentos de ciberdiplomacia e uma política de ciberdefesa a fim de se preparar melhor para a ocorrência de ciberataques e lhes dar resposta.

Neste domínio, a UE reforçou também a sua parceria estratégica com a NATO. Reconhecendo que 22 das 30 nações NATO fazem parte da UE, estas organizações assinaram na cimeira de Varsóvia uma declaração conjunta (EUROPEAN UNION-NORTH ATLANTIC TREATY ORGANIZATION, 2016). A cibersegurança e a ciberdefesa foram assumidas como áreas prioritárias de cooperação, sendo identificadas opções concretas, com efeito-imediato: "de forma a fortalecer a cooperação na área do treino, a partir de 2017, a UE e a NATO vão harmonizar os requisitos de treino e abrir os respetivos cursos de formação à participação mútua do seu *staff*" (EUROPEAN UNION-NORTH ATLANTIC TREATY ORGANIZATION, 2016, p. A-6).

Materializando a cooperação EU-NATO neste domínio, importa referir que Portugal, estabelecendo pontes entre projetos e iniciativas já lançados no âmbito NATO e UE, ligados à formação, educação e treino em ciberdefesa, ocupa uma posição central numa rede de centros de excelência e polos de conhecimento nacionais e internacionais, decorrente não só da liderança do Projeto CAIH e da coliderança da *Cyber Defence Discipline* da UE, mas também da liderança do projeto NATO *Smart Defense Multinational Cyber Defence Education and Training* (MNCDE&T), da instalação da *NATO Communications and Information Academy* (NCI Academy) em Oeiras e das estruturas nacionais associadas ao projeto DIANA (Alfeite e Tróia).

Favorecendo o desenvolvimento de uma visão política convergente e de uma estratégia cooperativa comum, constata-se também a existência de um conjunto alargado de outras iniciativas internacionais, já em curso ou a lançar pelas principais organizações a que Portugal pertence (NATO, UE, ONU/ITU e OCDE). De forma sintética, conforme refletido num estudo do IDN-CESEDEN (FREIRE; NUNES; ACOSTA, 2013), identificam-se no Anexo A as áreas comuns de cooperação internacional no ciberespaço, estruturando-as de acordo com os objetivos a atingir e com os elementos associados ao desenvolvimento de capacidades.

Salientando a sua relevância no domínio estratégico, operacional e económico/industrial, conclui-se que, para Portugal, a cibersegurança e a ciberdefesa surgem como áreas de natural cooperação civil-militar e como áreas prioritárias de desenvolvimento de capacidades cooperativas, nomeadamente, segundo uma perspetiva de "agregar e partilhar", adotando para esse efeito o conceito de *smart defence* no âmbito NATO e de *pooling & sharing* no contexto da UE.

5 SITUAÇÃO ATUAL: VISÃO CONJUNTURAL

O ciberespaço interseta transversalmente todos os vetores de projeção do poder nacional, incluindo os diversos domínios associados à segurança e defesa

do Estado e, consequentemente, segundo uma lógica multidomínio, também todos os domínios operacionais das Forças Armadas (mar, terra, ar e espaço). Requerendo mecanismos de governação transversais, capazes de garantir a necessária articulação entre a cibersegurança e a ciberdefesa nacional, a atuação eficaz das várias entidades responsáveis só será possível através da criação de uma "comunidade de interesse" civil-militar alargada no ciberespaço, capaz de explorar sinergias nacionais e a cooperação internacional.

Neste âmbito, salienta-se que a transversalidade das áreas relacionadas com o ciberespaço e a complexidade associada à coordenação e condução de operações de cibersegurança e ciberdefesa, faz com que o quadro legal aplicável seja relativamente extenso, disperso e tenha que se adaptar à contínua evolução da realidade a regular. Assinala-se também a inexistência de direito internacional específico, registando-se algumas insuficiências na legislação nacional, dificultando a sua compreensão e aplicação.

Apesar de a resiliência das tecnologias digitais ter vindo a aumentar, subsistem ainda algumas fragilidades ao nível dos processos associados à gestão de crises no ciberespaço e à partilha de informação situacional em tempo real, limitando a capacidade nacional para garantir uma atempada fusão e difusão da análise das ciberameaças emergentes num ambiente de segurança de complexidade crescente. Esta lacuna, conduz potencialmente a uma falta de coordenação operacional e à adoção de políticas não coordenadas, impedindo a partilha de informação crítica e resultando numa gestão inadequada dos riscos sociais, deixando o País vulnerável. Esta fragilidade estratégica poderá vir a ser explorada por potenciais adversários, sejam eles atores-Estado ou não Estado.

Atendendo à síntese analítica do contexto nacional e ao enquadramento internacional antes apresentados, importa salientar que o percurso nacional no domínio da cibersegurança e da ciberdefesa, reflete um desenvolvimento assimétrico destas duas áreas, tanto ao nível estrutural como operacional e genético, tornando difícil uma conceptualização estratégica integrada e consistente destas duas realidades.

Na área da cibersegurança, em 2021, Portugal dispõe de uma ENSC, aprovada em 2015 e atualizada/revista em 2020. Alinhada com esta visão estratégica, foi edificada uma estrutura nacional de cibersegurança, articulada: ao nível político-estratégico, através do CSSC/GNS; ao nível da coordenação operacional, através do CNCS; e, ao nível operacional/tático, através da rede nacional de *Computer Emergency Response Teams*.

Contrastando com esta situação, apesar dos esforços em curso, não existe ainda uma ENCD aprovada. Apesar da nova LOBOFA (2021) e da nova LOEMGFA (2022) terem aprovado a criação do CCICE e do COCiber, a estrutura de ciberdefesa implementada assenta ainda apenas no Centro de Ciberdefesa das Forças Armadas (coordenação operacional/tática) e na rede de *Computer Incident Response*

Capability dos vários Ramos das Forças Armadas (nível tático/técnico). Neste âmbito, salienta-se a existência de estudos recentes (Nunes, 2020) que apontam para a necessidade de definição urgente de uma estratégia militar para o ciberespaço e para a dinamização da edificação da capacidade de ciberdefesa nacional. Entre outras medidas apresentadas, é proposta a criação de um Conselho Superior de Defesa do Ciberespaço (CSDC), na dependência do MDN e de um Comando Operacional para o Ciberespaço, na dependência direta do CEMGFA. Estes órgãos, garantindo respetivamente o enquadramento político-estratégico e operacional da ciberdefesa, contribuirão decisivamente para melhorar a ligação com a estrutura nacional de cibersegurança, colmatando muitas das fragilidades existentes no processo de gestão de crises nacional, reforçando a resiliência cibernética do País.

Com a adoção destas medidas, a coordenação politico-estratégica e a operacionalização da cooperação internacional no domínio da ciberdefesa (e.g. com a NATO e UE) serão desde logo institucionalmente reforçadas, alinhando vertical e transversalmente as responsabilidades e competências das estruturas existentes e a levantar. Tal permitirá também ultrapassar os constrangimentos operacionais decorrentes do facto de a tutela política da Ciberdefesa (MDN) ser diferente do enquadramento político da Cibersegurança (GNS/Presidência do Conselho de Ministros) e porque passará a existir um comando operacional (COCiber), capaz de garantir uma efetiva atuação multidomínio e a articulação internacional das Forças Armadas no domínio das operações de ciberdefesa da Aliança.

A gestão de crises no ciberespaço, obrigando a uma avaliação permanente das ameaças, vulnerabilidades e riscos, exige assim uma resposta nacional coerente e articulada. Esta, respeitando os limites de competências dos vários atores, deverá envolver toda a sociedade, explorando sinergias nacionais e a cooperação internacional. Este objetivo, só será alcançável através do desenvolvimento de uma estratégia nacional de segurança e defesa do ciberespaço, transversal, equilibrada e integradora das suas áreas estruturantes.

6 POLÍTICAS DE DEFESA NO CIBERESPAÇO: PERSPETIVAS DE EVOLUÇÃO

À medida que os avanços tecnológicos e a interconetividade global aceleraram exponencialmente, assistimos a um crescimento sem precedentes das ameaças e dos riscos de segurança sistémicos, pondo em causa o desenvolvimento das sociedades de matriz digital. No início de 2022, foram tornados públicos sete ciberataques sucessivos a empresas e instituições nacionais, com grande impacto disruptivo. Em janeiro, foi atacado o grupo Impresa, do qual a estação de televisão SIC faz parte, e, em fevereiro, o site do Parlamento, a Cofina, o grupo Trust in News, detentor das revistas Visão e da Caras, a operadora de comunicações Vodafone e o grupo de laboratórios Germano de Sousa. Esta onda de ciberataques culminou

em março com um ciberataque ao grupo Sonae, afetando as operações de toda a cadeia de supermercados Continente.

Face ao número crescente de ciberataques, as noções de igualdade e justiça no acesso e utilização do ciberespaço, até agora prevalecentes no desenvolvimento das relações internacionais e na política dos Estados, tornaram-se elas mesmas fluídas e por vezes pouco claras, requerendo uma postura cooperativa da comunidade internacional, assente numa capacidade acrescida de diálogo e num alinhamento estratégico permanente, para garantir a cibersegurança e ciberdefesa do ecossistema digital.

A recente pandemia COVID-19, demonstrando que nenhuma instituição ou indivíduo pode enfrentar de forma isolada os desafios globais, tornou claro o enorme aumento de importância da Internet e do ciberespaço na garantia da resiliência dos Estados, provando que as mudanças impostas pela transformação digital, acelerada neste período atípico, são inevitáveis, por vezes mesmo irreversíveis, em praticamente todas as áreas de atividade e domínios da sociedade.

Na formulação das suas políticas de segurança, os Estados devem estar cada vez mais atentos aos principais desafios estratégicos e competitivos associados ao fenómeno da digitalização e à 4.ª revolução industrial, salientando-se a aceleração destes processos nos últimos anos e o facto de a transformação digital transcender, em muito, o processo de digitalização. Neste contexto, surgem inevitavelmente novos padrões de utilização competitiva do ambiente de informação, inerentes à existência de diferentes ritmos de transformação digital, quer ao nível das ferramentas tecnológicas, quer no que se refere aos processos e ao modelo de governo das empresas e das organizações do futuro.

Antecipando as dinâmicas de mudança do ambiente de segurança internacional, no caso específico da segurança da informação e do ciberespaço, a UE (2020b; 2022) propõe que a evolução das políticas de segurança e defesa dos seus EM decorra de forma a:

- assegurar que as políticas adotadas neste domínio refletem o espectro dinâmico da ameaça, nomeadamente, no que se refere ao crime organizado, terrorismo transnacional, atividades de radicalização social e ações desenvolvidas por outros atores (Estado e não-Estado) que afetem a consecução dos interesses e a salvaguarda da soberania nacional;
- envolver todas as instituições governamentais, a administração pública, o setor privado e todos os cidadãos individuais, seguindo uma aproximação inclusiva de toda a sociedade (*whole-of-society*);
- integrar, num todo coerente, as várias áreas políticas com um impacto direto na segurança e defesa do ciberespaço, reforçando a segurança do ecossistema digital;

- contribuir para a construção de uma resiliência nacional, sustentável no longo prazo.

Tendo consciência que a defesa do ciberespaço nacional depende da atuação sinérgica e "em rede" da sociedade portuguesa, em linha com a visão da UE, com caráter supletivo e complementar, considera-se também necessário promover o estabelecimento das seguintes prioridades políticas:

- investir na sensibilização e educação para a cibersegurança, tendo em vista melhorar a literacia digital e a consciencialização individual e coletiva da sociedade portuguesa para os riscos e ameaças emergentes da internet, ajudando a gerar competências através da formação e treino especializado, reduzindo assim as lacunas existentes ao nível do conhecimento associado à cibersegurança e ciberdefesa;
- fortalecer as sinergias nacionais e aumentar a cooperação internacional nestes domínios, de forma a facilitar o combate ao cibercrime e a reduzir as barreiras (ainda existentes) à cooperação no domínio da cibersegurança e ciberdefesa. Através da colaboração entre o sector público e privado, será possível melhorar o conhecimento transversal e a adoção das melhores práticas, fazendo face aos riscos associados a um contexto social de rápida inovação tecnológica;
- estimular a Investigação, Desenvolvimento e Inovação (ID&I) para identificar de uma forma mais clara as oportunidades e os desafios à cibersegurança, colocados pelas tecnologias disruptivas e redes emergentes, acelerando a adoção de soluções capazes de enfrentar o seu futuro impacto no ambiente de segurança internacional;
- promover a adoção de soluções de cibersegurança escaláveis, capazes de acelerar a adoção das melhores práticas e aumentar a ciberresiliência nacional.

Alicerçada nos objetivos e nas prioridades políticas enunciadas, de alcance nacional e internacional, a formulação de uma visão estratégica nacional para o ciberespaço, definida na sua dimensão estrutural, operacional e genética, oferecerá as ferramentas e permitirá identificar as medidas a adotar ao longo dos próximos anos. A implementação desta visão estratégica, articulada nas suas três dimensões, dependerá muito da capacidade nacional para congregar esforços e gerar uma atuação concertada por parte das várias entidades que contribuem para a cibersegurança e ciberdefesa do Estado.

7 CONCLUSÕES

Na formulação de uma visão político-estratégica para o ciberespaço, surgem descontinuidades, desafios emergentes e sinais de uma alteração substantiva

do ambiente de segurança internacional. Neste contexto, importa compreender a influência do ciberespaço, contextualizando o seu papel transformador das organizações e sociedades do futuro, projetando possíveis cenários de evolução competitiva e de confrontação.

À medida que a tecnologia se torna cada vez mais central na condução dos conflitos da era moderna, a fronteira entre a sua dimensão militar e civil tem vindo a diluir-se. Esta situação, oferecendo uma vantagem estratégica aos atores que detenham uma vantagem/supremacia tecnológica poderá contribuir para estimular a ocorrência de novos conflitos ou mesmo até originar a sua proliferação.

Vivemos num mundo volátil, incerto, complexo e ambíguo, onde a confrontação estratégica evidencia a transição de uma lógica simétrica para um contexto dissimétrico e cada vez mais híbrido. Os ciberataques apresentam um potencial disruptivo elevado, suscetível de originar a fragmentação digital das sociedades, ameaçando a sua resiliência, estabilidade económica e a coesão social. Esta evolução do espetro da ameaça, compromete a afirmação de uma agenda digital e a utilização livre e segura do ciberespaço.

Num mundo em rede, a segurança da informação e o ciberespaço não só adquirem uma importância estratégica acrescida como constituem também um fator essencial para a sobrevivência dos Estados. Uma continua observação do horizonte estratégico permitirá aos diversos atores, Estado e não-Estado, a possibilidade de agir com vantagem e gerar valor, a tempo de mitigar as vulnerabilidades e aproveitar as oportunidades.

Portugal enfrenta hoje o desafio de aprofundar o seu esforço de digitalização e abraçar os desafios da transformação digital, integrando e compatibilizando as escolhas tecnológicas de uma sociedade da era da informação com a segurança do ciberespaço. Consubstanciando-se neste domínio global sérios riscos para a salvaguarda dos interesses e para a defesa da soberania nacional, esta realidade não pode ser dissociada da necessidade de ajustamento permanente das políticas de defesa à envolvente estratégica e ao desenvolvimento de novos processos e capacidades.

O ecossistema digital nacional, permanentemente ligado ao ciberespaço, desempenha também um papel relevante para a cibersegurança da UE, para a ciberdefesa NATO e até para a cibersegurança global. Esta articulação e interdependência, impõe a Portugal a necessidade de honrar os compromissos políticos assumidos no quadro das organizações internacionais a que pertence, garantindo o alinhamento estratégico necessário para assegurar a segurança cooperativa e a defesa coletiva no ciberespaço, afirmando-se como parceiro relevante, num esforço conjunto destinado a assegurar a estabilidade do ambiente de segurança internacional. Tal exige a definição de políticas consistentes e estratégias coerentes com esta realidade, assentes numa edificação de capacidades credível.

Tanto ao nível da conceptualização como da operacionalização, Portugal tem vindo a amadurecer a sua visão estratégica para o ciberespaço. No entanto, face aos atuais e futuros desafios da segurança e defesa nacional, promovendo uma visão estratégica integrada para o ciberespaço, importa restabelecer e alargar o conceito de resiliência nacional, clarificar o enquadramento político e o papel a desempenhar pela defesa na gestão de crises no ciberespaço, reforçando a estrutura e acelerando o desenvolvimento da capacidade de ciberdefesa das Forças Armadas. Estes imperativos, contrariando a adoção de uma abordagem estratégica errática, exigem uma política de defesa para o ciberespaço, estruturada e afirmativa, evitando assim que a consecução dos objetivos políticos formulados seja perspetivada sem a existência de uma estratégia coerente e sem um plano de ação consistente, articulado nos seus domínios operacional, estrutural e genético.

O ciberespaço, materializa um domínio de exercício de cidadania, afirmação de valores, defesa de interesses e soberania nacional. Atendendo aos objetivos políticos traçados, às melhores práticas e aos projetos já em curso, tanto no plano nacional como internacional, num momento em que se perspetiva a revisão do conceito estratégico de defesa nacional, definido em 2013, as políticas de segurança e defesa nacional não podem deixar de integrar esta realidade. O futuro começa agora …

REFERÊNCIAS

EUROPEAN UNION-NORTH ATLANTIC TREATY ORGANISATION. Statement on the implementation of the Joint EU-NATO Declaration [Página *online*]. Disponível em: https://www.nato.int/cps/en/natohq/official_texts_138829.htm. Acesso em: 17 jul. 2021.

FREIRE, F.; NUNES, P.; ACOSTA, O. *Estratégia da Informação e Segurança do Ciberespaço*, trabalho de investigação conjunta (IDN-CESEDEN), IDN Nº12, Imprensa Nacional – Casa da Moeda, 2013.

NORTH ATLANTIC TREATY ORGANIZATION. (2010). NATO Strategic Concept 2010 [Página *online*]. Disponível em: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/ 20120214_strategic-concept-2010-eng.pdf Acesso em: 14 maio 2020.

NORTH ATLANTIC TREATY ORGANIZATION. *Walles Summit Declaration Press Release* 2014-120. [Página *online*]. Disponível em: https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en. Acesso em: 25 jul. 2021
NORTH ATLANTIC TREATY ORGANIZATION. *Enhanced NATO Policy on Cyber Defence* (Decisão PO/2014/0358). Bruxelas: Emergency Security Challenge Division, 2014b.

NORTH ATLANTIC TREATY ORGANIZATION. *Cyber Defence Pledge*. NATO Warsaw Summit Press Release (Comunicado 124). Bruxelas: NATO Allied Council, 2016a.

NORTH ATLANTIC TREATY ORGANIZATION. *Military Vision and Strategy on Cyberspace as a Domain of Operations* (Decisão de 12 de junho). Bruxelas: Military Committee, 2018.

NORTH ATLANTIC TREATY ORGANIZATION. London Declaration Press Release, 2019. Acesso em: 28 out. 2020. [Página *online*]. Retirado de Sistema Integrado de Redes de Emergência e Segurança de Portugal. Disponível em: https://www.nato.int/cps/en/natohq/official_texts_171584.htm. Acesso em: 25 jul. 2021.

NORTH ATLANTIC TREATY ORGANIZATION. Brussels Declaration Press Release, 2021a. [Página *online*]. Disponível em: https://www.nato.int/cps/en/natohq/news_185000.htm. Acesso em: 25 jul. 2021.

NORTH ATLANTIC TREATY ORGANIZATION. NATO 2030 Agenda Fact Sheet, 2021b. [Página *online*]. Retirado de: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf. Acesso em: 25 jul. 2021

NORTH ATLANTIC TREATY ORGANIZATION. NATO sharpens technological edge with innovation initiatives, 2022. [Página *online*]. Disponível em: https://www.nato.int/cps/en/natohq/news_194587.htm#:~:text=NATO%20Allies%20are%20launching%20a,the%20North%20Atlantic%20%E2%80%93%20or%20DIANA.

NUNES, P. F.V. (Coord.). *Contributos para uma Estratégia Nacional de Ciberdefesa.* IDN Cadernos, 28. Lisboa: Instituto da Defesa Nacional, 2018.

NUNES, P. F.V. *A Edificação da Capacidade de Ciberdefesa Nacional:* Contributos para a Definição de uma Estratégia Militar para o Ciberespaço. Coleção "ARES"*, 36. Lisboa: Instituto Universitário Militar, 2020*.

PORTUGAL. Conselho Superior de Defesa Nacional (2014). *Conceito Estratégico Militar,* Lisboa, 2014. Retirado de https://www.fd.unl.pt/docentes_docs/ma/FPG_MA_27255.pdf. Acesso em: 20 jan. 2022.

PORTUGAL. Decreto-Lei n.º 69/2014, de 09 de maio (2014). Cria o Centro Nacional de Cibersegurança *(CNCS)*. *Diário da República*, 1.ª Série, 89, 2712-2719. Lisboa: Presidência do Conselho de Ministros, 2014.

PORTUGAL. Estado-Maior-General das Forças Armadas. *Diretiva Estratégica do EMGFA 2018-2021*, de 18 abril de 2018. Lisboa: Chefe do Estado-Maior-General das Forças Armadas, 2018.

PORTUGAL. Estado-Maior-General das Forças Armadas. *Relatório do Estudo de Desenvolvimento da Capacidade de Ciberdefesa*. Lisboa: Grupo de Trabalho-Capacidade Ciberdefesa das FFAA, 2019a.

PORTUGAL. Lei Orgânica n.º 02/2019, de 17 de junho (2019). *Aprova a Lei de Programação Militar* (LPM) e revoga a Lei Orgânica n.º 7/2015. Diário da República, 1.ª Série, 114, 2982-2985. Lisboa: Assembleia da República, 2019.

PORTUGAL. Lei Orgânica n.º 46/2018, de 13 de agosto (2018). *Aprova o Regime Jurídico da Segurança do Ciberespaço*. Diário da República, 1.ª Série-A, 155, 4031-4037. Lisboa: Assembleia da República.

PORTUGAL. Ministério da Defesa Nacional. *Orientação para a Política de Ciberdefesa* (Despacho n.º 13692/MDN, de 11 de outubro). Lisboa: Ministro da Defesa Nacional, 2013. Acesso em: 8 abr. 2021

PORTUGAL. Ministério da Defesa Nacional. *Diretiva Ministerial de Orientação Política para o Investimento na Defesa* (Despacho n.º 4103/MDN, de 12 de abril). Lisboa: Ministro da Defesa Nacional, 2018. Acesso em: 4 fev. 2021.

PORTUGAL. Ministério da Defesa Nacional. *Proposta de Estratégia Nacional de Ciberdefesa* Lisboa: Direção-Geral de Recursos da Defesa Nacional, 2019a. Acesso: 3 fev. 2021

PORTUGAL. Ministério da Defesa Nacional. *Linhas Orientadoras para a Estratégia Nacional de Ciberdefesa-Horizonte 2019-23* (Despacho n.º 52/MDN, de 23 de outubro). Lisboa: Ministro da Defesa Nacional, 2019b. Acesso em: 14 maio 2020.

PORTUGAL. Ministério da Defesa Nacional. *Diretiva Ministerial de Planeamento de Defesa Militar* (Despacho n.º 2536/MDN, de 24 de fevereiro). Lisboa: Ministro da Defesa Nacional, 2020a. Acesso em: 16 maio 2020.

PORTUGAL. Ministério da Defesa Nacional. *Criação do Comité de Monitorização da Ciberdefesa* (Despacho n.º 15/2020, de 06 de fevereiro). Lisboa: Ministro da Defesa Nacional, 2020b. Acesso em: 29 maio 2020.

PORTUGAL. Resolução da Assembleia da República n.º 15/2005, de 07 de abril. Aprova a VII Revisão Constitucional da Constituição aprovada pela Assembleia Constituinte, 02 de abril de 1976. *Diário da República,* 1.ª Série, 74, 2979-2979. Lisboa: Assembleia da República, 2005.

PORTUGAL. Resolução do Conselho de Ministros n.º 115/2017, de 13 de julho de 2017. Cria o grupo de projeto denominado "Conselho Superior de Segurança do Ciberespaço". *Diário da República*, 1.ª Série, 163/2017, 5035 – 5037. Lisboa: Presidência do Conselho de Ministros, 2017.

PORTUGAL. Estado-Maior-General das Forças Armadas. *Proposta de Estratégia Nacional para a Ciberdefesa 2019-2023.* Lisboa: Grupo de Trabalho-Capacidade Ciberdefesa das FFAA, [2020)].

PORTUGAL. Resolução do Conselho de Ministros n.º 19/2013, de 21 de março. (2013). Aprova o Conceito Estratégico de Defesa Nacional. *Diário da República*, 1.ª Série, 67, 1981–1995. Lisboa: Presidência do Conselho de Ministros.

PORTUGAL. Resolução do Conselho de Ministros n.º 26/2013, de 11 de abril. Aprova a reforma "Defesa 2020". *Diário da República*, 1.ª Série, 77, 2285–2289. Lisboa: Presidência do Conselho de Ministros, 2013.

PORTUGAL. Resolução do Conselho de Ministros n.º 92/2019, de 05 de junho. *Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. Diário da República, 1ª Série, 108, 2888–2895. Lisboa: Presidência do Conselho de Ministros, 2019.

UNIÃO EUROPEIA. (2009). *EU Concept for Computer Network Operations in EU-led Military Operations* (Decisão EEAS13537/09). Bruxelas: European Union Military Staff, 2009.

UNIÃO EUROPEIA. *EU Concept for Cyber Defence for EU-led Military Operations* (Decisão EEAS01729/12). Bruxelas: European Council, 2012.

UNIÃO EUROPEIA. *EU Cyber Diplomacy Toolbox* [Página *online*]. 2017. Disponível em:http://data.consilium.europa.eu/doc/document/ST-7923-2017-REV-2/en/pdf. Acesso em: 25 jun. 2021.

UNIÃO EUROPEIA. *EU restrictive measures against cyber-attacks threatening the Union or its Member States* (Decisão ST/7299/2019/INIT), 2019. [Página *online*]. Disponível em: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32019D0797. Acesso em: 16 maio 2021.

UNIÃO EUROPEIA. Implementação do Decreto Regulamentar EU 2020/1124 - imposição de medidas restritivas, 2020a. [Página *online*]. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2020:246:FULL&from=EN. Acesso em: 16 maio 2021.

UNIÃO EUROPEIA. Estratégia de Segurança Europeia, 2020b. [Página *online*]. Retirado de:https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en. Acesso em: 16 maio 2021.

UNIÃO EUROPEIA. Estratégia de Cibersegurança da União Europeia, 2020c. [Página *online*]. Disponível em: https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy. Acesso em: 16 maio 2021.

UNIÃO EUROPEIA. *Shaping Europe's digital future*, 2020d. [Página online]. Retirado de https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273. Acesso em: 10 ago. 2021.

UNIÃO EUROPEIA. Recovery plan for Europe, 2020e. [Página online]. Disponível em: https://ec.europa.eu/info/strategy/recovery-plan-europe_en.

UNIÃO EUROPEIA. (2020f). *The Directive on security of network and information systems (NIS Directive)* [Página online]. Disponível em: https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive.

UNIÃO EUROPEIA. (2020g). *Migration and Home Affairs – EU Protection* [Página online]. Disponível em: https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/protection_en.

UNIÃO EUROPEIA. Bússola Estratégica para a Segurança e a Defesa da EU, 2022 [Página online]. Disponível em: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/pt/pdf.

ANEXO A

ÁREAS DE COOPERAÇÃO ESTRATÉGICA NACIONAL NO CIBERESPAÇO

Áreas Comuns de Cooperação Estratégica Internacional no Ciberespaço	Linhas de Desenvolvimento	NATO	UE	ONU	OCDE	Relevância Estratégica	Relevância Operacional	Relevância Económica/ Industrial	Área Nova?
Documentos Estratégicos (de Referência)		• Conceito Estratégico (2010) • Enhanced Policy on Cyber Defence (2014) • Conclusões da Cimeira de Gales (2014) • Conclusões da Cimeira de Varsóvia (2016) • Cyber Defence Pledge (2016) • Declaração Conjunta NATO-EU (06Dez16) • Efeitos Operacionais disponibilizados por Nações Aliadas (2018) • Agenda NATO 2030 (2022)	• Agenda Digital para a Europa (2010-20) • Estratégia de Segurança Global (2016) • Declaração Conjunta NATO-EU (06Dez16) • Cyber Diplomacy Toolbox (2017) • Diretiva NIS (2016) e sua revisão (2020) • Estratégia de Segurança Europeia (2020) • Estratégia de Cibersegurança Europeia (2020) • Digital Act (2021) • Bússola Estratégica da UE (2022)	• Carta das Nações Unidas (1945) • Tratado Internacional das Telecomunicações (2012) • Plano para a Cooperação Digital (2020) • Painel para a Cooperação Digital – The Age of Digital Interdependence (2020).	• Guidelines Seg SI e Redes (2002) • Recomendação Coop Internacional na Lei Proteção Privacidade (2007) • "Managing Digital Security and Privacy Risk" (2016) • Digital Economy Outlook (2017) • Digital Security Risk management for Economic and Social Prosperity (2018)	E- Elevada; M – Média; B - Baixa			S-Sim; N-Não
Defesa Coletiva	Cibersegurança/ Ciberdefesa	• Ciberdefesa (área prioritária) e 4º Domínio Operacional da Guerra	• Cibersegurança (área prioritária)	• Cibersegurança/e-Governance (área prioritária)	• Cibersegurança (área estruturante economia global)	E	E	E	S
	Combate ao Terrorismo	• Combate ao Terrorismo (área prioritária)	• Combate ao Cibercrime em geral (área prioritária)	• Regulação do Ciberespaço (área prioritária)	• Combate ao Cibercrime e Privacidade (área prioritária)	E	E	B	N
	Proteção Infraestruturas Críticas	• Segurança Energética (área prioritária)	• Proteção das Infraestruturas Críticas de Informação (área prioritária)	• Contenção de Ataques de larga escala (área prioritária)	• Proteção SI e Redes (área prioritária)	E	E	M	S
	Impacto das novas Tecnologias	• Análise das Tecnologias Emergentes (área prioritária)	• Análise das Tecnologias Emergentes (área prioritária)	• e-Governance e Normalização (área prioritária)	• Monitorização impacto económico das TIC (área prioritária)	E	E	E	N
Gestão de Crises	Cooperação Civil-Militar	• Aproximação Civil-Militar (Comprehensive Approach)	• Aproximação Civil-Militar (Comprehensive Approach)	• Cooperação Política	• Cooperação Político-Económica	E	E	M	S
	Compreensão do Ambiente Internacional	• Monitorização/Análise do Ambiente Internacional e Ameaças Híbridas	• Monitorização/Análise do Ambiente Internacional	• Monitorização do Ambiente Internacional	• Monitorização de Mercados e Economia Global	E	E	M	N
	Partilha de Informações (Intelligence Sharing)	• Melhoria da partilha de informações	• Melhoria da partilha de Informações	• Troca de informação em fora especializado	• Troca de informação em fora especializado	E	E	M	N
Segurança Cooperativa	Segurança e Defesa	• UE e Rússia	• NATO	• Cooperação Internacional	• Cooperação Internacional e Desenvolvimento	E	E	M	N
	Cibersegurança/ Ciberdefesa	• UE	• NATO, USA, China e Índia	• Cooperação Internacional	• Cooperação Internacional e Desenvolvimento	E	E	M	S

Desenvolvimento de Capacidades Cooperativas área da Cibersegurança/ Ciberdefesa		• Iniciativas de Smart Defence MNCDE&T-Portugal Lead POC:Information Assurance and Cyber Defence Capability Panel (CaP4 IACD); • Projeto DIANA (2021).	• Projetos PESCO; Financiamento FED Iniciativas de Polling&Sharing Cyber Defence Training and Exercises Platform (CDTEXP) – Portugal Lead Nation POC: ENISA e Project Team Cy Defence (PT CD) - EDA.	• Tratados Internacionais • Global Cybersecurity Agenda (GCA), da ITU.	• Recomendações e Guidelines POC: Working Party On Information Security And Privacy, da OCDE.	E	E	E	S
	Doutrina e Organização	• Política, Plano de Ação e Conceito de Ciberdefesa NATO, como ref[a]. • Partilha de informação e melhores práticas; • Cyber Pledge (Cimeira de Varsóvia, 2016); • Cyber Operations Center (2018).	• Cyber Defence Discipline (Lead Nations PT e FR) • Conceito de Computer Network Operations e Conceito de Ciberdefesa da UE, como ref[a]. • Partilha de informação e melhores práticas; • Joint Cyber Unit (2020)	• Princípios de regulação e cooperação no ciberespaço. • Partilha de informação e melhores práticas	• Recomendações e orientações. • Partilha de informação e melhores práticas	E	E	M	S
	Interoperabilidade	• Sinergias civis/ militares e cooperação com a comunidade de cibersegurança civil. Ex: NATO Crypto Interoperability Strategy (cooperação NATO-EU); NATO PKI; NATO Common Criteria CaT. • Declaração Conjunta NATO-EU (06Dez2016)	• Desenvolvimento, na área da cibersegurança, de uma rede europeia de CERTs (Ex:ENISA). • Na área da ciberdefesa, exploração de sinergias civis/militares e cooperação com a comunidade de cibersegurança civil. • Declaração Conjunta NATO-EU (06Dez2016)	• Adoção de políticas, princípios de normalização e requisitos técnicos	• Adoção de políticas, princípios de normalização e requisitos técnicos.	E	E	E	N
	Instalações	• Desenvolvimento partilhado de novas áreas para treino e exercícios de ciberdefesa; • Cyber Range (Estónia); • Cyber Lab na NCI Academy (Oeiras)	• Desenvolvimento partilhado de novas áreas para treino e exercícios de ciberdefesa;	• Desenvolvimento de centros especializados para cooperação internacional	• Desenvolvimento de centros especializados para cooperação internacional	E	E	B	N
	Liderança e Pessoal	• Campanhas coordenadas de sensibilização e formação na área da ciberdefesa;	• Campanhas coordenadas de sensibilização e formação na área da Cibersegurança;	• Campanhas coordenadas de sensibilização e formação na área da Cibersegurança	• Campanhas de sensibilização na área da cibersegurança;	E	E	B	N
	Material e Tecnologia	• Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum. Ex: Multinational Cyber Defence Capability Development (MNCD2); NATO Information Assurance Product Catalogue (NIAPC); • Pool de capacidades ciberdefesa apoio às operações NATO; • Projeto DIANA- Acelerador de Inovação (Alfeite) e Centro de Testes (Tróia).	• Criação de Centros de Competências Digitais e Innovation Hubs – CAIH (liderança nacional) • Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum. • Pool de capacidades de ciberdefesa para Quartéis-Generais de nível Operacional e Tático (OHQ/FHQ)	• Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum.	• Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum.	E	E	E	S
	Treino e Exercícios	• Pooling de recursos de treino/ educação; • Partilha de informação sobre ameaças e incidentes em contexto operacional de ciberdefesa para apoio de missões NATO (POC: NCIRC). • Declaração Conjunta NATO-EU (06Dez2016) • Exercício NATO Cyber Coalition (POC ACT).	• Pooling de recursos de treino/educação (e.g. CDTEXP); • Partilha de informação sobre ameaças e incidentes de cibersegurança (POC ENISA) e ciberdefesa (POC EUMS) para apoio de missões de segurança e defesa da UE (missões CSDP). • Declaração Conjunta NATO-EU (06Dez2016) • Exercício Cyber Europe.	• Pooling de recursos de treino/educação existentes;	• Nada a referir.	E	E	B	S

Fonte: FREIRE, NUNES, ACOSTA, 2013 (Adaptado).

LA CIBERSEGURIDAD EN EL ÂMBITO DE LA DEFENSA NACIONAL

María José Viega Rodríguez*

RESUMEN
Uruguay ha adoptado en su Ley N° 18.650 de Defensa Nacional un concepto amplio de ésta, comprendiendo tanto las acciones civiles como militares. El ciberespacio, considerado como el quinto ámbito de la Defensa Nacional, está previsto en el Decreto N° 371/020, así como las amenazas que pueden suscitarse dentro de éste. La ciberseguridad se encuentra contemplada en el Objetivo X de la Agenda Uruguay Digital 2025, aprobada por el Decreto N° 134/021 y su ecosistema está coordinado por la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC).
Palabras Clave: Ciberseguridad; ciberespacio; amenazas; Defensa Nacional; Uruguay.

A CIBERSEGURANÇA NO ÂMBITO DA DEFESA NACIONAL

RESUMO
O Uruguai adotou em sua Lei N° 18.650 de Defesa Nacional um conceito amplo sobre o assunto, compreendendo tanto as ações civís como as militares. O ciberespaço, considerado o quinto âmbito da Defesa Nacional, está previsto no Decreto N° 371/020, assim como as ameaças que podem surgir dentro desse campo. A cibersegurança se encontra contemplada no objetivo X da Agenda Uruguai Digital 2025, aprovada pelo Decreto N° 134/021 e seu ecossistema está coordenado pela Agência de Governo Eletrônico e Sociedade da Informação e Conhecimento (AGESIC).
Palavras-chave: cibersegurança; ciberespaço, ameaças, Defesa Nacional, Uruguai.

1 INTRODUCCIÓN

Uruguay aprobó la Ley de Defensa Nacional N° 18.650 el 19 de febrero de 2010, constituyendo el Marco para la Defensa Nacional de la República. El artículo 1° establece que:

* Doctora en Derecho y Ciencias Sociales y Escribana Pública por la Universidad Mayor de la República Oriental del Uruguay (UDELAR). Profesora de Informática Jurídica y Derecho Informático en la UDELAR. Gerente de la División Derecho Informático en AGESIC. Profesora de Derecho Informático en el Máster de Seguridad de la Información de la Facultad de Ingeniería (UDELAR). Profesora de Ética y Legislación en ORT. Posgrado de Derecho Informático: Contratos Informáticos, Contratos Telemáticos y Outsourcing en la Universidad de Buenos Aires. Experta Universitaria en Protección de Datos, UNED (ESPAÑA). Experta Universitaria en Administración electrónica, Universidad Oberta de Cataluña (España). Cursando Posgrado en Inteligencia Estratégica y la Maestría en Defensa Nacional en CALEN. Contacto: mjviega@gmail.com

> La Defensa Nacional comprende el conjunto de actividades civiles y militares dirigidas a preservar la soberanía y la independencia de nuestro país, a conservar la integridad del territorio y de sus recursos estratégicos, así como la paz de la República, en el marco de la Constitución y las leyes; contribuyendo a generar las condiciones para el bienestar social, presente y futuro de la población. (URUGUAY, 2010, p. 1).

La ley ha adoptado un concepto amplio de la Defensa Nacional, comprendiendo tanto acciones de carácter civil como militar, e implica la conservación de la integridad de su territorio. Complementariamente el artículo 2° establece que la Defensa Nacional constituye un derecho y un deber para la ciudadanía en su conjunto, constituyendo una función del Estado, que a su vez la caracteriza como permanente, indelegable e integral.

A su vez la Ley N° 19.775 de 26 de julio de 2019, Ley Orgánica de las Fuerzas Armadas, en el artículo 8° inciso primero establece:

> El ámbito espacial del Estado comprende el territorio continental e insular, incluyendo el subsuelo y las aguas jurisdiccionales, así como el espacio aéreo correspondiente a dichas zonas". Y en su inciso segundo se consigna a texto expreso al ciberespacio, cuando menciona: el ámbito espacial del Estado incluye al ciberespacio y al espectro electromagnético. (URUGUAY, 2019).

Por otra parte, el Decreto N° 371/020 de 23 de diciembre de 2020 que actualizó la Política de Defensa Nacional, considera dentro de las amenazas; la violación de nuestra soberanía terrestre, marítima, aeroespacial y del ciberespacio, considerando a los ciberataques como una amenaza que puede suscitarse dentro de éste. Por tal motivo, la ciberseguridad se encuentra contemplada en el Objetivo X de la Agenda Uruguay Digital 2025, aprobada por el Decreto N° 134/021 de 4 de mayo de 2021 y su ecosistema está coordinado por la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC).

Dentro del Ministerio de Defensa Nacional se encuentra el Equipo de Respuesta a Incidentes de Seguridad Informática de Defensa (D-CSIRT). En el ámbito civil, en el área pública, la Dirección de Seguridad de AGESIC que coordina al Centro Nacional de Respuestas de Incidentes de Seguridad Informática (CERTuy) y al Centro de Operaciones en Ciberseguridad (SOC), y también se cuenta con el CSIRT de la Administración Nacional de Telecomunicaciones (ANTEL). En el ámbito privado vamos a encontrar los sistemas de ciberseguridad de las empresas y organizaciones privadas, como por ejemplo los sistemas de los bancos.

2 CONCEPTUALIZACIÓN DE LA CIBERSEGURIDAD

El ciberespacio, conceptualizado en sus orígenes como "el lugar sin lugar", en el cual se creía que se podría realizar cualquier tipo de acción sin consecuencias, a lo largo de los años se ha ido demostrando que no es así. Si bien los temas de la ley aplicable y la jurisdicción competente no dejan de ser una cuestión desafiante, aún hoy, es posible implementar diferentes medidas, frente a las amenazas que sobrevienen en éste.

El ciberespacio se define como el espacio virtual que se origina al procesarse, comunicarse y almacenarse información digital por sistemas informáticos (CAMPS, 2022). La ciberseguridad se enmarca en un concepto más amplio que es la seguridad de la información. Esta última puede ser definida como el conjunto de medidas preventivas y reactivas tendientes a resguardar la información buscando mantener su confidencialidad, disponibilidad e integridad. En ese sentido se prioriza asegurar el uso de las redes y sistemas informáticos propios y negarlo a terceros (CAMPS, 2022).

La importancia de la ciberseguridad crece día a día. El aumento en la utilización de las tecnologías de la información y la comunicación (TIC's) como consecuencia de la pandemia incrementó exponencialmente los delitos informáticos. Así mismo su uso en fines militares en el marco de los conflictos internacionales es cada vez más frecuente, por ejemplo, los diferentes ciberataques en la guerra Rusia – Ucrania.

En el ciberespacio han desaparecido las fronteras físicas, es difícil conocer el origen de un ataque, así como quien lo ha ordenado, por lo que tener una estrategia clara sobre este ámbito es de fundamental importancia. Yuval Noah Harari reflexiona acerca de este punto en los siguientes términos:

> Pero si ahora Estados Unidos ataca a un país con capacidades para la ciberguerra, incluso moderadas, la contienda podría trasladarse a California o Illinois en cuestión de minutos. Programas malignos y bombas lógicas podrían interrumpir el tráfico aéreo en Dallas, hacer que chocaran trenes en Filadelfia y provocar la caída de la red eléctrica de Michigan. En la gran época de los conquistadores, la guerra era un asunto de daños reducidos y grandes beneficios. En la batalla de Hastings, en 1066, Guillermo el Conquistador se hizo con toda Inglaterra en un solo día al precio de apenas unos pocos miles de muertos. Por el contrario, las armas nucleares y la ciberguerra son tecnologías de daños elevados y pocos beneficios. Se pueden emplear estas herramientas para destruir países enteros, pero en absoluto para construir imperios rentables. (HARARI, 2018, p. 201).

En nuestro país el Decreto N° 134/021 aprueba la Agenda Digital Uruguay 2025 y el Objetivo X refiere a Ciberseguridad, en el que se establece: "Incrementar la ciberseguridad para prevenir y mitigar riesgos en el ciberespacio y avanzar en el cumplimiento del marco nacional de ciberseguridad, basado en la cooperación público y privada, garantizando la disponibilidad de los activos críticos de información". Este objetivo se divide en tres aspectos, establecidos en los puntos:

> […] 46. Adoptar el Marco de Ciberseguridad en servicios, infraestructura y redes críticas para el país, otorgando mayor seguridad, estandarización y confianza a todos los actores del desarrollo digital.
> 47. Desarrollar e impulsar trayectorias de formación en ciberseguridad para el desarrollo de capacidades a través de la educación formal y no formal.
> 48. Mejorar la eficiencia en la detección y respuesta a incidentes cibernéticos, mediante la implementación de nuevas tecnologías que permitan aplicar análisis predictivos y automatización de respuestas, entre otras. (URUGUAY, 2021).

En este sentido, es de destacar que se ha venido trabajando, tanto en la elaboración del Marco de Ciberseguridad realizado por AGESIC, como en la Guía para su implementación. Asimismo, el CERTuy ha realizado muchas jornadas de capacitación, así como campañas de concientización para niños y adultos. La preocupación por la ciberseguridad se debe a que en las relaciones telemáticas que se dan hoy día en todos los ámbitos de la vida humana, las diferentes personas pueden ser tanto atacantes como víctimas. Camps señala esta realidad en los siguientes términos:

> En este medio, los atacantes pueden ser de alta complejidad patrocinados por Estados o empresas privadas, pueden venir de grupos organizados con fines terroristas o activistas, de organizaciones delictivas o de simples individuos. Pueden ser dirigidos o genéricos y atacar blancos gubernamentales, empresariales o particulares con objetivos dispares según el caso. Lo blanco y lo negro no son norma en este ciberespacio donde priman los grises y no es siempre fácil determinar si un ataque es un delito común, un acto terrorista o un ataque que puede afectar la seguridad nacional, y lo que es peor aún no siempre se puede identificar al atacante. (CAMPS, 2016, p. 265).

3 LA DEFENSA NACIONAL EN EL DERECHO URUGUAYO

Como ya hemos hecho mención, la Ley N° 18.650 establece en su artículo primero que la Defensa Nacional comprende actividades civiles y militares, que deben contribuir a generar condiciones para el bienestar social, presente y futuro

de la población. En este sentido, la Defensa Nacional tiene que generar bienestar. En el artículo 2° se hace referencia a la ciudadanía en su conjunto, no solamente al ámbito militar, constituyendo la Defensa Nacional un derecho y un deber de la ciudadanía. En este ámbito encontramos que defensa y seguridad son dos conceptos inseparables, la defensa es una acción, mientras que la seguridad es una condición.

En lo referente a la soberanía, no se hace mención expresamente en la Ley N° 18.650 al ciberespacio, pero es considerado en los Decretos que establecen la Política de Defensa Nacional para los períodos de gobierno, y en ellos, tanto en el Decreto N° 105/014, como en el Decreto N° 371/020, aunque lo hacen en un sentido diferente.

El Decreto N° 105/014 hace referencia al potencial de desarrollo de las nuevas tecnologías y la interconexión de las redes de comunicación,

> […] tornándose una cuestión central para la educación y la información". Considera que estas nuevas herramientas han introducido una nueva dimensión en el ámbito de la seguridad y la defensa, mencionando entre los desafíos actuales los delitos económicos e informáticos. Al plantearse el escenario futuro hace referencia al ciberespacio de la siguiente manera: "Las líneas de comunicaciones por las que discurren bienes, servicios e información, particularmente las aguas internacionales y el ciberespacio, se reconfigurarán. (URUGUAY, 2021).

Finalmente, dentro de los objetivos de la Defensa Nacional, concretamente en los de carácter estratégico, hace referencia a fortalecer la presencia del Estado en los espacios terrestres, marítimo y aéreo, no haciendo referencia al ciberespacio. Sí lo considera dentro de los obstáculos que podrían enfrentarse: la materialización y los ataques cibernéticos.

En cambio, en el Decreto N° 371/020, en el punto III (URUGUAY, 2021). *Situación regional*, aparece el ciberespacio como uno de los espacios de interés estratégico, junto al terrestre, marítimo y aeroespacial. Concordantemente en el punto IX. *Amenazas*, se consideran los ciberataques como una de las amenazas que afectaría la disponibilidad, integridad o la confidencialidad de la información digital.

Hace hincapié en que podrá tener efectos lógicos o físicos, dependiendo del sistema objeto del ataque. Tiene en cuenta también que las amenazas criminales y terroristas tradicionales pueden materializarse en esta modalidad. Como ya se hizo mención en la introducción, al referirnos al concepto de Defensa Nacional en sentido estricto, la Ley N° 19.775 en el artículo 8° inciso 2° considera al ciberespacio dentro del ámbito espacial del Estado.

4 INSTITUCIONES CON COMPETENCIA EN CIBERSEGURIDAD

Partiendo de las consideraciones anteriores, teniendo en cuenta el concepto amplio de Defensa Nacional, vamos a analizar la situación de la ciberseguridad en nuestro país. Para ello se hará un breve recorrido descriptivo de las distintas instituciones gubernamentales involucradas. En la esfera pública, la AGESIC coordina el ecosistema de Ciberseguridad, incluyendo al CSIRT en el ámbito del Ministerio de Defensa Nacional, como a los organismos de carácter civil.

La AGESIC fue creada por el artículo 72 de la Ley N° 17.930 de 19 de diciembre de 2006, y tiene el cometido de liderar la estrategia de gobierno electrónico en Uruguay. Desde los inicios se entendió que el proceso de incorporar tecnologías a las instituciones del Estado debía estar centrado en el ciudadano, siendo más eficiente y eficaz en el desarrollo de sus funciones. Con esa consigna se impulsó la Ley de Protección de Datos Personales y Acción de Habeas Data N° 18.331 de 11 de agosto de 2008, entendiendo que la interoperabilidad era uno de los pilares para el desarrollo del gobierno electrónico. Por lo tanto, la comunicación de datos personales de los ciudadanos entre los organismos debía dar garantías de privacidad, sin obstaculizar el objetivo de que las personas no fueran cadetes del Estado, sino que éste solucione internamente aquellos aspectos que faciliten el relacionamiento y permita un mejor desempeño de la función estatal.

Por otra parte, se promueve la confianza y la seguridad en el uso de las TIC's y con este objetivo se crea por el artículo 119 de la Ley N° 18.172 de 31 de agosto de 2007 el Consejo de Seguridad de la Información, para apoyar a AGESIC en este tema. El Consejo está integrado por representantes de los siguientes organismos: Prosecretaria de la Presidencia de la República, Ministerio de Defensa Nacional, Ministerio del Interior, Administración Nacional de Telecomunicaciones y Universidad de la República.

Además, el Decreto N° 452/009, de 28 de setiembre de 2009, reglamentó las competencias establecidas por el artículo 55 de la Ley N° 18.046 de 24 de octubre de 2006, en la redacción dada por el artículo 118 de la Ley N° 18.172 de 31 de agosto de 2007, por el que se confiere a la AGESIC las facultades para establecer medidas de seguridad que hagan confiable el uso de las tecnologías de la información, concibiendo y desarrollando una política nacional en temas de seguridad de la información, que permita la prevención, detección y respuesta frente a incidentes que puedan afectar los activos críticos del país.

Acorde a la normativa vigente el ecosistema está constituido de la siguiente forma (URUGUAY, 2009):

- CERTuy con competencias a nivel nacional.
- Centro de Operaciones en ciberseguridad (SOC), es un área dentro de la Dirección de Seguridad de la Información de AGESIC.

- CSIRT de ANTEL a nivel de seguridad en las telecomunicaciones.
- Delitos informáticos y la Unidad de Cibercrimen, en el Ministerio del Interior, con competencias en delitos informáticos en general la primera y en cibercrimen, en especial casos de hackeos la segunda.
- Programa Salud.uy, soportado desde el punto de vista técnico por AGESIC, el programa nuclea tanto a instituciones de salud públicas como privadas.
- En la Academia, encontramos el Servicio Central de Informática de la UDELAR (SeCIU), el cual posee entre sus cometidos administrar los nombres de dominio en Uruguay.

En el ámbito público, pero en la esfera del Ministerio de Defensa, y por lo tanto vinculado a la Defensa Nacional en sentido estricto, es decir la defensa militar encontramos el CSIRT-D, con el cometido de la ciberdefensa. En el ámbito privado, a modo de ejemplo, hallamos los sistemas se ciberseguridad de los bancos privados, los prestadores de servicios de ciberseguridad y los prestadores de servicios de Internet (ISP) privados.

4.1 CERTuy

Según el CERT/CC, un CSIRT es una organización responsable de recibir reportes de incidentes de seguridad, analizarlos y responderlos. Dado que CERT es un término protegido y registrado en Estados Unidos por el CERT-CC, en otros países los equipos suelen tener distintas denominaciones (URUGUAY, 2013):

- CSIRT (Computer Security Incident Response Team - Equipo de respuesta a incidentes de seguridad informática).
- IRT (Incident Response Team - Equipo de respuesta a incidentes).
- CIRT (ComputerIncident Response Team - Equipo de respuesta a incidentes informáticos).
- SERT (Security Emergency Response Team - Equipo de respuesta a emergencias de seguridad).
- ISIRT (Information Security Incident Response Team - Equipo de respuesta a incidentes de seguridad de la información),

El CERTuy es el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay y fue creado por el artículo 73 de la Ley N° 18.362 de 6 de octubre de 2008, con el objetivo de regular los activos de información críticos del Estado, de acuerdo con los criterios que sugiera el Consejo de Seguridad de la Información. Este artículo fue reglamentado por el Decreto N° 451/009 de 28 de setiembre de 2009,

regulando el funcionamiento, cometidos, potestades, obligaciones y organización del CERTuy. En el artículo 3° se definen aspectos como: activos de información, activos de información críticos del Estado, evento de seguridad informática, incidente de seguridad informática, servicios vitales para la operación del gobierno y la economía del país, y sistema informático (VARELA; HERNÁNDEZ, 2018).

El CERTuy está conformado por un grupo de expertos responsables del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Sus principales objetivos son: centralizar, coordinar y optimizar los procesos de respuesta a incidentes en seguridad de la información; difundir mejores prácticas en seguridad de la información y realizar tareas preventivas (URUGUAY, 2022).

4.2 CENTRO DE OPERACIONES DE CIBERSEGURIDAD (SOC)

El SOC tiene como objetivo principal detectar en tiempo real eventos e incidentes de ciberseguridad en los Activos de Información Críticos del Estado, colectar y analizar información de ciberseguridad para prevenir y detectar incidentes de ciberseguridad. En el Sitio web.gub.uy se detallan como cometidos sustantivos (URUGUAY, 2022):

- Asesorar en la definición de políticas, metodologías y buenas prácticas en operaciones de ciberseguridad.
- Monitorear los sistemas informáticos que soporten activos de información críticos del Estado, así como los sistemas circundantes a éstos.
- Operar infraestructura de ciberseguridad del Estado.
- Colectar y analizar información histórica de ciberseguridad.
- Coordinar espacios de relacionamiento de múltiples partes interesadas en ciberseguridad de Seguridad de la Información.
- Interactuar con CERTuy y otros CSIRT para intercambiar información y coordinar operaciones de ciberseguridad.
- Interactuar con otros SOC, locales e internacionales para el intercambio y procesamiento de información y alertas de ciberseguridad.

4.3 COMPUTER INCIDENT RESPONSE TEAM DE AGENCIA NACIONAL DE TELECOMUNICACIONES (CSIRT DE ANTEL)

Conforme a la información institucional suministrada por ANTEL:

> El CSIRT de ANTEL es un Centro de Respuesta a Incidentes orientado a nuestra Comunidad Objetivo, la cual está integrada por ANTEL (la corporación y subsidiarias) y los clientes de ANTEL.

> Cuando ocurren incidentes de seguridad, es crítico que nuestra comunidad tenga un modo efectivo y coordinado de responder. La velocidad con la cual la organización pueda reconocer, analizar y responder a un incidente de seguridad limitará los daños y disminuirá los costos de recuperación. El CSIRT de ANTEL tiene como servicio central realizar una gestión de incidentes de seguridad eficaz y eficiente. Para ello, sus integrantes buscan, en el contexto de su Código de Conducta, relacionarse con equipos pares y con su comunidad, capacitarse permanentemente, estar al día tecnológicamente y así mejorar de manera continua todos los servicios brindados. (URUGUAY, 2022).

El CSIRT de ANTEL realiza diferentes servicios URUGUAY, 2022):

- Reactivos: alertas y manejo de incidentes.
- Proactivos: anuncios, detección de incidentes y desarrollo de técnicas y herramientas.
- Valor Agregado: capacitación y entrenamiento, análisis de riesgo, consultoría en seguridad y concientización de la comunidad en temas de seguridad

4.4 DEPARTAMENTO DE DELITOS TECNOLÓGICOS Y UNIDAD DE CIBERCRIMEN - MINISTERIO DEL INTERIOR

El Decreto N° 94/2019 de 25 de marzo de 2019 reglamenta el artículo 93 de la Ley N° 19.670 de 15 de octubre de 2018 (URUGUAY, 2018), relativo a la creación de la Dirección de Investigaciones de la Policía Nacional. A esta Dirección le compete la dirección, supervisión técnico-estratégica y coordinación de la Dirección General de Lucha contra el Crimen Organizado e INTERPOL y es la encargada, de acuerdo con el artículo 2° inciso 4° de proteger a la República de, entre otros, la ciberdelincuencia.

Por lo tanto, el Departamento de delitos tecnológicos de la Jefatura de Montevideo integra la Dirección General de Lucha contra el Crimen Organizado e INTERPOL trabaja para combatir la delincuencia virtual, es decir los llamados delitos informáticos. La Unidad de Cibercrimen fue creada por Resolución del Ministro del Interior Luis Alberto Heber el 30 de agosto de 2021, la que funciona en la órbita de la Dirección de Investigaciones de la Policía Nacional. La unidad tendrá como principales cometidos:

> […] la detección, investigación, persecución y represión de las conductas y acciones antijurídicas de amenazas, hackeo, ataque

> o daño contra la seguridad, confidencialidad y la integridad de sistemas informáticos", detalla la resolución del Ministerio del Interior. Y agrega: "Actividades que busquen comprometer sistemas informáticos, bancos o bases de datos y redes, sabotaje y espionaje informático. (LORENZO, 2021, [202]).

4.5 PROGRAMA SALUD.UY

La AGESIC entendió prioritario abordar el área de la Salud –como uno de los desafíos del gobierno electrónico, con el fin de modernizar los procesos y viabilizar mejoras en la calidad de las prestaciones de salud recibidas por los usuarios del sistema. El Decreto N° 405/011 de 23 de noviembre de 2011, aprobó la Agenda Digital Uruguay 2011-2015, entre cuyos objetivos se encontraba la creación de redes avanzadas para la salud y una Historia Clínica Electrónica (HCE) integrada a nivel nacional, en el entendido que las Tecnologías de la Información y Comunicaciones tienen un gran potencial para la mejora de la gestión de los servicios de salud (VIEGA, 2021).

En el año 2012 se firmó un convenio para llevar adelante la estrategia, entre el Ministerio de Salud Pública (MSP), el Ministerio de Economía y Finanzas (MEF) y la AGESIC, creándose el Programa Salud.uy para implementar dicha iniciativa. El Programa está constituido por un Comité de Dirección, que comenzó a funcionar el 8 de marzo de 2013. Consta, además, de un Consejo Asesor representado por todos los actores del sistema, teniendo su primera reunión el 25 de junio de 2013. Han existido también diferentes grupos asesores especializados a lo largo del proyecto, con representantes de las principales áreas involucradas en cada caso (VIEGA, 2021).

En este ámbito, se creó la Historia Clínica Electrónica Nacional (HCEN), en el cual la Historia Clínica Electrónica funciona como un sistema federado entre los distintos prestadores de salud, el intercambio de información clínica se convierte en el principal desafío, desde los puntos de vista técnico y jurídico. Desde el aspecto técnico se creó la Red Salud y la Plataforma de Salud, como infraestructura segura que permitiera la conexión de los distintos prestadores, tanto públicos como privados, a los efectos de permitir subir la información y habilitar los accesos.

El artículo 12 del Decreto N° 242/2017 de 31 de agosto de 2017 refiere a la seguridad de las HCE, estableciendo que será responsabilidad de cada Institución dotar de los mecanismos y procedimientos de administración e identificación electrónica a quienes accedan a la HCE. Todo acceso a la HCE debe quedar debidamente registrado y disponible. La información no podrá ser alterada o eliminada sin que quede registrada la modificación de que se trate.

Además, cada prestador es responsable de la gestión de la seguridad de su información. Por tanto, cada prestador va a gestionar sus accesos. Es importante que la información sea confidencial, pero también que la información sea íntegra y que esté disponible cuando se necesite. El artículo 17 establece a texto expreso,

entre otras obligaciones de las instituciones, las de garantizar el acceso y adoptar medidas de seguridad.

Por el Decreto N° 122/019 de 29 de abril de 2019 se facultó a los usuarios del Sistema Nacional Integrado de Salud (SNIS), de forma tal que pudieran controlar los accesos a su HCE, a través de la plataforma. En este contexto, el artículo 2° reguló la seguridad en los procesos, disponiendo que las instituciones de salud, públicas y privadas, que interactúen con la plataforma de HCEN, así como las personas para la gestión de sus accesos y la consulta de su HCE, deberán encontrarse debidamente identificadas a través de los instrumentos establecidos en la Ley N° 18.600, de 21 setiembre de 2009 y sus modificativas.

El artículo 4° reguló la solicitud de acceso y estableció que en el caso que una Institución de salud, pública o privada, requiera acceder a la información disponible en la plataforma de HCEN, debe realizarlo mediante una identificación única (orden de servicio), la que será registrada en la plataforma. Las instituciones de salud deberán garantizar mediante mecanismos informáticos seguros la autenticación de las personas cuyo acceso autorizan. La normativa establece además que AGESIC podrá acceder a la HCEN con la finalidad de proporcionar soporte técnico.

4.6 SERVICIO CENTRAL DE INFORMÁTICA UNIVERSITARIA

El SeCIU es el Servicio Central de Informática Universitaria, perteneciente a la Universidad de la República (UDELAR), siendo el responsable de asesorar a las autoridades universitarias sobre esta temática, así como de desarrollar y gestionar la infraestructura informática de la UDELAR relacionada con los emprendimientos institucionales y de brindar asesoramiento y apoyo informático a todos los servicios universitarios. También es responsable de la administración del UY en Internet, y es por ello por lo que lo consideramos en el presente trabajo.

El Decreto N° 92/014 de 7 de abril de 2014 reglamenta el artículo 149 de la Ley N° 18719 relativo a la estandarización de los nombres de dominio de la Administración Central, para todos los servicios vinculados con Internet. El decreto pretende garantizar a los organismos y a los funcionarios correos electrónicos institucionales seguros, por lo que se establecen lineamientos mínimos se seguridad para su intercambio. También establece criterios de seguridad para los centros de datos, considerándolo un elemento fundamental para el desarrollo del gobierno electrónico. Establece que los activos críticos de información deberán encontrarse en centros de datos existentes en el territorio nacional.

4.7 RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE DEFENSA (D-CSIRT)

En el marco del Ministerio de Defensa Nacional se creó el D-CSIRTque es el Equipo de Respuesta a Incidentes de Seguridad Informática de Defensa, creado por el Decreto N° 36/015 de 27 de enero de 2015.

> Su creación representa la primera organización en el ámbito específico de la Defensa Nacional encargada de atender asuntos de ciberdefensa. La comunidad objetivo a la que dirige su acción son las organizaciones dependientes de dicho Ministerio, entre las que se encuentran las Fuerzas Armadas. El centro además de atender los incidentes comunes a cualquier organismo se especializará en los incidentes específicos en materia de Defensa que ocurrieran. (CAMPS, 2016).

El en Visto del Decreto N° 36/015 desataca: la importancia de prevenir, atender y gestionar incidentes de seguridad cibernética que se puedan presentar en el marco de la Defensa Nacional. A su vez establece que: "Su misión es la de participar de forma eficaz y eficiente en la respuesta a incidentes cibernéticos sobre infraestructuras críticas y servicios esenciales de la comunidad objetivo, así como desarrollar capacidades de prevención y detección temprana de incidentes de seguridad informática en dicha comunidad" (URUGUAY, 2022).

En los artículos 4° y 5° del Decreto se establecen los objetivos generales y los específicos, señalándose en el artículo 8° que los servicios que se prestarán serán de carácter reactivo y proactivo, los que se encuentran especificados en los artículos 9° y 10. Fuera de fronteras, el D-CSIRT, para cumplir con su cometido, integra igualmente con múltiples redes y equipos de respuestas como el Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (CAMPS, 2016).

5 CONCLUSIONES

El tema objeto del presente trabajo es relativamente nuevo, por ello, es fundamental conocer el estado actual de la estructura organizativa nacional creada para hacer frente a las amenazas de la ciberseguridad. En ese sentido, también adquiere especial relevancia la capacitación en este tema, en virtud de ello se destaca, además de las campañas mencionadas, realizadas por el CERTuy, la labor que realiza desde el año 2014 el Centro de Altos Estudios Nacionales (CALEN) brindando cursos de extensión en Ciberseguridad, estando además incluida la asignatura en la Maestría en Estrategia Nacional y en el Postgrado de Inteligencia Estratégica, concientizando y capacitando tanto a civiles con interés en la materia, como a militares y policías.

En términos relativos, dada la complejidad del fenómeno queda mucho por hacer. No obstante, en el Reporte 2020 de la OEA y el BID sobre Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe, se ubica a Uruguay en un lugar muy favorable. Este documento analiza la situación en que

se encuentran los diferentes países de América Latina y realiza una comparación con el estudio anterior elaborado en 2016. Luego analiza cada uno de los países, considerando diferentes aspectos (VIEGA, 2020). En ese sentido se destaca que:

> De acuerdo al informe Uruguay ha progresado en todas las dimensiones desde el 2016 -cuando se realizó el primer reporte de ciberseguridad- y se encuentra liderando en cuatro de las cinco dimensiones a nivel de América Latina y el Caribe: Política y Estrategia de Seguridad Cibernética, Cultura Cibernética y Sociedad, Formación, Capacitación y Habilidades de Seguridad Cibernética y Estándares, Organizaciones y Tecnologías. Asimismo, el país alcanza la máxima puntuación en temas referidos a la organización y coordinación de respuesta a incidentes; el desarrollo de la temática en el gobierno y la confianza de las personas en el uso de servicios de gobierno, entre otros. (CIBERSEGURIDAD, 2020).

En función del análisis normativo y de la estructura organizativa realizado en el presente documento, podemos concluir que Uruguay ha incluido dentro de su marco legal a las amenazas provenientes del ciberespacio y también se cuenta con un número importante de instituciones, tanto del ámbito civil como militar, con cometidos en ciberseguridad. Si bien el país debe fortalecer su estrategia de ciberseguridad a nivel nacional, se ha estructurado un marco de ciberseguridad basado en los estándares internacionales y se ha obtenido una evaluación positiva por parte de organismos internacionales que permite estar en mejores condiciones de dar respuestas a los incidentes que se produzcan.

REFERENCIAS

CAMPS, P. *Curso de Ciberdefensa y Ciberseguridad*, 9. Calen: [*S.n*.], 2022.

CAMPS, P. Estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias en este ámbito. *Ciberdefensa y ciberseguridad:* nuevas amenazas a la seguridad nacional. Rio de Janeiro: Escola Superior de Guerra, 2016.

CIBERSEGURIDAD: Uruguay lider en América Latina y el Caribe. *E-HealthReporter,* 30 jul. 2020. Disponible en: https://ehealthreporter.com/ciberseguridad-uruguay-lider-en-america-latina-y-el-caribe/Accedido en: 27 abr. 2022.

HARARI, Y. *21 lecciones para el siglo XXI*. Buenos Aires: Editorial Sudamericana, 2018.

LORENZO, G. Ministerio del Interior creó Unidad para combatir hackers. *El País*, Montevideo, 20 sept. 2021. Disponible en: https://www.elpais.com.uy/informacion/policiales/ministerio-interior-creo-unidad-combatir-hackers.html. Accedido en: 27 abr. 2022.

¿QUÉ hace el CSIRT de ANTEL? [Montevideo]: CSIRT ANTEL, 2022. Disponible en: https://www.csirt-antel.com.uy/que_hace.Accedido en: 27 abr. 2022.

URUGUAY. Centro Nacional de Respuesta a Incidentes de Seguridad informática. División Centro de Operaciones de Ciberseguridad (SOC). Montevideo: CERTuy, 2022. Disponible en: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/institucional/estructura-del-organismo/division-centro-operaciones-ciberseguridad-soc. Accedido en: 27 abr. 2022.

URUGUAY. Centro Nacional de Respuesta a Incidentes de Seguridad Informática.¿*Qué es el CERTuy*? Montevideo: CERTuy, 2013. Disponible en: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/publicaciones/que-es-el-CERTuy Accedido en: 27 abr. 2022.

URUGUAY. Decreto N° *452/2009*. Administración Publica. Política de Seguridad de La Información. Montevideo: IMPO, 2010. Disponible en: Accedido en: 29 mar. 2021.

URUGUAY. *Ley N° 18.650/2010*. Ley Marco de Defensa Nacional. Montevideo: IMPO, 2010. Disponible en: https://www.impo.com.uy/bases/decretos/452-2009. Accedido en: 29 mar. 2021.

URUGUAY. *Decreto nº 36/2015*. Creación del Centro de Respuesta a Incidentes de Seguridad Informática en el Ministerio de Defensa Nacional (D-CSIRT). Montevideo: IMPO, 2015. Disponible en: https://www.impo.com.uy/bases/decretos/36-2015. Accedido en: 29 mar. 2022.

URUGUAY. *Decreto nº 134/2021.* Aprobación de la agenda Uruguay Digital 2025. Montevideo: 2021. Disponible en: https://www.impo.com.uy/bases/decretos/134-2021%EF%BB%BF. Accedido en: 27 mar. 2022.

URUGUAY. *Decreto nº 371/2020*. Apruébase la propuesta de Política de Defensa Nacional formulada por el Consejo de Defensa Nacional (CODENA). Montevideo: IMPO, 2020. Disponible en: https://www.impo.com.uy/bases/decretos-originales/371-2020. Accedido en: 20 abr. 2022.

URUGUAY. *Ley nº 19775*. Modificación de la Ley Orgánica de Las Fuerzas Armadas. Montevideo: IMPO, 2019. Disponible en: https://www.impo.com.uy/bases/leyes/19775-2019/143. Accedido en: 22 abr. 2022.

URUGUAY. Ministerio de Defensa Nacional. *Equipo de Respuesta a Incidentes de Seguridad Informática de Defensa (D-CSIRT).* Montevideo: MD, 2015. Disponible en: https://www.gub.uy/ministerio-defensa-nacional/tramites-y-servicios/servicios/equipo-respuesta-incidentes-seguridad-informatica-defensa-d-csirt. Accedido en: 27 abr. 2022.

VARELA, M.; HERNÁNDEZ, M. *Derecho informático e informática jurídica II.* Montevideo: Fundación de Cultura Universitaria, 2018.

VIEGA, M. Ciberseguridad 2020 - Uruguay. *Derecho y Tecnologías*, 2020. 1 vídeo (9min). Disponible en: https://www.youtube.com/watch?v=ujdboeuyLD4&t=. Accedido en: 27 abr. 2022.

VIEGA. M. La Historia clínica electrónica nacional como infraestructura crítica. *Revista CADE*: doctrina y jurisprudencia, Montevideo, 2021.

VIEGA, M. La Historia clínica electrónica nacional en Uruguay: su desarrollo e impacto jurídico. *E-salud, autonomía y datos clínicos,* Madrid, p. 393-417, 2021.

PATROCÍNIO

APOIO

Esta revista foi impressa na gráfica da ESCOLA SUPERIOR DE GUERRA
Fortaleza de São João - Av. João Luís Alves, s/n - Urca - Rio de Janeiro - RJ
CEP 22291-090 - www.esg.br

Escola Superior de Guerra

Av. João Luís Alves, s/nº

Fortaleza de São João - Urca

22291-090 - Rio de Janeiro - RJ

www.esg.br - E-mail: revistadaesg@esg.br

ISBN: 978-65-00-48550-9