Ciberdefesa e Cibersegurança: Novas Ameaças à Segurança Nacional

Rio de Janeiro
2016

Ciberdefesa e Cibersegurança: Novas Ameaças à Segurança Nacional

Rio de Janeiro, 2016

Ciberdefesa e cibersegurança: novas ameaças à segurança nacional / Organizador José Cimar Rodrigues Pinto. Rio de Janeiro: ESG, 2016.

280 p.: il. - color.; 16,5 x 23 cm.
ISBN: 978-85-68649-03-9

1. Escola Superior de Guerra (Brasil) 2. Defesa Nacional 3. Segurança Nacional.

CDD 003-5

Endereço para correspondência
Av. João Luis Alves, s/nº - Fortaleza de São João
Urca - Rio de Janeiro - RJ

SUMÁRIO

REPÚBLICA FEDERATIVA DO BRASIL

A DEFESA CIBERNÉTICA COMO EXTENSÃO DO PAPEL CONSTITUCIONAL DAS FORÇAS ARMADAS NA DEFESA NACIONAL

Aristides Sebastião Lopes Carneiro

REPÚBLICA DO CHILE

CIBERESPACIO BIEN PÚBLICO MUNDIAL EN TIEMPOS DE GLOBALIZACIÓN: POLÍTICA PÚBLICA DE CIBERSEGURIDAD UNA NECESIDAD IMPERIOSA Y LA CIBERDEFENSA COMO DESAFÍO DEL SIGLO XXI

Carolina Sancho Hirane

REPÚBLICA DA COLÔMBIA

LINEAMIENTOS DE POLÍTICA EN CIBERSEGURIDAD Y CIBERDEFENSA: LOGRANDO LA SEGURIDAD Y DEFENSA DE COLOMBIA EN UN MUNDO DIGITAL

Martha Liliana Sánchez-Lozano
Steven Jones-Chaljub

REPÚBLICA DE EL SALVADOR

EL CIBERESPACIO Y LA SEGURIDAD NACIONAL EN EL SALVADOR

Roberto Artiga Chicas

REPÚBLICA DOMINICANA

CIBERDELINCUENCIA: DESAFÍOS PARA LA DEFENSA Y LA SEGURIDAD EN REPÚBLICA DOMINICANA

Francisco A. Ovalle Pichardo

REINO DA ESPANHA

EL MODELO DE CIBERSEGURIDAD Y CIBERDEFENSA EN ESPAÑA

Ángel Gómez de Ágreda

ESTADOS UNIDOS MEXICANOS

LA CIBERSEGURIDAD Y CIBERDEFENSA EN EL CONTEXTO DE MÉXICO

Jesús García García
Julio Cesar Mondragón Pérez

REPÚBLICA DO PERU

CIBERDEFENSA, CIBERSEGURIDAD Y ECONOMÍA

Roberto Vizcardo Benavides

REPÚBLICA DE PORTUGAL

CONTRIBUTO PARA O ESTUDO DA CIBERSEGURANÇA EM PORTUGAL

João Manuel Assis Barbas

REPÚBLICA ORIENTAL DO URUGUAI

CIBERDEFENSA Y CIBERSEGURIDAD: NUEVAS AMENAZAS A LA SEGURIDAD NACIONAL, ESTRUCTURAS NACIONALES DE CIBERDEFENSA, ESTRATEGIAS DE CIBERSEGURIDAD Y COOPERACIÓN INTERAGENCIAS EN ESTE ÁMBITO

Pablo Edgardo Camps Lasserre

Prefácio

Esta obra põe em destaque a cibersegurança e ciberdefesa e traduz o resultado de questionamentos que, literalmente, ultrapassam fronteiras, não somente por sua atualidade e importância, mas por seus efeitos amplos e disseminados que abarcam largos espaços da convivência humana e estatal, quais sejam: as possibilidades de interferência positivas e negativas sobre os ecúmenos planetários.

Não por acaso, foi um dos temas eleitos para serem abordados, sob o enfoque acadêmico, pelos Diretores de Colégios de Defesa Ibero-Americanos em sua última conferência, realizada em 2015, em Cartagena, na Colômbia, com o fito de estudar tal fenômeno em suas múltiplas manifestações em âmbito internacional e em suas consequências para as diversas entidades estatais.

A cibernética, juntamente com as descobertas nucleares e espaciais, inscreve-se entre os grandes eventos da esfera científica e tecnológica ocorridos após a Segunda Guerra Mundial. Os avanços advindos com o desenvolvimento das novas tecnologias de informação e comunicação, posteriormente potencializados pelo advento da internet, apresentaram efeitos mais tardios, mas não com menor magnitude, do que aqueles decorrentes dos progressos ocorridos naqueles outros dois campos da ciência. Entretanto, ao contrário delas, não recebeu o mesmo tratamento em termos de mecanismos de fiscalização e controle em níveis internacionais.

Trata-se de fenômeno que implica um desenvolvimento rápido, de difícil acompanhamento, difuso diante de suas aparências mutáveis, que torna mais complexa a identificação dos componentes que podem se converter em ameaças, mormente os desdobramentos dos efeitos sobre os indivíduos, as sociedades e os Estados. Ele, também, traz à baila o desafio que se impõe entre a liberdade individual e as necessidades da segurança e defesa, ou, por outro viés, entre privacidade e controle de ameaças.

Assim sendo, por decisão expressa no âmbito das representações ibero-americanas, foram convidados intelectuais dispostos a apresentar suas contribuições para o debate do tema, no ambiente dessa consequência, em que compartilharam suas ideias com o público em geral, resultando na edição desta obra. Fiéis aos princípios definidos na primeira conferência, os capítulos foram organizados, segundo os critérios de ordenação em ordem alfabética das nacionalidades participantes do evento.

O Tenente-Coronel Aristides Sebastião Lopes Carneiro explora, em *A Defesa Cibernética como extensão do papel constitucional das Forças Armadas na Defesa Nacional,* a evolução da temática da cibernética no Brasil, particularmente

perscrutando as atividades em andamento, quais sejam: Programa Estratégico Defesa Cibernética na Defesa Nacional; Projeto Estratégico Defesa Cibernética; as experiências provenientes da organização dos Jogos Olímpicos e Paralímpicos Rio 2016; a concepção do Sistema Militar de Defesa Cibernética; as operações conjuntas; e a atuação colaborativa com outros atores civis e militares. A exposição tem o intuito de identificar as necessidades de segurança e verificar da atuação da defesa cibernética como extensão do papel constitucional das Forças Armadas na defesa nacional e estabelecer as ações necessárias à neutralização das potenciais ameaças cibernéticas que possam interferir com a consecução dos objetivos fundamentais da nação.

Já a Professora Doutora Carolina Sancho Hirane demonstra a importância da inclusão das questões da segurança e da defesa cibernéticas na agenda pública, em razão dos riscos, vulnerabilidades e ameaças decorrentes, com especial referência para o caso do Chile, na publicação *Política pública de ciberseguridad: una necesidad imperiosa y la ciberdefensa como desafío del siglo XXI*. A partir da identificação das características intrínsecas do ciberespaço, dos problemas associados e do papel da defesa cibernética, apresenta os principais desafios enfrentados por diversos países na formulação da política pública de cibersegurança em geral e da ciberdefesa em particular. Por sua relevância, a autora defende que tais preocupações devem se traduzir em Políticas Nacionais e/ou Estratégias Nacionais consentâneas com a segurança e o bem-estar da população, a estabilidade institucional e a soberania nacional, no contexto de uma Política de Segurança Cibernética Nacional como parte relevante da Defesa Nacional.

O trabalho conjunto da Professora Doutora Martha Liliana Sánchez Lozano, Coronel da Reserva da Força Aérea da Colômbia, e do Professor Steven Jones-Chaljub, expresso em *Lineamientos de política en ciberseguridad y ciberdefensa:* logrando la seguridad y defensa de Colombia en un mundo digital, descreve os rápidos avanços ocorridos nos níveis de acesso digital daquele país, os quais proporcionaram um vislumbre do potencial de ameaças e oportunidades encapsulados nesses processos. Ao relatarem incidentes vivenciados, analisam a primeira política direcionada para o enfrentamento das questões relacionadas com a cibersegurança e a ciberdefesa, com êxitos em diversos âmbitos, notadamente operacionais, legislativos, estratégicos e diplomáticos. Embora os autores verifiquem que esses progressos não se constituíram em uma linha de chegada, permitiram, no entanto, entrever novas necessidades, dentre as quais avulta a continuidade no aperfeiçoamento de um arcabouço de políticas públicas capazes de encarar o problema com a construção de um cenário ideal para o seu equacionamento.

O Coronel Roberto Artiga Chicas, em *El ciberespacio y la seguridad nacional en El*

Salvador prossegue o debate sobre o tema mediante a inclusão de questionamentos relacionados com o ciberespaço – características, ameaças, impactos sobre os objetivos nacionais, ações e organizações necessárias – que visam balizar possíveis respostas aos problemas decorrentes, particularmente em relação aos seus impactos sobre a Segurança Nacional de El Salvador, de forma a contribuir, intelectualmente, para a construção de políticas e estratégias de segurança cibernética adequadas aos esforços do Estado para combater tais ameaças. Seu diagnóstico mostra a ausência de uma Estratégia de Segurança Nacional, de instituições capazes de monitorar e prever ações futuras e de arcabouço jurídico, nos âmbitos nacional e internacional, que permitam orientar as ações necessárias.

No artigo *Ciberdelincuencia: desafíos para la defensa y la seguridad en República Dominicana,* do General de Brigada Francisco A. Ovalle Pichardo, as análises direcionam-se para a questão fundamental da delinquência no ciberespaço e suas consequências para a segurança e a defesa. Para tanto, realiza uma síntese das estruturas legislativas, de fiscalização, controle e repressão aos delitos dessa origem existentes em seu país: a República Dominicana. Destaca, particularmente, as referências aportadas pelo Convênio Budapest, o primeiro tratado internacional sobre crimes cometidos via Internet, que apresenta uma classificação específica para as diversas atividades delitivas. Ao concluir, relata a ausência de Políticas e Estratégias voltadas para o problema em seu país, propugna por integração das medidas de segurança concernentes ao ciberespaço abrangendo todos os níveis institucionais afetados por seus efeitos, cujos custos de implementação seriam amplamente favorecidos pelos benefícios que seriam alcançados.

O Tenente-Coronel Ángel Gómez de Ágreda, da Força Aérea da Espanha, mostra, em *El modelo de ciberseguridad y ciberdefensa en España,* a Estratégia Nacional de Segurança Cibernética do seu país. Fruto de decisão governamental emanada do mais alto nível político, deriva de ameaça identificada quando da elaboração da Estratégia de Segurança Nacional da Espanha. Em seu texto, o autor descreve o conteúdo daquele documento governamental; as relações e a organização da segurança cibernética sob o Conselho Nacional de Segurança Cibernética; a estrutura envolvida; o papel do Ministério da Defesa, particularmente do Comando Conjunto de Ciberdefesa; a integração dos aspectos cibernéticos em operações militares; e o estado atual da cibersegurança e ciberdefesa na Espanha. Como poderá ser observado, seu artigo contém respostas para muitos questionamentos e dúvidas apontados pelos demais autores.

O capítulo *La ciberseguridad y ciberdefensa en el contexto de México,* escrito pelo Coronel Jesús García García e pelo Capitão de Corveta Julio Cesar Mondragón Pérez, expõe uma visão geral dos aspectos de segurança cibernética e de defesa a

partir da perspectiva do México, com destaque para as ações empreendidas pelo governo mexicano como parte da Estratégia Nacional de Informação, para fortalecer e desenvolver as capacidades de cibersegurança e ciberdefesa em cada uma das instâncias de Segurança Nacional. Os autores abordam, inclusive, a participação ativa do setor privado como entidades de vanguarda em questões desta natureza, prevendo, ao final, a importância do comprometimento da sociedade como atores relevantes na proteção do ciberespaço.

O Coronel e Professor Doutor Roberto Vizcardo Benavides, do Peru, no seu texto, descreve a evolução das questões relativas ao Ciberespaço, à ciberdefesa e à cibersegurança. Nesse diapasão, procura perscrutar seus efeitos, particularmente, sobre a defesa e a economia. Ressalta o desenvolvimento das principais tecnologias de defesa, cujo progresso se encontra, cada vez mais, imbricado com o ciberespaço. Tal condição traz, por consequência, a ampliação das ameaças existentes, com a incorporação de novas interfaces, e as dificuldades para enfrentá-las. Na sequência, analisa a intercorrência desses avanços com a dimensão econômica e mostra a necessidade de um arcabouço jurídico que proporcione proteção legal para os alvos das ações, sejam de infraestrutura ou em ativos críticos de informação, propugnando, afinal, pela necessidade de se levar esse esforço ao âmbito regional.

O capítulo *Contributo para o estudo da cibersegurança em Portugal,* de autoria do Coronel João Manuel Assis Barbas, de Portugal, inicia com a premissa: a informação é um dos elementos componentes da expressão psicossocial do Poder Nacional. A capacidade de dominar a produção, gestão, utilização e manipulação da informação tornou-se um recurso desse Poder, cuja interdependência com as demais expressões do Poder e com a sociedade enseja a problemática da cibersegurança, associada nomeadamente à ciberdefesa. O Coronel Barbas procura explicitar a experiência do Instituto da Defesa Nacional de Portugal nesse domínio e na gestão de crises provenientes do ciberespaço, na conjuntura das iniciativas da União Europeia, no quadro legislativo nacional e em relatórios internacionais de referência.

Segundo o Tenente-Coronel Pablo Edgardo Camps Lasserre, no texto *Ciberdefensa y ciberseguridad:* nuevas amenazas a la seguridad nacional, estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias en este ámbito, as novas tecnologias de informação e comunicações, que deram origem ao ciberespaço, considerado o quinto domínio de interação humana. A cada dia mais abrangente, sua expansão faz surgir novas ameaças advindas de indivíduos, organizações ou Estados no intuito de explorar essa recente modalidade virtual e a fim de dar consecução aos seus interesses. Nesse cenário,

os Estados tiveram que se adaptar aos pilares e marcos regulatórios para prevenir e enfrentar este quadro, em que os limites são tênues, e os atores não podem ser claramente identificados. Assim sendo, tomando como referência o Uruguai, o autor examina o grau de capacidade de segurança e de defesa no ciberespaço, a partir do reconhecimento das ameaças, do enquadramento pela legislação nacional, das estruturas responsáveis pela prevenção e pela situação atual do país, em termos de uma estratégia de segurança cibernética.

Diante dessas ponderações, expostas por representantes dos países que tomam assento nas Conferências de Diretores de Colégios de Defesa Ibero-Americanos, podem-se referendar a atualidade da temática e a pertinência de investigações destinadas à reflexão acerca da construção de um arcabouço de políticas, estratégias, instituições e estruturas adequadas ao equacionamento da questão do espaço cibernético.

Boa leitura!

A DEFESA CIBERNÉTICA COMO EXTENSÃO DO PAPEL CONSTITUCIONAL DAS FORÇAS ARMADAS NA DEFESA NACIONAL

Aristides Sebastião Lopes Carneiro*

1 Introdução

Nos últimos anos, tem-se observado o aumento do risco de perpetração de ataques cibernéticos por Estados, organizações e, até mesmo, pequenos grupos com as mais diversas motivações. As nações estão em processo de adequação para lidar com a Cibernética em todos os campos do conhecimento. Por outro lado, o uso indevido deste conhecimento pode levar a danos de dimensões imprevisíveis para todo o mundo.

Diante desse quadro, podem-se elencar algumas das principais características do domínio cibernético:

- ✓ não possui limitações físicas de distância e espaço, nem fronteiras geograficamente definidas;
- ✓ é mutável e dependente das condições ambientais e da criatividade do ser humano, podendo os efeitos colaterais serem incontroláveis;
- ✓ há facilidade de acesso a ferramentas similares de Tecnologia de Informação (TI), tanto para os administradores de sistemas, como para os oponentes; e
- ✓ não existe sistema computacional totalmente seguro.

O Espaço Cibernético é *sui generis* e dual, visto que, normalmente, há dificuldade de se identificar a atribuição dos ataques, desconhecendo-se se sua proveniência vem de ações militares. Ademais, há uma infinidade de flancos cibernéticos sobre os quais não se tem controle. Entre as principais ameaças, podem ser elencados: o crime cibernético, o terrorismo cibernético, a espionagem cibernética, a atuação de hackers (mais especificamente crackers) e organizações de Estados.

Na atual conjuntura mundial, caracterizada pela incerteza, mutabilidade e volatilidade das ações potenciais, bem como pela presença de novos atores não estatais nas possíveis situações de conflito, a sociedade brasileira, em particular, a expressão militar do Poder Nacional, deverá estar permanentemente preparada, considerando os atuais e futuros contenciosos internacionais. Para tal, medidas

* Chefe do Núcleo da Escola Nacional de Defesa Cibernética (ENaDCiber), doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (com tese na área Cibernética); e especialista em Tecnologia e Projeto de Redes de Computadores pela Universidade Estácio de Sá. Contato: <Lcarneiro@cociber.eb.mil.br>

deverão ser adotadas de forma a capacitá-la a responder oportuna e adequadamente, antecipando os possíveis cenários adversos à Defesa Nacional.

Nesse contexto, o Brasil necessita dispor de capacidade para se contrapor aos possíveis ataques externos e internos que possam afetar sua soberania, de modo compatível com sua própria dimensão e suas aspirações político-estratégicas no campo internacional. Essa iniciativa possibilita ao país a consecução de objetivos estratégicos e a preservação dos interesses nacionais, além do exercício do direito de defesa assegurado pela Constituição Federal e pelo ordenamento jurídico internacional.

No âmbito militar, o Ministério da Defesa e as Forças Armadas estão buscando as competências necessárias à Defesa Nacional no domínio cibernético. Assim, a Defesa Cibernética vem se estabelecendo como procedimento fundamental ao êxito das operações militares em todos os escalões de comando, na medida em que viabiliza o exercício do Comando e Controle (C^2), por meio da proteção dos ativos de informação, ao mesmo tempo em que o mesmo é negado ao oponente. Na condição de atividade especializada, sua execução baseia-se em uma concepção sistêmica, com métodos, procedimentos, características e vocabulário peculiares.

2 Histórico

No contexto nacional, particularmente na área governamental, o tema foi tratado, inicialmente, como Segurança da Informação, o que se caracterizou com a criação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), por meio da Medida Provisória (MP) nº 2.216-37, de 31 de agosto de 2001, que alterou dispositivos da Lei nº 9.649, de 27 de maio de 1998. Ao novo órgão, entre outras competências, coube a coordenação das atividades de Segurança da Informação (BRASIL, 2001).

Pelo Decreto nº 5.772, de 8 de maio de 2006, foi criado o Departamento de Segurança da Informação e Comunicações (DSIC), no GSI/PR, com a missão de planejar e coordenar a execução das atividades de Segurança da Informação e Comunicações (SIC) na Administração Pública Federal (APF) (BRASIL, 2006a).

Em dezembro de 2008, o Decreto nº 6.703 aprovou a Estratégia Nacional de Defesa, definindo prioridades nos três setores estratégicos para a Defesa Nacional: Nuclear, Cibernético e Espacial (BRASIL, 2008a).

Em 29 de junho de 2009, o Comandante do Exército (CmtEx) instituiu o Setor Cibernético no Exército Brasileiro, determinando que fosse implantado por meio de um projeto, tendo o Estado-Maior do Exército como órgão de coordenação e o Departamento de Ciência e Tecnologia como elaborador da proposta relativa ao Setor.

A Diretriz Ministerial nº 0014, do Ministério da Defesa, de 9 de novembro de 2009, definiu providências para o cumprimento da Estratégia Nacional de Defesa (END) nos setores estratégicos da defesa, estabelecendo as responsabilidades para cada Força Armada. Ao Exército, coube a responsabilidade pela coordenação e integração do Setor Cibernético (BRASIL, 2009).

Na mesma diretriz, ficou acordado que, para cada área específica, inicialmente, seriam definidos a abrangência do tema e os objetivos setoriais. Em uma segunda fase, este último item seria detalhado em ações estratégicas e estudada a adequabilidade das estruturas existentes, propondo-se alternativas e soluções.

Em 22 de junho de 2010, o Comandante do Exército (CmtEx) aprovou a Diretriz de Implantação do Setor Cibernético (DSIC), por intermédio do Projeto Estratégico Defesa Cibernética, que será apresentada na seção 4 deste artigo. E, em 4 de agosto de 2010, criou o Centro de Defesa Cibernética (CDCiber) e ativou o Núcleo do Centro de Defesa Cibernética (Nu CDCiber), subordinado ao Departamento de Ciência e Tecnologia.

O Decreto nº 7.411, de 29 de dezembro de 2010, explicitou, nas atribuições do DSIC - Gabinete de Segurança Institucional da Presidência da República (GSI/PR) a sua competência de planejar e coordenar a execução das atividades de Segurança Cibernética e de Segurança da Informação e Comunicações na Administração Pública Federal. Em 20 de setembro de 2012, o Decreto Presidencial nº 7.809, entre outras medidas, incluiu, na Estrutura Regimental do Comando do Exército, o Centro de Defesa Cibernética (BRASIL, 2010b).

Posteriormente, o Ministério da Defesa, por intermédio da Portaria nº 3.405/MD, de 21 de dezembro de 2012, atribuiu ao Centro de Defesa Cibernética, do Comando do Exército, a responsabilidade pela coordenação e integração das atividades de Defesa Cibernética, no âmbito do Ministério da Defesa (MD), consoante o disposto no Decreto nº 6.703, de 2008 (BRASIL, 2008, 2012b).

Concomitantemente, a Portaria Normativa nº 3.389, do Ministério da Defesa, de 21 de dezembro de 2012, aprovou a Política Cibernética de Defesa. Entre seus objetivos, incluem-se os de desenvolver e de manter atualizada a doutrina de emprego do Setor Cibernético, cujos fundamentos estão consubstanciados naquela política (BRASIL, 2012c).

O Decreto Legislativo nº 373, de 12 de setembro de 2013, atualizou a Estratégia Nacional de Defesa (END) e aprovou o Livro Branco de Defesa Nacional. Nas premissas sobre o Setor Cibernético, citadas no documento, evidencia-se a proteção do espaço cibernético, que abrange um grande número de áreas, como: capacitação; inteligência; pesquisa científica; doutrina; preparo e emprego operacional; e gestão de pessoal (BRASIL, 2013).

Em 27 de outubro de 2014, a Portaria Normativa nº 2.777, do MD, definiu responsabilidades sobre a implantação das medidas que visam à potencialização da defesa cibernética nacional, nas quais figura a instituição do Comando de Defesa Cibernética (ComDCiber) e da Escola Nacional de Defesa Cibernética (ENaDCiber). E, em 18 de novembro de 2014, a Portaria Normativa nº 3.010, do MD, aprovou a Doutrina Militar de Defesa Cibernética (BRASIL, 2014b, 2014c).

Em 2 de janeiro de 2015, o Comandante do Exército criou o ComDCiber e a ENaDCiber, subordinados, inicialmente, ao CDCiber, e ativou seus núcleos, a contar de 1º de janeiro de 2015.

Em 13 de julho de 2015, a Presidente da República, pelo Decreto nº 8.491, alterou a Estrutura Regimental do Comando do Exército e a subordinação do CDCiber, definindo sua competência, caracterizada pelas seguintes ações:

> - Assessorar o Comandante do Exército e o Ministro da Defesa nas atividades do setor cibernético, formular doutrina e obter e empregar tecnologias.
> - Planejar, orientar e controlar as atividades operacionais, doutrinárias e de desenvolvimento das capacidades cibernéticas.
> - Executar atividades de exploração cibernética, em conformidade com as políticas e diretrizes do Ministério da Defesa. (BRASIL, 2015a).

Em 3 de março de 2016, o Estado-Maior do Exército emitiu a Portaria nº 61, que aprovou a Diretriz para a Implantação do Comando de Defesa Cibernética (ComDCiber) (BRASIL, 2016c).

3 Aspectos Jurídicos, Doutrinários e Normativos

2.1 Papel Constitucional das Forças Armadas (FA)

A Constituição Federal dispõe em seu Artigo 142 que:

> As Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, são instituições nacionais permanentes e regulares, organizadas com base na hierarquia e na disciplina, sob a autoridade suprema do Presidente da República, e destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem. (BRASIL, 1988, grifo nosso).

Sem comprometimento de sua destinação constitucional, cabe também às Forças Armadas o cumprimento das atribuições subsidiárias explicitadas na Lei Complementar (LC) nº 97, de 9 de junho de 1999. O Artigo 15 dessa LC dispõe sobre o emprego das Forças Armadas na defesa da Pátria e na garantia dos poderes constitucionais, da lei e da ordem, nos seguintes termos:

> § 1º Compete ao Presidente da República a decisão do emprego das Forças Armadas, por iniciativa própria ou em atendimento a pedido manifestado por quaisquer dos poderes constitucionais, por intermédio dos Presidentes do Supremo Tribunal Federal, do Senado Federal ou da Câmara dos Deputados.
> § 2º A atuação das Forças Armadas, na garantia da lei e da ordem, por iniciativa de quaisquer dos poderes constitucionais, ocorrerá de acordo com as diretrizes baixadas em ato do Presidente da República, após esgotados os instrumentos destinados à preservação da ordem pública e da incolumidade das pessoas e do patrimônio, relacionados no Art.144 da Constituição Federal.
> §3º Consideram-se esgotados os instrumentos relacionados no Art.144 da Constituição Federal quando, em determinado momento, forem eles formalmente reconhecidos pelo respectivo Chefe do Poder Executivo Federal ou Estadual como indisponíveis, inexistentes ou insuficientes ao desempenho regular de sua missão constitucional.
> § 4º Na hipótese de emprego nas condições previstas no § 3º deste artigo.
> Após mensagem do Presidente da República, serão ativados os órgãos operacionais das Forças Armadas, que desenvolverão, de forma episódica, em área previamente estabelecida e por tempo limitado, as ações de caráter preventivo e repressivo necessárias para assegurar o resultado das operações na garantia da lei e da ordem. (BRASIL, 1999).

4 Arcabouço Doutrinário e Normativo da Defesa Cibernética

O arcabouço doutrinário relacionado à Defesa Cibernética é orientado pelos seguintes documentos: Política Nacional de Defesa; Estratégia Nacional de Defesa; Livro Branco de Defesa Nacional; Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal.

A Política Nacional de Defesa define a Defesa Nacional como o "Conjunto de atitudes, medidas e ações do Estado, com ênfase no Campo Militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais e manifestas" (BRASIL, 2005). A

Defesa Nacional se manifesta pela aplicação efetiva do Poder Nacional, por intermédio de ações, visando a superar óbices, internos ou externos, que, de forma lesiva, possam afetar o atingimento ou a manutenção dos Objetivos Fundamentais.

A Estratégia Nacional de Defesa estabelece três setores estratégicos: o setor nuclear, a cargo da Marinha; o setor espacial, de responsabilidade da Força Aérea; e o setor cibernético, de incumbência do Exército. Entre as principais disposições da END aplicáveis à Defesa Cibernética, estão as seguintes:

> As capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede. Contemplarão o poder de comunicação entre os contingentes das Forças Armadas e os veículos espaciais. No setor cibernético, será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar. (BRASIL, 2008b, p. 33).

Com base nesses fundamentos, foram formulados os documentos norteadores das atividades cibernéticas no âmbito do Ministério da Defesa, a saber:

- ✓ Política Setorial de Defesa;
- ✓ Estratégia Setorial de Defesa;
- ✓ Doutrina Militar de Defesa Cibernética; e
- ✓ Concepção Operativa do Sistema Militar de Defesa Cibernética, atualmente em elaboração.

Essas publicações, por sua vez, constituem o embasamento doutrinário que orienta a elaboração das diversas normas técnicas reguladoras das atividades relacionadas à Defesa Cibernética, assim como as de cada Força singular sobre Guerra Cibernética.

5 Programa Estratégico Defesa Cibernética na Defesa Nacional

O Programa Estratégico Defesa Cibernética na Defesa Nacional, conduzido no âmbito do Ministério da Defesa (MD), tem a finalidade de incrementar as atividades relativas ao Setor Cibernético para assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelo MD e pelas Forças Armadas (FA) e a impedir ou dificultar sua utilização contra interesses da Defesa Nacional. Esses procedimentos incluem ações nas áreas de capacitação, doutrina,

ciência, tecnologia e inovação, inteligência e operações, no domínio da Defesa Nacional.

O Programa visa, também, capacitar e gerir talentos humanos necessários à condução das atividades do Setor Cibernético (StCiber) no campo da Defesa Nacional, e colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o Sistema de Inteligência de Defesa (SINDE) e com os órgãos de governo envolvidos com a Segurança da Informação e Comunicações (SIC) e Segurança Cibernética.

Outros objetivos do projeto são: desenvolver e manter atualizada a doutrina de emprego do StCiber; adequar as estruturas de Ciência, Tecnologia e Inovação (C,T&I) nas pesquisas e desenvolvimento de interesse para a Defesa Cibernética Nacional; cooperar com o esforço de mobilização nacional para assegurar a capacidade operacional e, em consequência, a capacidade dissuasória do StCiber. A seguir, são apresentados os projetos do Programa.

5.1 Criação do Comando de Defesa Cibernética

Segundo o Plano de Articulação e Equipamento da Defesa (PAED), "O Comando de Defesa Cibernética (ComDCiber) é o órgão responsável pela coordenação e integração das atividades do Setor Cibernético na Defesa Nacional." (BRASIL, 2014).

> O Comando conta com servidores militares e civis altamente especializados, com seu valor estratégico amparado no aumento da capacidade nacional de combate às ameaças cibernéticas contra os interesses nacionais. Ao dotar o MD e as Forças Armadas dos meios necessários para exercer a defesa e o controle contínuo do espaço cibernético de interesse para a Defesa Nacional, garantirá fluxo ágil e seguro de informações confiáveis e oportunas, impactando positivamente nas áreas científico-tecnológica e operacional da Defesa Nacional, da indústria nacional e do País. Entre os benefícios sociais mais diretos, destacam-se o incremento da segurança e da proteção das infraestruturas estratégicas dependentes do ambiente cibernético e a integração entre as ações do MD, das Forças Armadas e de todas as outras agências envolvidas nessas atividades (BRASIL, 2014).

Na figura abaixo, observam-se as áreas em que o ComDCiber desenvolve suas atividades: Recursos Humanos, Doutrina, Ciência e Tecnologia, Inteligência e Operações.

Figura 1- Áreas de atividades cibernéticas

Fonte: BRASIL, 2016a.

As atividades nessas duas últimas áreas são particularmente conduzidas pelo Centro de Defesa Cibernética, Organização Militar Diretamente Subordinada (OMDS) ao ComDCiber, responsável pelas funções operativas. Percebe-se que todas as ações nesses setores têm como base a Segurança da Informação e Comunicações e contam com a mobilização da capacidade cibernética nacional. Além disso, o emprego cibernético é sempre regido pelo amparo legal vigente.

A figura 2 apresenta o organograma inicial do Comando de Defesa Cibernética. O ComDCiber compõe- se da seguinte organização:

I - Comando, Estado-Maior Pessoal e Auxiliares

II - Gabinete

III - Estado-Maior Conjunto

iv - Departamento de Gestão e Ensino:

a) Divisão de Relações Institucionais;

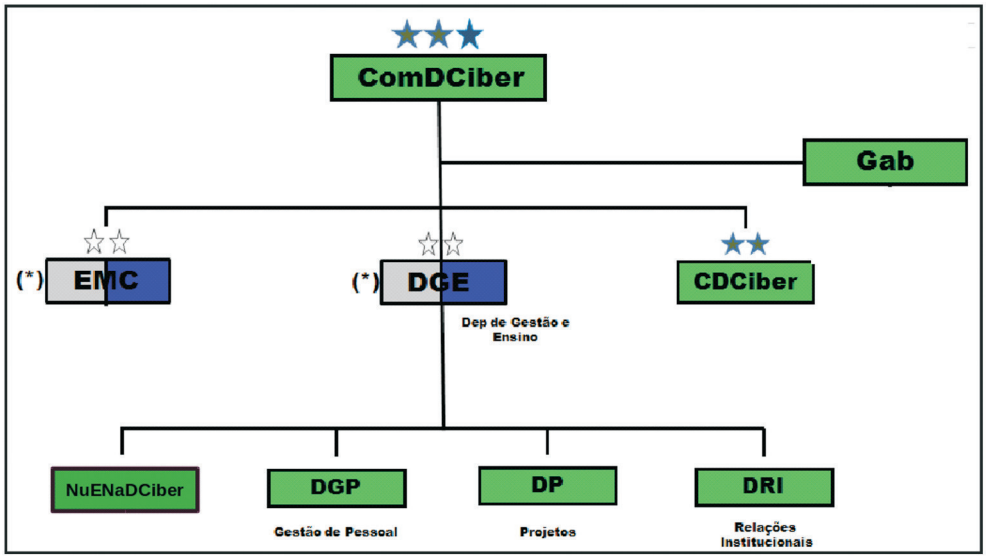
b) Divisão de Projetos;

c) Divisão de Gestão de Pessoal; e

e) Núcleo da Escola Nacional de Defesa Cibernética.

V - Centro de Defesa Cibernética

Figura 2- Organograma inicial do ComDCiber



Fonte: BRASIL, 2016a.

6 Escola Nacional de Defesa Cibernética

O projeto prevê a criação da Escola Nacional de Defesa Cibernética (ENaDCiber), considerada como centro polarizador de ensino e pesquisa da Defesa Cibernética Nacional. Essa estrutura de ensino terá caráter dual, civil e militar, e possibilitará avanços significativos na sensibilização, na conscientização, na formação e na especialização de cidadãos para a atuação no setor cibernético. "O projeto se alinha à END, que norteia a necessidade de se capacitar recursos humanos na área cibernética, em prol das operações conjuntas e interagências e para colaborar na proteção das infraestruturas estratégicas da Nação." (BRASIL, [2014]).

6.1 Observatório de Defesa Cibernética

O Plano de Articulação e Equipamento da Defesa (PAED) dispõe para o Observatório de Defesa Cibernética um espaço virtual colaborativo para a interação com os meios acadêmico, empresarial e militar, promovendo o intercâmbio entre os diversos setores e atores que possuam interesse no Setor Cibernético. Essa determinação trará benefícios sociais, uma vez que contribuirá para a disseminação do conhecimento do Setor Estratégico Cibernético, posicionando o Brasil na vanguarda desta área.

> O Observatório de Defesa Cibernética reunirá capacidades da sociedade civil e militar em torno da difusão do conhecimento do Setor Cibernético e promoverá a interação com programas e projetos congêneres ou similares em desenvolvimento nas Forças Armadas, no MD, e demais órgãos de governo, bem como em instituições civis públicas e privadas. Inicialmente, basear-se-á na reunião das capacidades inerentes à Comunidade de Segurança da Informação e Criptografia (ComSIC) e ao Comitê de Cibernética (COMCIBER) da ABIMDE. (BRASIL, [2014]).

7 Implantação e Consolidação do Sistema de Homologação e Certificação de Produtos de Defesa Cibernética

Este capítulo visa a certificar produtos (equipamentos e programas de Tecnologias de Informação e Comunicação (TIC) para o emprego no Setor Cibernético da Defesa Nacional. Seu valor estratégico está amparado no aperfeiçoamento dos dispositivos e dos procedimentos de segurança e a consequente redução das vulnerabilidades dos sistemas relacionados à Defesa Nacional. Esse sistema tem emprego dual mediante a avaliação e a certificação, sob demanda, de equipamentos voltados ao mercado nacional do setor de TIC, ampliando a segurança do espaço cibernético empenhado pela economia do país (BRASIL, [2014]).

8 Implantação e Consolidação da Estrutura de Desenvolvimento Conjunto de Defesa Cibernética

Este projeto propicia que as Forças Armadas atuem perfeitamente integradas e coordenadas no âmbito do Setor Cibernético. Seu valor estratégico está amparado no pleno funcionamento do Sistema Militar de Defesa Cibernética (BRASIL, [2014]).

8.1 Apoio à Pesquisa e ao Desenvolvimento de Produtos de Defesa Cibernética

O projeto Apoio à Pesquisa e ao Desenvolvimento de Produtos de Defesa Cibernética permitirá ao país o desenvolvimento de soluções nacionais (em software e hardware) que irão, paulatinamente, reduzir a dependência nacional de "soluções estrangeiras", que trazem riscos potenciais à Segurança Nacional na área cibernética, em particular à Defesa Cibernética.

> O projeto promoverá ações que contemplem a multidisciplinaridade e a dualidade civil e militar, além de promover o fomento à indústria nacional, gerando emprego e renda em áreas de elevado valor tecnológico agregado. Após sua implantação, dará ao País uma estrutura de desenvolvimento de produtos nacionais essenciais para obter e preservar a independência tecnológica no Setor Estratégico Cibernético. Este projeto será desenvolvido juntamente com o Ministério da Ciência, Tecnologia e Inovação (MCTI) e alinha-se à Estratégia Nacional de Defesa (END) ao desenvolver tecnologias que permitirão o planejamento e a execução da Defesa Cibernética no Brasil e atenderá ao objetivo preconizado na Política Cibernética de Defesa de implementar atividades de pesquisa e desenvolvimento. (BRASIL, [2014]).

8.2 Implantação e Consolidação de Estrutura de Gestão de Conhecimento de Defesa Cibernética

O Plano de Articulação e Equipamento da Defesa prevê a criação de uma estrutura para a elaboração da base conceitual, normativa e doutrinária, necessária para o emprego do Setor Estratégico Cibernético, no âmbito da Defesa Nacional.

"O projeto representa um avanço inédito nessa área, pois possibilitará: a sinergia entre os setores empresarial, acadêmico, governamental e militar; a geração de conhecimento alta- mente especializado; e o incremento de estudos prospectivos, [...]" (BRASIL, [2014]).

8.2.1 Implantação e Consolidação do Sistema de Gestão de Talentos

Estas ponderações têm o objetivo de realizar a obtenção, a gestão, a retenção e a mobilização de talentos humanos, necessários à condução das atividades do Setor Cibernético, na Defesa Nacional (BRASIL, [2014]).

8.2.2 Implantação e consolidação de Sistemas de Informações Seguras

O projeto de Implantação e Consolidação de Sistemas de Informações Seguras visa a "buscar inovações na área de Segurança da Informação e Comunicações, em especial a Criptografia, por intermédio da estruturação de uma rede de laboratórios virtuais em instituições de pesquisas públicas e privadas nacionais." (BRASIL, [2014]). Com isso, busca-se elevar a competência brasileira nesta área, reduzindo-se o gap em relação aos países mais desenvolvidos.

8.3 Implantação e Consolidação de Sistemas de Atuação em Rede

O plano procura desenvolver uma solução nacional em sistemas de atuação em rede de defesa, promovendo a interoperabilidade das comunicações móveis, em ambiente seguro, entre as Forças Armadas e as demais instituições governamentais nas operações interagências. E trará, como benefícios, o desenvolvimento de uma arquitetura de software e hardware nacional, com pesquisa e tecnologia própria; e a racionalização de recursos do Estado Brasileiro com a padronização de várias interfaces para múltiplas plataformas. No entanto, não prevê a aquisição de equipamentos e sistemas prontos. Trata-se de um projeto de desenvolvimento para obtenção de um produto nacional inovador. (BRASIL, [2014]).

9 Projeto Estratégico Defesa Cibernética

A implementação do Setor Cibernético foi iniciada por meio desse Projeto Estratégico, o qual tem sido conduzido pelo Exército Brasileiro, força líder no Setor Cibernético. Originalmente, o Projeto Estratégico Defesa Cibernética (PEDCiber) possuía como horizonte temporal um ciclo de vida de quatro anos (de 2011 a 2014). Atualmente, estipulou-se um novo horizonte temporal para conclusão até 2018, com recursos anuais (2016-18).

O PEDCiber possui dez subprojetos, sinteticamente descritos nesta seção, com base nas informações obtidas na pesquisa de campo com militares que atuam no projeto em epígrafe. Esses subprojetos deverão ser atualizados ao fim do ciclo de vida atual, a fim de permitir o lançamento das Subatividades e Ações a Realizar no Sistema de Informações Gerenciais e Acompanhamento (SIGA) para 2017.

9.1 Subprojeto Organização do Centro de Defesa Cibernética

O subprojeto destina-se à implantação da estrutura organizacional do Centro de Defesa Cibernética como organização militar diretamente subordinada ao Comando de Defesa Cibernética (ComDCiber), e reorientará as atribuições do Centro de Defesa Cibernética, adequando e implementando suas novas estruturas. O gerente responsável é o Chefe do CDCiber.

9.2 Subprojeto Planejamento e Execução da Segurança Cibernética

O propósito é dotar o Exército Brasileiro (EB) de infraestrutura para realizar todo o espectro de atividades cibernéticas, visando proteger e defender os ativos de informação da Força Terrestre nas áreas de Segurança e Defesa Cibernéticas. E, como resultado, expandirá e atualizará a infraestrutura física e lógica para realizar a Segurança e a Defesa Cibernéticas da Força. O gerente é o Chefe do Centro Integrado de Telemática do Exército (CITEx).

9.3 Subprojeto Estrutura de Apoio Tecnológico e Desenvolvimento de Sistemas

O subprojeto pretende implantar a estrutura de apoio tecnológico e de desenvolvimento de sistemas para atender as necessidades do Setor Cibernético, com estruturas físicas e recursos de apoio tecnológico, incrementado, assim, o conhecimento do setor.

9.4 Subprojeto Arcabouço Documental

O seu objetivo é a elaboração e a atualização de publicações doutrinárias e normativas relativas ao Setor Cibernético para a consolidação da sistemática e dos processos de elaboração, revisão, atualização, divulgação e prospecção de novos conhecimentos, bem como a verificação da aplicação dos documentos do arcabouço relativos ao setor.

9.5 Subprojeto Estrutura de Capacitação e de Preparo e Emprego Operacional

A instituição de estruturas de capacitação e de preparo e emprego operacional dirigidas às atividades de segurança, defesa e guerra cibernética, que garantam à Força Terrestre a possibilidade de atuar em rede de forma segura e integrada ao Sistema Militar de Comando e Controle do Ministério da Defesa, compõe sua finalidade. E tem, também, como intenção, a adequação e criação de cursos, sistemas, estruturas e tecnologias voltadas para gerar novas capacidades e aumentar a operacionalidade da Força Terrestre no setor cibernético.

9.6 Subprojeto Estrutura para a Produção do Conhecimento Oriundo da Fonte Cibernética

O subprojeto objetiva a implantação de estruturas direcionadas à produção do conhecimento oriundo da fonte cibernética, com o propósito de atender às demandas da atividade de Inteligência da Defesa. E da mesma forma, atualizará as estruturas, os processos e a capacitação gerando novas habilidades para o Sistema de Inteligência do Exército.

9.7 Subprojeto Estrutura de Pesquisa Científica na Área Cibernética

O subprojeto é destinado à orientação, à coordenação, à supervisão e ao fomento da classificação de recursos humanos de nível superior, à pesquisa científica tecnológica em instituições de ensino, civis e militares, e à extensão universitária no Instituto Militar de Engenharia, que atendam às necessidades do Setor Cibernético. Tem ainda a finalidade de incrementar a qualidade e a quantidade das pesquisas científicas no setor cibernético.

9.8 Subprojeto Gestão de Pessoal

O referido visa estruturar e consolidar a gestão de recursos humanos de modo a suprir as necessidades da Força Terrestre. As ações envolvidas na gestão de pessoal incluem organizar a procura e a admissão, gerir a capacitação e a administração do pessoal, bem como sua permanência nas atividades do setor cibernético.

9.9 Subprojeto Rede Nacional em Segurança da Informação e Criptografia (RENASIC)

Este integra e fomenta pesquisas nas áreas críticas do conhecimento relacionadas ao setor cibernético, por meio de uma equipe de pesquisadores e estudiosos do assunto. Entre outras iniciativas, a RENASIC mantém uma revista especializada em Segurança da Informação e Criptografia - Revista Enigma - e uma rede de laboratórios que é apresentada na tabela 1. O subprojeto RENASIC passou a compor o portfólio de projetos do Programa de Defesa Cibernética na Defesa Nacional a partir de 2016.

Quadro 1 – Laboratórios da RENASIC

Laboratório	Descrição	Órgão Financiador
VIRTUS	Técnicas Criptográficas Simétricas – IME. Criação de um sistema de criptoanálise nacional e de ferramentas para a proteção de sistemas móveis.	**FINEP**
PROTO	Protocolos Criptográficos Seguros – Universidade de Brasília. Desenvolvimento de sistemas de criptografia por chave única.	
QUANTA	Computação e Informação Quânticas – IQUANTA Acompanhamento desenvolvimento nacional e internacional sobre o assunto.	
LAPAD	Processamento de Alto Desempenho – LNCC. Proporciona o acesso ao processamento de alto desempenho à comunidade científica nacional.	
ASTECA	Técnicas Criptográficas Assimétricas – CASNAV Desenvolvimento de um produto de segurança corporativa.	
LATIM	Implementações Seguras – CTI Renato Archer. Desenvolvimento de um sistema de gestão de identidades e outro de defesa contra ataques laterais.	
LAPROJ	Acompanhamento de Projetos – UFMG Acompanhamento de Projetos e Desenvolvimento de componente básico (hardware) do Sistema KeyBITS.	
LABIN	Inteligência de Redes – ITA Análise do tráfego de redes e proteção de pacotes sigilosos.	
SALTAR	Sistema de Análise de Link e Tráfego de Dados em Redes de Comunicações – Universidade de Brasília Detecção de anomalias no comportamento de redes de comunicações.	EB
LaSEC^2	Laboratório de Segurança Eletrônica, de Comunicações e Cibernética – Parque Tecnológico de Itaipu. Desenvolvimento de ferramentas para a segurança dos ativos de informação da Administração Pública Federal.	

Fonte: BRASIL, 2016a.

9.10 Subprojeto Rádio Definido por Software (RDS) de Defesa

O subprojeto tem, como propósito, desenvolver o rádio definido por software mediante a pesquisa e o desenvolvimento de protótipos de rádios, forma de onda e de plataformas de desenvolvimento de formas de onda, além de promover a interoperabilidade nas comunicações rádio das Forças Armadas. O RDS,

à semelhança da RENASIC, também passou a compor o portfólio de projetos do Programa Defesa Cibernética na Defesa Nacional a partir de 2016.

10 Jogos Olímpicos e Paralímpicos Rio 2016

As atividades relativas à preparação para os Jogos Olímpicos e Paralímpicos Rio 2016 têm abrangido ações diversas, como a conscientização dos usuários dos ativos de informação, a adoção de boas práticas previstas nas normas de SIC, maior colaboração e fiscalização das empresas terceirizadas que prestam serviços de TIC e aquisição de novas soluções para aumentar a proteção cibernética e a consciência situacional.

Como pontos fortes da atuação do Centro de Defesa Cibernética (CDCiber) em grandes eventos, podem-se citar: trabalho preventivo, atuação conjunta, articulação em Destacamentos Conjuntos de Defesa Cibernética (DstCjDefCiberRmto) e o trabalho colaborativo em ambiente interagências.

As principais operações técnicas, realizadas nos jogos, incluem: avaliação de riscos; de- tecção automática de incidentes; pesquisa e análise; análise de incidentes de segurança; trata- mento de incidentes de segurança; assistência de recuperação a incidentes; coordenação da resposta a incidentes; distribuição de alertas, recomendações e estatísticas.

11 Sistema Militar de Defesa Cibernética (SMDC)

A Concepção Operacional do Sistema Militar de Defesa Cibernética, em elaboração, define o Sistema Militar de Defesa Cibernética (SMDC) como "um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal, essenciais para realizar as atividades de defesa no espaço cibernético". (COSTA, 2015). O Comando de Defesa Cibernética (ComDCiber), órgão central do Sistema, é a Organização Militar responsável pela orientação, supervisão e condução das atividades do SMDC.

> O SMDC tem por finalidade assegurar, de forma conjunta, o uso efetivo do espaço cibernético pelas Forças Armadas, bem como impedir ou dificultar a sua utilização contra interesses da Defesa Nacional. Além disso, cabe ao SMDC assegurar a proteção cibernética do Sistema Militar de Comando e Controle (SISMC^2), garantindo às Forças Armadas a capacidade de atuar em rede com segurança, bem como atuar colaborativamente na proteção das infraestruturas críticas da informação de interesse da Defesa Nacional, definidas pelo Ministério da Defesa. (COSTA, 2015).

A Concepção Operacional do SMDC prevê a interação ativa deste sistema com outros sistemas e órgãos inseridos também no ambiente da Defesa Nacional, tais como o Sistema Militar de Comando e Controle (SISMC2), o Sistema de Inteligência de Defesa (SINDE), o Sistema Nacional de Mobilização (SINAMOB), o Sistema de Mobilização Militar (SISMOMIL), o Sistema de Defesa Aeroespacial Brasileiro (SISDABRA), o Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB) e o Sistema de Ciência, Tecnologia e Inovação de Interesse da Defesa Nacional (SisCTID).

Para que o SMDC seja capaz de cumprir sua finalidade, as Forças Armadas devem dispor das seguintes capacidades de Defesa Cibernética: proteção, exploração e ataque cibernéticos.

De acordo com o Planejamento Baseado em Capacidades (PBC) do Exército Brasileiro, o conceito de capacidade é entendido como "a aptidão requerida de uma força ou organização militar para que possa cumprir determinada missão ou tarefa". (BRASIL, 2015) Uma nova capacidade é produzida a partir do desenvolvimento de um conjunto de sete fatores determinantes, inter-relacionados e indissociáveis: Doutrina, Organização (e processos), Adestramento, Material (e sistemas), Educação, Pessoal e Infraestrutura, que formam o acrônimo DOAMEPI.

Para alcançar a efetividade operacional conjunta de combater no domínio cibernético, precisam ser mapeadas e desenvolvidas as capacidades estruturantes e operativas que o SMDC tem de possuir com a finalidade de cumprir missões ou tarefas relacionadas à Defesa ou Guerra Cibernéticas.

12 O Sistema Militar de Defesa Cibernética (SMDC) e as Operações Conjuntas

Segundo Costa (2015), para o perfeito entendimento do emprego das capacidades operativas do SMDC nas operações conjuntas, coordenadas pelo Ministério da Defesa, torna-se necessário conhecer como os seus órgãos componentes relacionam-se nos diferentes níveis de decisão.

No nível político, em que o ambiente operativo é interagências, o Comando de Defesa Cibernética (ComDCiber), órgão central do SMDC, atua de forma colaborativa com entidade da Presidência da República encarregada da Segurança Cibernética nacional e com o Comitê Gestor da Internet no Brasil (CGI.br).

> Nesse nível, o CDCiber estabelece um canal técnico com o Centro de Tratamento de Incidentes de Redes de Computadores da Administração Pública Federal (CTIR Gov) e com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), órgão do CGI.br. (COSTA, 2015).

No nível estratégico, o ComDCiber é a organização responsável pela coordenação e integração das ações de Defesa Cibernética no âmbito do Ministério da Defesa, cabendo-lhe: assessorar o Comandante do Exército e o Ministro de Estado da Defesa nas atividades do setor, formular doutrina e obter e empregar tecnologias; planejar, orientar e controlar as atividades operacionais, doutrinárias e de desenvolvimento das capacidades cibernéticas; e executar atividades de exploração cibernética, em conformidade com as políticas e diretrizes do Ministério da Defesa.

Costa (2015) explica que, "para cumprir suas tarefas no nível estratégico, o CDCiber desenvolve continuamente as capacidades operativas necessárias à condução das ações cibernéticas em todo o espectro dos conflitos, em operações conjuntas ou singulares.".

Em situação de normalidade institucional, o ComDCiber coordena e integra a Defesa Cibernética com diversos órgãos do Ministério da Defesa, da Marinha do Brasil, do Exército Brasileiro e da Força Aérea Brasileira ligados ao SMDC, além de diversas instituições civis, conforme se observa na figura 3.

Figura 3 – Atuação colaborativa

Fonte: BRASIL, 2016a.

O Centro de Defesa Cibernética (CDCiber) mantém canal técnico permanente com os órgãos de Defesa Cibernética dos Comandos das Forças Armadas, com as Equipes de Tratamento de Incidentes de Redes (ETIR) do Ministério da Defesa e

de outras organizações parceiras e, também, com a Força Conjunta de Guerra Cibernética (F Cj G Ciber), quando constituída.

O Emprego no nível operacional corresponde às ações cibernéticas no interior de um Teatro de Operações (TO) ou de uma Área de Operações (A Op). "Nesse nível, o Estado- Maior Conjunto (EMCj) do Comando Operacional será composto por elementos de Guerra Cibernética das três Forças Armadas." (BRASIL, 2016a).

> O Comandante Operacional, assessorado pelo seu EMCj, emitirá Ordem de Coordenação (O Coor) estabelecendo as prioridades, a responsabilidade pela execução das ações cibernéticas, o momento do desencadeamento e as medidas de coordenação necessárias. O Comandante Operacional também será responsável, dentro do controle da operação planejada, pela avaliação do desempenho operacional e dos efeitos das ações cibernéticas realizadas em proveito da campanha. (BRASIL, 2016a).

No nível tático, poderá ser constituída uma F Cj G Ciber, diretamente subordinada ao Comandante Operacional, encarregada de planejar e executar as ações cibernéticas previstas no Plano Operacional. A F Cj G Ciber também coordena as ações cibernéticas sob a responsabilidade das demais Forças Componentes (F Cte).

Costa (2015) comenta que, nesse nível, "cada F Cte, por sua vez, deverá constituir o seu Dst G Ciber com as capacidades visualizadas para apoiar a operação planejada, ligando-se à F Cj G Ciber por meio do canal técnico estabelecido para a operação."

13 Conclusão

No cenário atual, no que tange à Defesa Nacional, o Estado brasileiro deve dispor de capacidades cibernéticas para identificar e se contrapor às ameaças orientadas aos ativos de informação estratégicos do país ou às infraestruturas críticas de interesse para a Defesa Na- cional.

Como foi visto ao longo do presente artigo, ações concretas visando à potencialização da Defesa Cibernética nacional estão sendo implementadas, e novas capacidades geradas no âmbito da Defesa, de forma a tornar as Forças Armadas aptas a combater no domínio cibernético, com efetividade operativa, no amplo espectro dos conflitos, agregando valor à Segurança Cibernética brasileira.

Entre as principais iniciativas em curso, destacam-se o Programa Estratégico Defesa Cibernética na Defesa Nacional, o Projeto Estratégico Defesa Cibernética,

o emprego da De- fesa Cibernética nos Jogos Olímpicos e Paralímpicos Rio 2016, a concepção do Sistema Mili- tar de Defesa Cibernética, o emprego da Defesa Cibernética nas Operações Conjuntas, e a atuação colaborativa com outros atores civis e militares da sociedade brasileira, representada pelos segmentos governamentais, acadêmicos e empresariais.

Segundo diretriz da Estratégia Nacional de Defesa, para se alcançar a efetividade, a eficácia e a eficiência nessas ações, é preciso que se intensifique a interação e a colaboração entre o Ministério da Defesa e os demais atores envolvidos com o Setor Cibernético, nos níveis nacional e internacional.

Por último, mas não menos importante, deve ser destacado que todas essas iniciativas relacionadas ao desenvolvimento da Defesa Cibernética trazem benefícios não só às Forças Armadas, mas ao país como um todo. A criação de capacidades nesse setor propicia a proje- ção do Brasil no cenário internacional, bem como proporciona melhores possibilidades de solução de problemas relacionados ao trato de informações digitais.

Referências

BRASIL. Constituição da República Federativa do Brasil. Brasília, DF, 1988.

_____. Decreto nº 373, de 25 de setembro de 2013. Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional, encaminhados ao Congresso Nacional pela Mensagem nº 83, de 2012 (Mensagem nº 323, de 17 de julho de 2012, na origem). Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 26 dez. 2013. Seção 1, p. 1.

_____. Decreto nº 5.772, de 8 de maio de 2006. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República, e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 09 maio 2006a.

_____. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defe- sa, e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 19 dez. 2008a.

_____. Decreto nº 7.411, de 29 de dezembro de 2010. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 30 dez. 2010b.

BRASIL. Decreto nº 7.809, de 20 de setembro de 2012. Altera os Decretos nº 5.417, de 13 de abril de 2005, nº 5.751, de 12 de abril de 2006, e nº 6.834, de 30 de abril de 2009. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 21 set. 2012a.

_____. Decreto nº 8.491, de 13 de julho de 2015. Altera o Anexo I ao Decreto nº 5.751, de 12 de abril de 2006, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Grupo-Direção e Assessoramento Superiores - DAS e das Funções Gratificadas do Comando do Exército do Ministério da Defesa. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 14 jul. 2015a.

_____. Exército. Centro de Defesa Cibernética. Palestra Institucional. Brasília, DF, 2016a.

_____. _____. Estado-Maior. Planejamento Baseado em Capacidades. Brasília, DF, 2015

_____. _____. _____. Palestra para a ESG. Brasília, DF, 2015b.

_____. _____. _____. Palestra sobre os Jogos Olímpicos Rio 2016. Brasília, DF, 2016b.

_____. _____. _____. Portaria nº 61, de 3 de março de 2016. Aprova a Diretriz para a Implantação do Comando de Defesa Cibernética. Boletim do Exército, Brasília, DF, n. 10, 2016c.

_____. _____. Núcleo do Comando de Defesa Cibernética. Regulamento do Núcleo do Comando de Defesa Cibernética. Brasília, DF, [2016]. No prelo.

_____. Lei Complementar nº 97, de 09 de junho de 1999. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 10 jun. 1999.

_____. Ministério da Defesa. Concepção operacional do Sistema Militar de Defesa Cibernética. [Brasília, DF, 20--]. No prelo.

BRASIL. Ministério da Defesa. Estratégia Nacional de Defesa. 2. ed. Brasília, DF, 2008b.

_____. _____. Diretriz Ministerial nº 14/2009, de 09 de novembro de 2009. Dispõe sobre integração e coordenação dos setores estratégicos da Defesa. Brasília, DF, 2009.

_____. _____. Doutrina Militar de Defesa Cibernética. Brasília, DF, 2014b.

_____. _____. Plano de Articulação e Equipamento de Defesa (PAED). Brasília, DF, [2014].

_____. _____. Política Cibernética de Defesa. Brasília, DF, 2012b.

_____. _____. Portaria Normativa nº 2.777, de 27 de outubro de 2014. Dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional e dá outras providencias. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 28 out. 2014c.

_____. Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012. Aprova a Política Cibernética de Defesa. Brasília, DF, 21 dez. 2012c.

_____. Portaria nº 3.405/MD, de 21 de dezembro de 2012. Atribui ao Centro de Defesa Cibernética, do Comando do Exército, a responsabilidade pela coordenação e integração das atividades de Defesa Cibernética, no âmbito do Ministério da Defesa, consoante o
disposto no Decreto nº 6.703/08. Brasília, DF, 21 dez. 2012d.

_____. Presidência da República. Casa Civil. Medida Provisória (MP) nº 2.216-37, de 31 de agosto de 2001. Altera dispositivos da Lei no 9.649, de 27 de maio de 1998, que dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 01 set. 2001. Edição extra.

COSTA, Alan Denilson Lima. O SMDC e seus reflexos para a Defesa Nacional. Brasília, DF: [s.n], 2015.

CIBERESPACIO BIEN PÚBLICO MUNDIAL EN TIEMPOS DE GLOBALIZACIÓN: POLÍTICA PÚBLICA DE CIBERSEGURIDAD UNA NECESIDAD IMPERIOSA Y LA CIBERDEFENSA COMO DESAFÍO DEL SIGLO XXI

Carolina Sancho Hirane*

> A pesar de los avances prometedores que hemos logrado hasta el momento, la necesidad de continuar con cooperación multilateral y la creación de capacidad sigue siendo igual de urgente. Las tecnologías de la información y las innumerables formas en que las utilizamos siguen evolucionando a un ritmo acelerado, al igual que las vulnerabilidades que traen consigo y los actores y las amenazas que buscan aprovecharse de estas. Solo trabajando juntos podemos seguir el ritmo y asegurar que los beneficios de este dominio digital nuevo y en expansión supere los riesgos y los costos. (ALMAGRO, 2016, p. XII).

1 Introducción[1]

Transcurrida la primera mitad del siglo XXI constatamos que el ciberespacio es un ambiente cotidiano donde personas, organizaciones y gobiernos interactúan en forma creciente para comunicarse, realizar transacciones económicas e inclusive gestionar diversas actividades grupales a nivel nacional e internacional. La importancia que actualmente tiene el ciberespacio junto a las características que presenta ha llevado a identificarlo como un bien público mundial.

Asimismo, la ciberseguridad constituye un tema cada vez más relevante en la agenda pública, toda vez que aumenta la evidencia sobre la existencia de riesgos, vulnerabilidades y amenazas ocasionadas por ciberataques, ciberdelitos, ciberguerras e inclusive ciberespionaje, los cuales pueden tener un origen diverso: delincuentes,

1 Algunas ideas expresadas han sido presentadas anteriormente en otros trabajos de la autora. Al respecto ver (HIRANE, 2012; HIRANE, 2013a; HIRANE, 2013b; HIRANE, 2016).

* Doctora en Conflictos, Seguridad y Solidaridad, Universidad de Zaragoza. Magíster en Ciencia Política y Administrador Público, Universidad de Chile. Profesora de Inteligencia en ANEPE. Ha sido profesora de "Análisis de Conflictos Internacionales Actuales" y "Construcción de Procesos de Paz" en Universidades chilenas. Se ha desempeñado en la Contraloría General de la República y como Jefa del Departamento de Crimen Organizado en el Ministerio del Interior y Seguridad Pública de Chile. Contacto: <carolina.sancho @anepe.cl>.

interesados en obtener ganancias en forma ilegal; personas que desean alertar sobre la vulnerabilidad de sistemas informáticos; e inclusive Estados que reconocen en el ciberespacio una dimensión más para defender o promover sus intereses nacionales y lo utilizan como escenario para debilitar al adversario o enemigo.

En esta perspectiva, la existencia de políticas nacionales y/o estrategias nacionales de ciberseguridad constituyen una respuesta obligada de parte de los países si el objetivo es proteger la seguridad y bienestar de la población, la estabilidad institucional y la soberanía nacional. En este contexto, la ciberdefensa emerge como parte relevante de la función defensa nacional que requiere ser desarrollada desde los ministerios de Defensa, para garantizar la adecuada protección de los intereses nacionales ante un ciberincidente que pueda afectar la seguridad nacional. No obstante, la formulación de una política de ciberdefensa obliga a repensar los supuestos, las medidas y los objetivos a partir de los cuales es posible defender al país ante un ataque desde el ciberespacio.

Este artículo tiene como finalidad describir y problematizar los principales desafíos que enfrentan los países al momento de formular una política pública de ciberseguridad, en general, y ciberdefensa en particular, haciendo especial referencia al caso chileno.

El desarrollo de este artículo contempla cuatro ejes: el primero identifica las principales características que presenta el ciberespacio, haciendo especial referencia a su condición de un bien público. El segundo eje describe los principales problemas asociados a la seguridad en el ciberespacio y el rol de una política pública de ciberseguridad en el nivel nacional, que integre la dimensión internacional del tema en su formulación. El tercer eje reflexiona en torno al papel de la ciberdefensa en el marco de una política nacional de ciberseguridad y los desafíos a considerar en su elaboración desde el sector defensa. Finalmente, el cuarto eje revisa los avances en el caso chileno con relación a la política de seguridad y defensa en el ciberespacio.

2 Ciberespacio: Uso Creciente de un Bien Público Mundial

El ciberespacio puede ser entendido como un ambiente creado a partir de la revolución de la tecnología de la información y las comunicaciones (TIC) cuyo uso aumenta exponencialmente debido a las ventajas que ofrece en términos de rapidez en las comunicaciones independiente de las distancias involucradas, facilidad en el acceso e intercambio de grandes cantidades de datos e información y bajos costos en su uso en términos comparados. A continuación, se hará referencia a las principales características y tendencias que presenta, como también, a su condición de bien público mundial (BPM).

3 Principales Características y Tendencias

El ciberespacio es producto de la revolución en las TIC y una de sus principales consecuencias, el fenómeno de la globalización, entendido como un "proceso o (serie de procesos) que engloba una transformación en la organización especial de las relaciones y transacciones sociales" (HELD et al, 2002, p. XLIX) que puede ser "evaluada en función de su alcance, intensidad, velocidad y repercusión, y que genera flujos y redes transcontinentales o interregionales de actividad, interacción y ejercicio del poder" (HELD et al, 2002, p. XLIX). En efecto, por un lado, la globalización ha producido un cambio en las relaciones sociales reconfigurando las relaciones de poder. Por ejemplo, desde una perspectiva estatal, el poder del Estado se modifica en cuanto cede cuotas de poder a nivel supranacional y/o internacional y también a nivel local. Sin embargo, ello no implica que pierda importancia o vigencia. Al contrario, se refuerza su relevancia por cuanto es el articulador de las diferentes relaciones entre actores locales, nacionales, internacionales y transnacionales.

Por otro lado, el acceso creciente a las TIC ha influido en lo que algunos han denominado un nuevo momento en la historia del hombre caracterizado –entre otros aspectos- por la desaparición de la distinción entre distancia y tiempo. En este sentido, recordemos que hace más de una década Manuel Castells en su obra de tres tomos denominada "La era de la información" nos proponía la existencia de un nuevo paradigma llamado la "Era Informacional", por cuanto se trataba de "un nuevo modo de desarrollo informacional" en donde la "fuente de la productividad estriba en la tecnología de la generación del conocimiento, el procesamiento de la información y la comunicación de símbolos." (CASTELLS, 1999, p. 43).

Ello puede constatarse, por ejemplo, cuando recibimos y enviamos un correo electrónico, situación en la cual a través de una única acción estamos generando, procesando y comunicando símbolos. En efecto, tal como indica Kissinger "lo nuevo en nuestra época es el promedio del cambio del poder informático y la penetración de la tecnología de la información en todas las esferas de la existencia." (2016, p. 342). Otro ejemplo se relaciona con la creciente valoración de las bases datos. En efecto, la profesora titular de la Universidad Politécnica de Madrid y experta en big data, Ernestina Menasalvas afirma:

> […] algunos dicen que los datos son el nuevo petróleo del siglo XXI y ya se dice que el *data scientist* será la profesión

> más demandada en las próximas décadas. Son especialistas que se van a demandar en todos los países y en todos los sectores. Será un proceso similar al que ocurrió en la década de los 60 con la automatización. Además, a día de hoy no hay tanta gente formada en este campo. Por otro lado, la tecnología de datos no hace más que avanzar, cada vez hay más datos y cada vez está más generalizada. Ahora recibimos datos de manera continua y en tiempo real y tenemos que conseguir ordenarlos y analizarlos a tiempo. (VILLAMEDIANA, 2015).

De acuerdo a Castells (1999), es posible advertir algunas características de este nuevo paradigma de desarrollo, su tendencia a ser integrador, complejo e interconectado. Ello se explica porque son tecnologías que actúan sobre la información, cuentan con una alta capacidad para penetrar y modificar la vida cotidiana de las personas, presentando una creciente convergencia, debido a que se trata de distintas tecnologías específicas que actúan en un mismo sistema integrado. Todo lo cual ha generado una nueva estructura social denominada RED y a través de estas un modo de gestión del poder más descentralizado en comparación con las tradicionales organizaciones estructuradas en distintos niveles de jerarquía.

Cada uno de estos aspectos puede observarse en la práctica por medio de un teléfono inteligente o *smartphone*, pues ofrece diferentes tecnologías (desde un despertador pasando por un cronómetro hasta un GPS y la posibilidad de comunicación instantánea con cualquier lugar del mundo donde exista similar tecnología). Aplicaciones como *Skype*, *Whatsapp* o *Messenger* ilustran esta idea. De esta manera "los efectos de la revolución se extienden a todos los niveles de organización humana. Los individuos que usan *smartphones* (…) hoy poseen información y capacidades analíticas superiores a muchas agencias de inteligencia de una generación atrás." (KISSINGER, 2016, p. 343).

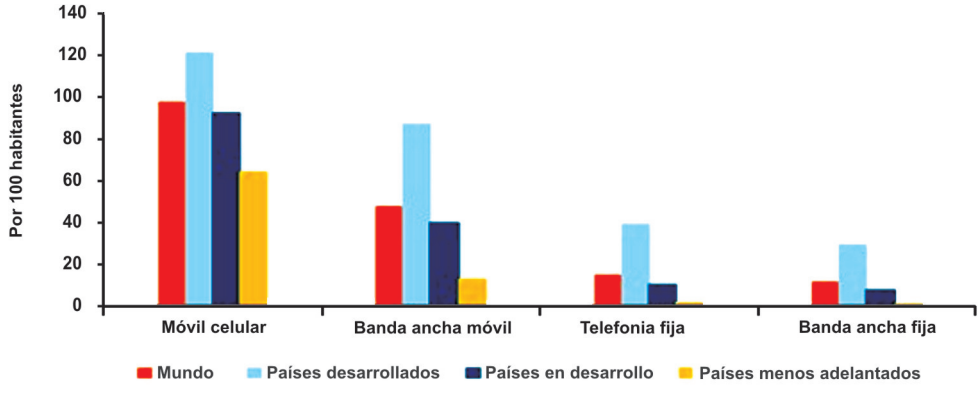
Cabe mencionar que esta tecnología tiene una creciente penetración mundial, según información proporcionada por el Director de la Oficina de Desarrollo de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT), en el informe "Medición de la Sociedad de la Información 2015", señala que:

> La proporción de la población mundial cubierta por las redes móviles y celulares es ahora de más del 95%, mientras que el número de abonados a telefonía móvil celular se ha

> incrementado de 2.200 millones en 2005 a unos 7.100 millones en 2015 […] El número de abonados a la banda ancha móvil en todo el mundo ha crecido, de 800 millones en 2010, a unos 3.500 millones en 2015, al mismo tiempo que la cifra de abonados de banda ancha fija ha aumentado mucho más lentamente, a unos 800 millones en la actualidad. El número de usuarios de Internet también ha crecido rápidamente, y actualmente se estima en más del 40% de la población mundial. (UNIÓN…, 2015, p. 1).

No obstante, este acceso a las TIC no está distribuido homogéneamente en la población mundial, detectándose la persistencia de una brecha digital observada "tanto entre los países como dentro de los países, en particular entre las zonas urbanas y rurales. En muchos todavía persiste una brecha digital entre hombres y mujeres, y la diferencia puede ser amplia entre las personas con ingresos más altos y las con ingresos más bajos." (UNIÓN…, 2015, p. 2). El gráfico Nº 1 permite apreciar el nivel de acceso a las TIC de acuerdo al grado de desarrollo de los países.

Gráfico 1 - Acceso a las TIC según el estado de desarrollo, 2015*

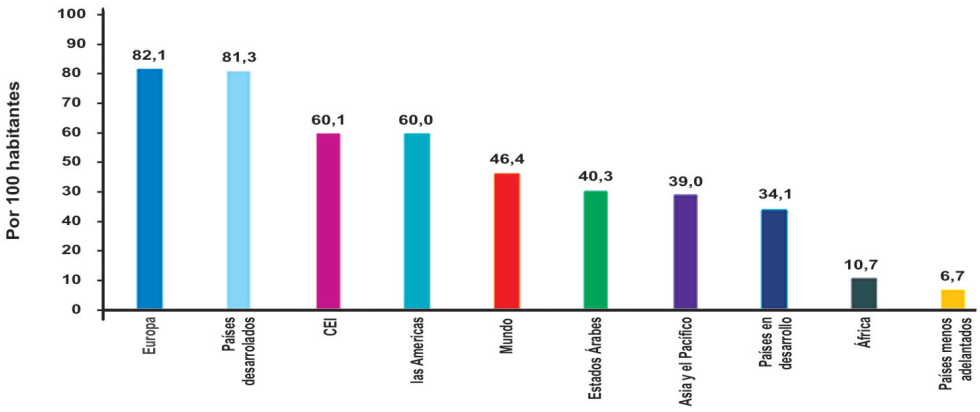


Nota: * Estimaciones: las cifras se refieren a los abonados.

Fonte: UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, 2015

En este sentido, podemos afirmar que no todos los países, gobiernos y comunidades están igualmente globalizados. Asimismo, el nivel de globalización medido en función del nivel de acceso a las TIC puede ser cuantificado. En efecto, el informe "Medición de la Sociedad de la Información 2015" permite constatar las diferencias en el acceso a las tecnologías de la información en los países desarrollados y en desarrollo (Gráfico 2).

Gráfico 2 - Hogares con acceso a Internet, por región y nivel de desarrollo, 2015*



Nota: * Estimación

Fonte: UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, 2015

No obstante, aun cuando se reconoce la existencia de una brecha en el desarrollo digital de los países, el ciberespacio se continúa desarrollando y los Estados, de acuerdo a sus posibilidades, participan de ello. Una de las importantes tendencias en este ambiente es el "*big data*", entendido como:

> […] conjuntos de datos cuyo volumen, variedad y velocidad superan los correspondientes a los conjuntos de datos habituales. Su aparición denota adelantos tecnológicos que permiten captar, almacenar y procesar cantidades de datos cada vez mayores de diferentes fuentes de datos. De hecho, una de las tendencias primordiales que fomenta el surgimiento de "*big data*" es la "conversión en datos" y la digitalización masivas, también de actividad humana, en "árboles" o "huellas" digitales. En un mundo cada vez más digitalizado, los "*big data*" se generan de forma digital a partir de diversas fuentes, entre ellas registros administrativos (por ejemplo antecedentes bancarios o historiales clínicos electrónicos), transacciones comerciales entre dos entidades (como, por ejemplo, compras en línea o transacciones con tarjeta de crédito), sensores y dispositivos de localización (por ejemplo teléfonos móviles o dispositivos GPS) y actividades de los usuarios en Internet (entre ellas búsquedas y contenidos de los medios sociales). (UNIÓN…, 2014, p. 39).

Las principales características de los "*big data*" (UNIÓN…, 2014, p. 39) son: velocidad, debido a la rapidez con la que se generan y analizan los datos; variedad,

contienen diferentes tipos y formas de datos, incluidos grandes volúmenes de datos no estructurados; valor, debido al desarrollo socioeconómico potencial de los "*big data*"; veracidad, dada por el nivel de calidad, exactitud e incertidumbre de los datos y las fuentes de datos y; volumen, pues son cantidades ingentes de datos generados a través de la "conversión en datos".

De esta manera, las cualidades de los "*big data*" encierran grandes posibilidades de mejorar la puntualidad e integridad de las estadísticas oficiales. Por ejemplo, para formular políticas a favor del desarrollo social y económico (UNIÓN..., 2014, p. 40). En efecto, los diversos usos dados a la información en el ciberespacio facilitan una serie de acciones que antiguamente requerían más tiempo y dinero.

4 Ciberespacio como Bien Público Mundial (BPM)

Las cualidades que presenta el ciberespacio con relación a los beneficios que ofrece a la población lo han convertido en un bien público mundial (KAUL; GRUNBERG; STERN, 2001; SPAR, 1999), como por ejemplo, el uso de la Internet como el medio de comunicación más rápido, económico e instantáneo conocido a la fecha. En este sentido, recordemos que los BPM pueden ser puros e impuros. Mientras que en los primeros hay imposibilidad de que exista rivalidad y exclusión en su uso y/o consumo, en el caso de los BPM impuros si existe la posibilidad de que el uso y/o consumo del bien presente rivalidad y/o exclusión, siendo este último caso el que corresponde al ciberespacio.

Desde esta perspectiva, un:

> [...] bien público mundial puro se distingue por su universalidad, es decir, beneficia a todos los países, personas y generaciones. Un bien público mundial impuro tendería hacia la universalidad en cuanto beneficiaría a más de un grupo de países, y no discriminaría contra ningún segmento de la población o conjunto de generaciones. (KAUL; GRUNBERG, STERN, 2001, p.13).

El principal motivo de considerar en la misma categoría a los BPM puros e impuros está dado porque:

> [...] ambos tipos de bienes públicos mundiales plantean similares desafíos normativos. El principal entre ellos es la cuestión que se aborda reiteradamente en la bibliografía sobre relaciones internacionales y cooperación: en la esfera internacional, donde no hay ningún gobierno, ¿cómo se producen los bienes públicos? (KAUL; GRUNBERG, STERN, 2001, p.13).

Este cuestionamiento cobra especial relevancia desde la perspectiva de la regulación del ciberespacio, reflexión que se ha explicitado a través de la pregunta ¿cómo lograr la gobernanza en el ciberespacio? Algunos de los principios planteados para orientar su uso son: libertad de expresión, libre acceso, neutralidad y respeto a los derechos humanos. Sobre este aspecto, la serie de Conferencias Globales del Ciberespacio[2] (CGCS) realizadas en 2011 (Londres), 2012 (Budapest), 2013 (Seul) y 2015 (Holanda) han incorporado este tema en su agenda, haciendo posible el diálogo entre los países, con la participación de los diversos actores involucrados: gobierno, sociedad civil, academia y las empresas. Este foro volverá a reunirse en 2017 (México), debido a que ninguna de las materias tratadas están agotadas y nuevas materias requieren ser abordadas.

No obstante, es posible contar con algunas respuestas mínimas al considerar el ciberespacio como un BPG[3]. En efecto, de ello se desprende que el Estado tiene un importante rol en su provisión aun cuando parte importante de su gestión sea responsabilidad de particulares. Recordemos por ejemplo, que de acuerdo al Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas, elaborado por la Organización de Estados Americanos (OEA) y la empresa *Trend Micro*, "más del 80% de la infraestructura que potencia el Internet y administra los servicios esenciales es propiedad del sector privado y es operada por este." (TREND MICRO; ORGANIZACIOÓN..., 2005, p. 3).

La cualidad de bien público que presenta el ciberespacio implica que se presentan deficiencias en su oferta, en cuanto a su cobertura, disponibilidad, calidad y seguridad. Por este motivo, las autoridades nacionales tienen una importante responsabilidad en la regulación de la existencia, uso y condiciones de funcionamiento del ciberespacio, particularmente en todo lo referido a la seguridad de este. Asimismo, la condición global de este BPM implica la formulación de "una nueva clase de política pública, que está definida por una cantidad cada vez mayor de intereses que traspasan las fronteras nacionales." (KAUL; GRUNBERG, STERN, 2001, p. XXVII). Esta política está referida a aquellos bienes entendidos como BPM y pueden clasificarse en tres categorías:

> 1 La primera clase es la de los *bienes públicos globales naturales*, como la capa de ozono y la estabilidad climática

2 Instancia en la cual se reúnen expertos sobre el ciberespacio de todo el mundo, destaca por su capacidad de convocatoria a gobiernos, sociedad civil y academia. Al respecto ver <https://www.gccs2015.com/>.

3 Para efectos de este trabajo se considerará como sinónimo bienes públicos globales (BPG) y bienes públicos mundiales (BPM), en efecto, se constata que la misma noción es conceptualmente tratada en las acepciones indicadas dependiendo del autor al que se hace referencia.

> 2 La segunda clase de bienes es la formada por los *bienes públicos globales de producción humana*, que comprenden tanto el conocimiento científico y técnico como los principios y las normas, pasando por la herencia común de la humanidad e infraestructuras internacionales como Internet. En esta categoría se ubica una política que regule el uso del ciberespacio.
> 3 La tercera clase de BPG son los denominados objetivos de política global, que incluyen la paz, la salud pública y estabilidad financiera. (MARÍN; GARCÍA-VERDUGO, 2003, p. 109).

El ciberespacio como BPM, por un lado, otorga un rol clave e insustituible a las máximas autoridades nacionales en la regulación de su uso y por otro obliga a considerar la cooperación internacional como una condición necesaria para el adecuado funcionamiento de este BPM. En efecto, son necesarias instancias de coordinación multilaterales internacionales, pues ningún país por si solo puede satisfacer sus necesidades de comunicación global en el ciberespacio, ni puede definir en forma vinculante protocolos de telecomunicaciones entre los países, empresas y organizaciones. De esta manera, resulta clave la acción de organismos especializados internacionales como, por ejemplo, la UIT para establecer protocolos comunes de actuación en las comunicaciones, como también, entidades como el Consejo de Europa, cuyo trabajo en el establecimiento de un tratado internacional en materia de ciberdelincuencia – Convenio sobre la Ciberdelincuencia – ha constituido un aporte valioso en la cooperación entre los países signatarios para perseguir este ilícito.

5 Amenazas y Riesgos en el Ciberespacio

El ciberespacio no está exento de riesgos y amenazas, siendo necesaria la garantía de estándares mínimos de seguridad en su uso, lo cual requiere enfrentar importantes desafíos a nivel nacional e internacional. Entre ellos destaca, en el nivel nacional, la formulación de una política pública de ciberseguridad que contemple e integre los diferentes aspectos involucrados en este tema con la finalidad de evitar que un ciberincidente ponga en riesgo la vida de las personas, su patrimonio y/o la seguridad nacional. A nivel internacional cobra relevancia la necesidad de participar en instancias de diálogo multilaterales, donde sean abordados temas como: la gobernanza en internet; estándares mínimos de seguridad en el ciberespacio y la participación en convenios o resoluciones internacionales sobre situaciones que afectan la ciberseguridad y que involucran a diferentes países del mundo.

En materia de ciberseguridad es frecuente encontrar una reflexión que ayuda a introducir la importancia de este tema

> […] una cadena es tan segura como el más débil de sus eslabones y en el ciberespacio, es posible identificar dos tipos de organizaciones, aquellas que han sido hackeadas y lo saben y aquellas que han sido hackeadas y no lo saben. En este sentido, cabe preguntarse, ¿en qué categoría se ubican las principales organizaciones, entidades y empresas con las que usted se vincula? (HIRANE, 2013a).

6 Aproximación a las Amenazas y Riesgos en el Ciberespacio

Junto a los beneficios que brinda el ciberespacio, es posible también encontrar su lado oscuro representado por los peligros que han sido detectados. Por ejemplo, el Informe de Riesgos Mundiales 2013 elaborado por el Foro Económico Mundial (FEM) advirtió sobre el peligro de los "incendios digitales en un mundo hiperconectado." (WORLD…, 2013). Con ello se refería a las consecuencias sociales -e inclusive políticas- que puede generar la información falsa difundida en Internet, resultado de un error humano o una acción deliberada, siendo esta última la que genera mayores desafíos desde la perspectiva de la seguridad de la información en el ciberespacio. Ejemplo de ello pudo observarse cuando las autoridades de EE.UU., los medios de comunicación, el mercado bursátil y la opinión pública mundial durante algunos minutos fueron sorprendidos con la noticia publicada en el *twitter* de la agencia *Associated Press* (AP) que indicaba: "Dos explosiones en la Casa Blanca y el Presidente Obama herido" (Figura N° 1), la cual correspondió a difusión de información falsa resultado de un hackeo a la cuenta de *twitter* de la agencia *Associated Press* (AP). No obstante, hubo consecuencias inmediatas, como por ejemplo la baja en las acciones, según lo reflejó ese día el índice del *DOW Jones* (Figura 2).

Figura 1 - Cuenta AP intervenida

Fuente: EL PAÍS, 2013.

Figura 2 - Impacto en DOW Jones

Fuente: EL PAÍS, 2013.

Actualmente una creciente cantidad de países identifican los ataques cibernéticos como un peligro tanto o más importante que los ataques terroristas para la seguridad nacional y los entienden como una amenaza seria a la seguridad del país desde una perspectiva política, económica, social y tecnológica.

En este sentido, James Clapper, Director de la Oficina de Inteligencia Nacional, en una exposición ante el Comité de Inteligencia del Senado con motivo del informe anual sobre los peligros para la seguridad de EE.UU., abordó uno de los problemas que enfrentan en seguridad cibernética señalando que "en algunos casos, el mundo está aplicando tecnologías digitales con mayor rapidez que nuestra capacidad para entender las implicaciones que se puedan derivar para nuestra seguridad y para tratar de mitigar los nuevos riesgos." (SAIZ, 2013).

De esta manera, es posible reconocer la vulnerabilidad de los sistemas de información cibernéticos y la importancia de contar con niveles mínimos de seguridad en la gestión de la información digital, es decir, en su generación, almacenamiento y distribución. Asimismo, nos recuerda la variedad de posibles amenazas que estos sistemas pueden ser objeto, por ejemplo: hackeo; ataques distribuidos por denegación de servicio (DDoS); robo de información y los diferentes tipos de virus que pueden afectar al sistema de información digital, entre otros.

Recordemos que "los ciberataques son muy rentables en términos de esfuerzo necesario para su ejecución, riesgos que se asumen y beneficios económicos o políticos que se pueden obtener y afecta transversalmente tanto al sector público, al

sector privado como a los ciudadanos." (CANDAU, 2010, p. 259). Además, no existe una legislación armonizada que permita una lucha efectiva contra estas amenazas.

En este contexto la ciberseguridad adquiere preponderancia, pues deja en evidencia que el desarrollo de las tecnologías de la información -*software* y *hardware*-, debe ir acompañado de un similar desarrollo de protección a la información que es procesada por estas tecnologías. Ello se refuerza al observar una síntesis del "estado de riesgo en el ciberespacio" (INSTITUTO..., 2012), que sistematiza los diversos tipos de amenazas detectados y los clasifica en diferentes niveles de riesgo, tal como se indica en la figura 3.

Cuadro 1 - Resumen de Estado de Riesgo del Ciberespacio

AUTORÍA	OBJETIVOS		
	Gobierno	**Sector Privado**	**Ciudadanos**
Ataques patrocinados por otros Estados	Espionaje, ataques contra infraestructuras críticas, APT	Espionaje, ataques contra infraestructuras críticas, APT	
Ataques patrocinados por Privados	Espionaje	Espionaje	
Terroristas, extremismo político e ideológico	Ataques contra redes y sistemas; contra servicios de Internet; infección con *malware*; contra redes, sistemas o servicios de terceros	Ataques contra redes y sistemas, ataques contra servicios de Internet, infección con *malware,* ataques contra redes, sistemas o servicios de terceros	
Hacktivistas	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con *malware*, ataques contra redes, sistemas o servicios de terceros	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con *malware*, ataques contra redes, sistemas o servicios de terceros	Robo y publicación de datos personales

Crimen Organizado	Espionaje	Robo de identidad digital y fraude	Robo de identidad digital y fraude
Ataques de bajo perfil	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con *malware*, ataques contra redes, sistemas o servicios de terceros	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con *malware*, ataques contra redes, sistemas o servicios de terceros	
Ataques de personal con accesos privilegiados (*Insiders*)	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con *malware,* ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con *malware*, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT	
Impacto	**Alto**		
	Medio		
	Bajo		

Fuente: INSTITUTO ESPAÑOL DE CIBERSEGURIDAD, 2012.

Agrava esta situación la detección de los denominados "*Malware*", es decir, software maliciosos que ya han causado daño en países alertándonos del peligro que hay tras su actuar. De acuerdo a un reporte de la empresa de seguridad informática Kaspersky, los *malware* pueden agruparse "en amenazas conocidas (70%), amenazas desconocidas (29%) y amenazas sofisticadas (1%)." (KASPERSKY, 2015, p. 3), estas últimas denominadas también como "*Advanced Persistent Threats*" (APT) o "Amenazas Avanzadas Permamentes" y son particularmente peligrosas porque se trata de "ataques polivalentes, continuados y dirigidos.

Diseñados para introducirse en una red, merodear de forma invisible y recopilar datos confidenciales, una vez introducidos pueden pasar desapercibidos durante años." (KASPERSKY, 2015, p. 3).

Para ilustrar su modo de funcionamiento y posibles daños que pueden generar se hará referencia a tres de ellos: *Darkhotel, Flame y Stuxnet*. El primero es descrito en un reporte de Kaspersky:

> Una APT conocida como "Darkhotel" utilizó el *Wi-Fi* en hoteles de lujo para robar los datos de los huéspedes durante siete años antes de que se descubriera. Esta fue especialmente interesante, ya que tenía un objetivo muy específico (los altos ejecutivos y directores ejecutivos) e ilustraba de forma muy clara el reto que se presenta a la seguridad de IT cuando los *endpoints* [terminales] (portátiles y *tablets* empresariales) operan fuera del perímetro de seguridad de la red de la empresa. (KASPERSKY, 2015, p. 3).

En el caso de *Flame*, este fue detectado en 2010, aun cuando se sospecha que ya en 2006 estaba operando en los sistemas informáticos. Tiene la capacidad de que al infectar el sistema comienza a realizar una compleja serie de operaciones, incluyendo espiar en el tráfico de Internet, tomar imágenes de pantallas de computador, grabar conversaciones, interceptar teclados y demás (KASPERSKY..., 2012), explicó Vitaly Kamluk, experto en *malware* de la empresa Kaspersky. Entre los países afectados se encuentran Irán, Israel, Sudán, Siria, Líbano, Arabia Saudita y Egipto.

Por su parte, el gusano informático *Stuxnet* presenta un mayor riesgo por cuanto espía y reprograma sistemas industriales, particularmente los SCADA (Supervisión, Control y Adquisición de Datos) (ANABALÓN; DONDERS, 2014), además cuenta con capacidad para afectar instalaciones industriales. En Irán, fue usado para afectar incluso infraestructura nuclear entre 2009 y 2010, donde atacó en forma reiterada cinco plantas a lo largo de 10 meses, según un análisis realizado por *Symantec*. Actualmente es considerado el primer virus para afectar sistemas industriales.

Junto a lo indicado, es posible constatar la proliferación de estos "*malware*" tal como se indica en el Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas (TREND MICRO; ORGANIZATION, 2015) donde son identificados los principales *malware* detectados en 2014, tal como se indica a continuación en la figura n° 4.

Cuadro 2 - Las Principales Familias de Malware de 2014

FAMILIA DE MALWARE	DESCRIPCIÓN
KEYGEN	Genera números de serie para entrar a los programas que requieren números de serie válidos para que los programas funcionen completamente.
DUNIHI	Esta familia de malware normalmente es malware VBS ofuscado que es capaz de propagarse infectando unidades removibles; puede llegar como un archivo anexo del correo no deseado.
ACTIVATOR	Quiebra la aplicación y el usuario puede instalarla manualmente. Sus rutinas le permiten a los usuarios evadir las técnicas de registro y protección de las aplicaciones. Esto les permite utilizar la versión registrada de las aplicaciones.
DOWNAD/Conficker	Esta explota una vulnerabilidad del servicio del servidor que, cuando es explotada, permite que un usuario remoto ejecute el código arbitrario en el sistema infectado para propagarse a las redes
CONDUIT	Se incluye en los paquetes de malware como un componente de malware, como un archivo entregado por otro malware, o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
PRODUKEY	Una aplicación que muestra la identificación del producto y la clave del CD de cierto software si se instala en el sistema afectado. Esta herramienta de hackeo puede ser instalada manualmente por el usuario.
SAFNUT	Se incluye en los paquetes de malware como un componente de malware. Llega al sistema como un archivo entregado por otro malware o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
AGENT	Normalmente trae consigo cargas o realiza otras acciones maliciosas, que van desde moderadamente molestas hasta las irreparablemente destructivas. También pueden modificar las configuraciones del sistema para que se inicie automáticamente. Para restaurar los sistemas afectados podrían requerirse procedimientos además del análisis con un programa antivirus.
CROSSRDR	Se incluye en los paquetes de malware como un componente de malware. Llega al sistema como un archivo entregado por otro malware o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
FAKEAV	Crea carpetas en los sistemas afectados y entrega varios archivos, incluyendo una copia de sí mismo y un archivo malicioso. Realiza varios cambios al registro, uno de los cuales permite que se ejecute cada vez que el sistema arranca.

Fuente: TREND MICRO; ORGANIZATION OF AMERICAN STATES, 2015.

Bajo un enfoque de la seguridad interior, los ciberdelitos también forman parte de los riesgos y amenazas en el ciberespacio. Muchas veces se trata de delitos que históricamente se han realizado y que ahora utilizan el ciberespacio para su realización. Por ejemplo, la venta de drogas a través de páginas de internet de difícil acceso (*deepweb*); estafas por medio de la clonación de tarjetas bancarias y; secuestro, pero ahora de cuentas de correo o aparatos electrónicos con acceso a internet (computadores, *tablets* o teléfonos inteligentes) los cuales son infectados con un tipo de virus informático que bloquea *mails*, ordenadores o teléfonos y exige dinero para el retorno de archivos lo que se conoce como *ransomware*. (ASÍ..., 2016).

Se adiciona a lo indicado, que los tradicionales activistas también han encontrado un espacio para manifestarse. De este modo, los ciberhacktivistas han promovido sus causas por Internet y para obtener la visibilidad necesaria han hackeado diversas páginas, ejemplo emblemático de ello ha sido *Anonymus*. No obstante, dada su estructura en red y anonimato en la acción y discurso, para la

autoridad es muy difícil poder identificarlos y monitorearlos cuando sus acciones afectan el orden público (LIÑÁN, 2015).

Por este motivo es necesario dimensionar adecuadamente estas amenazas, perspectiva en la cual el profesor Nye nos orienta señalando:

> Si bien se suele considerar al llamado "hacktivismo" de grupos ideológicos esencialmente como un fastidio molesto en esta etapa, siguen existiendo cuatro categorías importantes de ciberataques a la seguridad nacional, cada uno de ellos con un horizonte temporal diferente: la ciberguerra y el espionaje económico están en gran medida asociados con los estados, mientras que el delito cibernético y el ciberterrorismo están básicamente asociados con actores no estatales. Para Estados Unidos, los costos más elevados hoy en día surgen del espionaje y del delito, pero en la próxima década aproximadamente, la guerra y el terrorismo podrían convertirse en mayores amenazas de lo que son hoy. (NYE, 2012).

Entre los riesgos en el uso del ciberespacio, destaca la posibilidad de explotar la vulnerabilidad que genera la insuficiente protección de información sensible que se encuentre en formato electrónico. La filtración de información, particularmente desde los Servicios de Inteligencia – lo que constituye un problema de contrainteligencia- puede afectar la seguridad de los países. Situaciones recientes, asociadas al clásico problema de la protección de la información sensible para evitar fugas y difusión no deseada de ella, han alcanzado alta visibilidad y recuerdan que el problema está vigente. Por ejemplo, algunas situaciones en los EE.UU. han generado repercusiones más allá de sus fronteras en diferentes continentes. Se trata de los casos protagonizados por el soldado Manning y el ex funcionario de la Agencia Nacional de Seguridad (NSA) Edward Snowden. Ambos accedieron a información secreta del Departamento de Defensa de EE.UU. y la difundieron a la opinión pública por medio de *Wikileaks*, produciendo problemas diplomáticos y de seguridad al gobierno norteamericano. En opinión del general Michael Hayden, Director de la Agencia Central de Inteligencia (CIA) y de la NSA durante el período de dos presidentes de Estados Unidos (Bill Clinton y George W. Bush), los documentos filtrados por Snowden han sido "la destrucción de secretos legítimos de Estados Unidos más grande de la historia de mi país [...] casi mil objetivos de inteligencia extranjeros han cambiado su comportamiento basándose en las revelaciones de Snowden." (XIMENEZ, 2016).

En síntesis, podemos afirmar que la mayor parte de las amenazas en el ciberespacio son transnacionales y se caracterizan por ser: flexibles (presentan una estructura horizontal), ambiguas (su arquitectura es difusa), globales (su ámbito de acción es transnacional) y versátiles (son capaces readaptarse al entorno). Asimismo,

es importante tener presente que el ciberespacio puede ser un medio o un objetivo para la realización de ilícitos. En el primer caso se trata especialmente de prácticas delictuales con un daño limitado a personas, organizaciones o instituciones. En el segundo, la probabilidad de generar importantes daños a la infraestructura crítica del país (energía, comunicaciones, transporte, sistema financiero, sanitario, de alimentación, entre otros) puede convertirse en un problema de seguridad nacional.

7 Formulación de Políticas Públicas de Ciberseguridad: Imperativo a Nivel Nacional

La existencia de amenazas, riesgos y vulnerabilidades en el ciberespacio genera al menos dos desafíos. Por un lado, desarrollar una capacidad para prevenir y/o detectar oportunamente la ocurrencia de un ciberincidente e identificar su origen. Por otro, garantizar que la información virtual cumpla con los requisitos de: disponibilidad, integridad, oportunidad, confiabilidad, interoperabilidad y seguridad. Ambos deben estar contenidos en una política pública de ciberseguridad cuya existencia es responsabilidad de las máximas autoridades políticas del país y, en el caso de Chile, es una tarea en la cual aún se está trabajando, toda vez que ello va en particular beneficio de los ciudadanos debido a que "grandes organizaciones podrían tal vez, dotarse de una seguridad cibernética eficaz, pero las personas individuales y los grupos reducidos difícilmente podrían hallarse en condiciones de alcanzar tal objetivo." (LAQUEUR, 2015, p. 13).

Ofrecer un mínimo de seguridad en el ciberespacio obliga a buscar respuesta a preguntas del tipo ¿cuáles son los desafíos que enfrentamos en el ciberespacio desde una perspectiva de seguridad? La respuesta obliga a identificar lo que es necesario proteger, es decir, "la información e infraestructura crítica" que podemos definirla como

> […] aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad, o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros. (TORRES, 2011, p. 347).

En este ámbito, para lograr proteger la información crítica de un país implica considerar a diversos servicios y organizaciones estratégicas, lo cual obliga a convocar a actores de diversa naturaleza, provenientes de la administración civil del Estado y a las Fuerzas Armadas y de Orden y Seguridad, junto a variados estamentos dentro de la sociedad civil, quienes deben garantizar que esa información cumpla con las siguientes características: disponibilidad, integridad, oportunidad, confiabilidad,

interoperabilidad, seguridad.

De acuerdo a lo indicado, la búsqueda de la seguridad en el ciberespacio requiere enfrentar desafíos nacionales e internacionales. Entre los nacionales cabe destacar al menos los siguientes:

- Formulación de una política pública de ciberseguridad, expresada en una Estrategia o Política Nacional de Ciberseguridad.
- Creación de autoridades nacionales en materia de ciberseguridad.
- Implementación de Centros especializados y coordinados en monitoreo, alarma y respuesta frente a ciberincidentes (CSIRT: Centro de Respuesta a Incidentes de Seguridad Informática / (Computer Security and Incidente Response Team).
- Organización de entidades tipo CLCERT Grupo Chileno de Respuesta a Incidentes de Seguridad Computacional / Chilean Computer Emergency Response Team.
- Contemplar directrices que consideren, entre otros múltiples aspectos:

  - ✓ Legislación específica y actualizada sobre el tema.
  - ✓ Mejora de la capacidad de coordinación interagencial.
  - ✓ Capacidad operacional para combatir el cibercrimen.
  - ✓ Aspectos mínimos en la formulación de protocolos de ciberseguridad.
  - ✓ Promover una cultura de ciberseguridad.
  - ✓ Desarrollar recursos industriales y tecnológicos para la ciberseguridad.
  - ✓ Disponer de planes para enfrentar ciberincidentes que contemplen acciones de prevención, respuesta, mitigación y ciberresiliencia.

Respecto a los desafíos internacionales, resultan de especial relevancia:

- Cooperación internacional ante ciberincidentes.
- Establecer estándares comunes en materia de ciberseguridad.
- Generación de instancias compartidas de formación profesional y de investigación académica en estas materias.
- Participación en foros multilaterales como son MERIDIAN4 y la Conferencia Global del Ciberespacio, entre otros.

4 Instancia en la que se reúnen decisores políticos gubernamentales sobre Protección de la Información en Infraestructura Crítica. Al respecto ver "La conferencia de Meridian reúne en España a decisores políticos en protección de infraestructuras críticas" (2015). Disponible en: <http://www.redseguridad.com/actualidad/info-tic/la-conferencia-meridian-reune-en-espana-a-decisores-politicos-en-proteccion-de-infraestructuras-criticas >

No obstante, es relevante considerar que estas medidas buscan reducir la vulnerabilidad del ciberespacio debido a que frente a la interrogante "¿Un lugar 100% seguro y privado, donde nadie pueda acceder a tus datos?" (ALALUF, 2013), la respuesta probablemente sería "Seguro que existe: en Siberia. Allá no hay teléfonos, conectividad, electricidad ni nada. Es por lejos el lugar más seguro que conozco", en opinión del experto Eugene Kaspersky.

8 Ciberdefensa: Desafío en el siglo XXI

En el marco de una política de ciberseguridad, el sector defensa constituye un actor de especial importancia debido a que la defensa en el ciberespacio orientada a garantizar la seguridad nacional es su responsabilidad. En este sentido, reflexiones del tipo "¿Cómo será el 11S cibernético?, ¿estamos preparados para ello?" (NYE, 2012), son cada vez más frecuentes.

Una adecuada aproximación a la ciberdefensa requiere distinguir entre ciberseguridad y ciberdefensa. En efecto, mientras que la primera

> […] tiene una connotación eminentemente de protección, la ciberdefensa engloba otras acciones más allá de las puramente defensivas; entre ellas, la denominada ciberdefensa activa, la ciberinteligencia, y todo un abanico de acciones ofensivas: la intrusión, la infección, la denegación de servicios o la alteración de la información, que puede llevar aparejada incluso la destrucción física. (CUBEIRO, 2016, p. 45).

Sin embargo, a diferencia de otras dimensiones de la guerra "el ciberespacio no es un ámbito análogo al de la tierra, mar, aire o estratósfera, no tiene distancias, posiciones ni territorios que puedan ocuparse; el ciberespacio no puede ser conquistado." (BORG, 2015, p.65). Entonces, ¿qué puede ocurrir en el ciberespacio que justifique una ciberdefensa?

En la práctica son diversas las situaciones generadas en el ciberespacio que han afectado la seguridad de los países. Un ejemplo destacado se encuentra en el ataque sufrido por Estonia en el año 2007, considerado por algunos como la primera "ciberguerra" (CLARKE; KNAKE, 2011). Se habría producido entre Estonia y Rusia (aunque diversas fuentes le atribuyen el ataque, no han reconocido oficialmente su autoría) con motivo de la decisión de las autoridades de Estonia de retirar de una plaza una estatua que representa al soldado soviético y enviarla a un cementerio. Esta medida produjo ataques simultáneos a páginas *Web* del Parlamento estonio, bancos, ministerios, periódicos y agencias de comunicación, entre otras. En efecto,

> Estonia había sido víctima de un ataque distribuido de denegación de servicio o DDoS, por sus siglas en inglés. Por lo general, un DDoS es una molestia menor, no una de las principales armas del arsenal ciberespacial. Básicamente se trata de una avalancha programada con antelación y diseñada para sobrecargar o bloquear la red con un gran flujo de información. El ataque es "distribuido" en el sentido de que en él participan miles de ordenadores, e incluso cientos de miles, que envían solicitudes de conexión electrónica a un puñado de blancos en Internet. Los ordenadores atacantes forman lo que se conoce como *botnet*, una red de ordenadores robots o "zombis" controlada en forma remota. Los zombis que participan en el ataque siguen instrucciones que se han cargado sin que sus propietarios se enteren. De hecho, usualmente los propietarios de estos ordenadores no pueden siquiera saber cuándo sus máquinas se convierten en zombis o están participando en un DDoS. Un usuario puede advertir que su portátil está funcionando un poco más lento de lo normal o que tarda más en acceder a la Web, pero ese será el único indicador de lo que realmente ocurre. Toda la actividad mal intencionada tiene lugar en segundo plano y no es visible en la pantalla del usuario. En este mismo momento, su propio ordenador podría formar parte de una *botnet*. (CLARKE; KNAKE, 2011, p. 33).

La situación ocurrida obligó a que posteriormente la OTAN creara un centro de ciberdefensa, que ciertamente no fue muy útil cuando en 2008 Georgia fue víctima de ciberataques presumiblemente por Rusia (según fuentes independientes de información), durante un enfrentamiento entre Osetia del Sur y Georgia, en más de 2 horas se impidió "que los georgianos supieran qué estaba pasando y para ello lanzaron ataques DDoS contra las páginas *web* de medios de comunicación locales y organismos de gobierno. Asimismo, bloquearon el acceso de Georgia a las *webs* de la CNN y BBC." (CLARKE; KNAKE, 2011, p. 38).

Incidentes similares han ocurrido en otros lugares en el último tiempo, en la figura nº 5 son mencionados algunos episodios destacados de ciberguerra (TORRES, 2013, p. 339), pudiendo apreciarse la diversidad en el modo de concretarse y la variedad de países afectados, es decir, esta situación puede afectar a cualquier Estado-Nación y el modo de ocurrencia es impredecible.

Cuadro 3 - Episodios Destacados de Ciberguerra

Fecha	Denominación	Resumen
1982	Explosión en el sistema de distribución de gas (Unión Soviética)	Los servicios de inteligencia estadounidenses introdujeron una *bomba lógica* en un software de c*ontrol* de infraestructuras gasísticas que había sido robado por espías soviéticos a una empresa canadiense
2003 2005	Titan Rain	Conjunto de ataques coordinados contra empresas estratégicas e instituciones estadounidenses presumiblemente procedentes de China
2007	Ciberataque contra Estonia	La retirada en este país de una estatua del período soviético desencadena un conjunto de graves ataques procedentes de Rusia que afectan a las instituciones estatales, bancos y medios de comunicación
2007	Ciberataque contra Siria	La aviación israelí bombardea una instalación nuclear secreta. El ataque aéreo fue precedido de un ciberataque que engañó a los sistemas de defensa aérea e impidió detectar la incursión de los aviones en el territorio sirio
2008	Guerra en Osetia del Sur	De manera paralela al conflicto hubo ciberataques coordinados desde Rusia contra sitios gubernamentales de Georgia que quedaron inutilizados y tuvieron que ser reubicados en servidores de otros países
2010	Stuxnet	Un troyano provoca la destrucción de maquinaria del programa nuclear iraní

Fuente: TORRES, 2013.

A partir de los hechos descritos, algunos autores señalan que la "ciberguerra", entendida como aquella que "se aplica a aquellas acciones realizadas por un Estado–Nación con el fin de penetrar los ordenadores o las redes de otra nación y el propósito de causar daños o perturbar su adecuado funcionamiento." (CLARKE; KNAKE, 2011, p. 23) y que "posee al menos las siguientes características: es real, sucede a la velocidad de la luz, es global y evita el campo de batalla." (CLARKE; KNAKE, 2011, p. 54-55), ya ha comenzado. No obstante, se constata ausencia de consenso al respecto. En efecto, desde otra perspectiva, se plantea que la ciberguerra

> […] a pesar de ser un término utilizado con profusión, hasta la fecha no ha habido ninguna ciberguerra en sentido estricto

> del término. Casos como los ciberataques a Estonia en 2007 y a Georgia en 2008, en los que numerosos indicios apuntan a que estuvieron o bien apoyados o bien realizados por fuerzas gubernamentales rusas, no se ajustan a definiciones tradicionales de guerra, ya que ni hubo declaración de guerra ni una intervención de Estados identificables en la confrontación. (CUBEIRO, 2016, p. 48).

Sin embargo, más allá de la identificación de un incidente en el ciberespacio como un ataque con una magnitud tal que constituye un peligro a la seguridad nacional, resulta importante tener en consideración que el

> […] dominio cibernético trasnacional plantea nuevas preguntas sobre el sentido de la seguridad nacional. Algunas de las respuestas más importantes deben ser nacionales y unilaterales, con énfasis en la profilaxis, la redundancia y capacidad de recuperación. Sin embargo, es probable que los principales Gobiernos no tarden en descubrir que la inseguridad creada por los actores cibernéticos no estatales requerirá una cooperación más estrecha entre los países. (NYE, 2013).

En efecto, hay países, como por ejemplo EE.UU., que incursionan en el desafío de formular una política de ciberdefensa. Según Laqueur, el "Pentágono dispone de una lista de armas cibernéticas destinadas al espionaje y sabotaje propios de la ciberguerra (caso del ataque *Stuxnet*). En todas las principales operaciones ofensivas tales como la de introducir un virus en las redes de países extranjeros, se precisa la aprobación del presidente." (LAQUEUR, 2015, p. 13). Cabe destacar que las más importantes decisiones estratégicas quedan bajo responsabilidad de la máxima autoridad política.

Complementando lo indicado sobre los esfuerzos de EE.UU. en la materia, el general Keith Alexander, Jefe del Comando Cibernético del Pentágono[5], ha señalado que se han "creado 13 unidades especiales de programadores y expertos informáticos para desarrollar contraofensivas en países extranjeros en el caso de que las principales redes informáticas de EE.UU. se vieran atacadas." (LAQUEUR, 2015, p. 13), dejando entrever que la ciberseguridad no solo tiene una arista defensiva, sino también una ofensiva[6], que puede entenderse en el marco de las amenazas que enfrentan dado su posicionamiento internacional. A modo de

5 Ocupó el cargo hasta marzo de 2014.

6 Aspecto que queda claramente explicitado en la Cyber Strategy del Departamento de Defensa de Estados Unidos, difundida en 2015.

ejemplo, cabe recordar un incidente ocurrido durante enero de 2015 cuando fue hackeada la cuentatwitter del Comando Central de EE.UU. El ataque fue realizado por un grupo llamado "*CyberCaliphate*", el cual publicó mensajes extremistas y los datos personales de miembros del Pentágono" (EL ESTADO, 2015), uno de ellos se presenta en la figura n° 6.

Figura 3 - Mensaje colocado en cuenta hackeada al pentágono

Fuente: SOYCHILE, 2016.

Este tipo de situación puede llevar a preguntarnos si la "tecnología de internet ha superado la estrategia y la doctrina, al menos por ahora" particularmente cuando es "más fácil emprender ciberataques que defenderse de ellos, lo que posiblemente estimulará una propensión ofensiva en la construcción de nuevas capacidades" (KISSINGER, 2016, p. 345).

Se suma a ello dudar si "una agresión 'virtual' merece una respuesta 'cinética': y en qué grado y según qué ecuaciones de equivalencia" (KISSINGER, 2016, p. 347). De estas inquietudes sería posible afirmar que "un nuevo mundo de teoría y doctrina estratégica disuasiva, que hoy está dando sus primeros pasos, requiere elaboración urgente." (KISSINGER, 2016, p. 347).

Sobre este aspecto Nye (2015) ha señalado que en ocasiones:

> […] se dice que la disuasión no es una estrategia eficaz en el ciberespacio, debido a lo difícil que resulta atribuir el origen de un ataque y la gran cantidad de actores estatales y no estatales que pueden estar implicados. A menudo no estamos seguros

> de quién son los bienes que podemos retener y por cuánto tiempo.

Pero él mismo aclara algunos aspectos de esta afirmación, estimulando a creer que nos encaminamos hacia la generación de medidas disuasivas que pueden evitar ataques en el ciberespacio.

En efecto, Nye (2015) plantea que "la atribución es cuestión de grados", aunque:

> […] atribuciones rápidas y de alta calidad suelen ser difíciles y caras, pero no imposibles. Los gobiernos no sólo están mejorando sus capacidades, sino que varias empresas del sector privado han ido entrando al juego, y su participación reduce los costes políticos de divulgar las fuentes. Muchas situaciones son cuestión de grados, y a medida que la tecnología mejora la dimensión forense de la atribución, puede aumentar la fuerza disuasoria.

Asimismo, frente a la tesis de una ausencia de normas en el ciberespacio y más aún en el caso de un enfrentamiento en este, Nye señala:

> […] los principales estados han acordado que la ciberguerra estará limitada por las leyes de los conflictos armados, que exige discriminar entre objetivos militares y civiles, además de proporcionalidad en cuanto a las consecuencias. En julio de este año el Grupo de Expertos de Gobierno de las Naciones Unidas recomendó excluir de los ciberataques a los objetivos civiles, y en la cumbre del G-20 del mes pasado se respaldó esa norma. (NYE, 2015).

Se adiciona a lo indicado la creciente valoración del Manual de Tallin, documento que permite ser aplicado a conflictos que involucran al sector defensa en el ciberespacio. De esta manera, en una perspectiva de mediano plazo, es muy probable que disminuya la ventaja de las acciones ofensivas por sobre las defensivas. Tal como lo explica Nye:

> La relación entre las variables de la disuasión cibernética es dinámica, y sobre ella influirán la tecnología y el aprendizaje; la innovación ocurrirá a un ritmo mayor que en el caso de las armas nucleares. Por ejemplo, los avances en las investigaciones forenses de atribución pueden mejorar el papel del castigo, y los avances en defensa a través del cifrado pueden mejorar la

> disuasión por denegación. Como resultado, es posible que con el tiempo vaya cambiando la actual ventaja de las estrategias ofensivas sobre las defensivas. (NYE, 2015).

En este sentido, resultan claves las decisiones y medidas que las autoridades nacionales y del sector defensa tomen sobre el tema a nivel nacional e internacional, por este motivo es posible afirmar que hoy la ciberdefensa es un desafío y el modo en que sea abordado condicionará el tipo de estrategia que predominará en el ciberespacio en el mediano y largo plazo.

9 Caso Chileno: una Breve Aproximación

En Chile la ciberseguridad es un tema de importancia creciente debido al aumento en el uso del ciberespacio por parte de personas, organizaciones e instituciones públicas y privadas. En efecto, el país -tal como lo ha indicado el Subsecretario de Defensa, Sr. Marcos Robledo:

> […] ostenta tasas de penetración a Internet de más de un 64% de la población -la mayor cifra en la región- se utilizan intensivamente las redes sociales, se realizan cada vez más trámites en línea y crecientemente vamos aprovechando las ventajas del comercio electrónico. El sector público, en tanto, cada vez depende más de las redes digitales para llevar a cabo sus funciones, tendencia que esperamos siga creciendo. (ROBLEDO, 2015).

Sin embargo, también han ocurrido incidentes de seguridad en el ciberespacio que obligan a revisar las actuales prácticas en la materia y genera el desafío de contar con una política pública de ciberseguridad que oriente, regule y coordine a los diferentes actores involucrados en el tema.

Entre los incidentes en el ciberespacio que se han detectado en el caso chileno, es posible encontrar Información falsa difundida por internet cuando se alertó por las redes sociales, de un eventual desabastecimiento de combustible en bombas de bencina en Santiago, lo cual debió ser desmentido por la autoridad pues algunos lugares de venta de este producto empezaron a colapsar por la llegada de gran cantidad de clientes a cargar su auto. En la figura nº 7 se presenta el desmentido que la empresa afectada debió emitir para evitar mayores trastornos en la capital.

Figura 4 - Comunicado empresa afectada por falsa información en redes sociales

COMUNICADO OFICIAL COPEC

SANTIAGO. 08 de julio de 2015.- En relación a una información que ha circulado en las últimas horas en redes sociales que asevera que habría problemas de suministro de combustibles para el día de mañana, **COPEC** se hace el deber de desmentir de forma tajante esta situación.
De esta manera, la empresa ratifica que este jueves 9 de julio el expendio de combustibles en las estaciones de servicio se realizará de forma absolutamente normal a lo largo de todos los puntos de su red en el país.
COPEC se hace el deber de aclarar esta situación para tranquilidad de sus clientes y usuarios.

COPEC
Primera en servicio

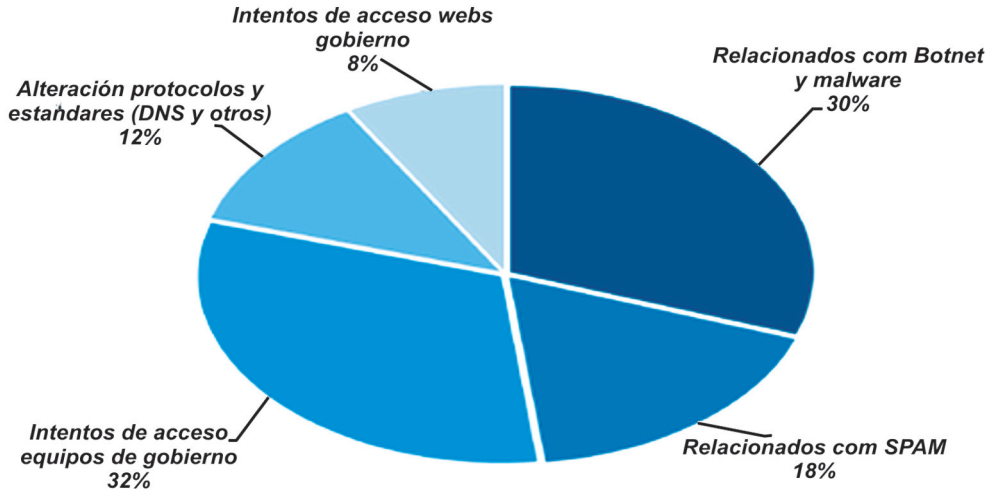
Fuente: LA TERCERA, 2015.

Acceso a información sensible de servicios públicos a personas no autorizadas, como por ejemplo ocurrió en el Registro Civil e Identificación (MUÑOZ, 2014) y recientemente en el Ministerio de Salud, donde se ha detectado que "la información contenida en esos tres millones de archivos alojados en 'carpetas compartidas' estaba accesible y despojada de todo circuito de seguridad desde hacía por lo menos un año" (CARVAJAL; JARA, 2015).

Delitos informáticos, por ejemplo en el caso de las denuncias de fraudes con tarjetas bancarias, estas aumentaron un 94% en el período 2014–2015, de acuerdo a datos de la Fiscalía Nacional (DÍAZ, 2015).

Diversos patrones potencialmente maliciosos detectados en la Red de Conectividad del Estado (RCE). A continuación, se presenta como ejemplo lo detectado durante el periodo 2014 (COMITÉ..., 2016, p. 5).

Gráfico 3 - Conductas sospechosas y maliciosas detectadas en la RCE.



Fuente: DIVISIÓN INFORMÁTICA DEL MINISTERIO DEL INTERIOR, 2015.

Los incidentes identificados justifican revisar si los niveles nacionales de seguridad en el ciberespacio cumplen con estándares internacionales. En este sentido, el tema ha estado presente en la agenda de gobierno. En efecto, al inicio del gobierno de la presidente Michelle Bachelet se ha impulsado la formulación de una política pública en materia de ciberseguridad, pues los organismos y las acciones establecidas sobre la materia están dispersos y se estima necesario integrar los esfuerzos de la autoridad pública en un único documento que coordine los esfuerzos y que integre al sector privado y sociedad civil en ello (CHILE, 2015b).

Durante 2014 se emitió un decreto que explicita el interés de la autoridad en formular una política nacional de ciberseguridad, para lo cual se establece considerar la firma de la Convención de Budapest del Consejo de Europa (Convención contra la Ciberdelincuencia). Se recomendó hacerlo y se solicitó al Ministerio de Relaciones Exteriores iniciar los trámites en este sentido (CHILE, 2015c).

Por otro lado, fue planteada la necesidad de contar con una Estrategia Nacional de Ciberseguridad, denominada Política Nacional de Ciberseguridad y para concretar este requerimiento en 2015 fue creada una comisión asesora, de carácter permanente, denominada Comité Interministerial sobre ciberseguridad (CICS) donde participan representantes de las siguientes entidades (ÁLVAREZ, 2015):

- ✓ Subsecretaría de Interior y Seguridad Pública;
- ✓ Subsecretaría de Defensa Nacional;
- ✓ Subsecretaría de Relaciones Exteriores;
- ✓ Subsecretaría de Justicia;
- ✓ Subsecretaría General de la Presidencia;
- ✓ Subsecretaría de Telecomunicaciones
- ✓ Subsecretaría de Economía
- ✓ Subsecretaría de Hacienda y;
- ✓ Agencia Nacional de Inteligencia.

El CICS en su diagnóstico inicial ha detectado que es necesario contar con una política integral sobre ciberseguridad en Chile, con un marco normativo actualizado y dinámico, que responda a estándares internacionales y ha tenido en especial consideración lo señalado en el programa de gobierno de la presidente Michelle Bachelet respecto a desarrollar una estrategia de seguridad digital que proteja a usuarios privados y públicos.

Asimismo, se ha propuesto definir para 2016 una política nacional de ciberseguridad que contemple (ÁLVAREZ, 2015):

- ✓ Un Plan que contenga medidas, planes y programas específicos.
- ✓ Identificar riesgos, amenazas y brechas en ciberseguridad.
- ✓ Propuesta de estructura orgánica pública.
- ✓ Propuesta de modificaciones legales en la materia.
- ✓ Coordinación con actores relevantes públicos y privados.

Junto a lo indicado, se han establecido como bases para una política nacional de ciberseguridad cuatro objetivos específicos, los cuales corresponden a (ÁLVAREZ, 2015):

- ✓ Resguardar la seguridad de las personas en el ciberespacio.
- ✓ Proteger la seguridad del país en el ciberespacio.
- ✓ Promover la colaboración y coordinación entre instituciones, tanto públicas como privadas.
- ✓ Gestionar los riesgos del ciberespacio.

Además, se han establecido seis líneas de trabajo (ÁLVAREZ, 2015):

- ✓ Infraestructura (crítica)[7] de la información.
- ✓ Prevención y sanción.
- ✓ Sensibilización, formación y difusión.
- ✓ Cooperación y relaciones internacionales.
- ✓ Fomento productivo / desarrollo estratégico.
- ✓ Institucionalidad de la ciberseguridad.

Se espera que en 2016 esta política esté formulada[8] y de acuerdo a lo indicado por el Subsecretario de Defensa, Sr. Marcos Robledo ella:

> […] buscará promover la identificación y gestión de riesgos en el ciberespacio para que el sector público, privado, la sociedad civil y el mundo académico puedan prevenir, minimizar y sobreponerse a estos, con especial énfasis en aquellas infraestructuras críticas para el funcionamiento del país, tales como los servicios de telecomunicaciones,

7 El paréntesis y su contenido ha sido colocado por la autora.

8 Hasta el 18 de Marzo de 2016, ha sido puesta a disposición de la comunidad en el marco de la Consulta Ciudadana, establecida en la Ley 20.500.

> de electricidad o de agua potable, el transporte público o los servicios financieros, junto con las instituciones que resguardan la seguridad y soberanía de nuestro país, como la Defensa Nacional. (ROBLEDO, 2015).

10 Institucionalidad Nacional y Participación Internacional

Actualmente, la responsabilidad en materia de ciberseguridad recae en diferentes instituciones públicas nacionales. Sin embargo, se hará especial mención a las entidades vinculadas al tema en los Ministerios del Interior y Seguridad Pública (MISP) y de Defensa Nacional, respectivamente.

En el caso del MISP, su participación se orienta en el marco de sus atribuciones y competencias en el resguardo del orden y seguridad pública. En este sentido, varios tipos de ciberincidentes y el cibercrimen son parte de su responsabilidad. Para ello cuenta con las siguientes entidades especializadas en la materia:

- Departamento de Crimen Organizado, dependiente de la División Estudios en la Subsecretaría de Interior: aborda el tema del ciberdelito, desde la perspectiva de política pública y está presente en la coordinación del CICS para la formulación de la política nacional de ciberseguridad.
- División Informática, dependiente de la Subsecretaría de Interior: encargada de la política de seguridad de los sistemas informáticos y la Red de Conectividad del Estado (RCE) y administración del CSIRT nacional.
- Agencia Nacional de Inteligencia (ANI), particularmente por su rol establecido en la Ley 19.974 "Sobre el Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia", donde se establece en el artículo 8 letra c "proponer normas y procedimientos de protección de los sistemas de información crítica del Estado".
- Policía de Investigaciones (PDI): cuenta con una entidad especializada, la Brigada de Ciberdelitos, para investigar delitos informáticos que lesionen los intereses de personas u organizaciones.
- Carabineros ha asignado a OS9 los temas relacionados con delitos informáticos, para investigar incidentes en el ciberespacio que constituyen delito y de este modo perjudiquen a los ciudadanos, empresas o instituciones.

El Ministerio de Defensa Nacional, por medio de la Subsecretaría de Defensa, participa junto a la Subsecretaría de Interior en la coordinación de las reuniones orientadas a generar una propuesta de Política Nacional de Ciberseguridad. Asimismo, ha trabajado con el Estado Mayor Conjunto (EMC) y las ramas de las

FF.AA., en un aspecto específico de la seguridad en el ciberespacio -la ciberdefensa- entendida en sentido amplio como aquellos planes y acciones provenientes desde las FF.AA. para protegerse y defenderse de un ciberataque. En este sentido, ha señalado el Subsecretario de Defensa:

> […] creemos que también es necesario modernizar la Defensa Nacional para hacer frente a los nuevos desafíos que impone el ciberespacio. Para ello estamos preparando una política de ciberdefensa, que permita planificar y disponer de manera eficiente y adecuada los medios y capacidades de la Defensa Nacional en torno a la tarea de proteger la información y redes militares del país, y asistir al resto del país en estas tareas, y diversos proyectos que nos permitirán tener redes confiables, disponibles y accesibles, acorde a estándares internacionales en la materia. Ese trabajo se verá reflejado en el Libro de la Defensa que será publicado el año 2017, donde dedicaremos un capítulo a la ciberdefensa, como una de las prioridades a futuro del sector. (ROBLEDO, 2015).

Junto a lo indicado, desde el Ministerio de Defensa Nacional se participa activamente en instancias internacionales sobre el tema. Entre ellas cabe mencionar la CGCS 2015, lo cual se inserta en la búsqueda de la obtención de:

> […] un entorno digital libre, abierto y seguro que garantice el respeto y promoción de los derechos humanos e impulse un desarrollo integral e inclusivo, Chile ha decidido adoptar un papel activo en las instituciones y procesos que conforman la gobernanza de internet; asimismo, promueve el valor del ciberespacio como un bien público global, donde se avance hacia nuevas formas de gobernanza de bienes comunes y que involucre a múltiples partes involucradas. (CHILE, 2015a).

Asimismo, en el marco del Consejo de Defensa Suramericano (CDS) de la Unión de Naciones Suramericanas (UNASUR) desde Chile se han apoyado las propuestas contenidas en el Plan de Acción 2012 y 2013.

En efecto, mientras en el Plan del 2012 se planteó la "conformación de un Grupo de Trabajo para evaluar la factibilidad de establecer políticas y mecanismos regionales para hacer frente a las amenazas cibernéticas o informáticas en el ámbito de la defensa" en el segundo se propuso "establecer una política y mecanismos regionales para hacer frente a las amenazas cibernéticas e informáticas en el ámbito de la defensa" (ROBLEDO, 2015). No obstante, uno de los mayores impulsos

dados al tema fue en la reunión de Surinam (2013), en la cual los Jefes de Estado y de Gobierno de los países miembros de UNASUR solicitaron al CDS y al Consejo Suramericano de Infraestructura y Planificación (CSIP) "avanzar en sus respectivos proyectos de defensa cibernética y en la interconexión con redes de fibra óptica entre nuestros países con vistas a tornar más seguras nuestras telecomunicaciones, promover el desarrollo de tecnologías regionales y la inclusión digital." (ROBLEDO, 2015).

11 Propuesta de Política Nacional de Ciberseguridad

En el marco de la elaboración de la política pública de ciberseguridad se plantea que seguridad y libertad son:

> […] conceptos complementarios entre sí, y que el combate a los ciberdelitos y otras amenazas en las redes digitales no pueden convertirse en excusas para atropellar derechos humanos como la privacidad y la libertad de expresión, sino un modo de garantizar plenamente estos derechos en el ciberespacio. (ROBLEDO, 2015).

En efecto, de acuerdo a la Propuesta de Política Nacional de Ciberseguridad (PNCS), su objetivo es contener "los lineamientos políticos del Estado de Chile en materia de ciberseguridad, con una mirada que apunta al año 2022, para alcanzar el objetivo de contar con un ciberespacio libre, democrático, abierto, seguro y resiliente." (COMITÉ…, 2016, p. 4).

En este sentido, se establecen como fundamentos que justifican contar con una PNCS:

- ✓ Para resguardar la seguridad de las personas en el ciberespacio;
- ✓ Para proteger la seguridad del país;
- ✓ Para promover la colaboración y coordinación entre instituciones;
- ✓ Para gestionar los riesgos del ciberespacio. (COMITÉ…, 2016, p.5).

En esta perspectiva, en el documento se reconoce la existencia de riesgos en el ciberespacio señalando:

> […] atendida la naturaleza global del ciberespacio, los riesgos y amenazas provienen de Chile y del exterior, y se originan tanto en actividades delictuales como en labores de espionaje y vigilancia llevadas a cabo con diversos fines, afectando la

> confidencialidad, integridad y disponibilidad de los activos de información en el ciberespacio, y con ello, los derechos de las personas. (COMITÉ..., 2016, p.5).

Asimismo, son planteadas tres políticas complementarias en materia digital sobre las cuales se está trabajando en forma paralela pero coordinada. Se trata de: la Agenda digital 2020, la política de ciberdefensa y la política internacional para el ciberespacio.

Especial mención se hará con respecto a la segunda política indicada, la cual corresponde a la de ciberdefensa, señalándose al respecto en el documento:

> Dado que las redes y sistemas de información de la Defensa Nacional constituyen una infraestructura crítica para la seguridad exterior y el ejercicio de la soberanía del país, y a las atribuciones constitucionales y legales de la Defensa Nacional, el Ministerio de Defensa, durante el año 2016 preparará y publicará políticas específicas de ciberdefensa, que contemplen las definiciones políticas en torno a cómo serán protegidas estas redes, y cómo las capacidades de la Defensa Nacional pueden colaborar en la formación de un ciberespacio libre, abierto, seguro, democrático y resiliente para el país. (COMITÉ..., 2016, p. 8).

Junto a lo indicado, en el documento se establecen los objetivos de política para el año 2022 y 42 medidas de política pública para el período 2016–2017. Los objetivos formulados son:

> El país contará con una infraestructura de la información pública y privada resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos [...].
> El Estado velará por los derechos de las personas en el ciberespacio, mediante la prevención y sanción efectiva de delitos, garantizando el pleno respeto de los derechos humanos [...].
> Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales [...].
> El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales [...]
> El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos. (COMITÉ..., 2016, p. 9-15).

En síntesis, para el caso chileno, la seguridad en el ciberespacio está en la agenda de la autoridad política y durante el período 2014–2016 se ha trabajado en la preparación de la Política Nacional de Ciberseguridad, donde laboran coordinadamente el Ministerio del Interior y Seguridad Pública, junto al Ministerio de Defensa Nacional y otras reparticiones de la Administración del Estado vinculadas directamente con esta materia en el Poder Ejecutivo. Se constatan importantes avances en la formulación de la política a nivel nacional, fundamentalmente con la generación de instancias de trabajo que integran a diferentes actores vinculados al tema, los cuales han propuesto una política nacional de ciberseguridad que está en espera de respuesta por parte de las máximas autoridades nacionales. A nivel internacional, la participación en diferentes grupos de trabajo sobre el tema, permite apreciar el modo en que ambas dimensiones claves de la ciberseguridad están contempladas en el trabajo de las autoridades. Entre los desafíos destaca el cumplimiento de las programaciones realizadas y los objetivos formulados para contar con una política nacional de ciberseguridad e iniciar su implementación en 2016.

De acuerdo a lo indicado, es posible afirmar que en el caso chileno el incremento en el uso de ciberespacio ha estimulado a la autoridad a formular una política pública de ciberseguridad que debiera estar lista en 2016 y a enfrentar el desafío de tener una política de ciberdefensa, acorde con las necesidades nacionales y ya se están dando los primeros pasos en este camino.

12 Conclusiones

El ciberespacio es un ambiente en el cual se desarrollan de modo creciente las interacciones de las personas en el ámbito social, económico, político, educacional, entre otros. Además, permite ilustrar la forma en que la revolución de las TIC ha potenciado el fenómeno de la globalización, haciendo posible de esta manera el desarrollo de acciones desde organizaciones que están generando cambios y, con ello, reconfigurando la forma en que el poder es ejercido por personas, instituciones y gobiernos.

El ciberespacio no solo posee ventajas como mayor rapidez y economía en las comunicaciones y transacciones entre personas, beneficios que lo han llevado a ser reconocido como un bien público global, siendo el Estado quien debe encargarse de su adecuada provisión.

También el ciberespacio presenta riesgos y amenazas producto de incidentes originados en acciones deliberadas para generar daño en la información electrónica y/o a los sistemas que la controlan, lo cual puede manifestarse como un asunto delictual (robo de clave) o un problema de seguridad del país (ataque a alguna infraestructura crítica).

Para evitar ese tipo de situaciones es necesario entender la ciberseguridad como condición que garantiza, de acuerdo a estándares internacionales, la preservación de las características de información virtual (disponibilidad, integridad, oportunidad, interoperabilidad, confidencialidad y seguridad) con la finalidad de resguardar la vida de personas, la integridad, estabilidad y normal funcionamiento de los países y su prosperidad económica. Ello implica evitar –en lo posible- la ocurrencia de cibercrimen, ciberespionaje, ciberhacktivismo e inclusive ciberguerra y, en caso de producirse alguno de ellos, contar con un plan de contingencia que contemple acciones de prevención, respuesta, mitigación y resiliencia, con la finalidad de enfrentar en la mejor forma posible el ciberincidente manifestado.

En efecto, esta dimensión en la cual se producen interacciones sociales en forma creciente no está exenta de riesgos y amenazas, siendo necesaria la garantía de estándares mínimos de seguridad en su uso, lo cual requiere enfrentar importantes desafíos a nivel nacional e internacional. Entre ellos destaca en el nivel nacional la formulación de una política pública de ciberseguridad, que contemple e integre los diferentes aspectos involucrados en este tema con la finalidad de evitar que un ciberincidente ponga en riesgo la vida de las personas, su patrimonio y/o la seguridad nacional. A nivel internacional, cobra relevancia la necesidad de participar en instancias de diálogo multilaterales, donde Chile promueva su visón con respecto a temas como: la gobernanza en internet; estándares mínimos de seguridad en el ciberespacio y la participación en convenios o resoluciones internacionales sobre situaciones que afectan la ciberseguridad y que involucran a diferentes países del mundo.

En esta perspectiva, una política pública de ciberseguridad es clave para garantizar el adecuado funcionamiento del ciberespacio y la información que en este es generada, almacenada y transferida. Estas orientaciones establecerán el nivel mínimo en el cual organizaciones públicas y privadas deberán gestionar la información, particularmente en el caso de aquellas consideradas como críticas para el país, constituyendo una tarea ineludible para las máximas autoridades de los países y un desafío urgente para el caso chileno, en el cual se está trabajando.

Referencias

ALALUF, Alejandro. Tecnología: la ciberseguridad de Mr. K. *Qué Pasa*, Santiago, 15 agosto 2013. Disponible en: <http://www.quepasa.cl/articulo/tecnologia/2013/08/23-12457-9-tecnologia-la-ciberseguridad-de-mr-k.shtml/>. Fecha de acceso: 06 feb. 2016.

ALMAGRO, Luis. Mensaje del Secretario General de la OEA. In: ORGANIZATION OF AMERICAN STATES; INTER-AMERICAN DEVELOPMENT BANK. *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?* Washington, DC, 2016. Disponible en: <https://publications.iadb.org/handle/11319/7449?locale-attribute=en&locale-attribute=pt&locale-attribute=es&>. Fecha de acceso: 03 marzo 2016.

ÁLVAREZ, Daniel. Ciberseguridad en el contexto local. In: SEMINARIO INTERNACIONAL CIBERSEGURIDAD Y CIBERDEFENSA EN CHILE, 2015, Santiago. *Anais*..., Santiago: Facultad de Derecho, Universidad de Chile, 2015.

ANABALÓN, Juan; DONDERS, Eric. Una revisión de ciberdefensa de infraestructura crítica. *Revista ESD*: Estudios de Seguridad y Defensa, Santiago, n. 3, p. 131-164, 2014. Disponible en: <http://esd.anepe.cl/wp-content/uploads/2014/11/art5.pdf>. Fecha de acceso: 20 marzo 2016.

ASÍ secuestraron mi teléfono los piratas informáticos. *BBC Mundo*, [S.l.], 04 marzo 2016. Disponible en: <http://www.bbc.com/mundo/noticias/2016/03/160304_tecnologia_telefono_smartphone_secuestro_il>. Fecha de acceso: 06 marzo 2016.

BORG, Scott. No es una guerra fría. *Vanguardia Dossier*, [S.l.], n. 54, enero/marzo 2015.

CANDAU, Javier. Estrategias Nacionales de Ciberseguridad: Ciberterrorismo. *Cuadernos de Estrategia*, Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio, Madrid, n. 149, dic. 2010. Disponible en: <http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf>. Fecha de acceso: 26 feb. 2016.

CARVAJAL, Víctor; JARA, Matías. Grave falla en la red del Minsal dejó expuesta información confidencial de pacientes. *Ciper*, Santiago, 5 marzo 2016. Disponible en: <http://ciperchile.cl/2016/03/05/grave-falla-en-la-red-del-minsal-dejo-expuesta-informacion-confidencial-de-pacientes/>. Fecha de acceso: 23 feb. 2016.

CASTELLS, Manuel. *La era de la información*: economía, sociedad y cultura. Ciudad de México: Editorial Siglo XXI, 1999. (El poder de la identidad, v. 2.).

CLARKE, Richard; KNAKE, Robert. *Guerra en la red*: los nuevos campos de batalla. Barcelona: Ariel, 2011.

CUBEIRO, Enrique. Ciberdefensa. In: DÍAZ, Antonio (Ed.). *Conceptos fundamentales de inteligencia.* Valencia: Tirant lo Blanch, 2016. (Inteligencia y Seguridad).

CHILE. Ministerio de Relaciones Exteriores. *Subsecretario Riveros viaja a La Haya para participar en Conferencia Global del Ciberespacio*. Santiago, 2015a. Disponible en: <http://www.minrel.gob.cl/subsecretario-riveros-viaja-a-la-haya-para-participar-en-conferencia-global-del-ciberespacio/minrel/2015-04-14/150737.html>. Fecha de acceso: 17 dic. 2015.

_____. Ministerio del Interior y Seguridad Pública. *Cuenta Pública 2015*. [Santiago], 2015b. Disponible en: <http://www.gob.cl/cuenta-publica/2015/sectorial/2015_sectorial_ministerio-interior-y-seguridad-publica.pdf>. Fecha de acceso: 02 abr. 2016.

_____. *Gobierno crea comité para elevar estándares en materia de ciberseguridad*. Santiago, 2015c. Disponible en: <http://subinterior.gob.cl/noticias/2015/04/20/gobierno-crea-comite-interministerial-para-elevar-estandares-en-materia-de-ciberseguridad/>. Fecha de acceso: 20 enero 2015.

COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD. *Propuesta de Política Nacional de Ciberseguridad (PNCS) 2016–2022*. Santiago, 2016. Disponible en: <http://ciberseguridad.interior.gob.cl/media/2016/02/Borrador-Consulta-P%C3%BAblica-PNCS.pdf>. Fecha de acceso: 9 marzo. 2016.

DÍAZ, Felipe. Fraudes con tarjeta bancaria casi se duplicaron en 2015. *La Tercera*, [Santiago], 20 enero 2016. Disponible en: <http://www.latercera.com/noticia/nacional/2016/01/680-664890-9-fraudes-con-tarjetas-bancarias-casi-se-duplicaron-en-2015.shtml>. Fecha de acceso: 10 enero 2016.

EL ESTADO Islámico hackeó el Twitter del Pentágono. *Soychile*, Santiago, 12 enero 2015. Disponible en: <http://www.soychile.cl/Santiago/Internacional/2015/01/12/298787/El-Estado-Islamico-hackeo-el-Twitter-del-Pentagono.aspx>. Fecha de acceso: 12 marzo 2016.

HELD, David et al. *Transformaciones globales*: política, economía y cultura. [S.l.]: Oxford University, 2002.

HIRANE, Carolina Sancho. Ciberespacio: delitos, amenazas a la seguridad y ¿guerras? *ANEPE*, Santigo, 2012. Disponible en: <http://www.anepe.cl/2012/07/ciberespacio-delitos-amenazas-a-la-seguridad-y-guerras/>. Fecha de acceso: 02 marzo 2016.

HIRANE. Ciberseguridad: enfrentando riesgos y amenazas en un mundo globalizado. *ANEPE*, Santiago, 2013a. Disponible en: <http://www.anepe.cl/2013/06/ciberseguridad-enfrentando-riesgos-y-amenazas-en-un-mundo-globalizado/>. Fecha de acceso: 02 marzo 2016.

_____. Cultura de ciberseguridad: tarea pendiente en la era de la información? *ANEPE*, Santiago, 2013b. Disponible en: <http://www.anepe.cl/2013/11/cultura-de-ciberseguridad-tarea-pendiente-en-la-era-de-la-informacion/>. Fecha de acceso: 02 marzo 2016.

_____. El ciberespacio como bien público y la ciberseguridad como problema: algunos dilemas y desafíos en tiempos de globalización. In: ACADEMIA NACIONAL DE ESTUDIOS POLÍTICOS Y ESTRATEGICOS (Chile). *Desafíos de la Seguridad y Defensa en el mundo contemporáneo*. [Santiago], 2016. En impresión.

INSTITUTO ESPAÑOL DE CIBERSEGURIDAD. *La Ciberseguridad Nacional, un compromiso de todos*: la necesidad de evolucionar de una cultura reactiva a una de prevención y resiliencia. Madrid, 2012. Disponible en: <https://www.ismsforum.es/ficheros/descargas/informe-scsi1348666221.pdf>. Fecha de acceso: 16 enero 2016.

KARPERSKY. *Los riesgos futuros: protéjase*. [S.l.], 2015. Disponible en: <http://go.kaspersky.com/rs/802-IJN-240/images/APT_Report_ONLINE_AW_ES.pdf>. Fecha de acceso: 17 feb. 2016.

KARPESKY habla sobre el virus flame. *Coordinación en Seguridad de la Información (México)*, [S.l.], 01 jun. 2012. Disponible en: <http://www.seguridad.unam.mx/noticia/?noti=377>. Fecha de acceso: 02 abr. 2016.

KAUL, Inge; GRUNBERG, Isabelle; STERN, Marc A. *Bienes Públicos Mundiales*: la cooperacion internacional en el siglo XXI. [S.l.]: Oxford University, 2001.

KISSINGER, Henry. *Orden mundial*: Reflexiones sobre el carácter de las naciones y el curso de la historia. [S.l.]: Debate, 2016.

LA CONFERENCIA de Meridian reúne en España a decisores políticos en protección de infraestructuras críticas. *Red Seguridad*, [S.l.], 22 jul. 2015. Disponible en: <http://www.redseguridad.com/actualidad/info-tic/la-conferencia-meridian-reune-en-espana-a-decisores-politicos-en-proteccion-de-infraestructuras-criticas>. Fecha de acceso: 17 dic. 2015.

LAQUEUR, Walter. La guerra cibernética. *Vanguardia Dossier*, [S.l.], n. 54, 2015.

LIÑÁN, José Manuel Abad. Anonymus declara la guerra al ISIS: quiénes son y qué han conseguido. *El País*, Madrid, 18 nov. 2015. Disponible en: <http://tecnologia.elpais.com/tecnologia/2015/11/17/actualidad/1447752730_293113.html>. Fecha de acceso: 4 enero 2016.

MARÍN, José; GARCÍA-VERDUGO, Javier. *Bienes públicos globales, política económica y globalización*. Barcelona: Ariel, 2003.

MUÑOZ, Daniela. Registro civil denuncia copia irregular de bases de datos de carnés y pasaportes. *La Tercera*, [Santiago], 22 marzo 2014. Disponible en: <http://www.latercera.com/noticia/nacional/2014/03/680-570673-9-registro-civil-denuncia-copia-irregular-de-bases-de-datos-de-carnes-y-pasaportes.shtml>. Fecha de acceso: 21 feb. 2016.

NYE, Joseph S. Ciberguerra y Ciberpaz. *Project Sindicate*, Cambridge, 10 Apr.. 2012. Disponible en: <http://www.project-syndicate.org/commentary/cyber-war-and-peace/spanish>. Fecha de acceso: 15 marzo 2016.

_____. El rugido del clic del ratón. *El País*, [S.l.], 10 oct. 2013. Disponible en: <http://elpais.com/elpais/2013/09/13/opinion/1379069360_411737.html>. Fecha de acceso: 14 marzo 2016.

_____. ¿Se puede ejercer la disuasión en la guerra cibernética? *Project Sindicate*, Cambridge, 10 dic. 2015. Disponible en: <https://www.project-syndicate.org/print/cyber-warfare-deterrence-by-joseph-s--nye-2015-12/spanish>. Fecha de acceso: 23 feb. 2016.

ROBLEDO, Marcos. Discurso en la Inauguración del Seminario Internacional. In: SEMINÁRIO INTERNACIONAL CIBERSEGURIDAD Y CIBERDEFENSA EN CHILE, 2015, Santiago. *Anais*..., Santiago: Facultad de Derecho, Universidad de Chile, 2015.

SAIZ, Eva. Los ciberataques sustituyen al terrorismo como primera amenaza a EE UU. *El País*, Washington, DC, 13 marzo 2013. Disponible en: <http://internacional.elpais.com/internacional/2013/03/13/actualidad/1363187707_199021.html>. Fecha de acceso: 15 feb. 2016.

TORRES, Anselmo del Moral. *Cooperación Policial en la Unión Europea*: la necesidad de un modelo de inteligencia criminal eficiente. [S.l.]: Editorial Dikinson, 2011.

TORRES, Manuel. Ciberguerra. In: JORDÁN, Javier (Coord.). *Manual de Estudios Estratégicos y Seguridad Internacional*. Madrid: Plaza y Valdés, 2013.

TREND MICRO; ORGANIZATION OF AMERICAN STATES. *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas 2015*. Irving, 2015. Disponible en: <https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf>. Fecha de acceso: 20 feb. 2016.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. *Informe sobre medición de la Sociedad de la Información 2014*: resumen ejecutivo. Ginebra, 2014. Disponible en: <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS_2014_Exec-sum-S.pdf >. Fecha de acceso: 11 feb. 2016.

_____. *Informe sobre medición de la Sociedad de la Información 2015*: resumen ejecutivo. Ginebra, 2015. Disponible en: <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-ES-S.pdf>. Fecha de acceso: 11 feb. 2016.

VILLAMEDIANA, Miriam. Los datos son el nuevo petróleo del siglo XXI. *Euroexpress*, [Madrid], 01 jul. 2015. Disponible en: <http://www.euroxpress.es/noticias/los-datos-son-el-nuevo-petroleo-del-siglo-xxi>. Fecha de acceso: 13 enero 2016.

WORLD ECONOMIC FORUM. *Global Risks 2013*: eighth edition. Ginebra, 2013. Disponible en: <http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf>. Fecha de acceso: 08 enero 2016.

XIMENEZ, Pablo. Michael Hayden: 'Me preocupa que Trump pueda ser presidente'. *El País*, Los Angeles, 05 marzo 2016. Disponible en: <http://internacional.elpais.com/internacional/2016/03/04/actualidad/1457076618_844331.html>. Fecha de acceso: 05 marzo 2016.

LINEAMIENTOS DE POLÍTICA EN CIBERSEGURIDAD Y CIBERDEFENSA: LOGRANDO LA SEGURIDAD Y DEFENSA DE COLOMBIA EN UN MUNDO DIGITAL[1]

Martha Liliana Sánchez-Lozano*
Steven Jones-Chaljub**

1 Introducción

Colombia ha presentado una tendencia creciente en los niveles digitalización desde hace varios años, lo cual ha traído grandes oportunidades y amenazas para el país. El número de suscriptores a internet (fijo dedicado y móvil) en Colombia pasó de 687.637 en el 2005 a 10'112.622 en el primer trimestre del 2015 (CONSEJO..., 2016, p. 27; COLOMBIA, 2015a, p. 9). En términos territoriales, este nivel de penetración representó una conectividad de 1.078 municipios de un total de 1.123 (COLOMBIA, 2015b, p. 7-11), y la instalación de 7621 centros de acceso comunitario para las zonas apartadas y centros rurales con más de 100 habitantes (CONSEJO..., 2016, p. 27). Los beneficios de la conectividad se evidencian en diferentes sectores, siendo el financiero uno donde mayor injerencia se tiene. El número de operaciones monetarias usando internet como canal pasó de 31.66% en el 2012 a 42.62% en el 2015, lo cual significó un 35% más de transacciones (SUPERINTENDENCIA..., 2015, p. 5-7). Se estima que la digitalización entre los años 2005 y 2013, representó un crecimiento acumulado del 6.12% del Producto Interno Bruto nacional (SUPERINTENDENCIA..., 2015, p. 5-7).

Los altos niveles de conectividad incrementan la dependencia de los diferentes actores (ej. individuos, empresas, instituciones públicas y privadas, etc.) en las Tecnologías de la Información y Comunicación (TIC), lo que significa mayor

1 Artículo vinculado al proyecto: Construcción de capacidades de Ciberseguridad y Ciberdefensa para un entorno digital estable y seguro, del grupo de Investigación de Ciberdefensa del programa de Maestría de Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra de Colombia.

* Coronel Martha Liliana Sánchez Lozano, Oficial de la Fuerza Aérea de Colombia. Cuenta con formación universitaria en ingeniería de sistemas, Especialidad en Sistemas de Información, Maestría en Administración de Negocios (MBA), y Doctorando en Derecho Internacional. Actualmente se desempeña como Directora de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra (ESDEGUE). Contacto: <martha.sanchez@esdegue.edu.co>

** Steven Jones-Chaljub es Especialista en Contra-Terrorismo, Magister (MA) en Seguridad Internacional y Magister (M.Sc) en Estudios Estratégicos. Actualmente se desempeña como docente investigador de la Escuela Superior de Guerra (ESDEGUE) y asesor en seguridad y defensa nacional para el Comando General de las Fuerzas Militares de Colombia. Contacto: <steven.jones@esdegue.edu.co>

impacto negativo proveniente de las amenazas que rondan en el ambiente digital. Colombia es consciente de esto y, debido a diferentes experiencias nacionales e internacionales, ha invertido importantes recursos y tiempo en desarrollar capacidades de ciberseguridad y ciberdefensa. El principal esfuerzo del país puede rastrease al año 2011 donde desarrolló su primera política pública en materia, conocida bajo la nomenclatura 'CONPES 3701: Lineamientos de Política para ciberseguridad y ciberdefensa'. A partir de este momento el país ha llevado un camino con grandes logros operativos, legislativos, estratégicos y diplomáticos.

El presente artículo tiene como objetivo presentar el desarrollo que Colombia ha tenido en el tema de seguridad y defensa en un mundo digital. Para ello se hace una presentación básica de los incidentes cibernéticos que sirvieron de catalizadores para comenzar el proceso, y una descripción del CONPES 3701 (CONSEJO..., 2011) y un recuento de sus logros. De igual manera, se analizan las razones que obligaron al país a actualizar su política, y se expondrán los principales elementos de esta. Finalmente, se describirá el escenario ideal que Colombia pretende alcanzar en términos de ciberseguridad y ciberdefensa. De antemano se concluyó que el proceso de digitalización de Colombia, por ser una fuente de grandes oportunidades y retos, obligó al país a entrar en una dinámica de construcción de política pública encaminada a potenciar y desarrollar capacidades de ciberseguridad y ciberdefensa. Igualmente, se concluyó que los avances del país, manifiestos en la creación de diferentes estructuras operacionales (ColCERT, CSIRT, Comando Conjunto Cibernético de las Fuerzas Militares, Centro Cibernético Policial (CCP), y los Comandos Cibernéticos de cada una de las Fuerzas) y herramientas jurídicas, requieren seguir su camino de mejora para alcanzar el ideal requerido para el futuro contexto estratégico nacional.

2 Recorrido de Colombia hacia la Seguridad y Defensa en el Contexto Digital

No es un misterio que las Tecnologías de la Información y Comunicación (TIC), al igual que los mayores niveles de conectividad, traen grandes beneficios y oportunidades para los diferentes usuarios (BAKER, 2014, p. 122-123). De igual manera, tampoco lo es el hecho que el ciberespacio, entendido tanto en su componente físico como virtual, trae consigo retos con capacidad de impacto económico, político y social. [2] Estos retos no discriminan según la naturaleza de los

2 La legislación Colombiana entiende el término 'ciberespacio' de la siguiente manera: "es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios" (Resolución 2258 de 2009, Comisión de Regulación de Comunicaciones de la República de Colombia).

usuarios; son igualmente vulnerables los Estados, las organizaciones públicas y privadas, y los individuos. Colombia no es la excepción en este sentido. En el año 2011 Colombia prendió las alarmas frente a la necesidad de adquirir capacidades en ciberseguridad y ciberdefensa, planteando la primera política pública con referencia directa a esta materia. El documento fue desarrollado el 14 de julio de 2011 por el Consejo Nacional de Política Económica y Social, máxima autoridad de planeación, adjudicándole la nomenclatura de 'CONPES 3701'.

La creación del CONPES 3701 (CONSEJO…, 2011) no responde a una casualidad, sino como consecuencia a los incidentes cibernéticos ocurridos internacional y nacionalmente, siendo estos últimos evidencia de las debilidades del país. Actualmente existe una deficiencia en información estadística que permita realizar un análisis histórico certero de incidentes cibernéticos ocurridos en Colombia antes del 2012, fecha promedio de la materialización de las iniciativas del CONPES 3701 (CONSEJO…, 2011). Sin embargo, hay datos aislados que permiten hacer un mapeo de la situación nacional en el periodo 2009-2011, al igual que identificar hechos catalizadores.

El 23 de diciembre de 2009 se desmanteló, en una operación conjunta entre *Panda Security*, FBI y la Guardia Civil Española, una de las más grandes *Botnets* para *cyberscamming* y *DDoS* conocidas hasta la fecha: *Botnet* 'Mariposa'. En la cuenta de afectación de Mariposa- 13 millones de computadores, 190 países y 31.901 ciudades – Colombia se encontró en la quinta posición con 4.94% de las infecciones, dos de sus ciudades principales también lograron la lista de mayor número de IP comprometidas (i.e. Bogotá, d.C, 2.68% y Medellín 0.65%) (OVER…, 2010). Ese mismo año, *McAffe Labs* ya había identificado a Colombia como el origen de 1.9% del *Spam* mundial, por encima de países con mayor nivel de conectividad y población como Rusia (MCAFEE LABS, 2010, p. 11).

El año 2009 tuvo un recuento importante de delitos informáticos. En el marco de la Ley 1273/09, se reportaron 575 delitos informáticos discriminados de la siguiente manera: 259 accesos abusivos a un sistema informático; 247 hurtos por medios informáticos; 17 intercepciones de datos informáticos; 35 violaciones de datos personales; 8 transferencias no consentidas de activos; 5 suplantaciones de sitios *Web*; 1 obstaculización ilegítima de un sistema informático. El 2010 presentó un incremento en la cantidad de delitos y

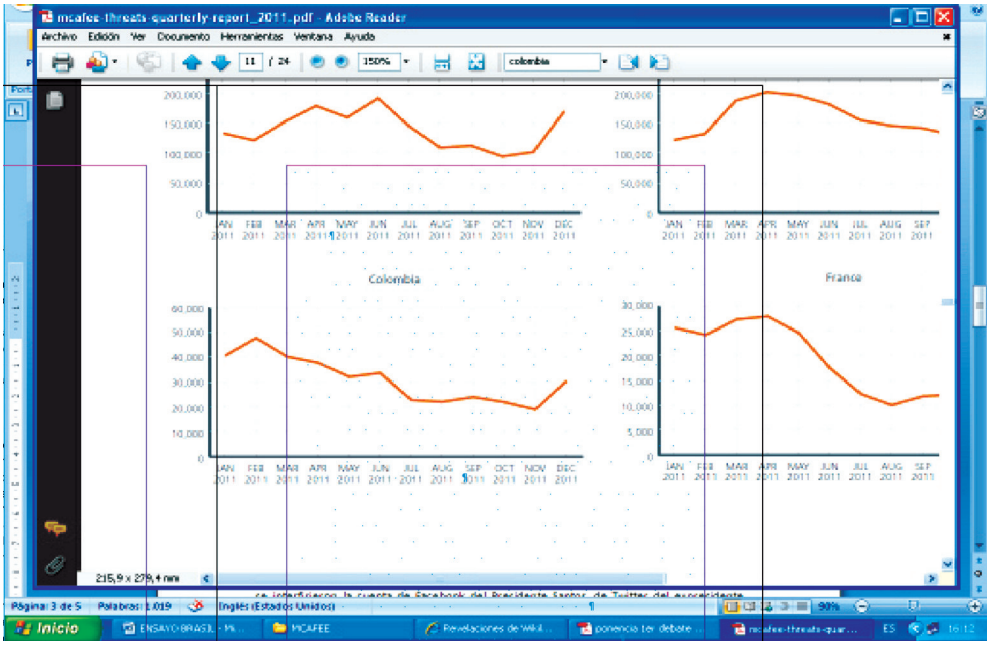
contravenciones informáticas de un 73% (CONSEJO…, 2011, p. 10).

Las filtraciones de los cables secretos de los Estados Unidos publicados por *Wikileaks* entre 2010-2011, tuvieron un coletazo importante en las relaciones diplomáticas entre Colombia y sus vecinos, particularmente con Venezuela y Ecuador (CALDERÓN, 2010). Tensiones generadas por la estrecha relación entre Colombia y el país norteamericano en la lucha contra las drogas y el terrorismo, y por las diferencias políticas con el Movimiento Bolivariano del fallecido Expresidente Hugo Chávez (LEÓN, 2010). En el año 2010 Colombia mantuvo la tendencia como fuente de *Spam*, entrando nuevamente al *McAffe Labs Report* (2011, p. 11) como caso de estudio.

El 4 de abril de 2011, el otrora Ministro del Interior y Justicia, ahora Vicepresidente de la República de Colombia, Germán Vargas Lleras presentó al Congreso el Proyecto de Ley 241 de 2011, conocida por la opinión pública como Ley Lleras, por la cual se buscaba regular la responsabilidad por las infracciones al derecho de autor y los derechos conexos en internet (COLOMBIA, 2011). El 15 de abril del mismo año, las páginas web de Presidencia, Senado, Ministerio del Interior, y la plataforma de trámites Gobierno en Línea, sufrieron ataques *DDoS* que las inhabilitaron totalmente por varias horas (COLECTIVO…, 2011). El incidente se atribuyó al grupo hacktivista *Anonymous*. Estos ataques se repitieron el 20 de julio de 2011 donde, en el marco de lo que *Anonymous* denominó 'Operación Independencia', se le negó el servicio a la página *web* del Ministerio de Defensa, y se interfirieron las cuentas de *Facebook* y *Twitter* del Presidente Santos y Expresidente Uribe (PÁGINAS…, 2011). La arremetida de *Anonymous* continuó hasta el 2012, exacerbada por la presentación de una nueva versión de la Ley Lleras (Ley 201 de 2012) y la Cumbre de las Américas.

Según el *McAfee Threats Report*, Colombia presentó en el año 2011 un aumento significativo de computadores *Zombie* utilizados como remitentes de *Malware* para la creación de *botnets*, superando a países como Japón, España, Australia, Portugal, Reino Unido y Venezuela (MCAFEE LABS, 2011, p. 11-13). Aunque no existe información suficiente para establecer una correlación directa entre la implementación del CONPES 3701 (CONSEJO…, 2011) y la tendencia decreciente de computadores *Zombie*, es interesante notar que a partir de julio de 2011 Colombia alcanzó los niveles más bajos de infección (Ver Imagen n° 1).

Imagen 1 - Evolución de las Botnets en Colombia

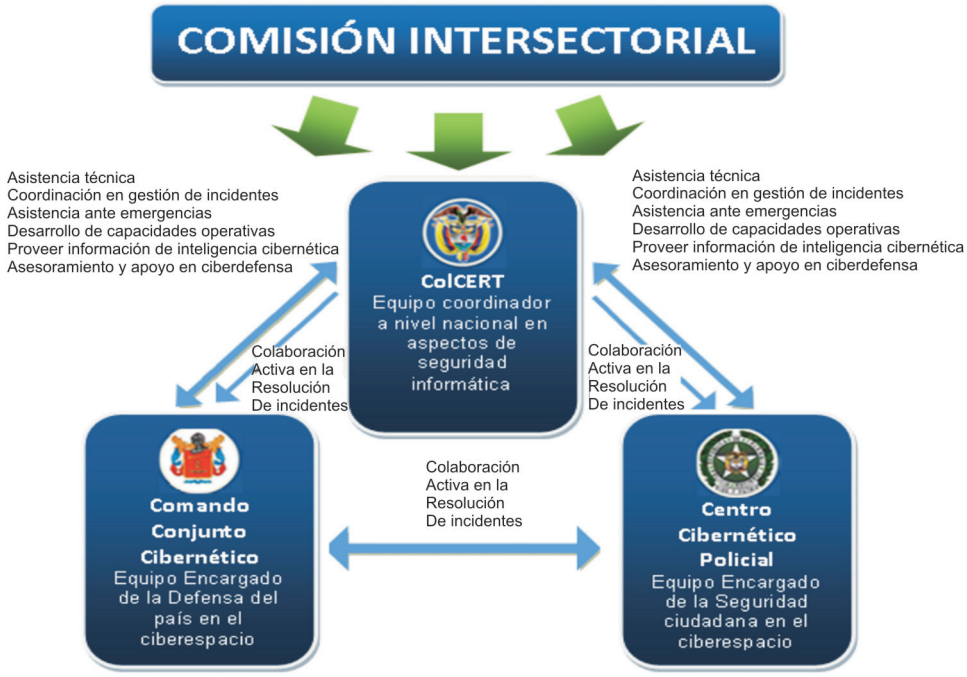


Fuente: Report: Fourth Quarter 2011. p. 11 (MCAFEE LABS, 2012)

El CONPES 3701 (CONSEJO..., 2011) se creó para dar respuesta a incidentes cibernéticos símiles a los reportados entre 2009-2011 en Colombia. Así lo establece el documento en su introducción cuando afirma que "el Gobierno Nacional requiere conocer y actuar de forma integral frente amenazas informáticas [...] [que puedan] comprometer información, afectar infraestructura crítica del país y poner en riesgo la seguridad y defensa del Estado." (CONSEJO..., 2011, p. 4-5). Para ello, el CONPES 3701 (CONSEJO..., 2011) establece tres ejes estratégicos: desarrollo de capacidades de ciberseguridad y ciberdefensa, fortalecimiento del cuerpo normativo, y capacitación especializada.

El desarrollo de capacidades de ciberseguridad y ciberdefensa dentro del CONPES 3701 (CONSEJO..., 2011), se concibió con el objetivo de prevenir, coordinar, atender, controlar, generar recomendaciones y regular incidentes o emergencias cibernéticas (CONSEJO..., 2011, p. 20). Para ello se concibieron cuatro organismos: comisión intersectorial, Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), Comando Conjunto Cibernético de las Fuerzas Militares (CCOC), Centro Cibernético Policial (CCP).

Imagen 2 - Modelo de Coordinación de las Instituciones de Ciberseguridad y Ciberdefensa



Fuente: CONPES 3701. (CONSEJOS..., 2011). Lineamientos de Política para Ciberseguridad y Ciberdefensa. Bogotá D.C., p. 21.

La Comisión Intersectorial se planteó como el cuerpo de direccionamiento estratégico de carácter interagencial encargado de fijar lineamientos para política. Por su parte, el ColCERT se diseñó como el grupo que da forma a los lineamientos estratégicos, coordinando las acciones necesarias para proteger al Estado colombiano frente a amenazas cibernéticas que atenten o comprometan su seguridad y defensa nacional. Dentro de los objetivos específicos diseñados para el ColCERT caben resaltar su rol como asesor de los *Computer Security Incident Response Team* (CSIRT) sectoriales, y su función como fuente de inteligencia para el CCP y CCOC. [3] Estos dos últimos organismos se plantearon según la naturaleza del ente que los administra. El CCP se diseñó para el apoyo y protección ante delitos cibernéticos, mientras que el CCOC para prevenir y contrarrestar amenazas

3 Los CSIRT sectoriales que existen actualmente en Colombia son: CSIRT-Policía Nacional; CSIRT-Cámara Colombiana de Informática y Telecomunicaciones; CSIRT- Empresa de Telecomunicaciones de Bogotá S.A ESP; DigiCSIRT- DigiSOC Computer Security.

o ataques cibernéticos que afecten los valores e intereses nacionales (CONSEJO…, 2011, p. 20-24).

A partir del año 2011 y hasta el 2015, año de la creación del nuevo borrador de CONPES en materia cibernética, el Estado colombiano ha cumplido en un 90% con lo planteado por el Consejo Nacional. Se crearon y pusieron en operación el ColCERT, CCOP y CCOC con grandes resultados (CONSEJO…, 2016, p. 33). Los logros más representativos del CCOC fueron: la creación de un comité de ciberdefensa de las Fuerzas Militares; adquisición de la plataforma de entrenamiento y ciberdefensa; cooperación internacional con Estados Unidos, OEA, y España; 38 cursos de capacitación y 340 servidores entrenados; adquisición de plataformas operacionales en ciberdefensa; identificación de infraestructuras críticas cibernéticas nacionales; elaboración del manual de ciberdefensa conjunta (COMANDO…, 2015).

Igualmente los incidentes digitales nacionales, el CCP agenció 2.652 incidentes en el año 2013, mientras que para el año 2015 el CCP y CSIRT de la Policía Nacional atendieron 6.366 incidentes, incrementando la cobertura de capacidades operativas en un 140%. De estos últimos el 34,4% corresponden *defacement*, 15,5% a estafa en compra / venta de servicios en Internet, 8,9% a usurpación de identidad, 7% a *phishing* y 5,2% a *smishing*. No sólo hubo logros en atención a incidentes, también el cuerpo jurídico y las capacidades permitieron un aproximado de 330 capturas para el periodo comprendido 2014-2015, y un bloqueo de 3.643 *URL* dentro del programa *Te Protejo* por concepto de pornografía infantil (CONSEJO…, 2016, p. 61-63). A destacar la captura hecha en el año 2014 de alias 'gemido ruidoso', uno de los mayores distribuidores de pornografía infantil de Colombia a la fecha. Esta operación fue posible gracias al trabajo entre la Policía de Manchester (UK), Interpol y el Centro Cibernético Policial (CCP) (ASÍ…, 2015).

El CONPES 3701 (CONSEJO…, 2011) reconoció que el Estado tenía una clara debilidad en regulación y legislación en materia cibernética, y como tal recomendó fortalecer el cuerpo legal y cooperación internacional. Desde julio del año 2011, Colombia desarrolló 11 herramientas jurídicas (4 leyes y 7 decretos) en materia cibernética; algunas para seguridad y defensa, otras para regular servicios electrónicos

Cuadro 1 - Principales Herramientas Jurídicas en Materia Cibernética

NOMENCLATURA	TEMÁTICA
Ley 1480 de 2011	Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas.
Decreto Ley 019 de 2012	Racionalización de trámites a través de medios electrónicos. Criterio de seguridad.
Ley 1581 de 2012	Ley estatutaria de Protección de datos personales.
Ley 1623 de 2013	Ley de Inteligencia –Criterios de seguridad.
Ley 1712 de 2014	Transparencia en el acceso a la información pública.
Decreto 2364 de 2012	Firma electrónica.
Decreto 2609 de 2012	Expediente electrónico.
Decreto 2693 de 2012	Gobierno electrónico.
Decreto 1377 de 2013	Protección de datos personales.
Decreto 1510 de 2013	Contratación Pública electrónica.
Decreto 333 de 2014	Entidades de certificación digital.

Fuente: CÁRDENAS, 2014. Instrumentos Normativos de Ciberseguridad. Certicámara.

En cooperación internacional Colombia también ha tenido grandes avances; se han adelantado experiencias e información con países como Estonia, España, Estados Unidos, Israel, Brasil, Chile, México, Corea del Sur, entre otros. En el caso particular de asistencia bilateral con Corea del Sur, Colombia firmó un acuerdo de transferencia de conocimiento en Tecnologías de Información y Comunicación (TIC) en temáticas como ciberseguridad, seguridad de la información y gobierno electrónico (ANDERSON, 2015). De igual manera, se han tenido acercamientos con organizaciones como Naciones Unidas, OTAN, el Comité Interamericano Contra el Terrorismo (CICT) de la Organización de Estados Americanos (OEA), Foro Económico Mundial, OECD, e Interpol (CONSEJO…, 2016, p. 13; COMANDO…, 2015-2016).

Dentro de los logros de política internacional más destacables, Colombia fue invitada por el Consejo de Europa en el año 2011 a adherirse a la Convención Sobre Delito Cibernético, conocido también como Convenio de Budapest, lo que le convierte en una de las pocas excepciones de países no miembros en formar parte de esta herramienta de política internacional (i.e. Estados Unidos, Japón, Canadá y República Dominicana). A la fecha, la adhesión de Colombia a la Convención está siendo analizada por los respectivos entes gubernamentales, pero el panorama

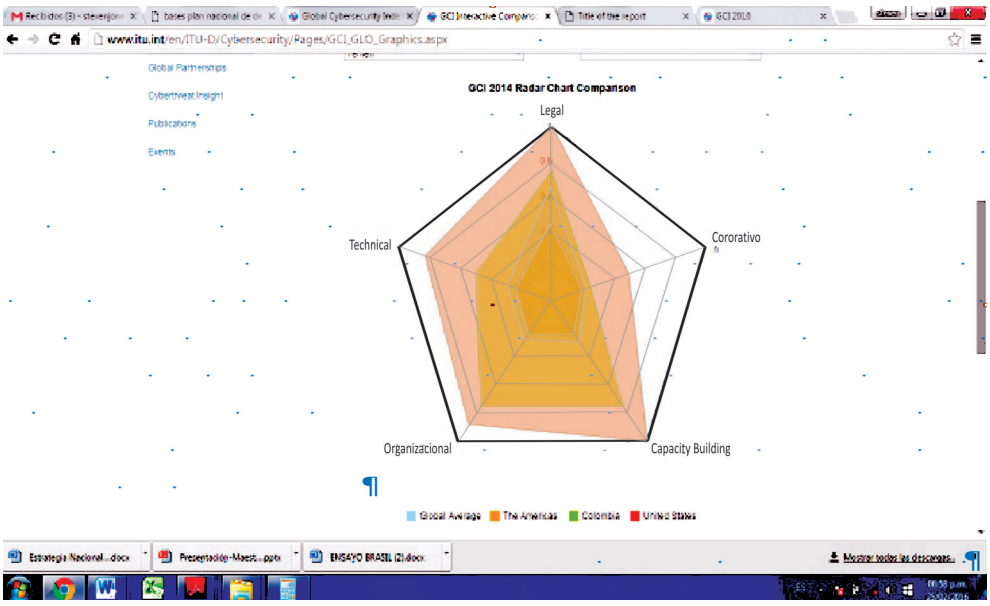
parece ser positivo. Así lo dejó entrever la Viceministra de Tecnologías y Sistemas de la Información, María Isabel Mejía, cuando afirmó que "[el Convenio de Budapest] se tiene que convertir en una ley de la República para la guerra contra el cibercrimen." (MEDINA, 2015). Es igualmente destacable que el COLCERT haya logrado vincularse al *Forum of Incident Response and Security Teams (FIRST)*, importante espacio para el intercambio de información y cooperación en asuntos de interés común frente a la seguridad cibernética (FORUM…, [2015?]).

En reconocimiento que la temática de ciberseguridad y ciberdefensa es multidisciplinaria, y que los diferentes actores tienen experiencias que pueden ser incorporadas para formas mejores prácticas, Colombia también ha tenido acercamientos asistenciales con firmas multinacionales. Tal es el caso de *Microsoft* donde se firmó un memorando de entendimiento para programas como: *Cybercrime Center, Cyber Threat Intelligence Program (CTIP), Security Cooperation Program (SCP)* (COLOMBIA, 2013). Dentro de las tendencias a trabajar que más afectan a Colombia se resaltó el *phishing, smishing,* software espía (*malware* o troyanos), *key logger* y clonación de tarjetas de débito y crédito.

Los avances desde la firma del CONPES 3701 (CONSEJO…, 2011) son, hasta la fecha, impresionantes para un periodo de tiempo tan corto; éstos han ubicado a Colombia, según el *Global Cibersecurity Index* de la Unión Internacional de Telecomunicaciones (UIT), en una posición ventajosa respecto al promedio mundial y de las Américas. El Índice se calcula en base a cinco variables: legislación, cooperación, construcción de capacidades, organización, y conocimiento técnico. En estas variables, Colombia se encuentra en el rango de 0.6-0.8 sobre 1 para legislación, construcción de capacidades, y organización. (Ver Imagen 3).

El Índice también deja entrever, por medio de las variables de conocimiento técnico y cooperación, que los logros de Colombia siguen siendo insuficientes para cerrar la brecha existente entre capacidades y el contexto estratégico cibernético. Como es de conocimiento general, el ciberespacio es el dominio de interacción más dinámico que existe, y el único que el hombre puede moldear a conveniencia. En este sentido, no es equivocado decir que la política diseñada para atender necesidades gestadas en el ciberespacio tiene una caducidad acelerada, y que los Estados deben replantear sus aproximaciones periódicamente. Bajo esta lógica, Colombia se encuentra desarrollando un nuevo CONPES titulado: 'Política Nacional de Seguridad Digital en Colombia'.

Imagen 3 - Global Cibersecurity Index. Comparativo



Fuente: UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT). Herramienta de Análisis Comparativo, [20??].[4]

El Plan Nacional de Desarrollo (PND) 2014-2018, y la Política de Seguridad y Defensa 'Todos por un Nuevo País', son documentos primarios que dan línea política y estratégica a la 'Política Nacional de Seguridad Digital en Colombia' – a partir de ahora CONPES 0000.[5] Directamente, en las bases del PND, documento soporte del Plan, se establece que el respeto de la soberanía nacional y la protección de los intereses nacionales implica un reconocimiento del dominio ciberespacial – también conocido como quinto dominio, y que ello implica que el país debe desarrollar sus capacidades de neutralización y reacción frente amenazas que atenten contra la crítica digital (DNP, 2014, pp. 353, 355). Las bases del PND, establece como meta atender en el año 2018 un total de 10.461 incidentes cibernéticos, 186% más incidentes frente a las cifras presentadas en el 2013 (DNP, 2014, p. 353);

4 La herramienta de análisis comparativo de la Unión Internacional de las Comunicaciones es accesible en: <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI_GLO_Graphics.aspx >.

5 A la fecha, el documento se encuentra en producción, razón por la cual no se le ha adjudicado una nomenclatura. Se adoptó 'CONPES 0000' por facilidad metodológica del presente artículo, y con el objetivo de distinguirlo de su predecesor (i.e. CONPES 3701). El documento de trabajo se encuentra disponible al público interesado en el siguiente hipervínculo: <http://www.mintic.gov.co/portal/604/articles-14481_recurso_1.pdf >.

particularmente, se establece que la estrategia nacional de ciberseguridad debe cumplir las iniciativas que se listan a continuación (Ver Tabla 2).

Cuadro 2 - *Iniciativas de Ciberseguridad según Bases del PND*

Consolidación del Grupo de Respuestas a Incidentes Cibernéticos de Colombia (ColCERT), como ente articulador del gobierno.
Creación y fortalecimiento del Observatorio del Ciberdelito y el Centro de Mando y Control, comunicaciones y Coordinación del Cibercrimen (C4) de la Policía.
Fortalecimiento de la capacidad de protección de las Fuerzas Militares y la Policía de sus propios activos digitales.
Armonización del marco legal con las necesidades en materia de prevención, detección y atención del Ciberdelito.
Creación de los Centros de Respuesta Cibernética Sectoriales (CSIRTs)
Fortalecimiento de los mecanismos de cooperación internacional, propiciando el intercambio de mejores prácticas y de información y la creación de redes de vigilancia y alerta internacionales.

Fuente: COLOMBIA, 2014. Bases del Plan Nacional de Desarrollo: Todos por un Nuevo País. Bogotá. p. 353-355.

El lineamiento estratégico anteriormente descrito es recapitulado por la Política de Seguridad y Defensa, imponiendo así mayor responsabilidad a las instituciones que componen la Fuerza Pública (i.e. Fuerzas Militares y Policía Nacional) frente al ciberespacio. Esta política busca construir una Colombia en paz, equitativa y educada, bajo los principios de buen gobierno, sostenibilidad, bienestar de la Fuerza Pública, transparencia, y respeto por los derechos humanos. Para ello, se establecieron nueve (9) objetivos estratégicos, destacándose la necesidad de combatir las nuevas y tempranas expresiones de crimen organizado, garantizar la soberanía e integridad del territorio nacional, protegiendo los intereses nacionales, y transformar y modernizar de forma continua el Sector Defensa (COLOMBIA, 2016, p. 10-35).

El CONPES 0000 (CONSEJO..., 2016) es en sí mismo novedoso porque introduce un nuevo enfoque para la seguridad digital: la gestión del riesgo en Colombia. Esta nueva forma de entender los retos en el ciberespacio se desprende de las recomendaciones de la Organización Económica para la Cooperación y Desarrollo (OECD). La OECD ofrece un foro donde los gobiernos de los países miembros trabajan conjuntamente para la solución de problemas comunes que afectan el

bienestar económico y social de las personas (ORGANISATION…, 2015). Colombia está en proceso de adhesión a la organización, razón por la cual asume con gran compromiso los lineamientos de política pública sugeridos por esta. Adicionalmente, el nuevo enfoque en el CONPES 0000 (CONSEJO…, 2016) afirma que, sin prejuicio del enfoque inicial del documento CONPES 3701 (CONSEJO…, 2011) respecto a objetivos de defensa y seguridad, el énfasis en la gestión del riesgo es incluyente y facilita conciliar elementos sociales y económicos con la seguridad y defensa del Estado. (CONSEJO…, 2016, p. 51-52).

Según la OECD, en la medida que se cuente con una aproximación basada en la administración del riesgo, y siempre que se mantenga un enfoque económico y social, los riesgos digitales pueden aproximarse como riesgos económicos. Adicionalmente, aseguran que una aproximación diferencial de la seguridad digital genera una respuesta excluyente que contraviene la naturaleza transversal del ámbito digital. Esta transversalidad implica que los actores sufren los impactos provenientes de los riesgos digitales y, en consecuencia, se requiere de un esfuerzo cooperativo para gestionarlos. En este sentido, una gestión adecuada implica diseñar medidas de seguridad que hagan de los riesgos aceptables con relación al beneficio económico percibido por las actividades en juego (ORGANISATION…, 2015, p. 4).

Bajo la lógica de la OECD, el CONPES 0000 (CONSEJO…, 2016) parte de la premisa que mayor confianza en el entorno digital significará mayor prosperidad económica, política y social, y que esta puede construirse mitigando el riesgo proveniente de vulnerabilidad y amenazas a niveles aceptables (CONSEJO…, 2016, p. 13-47). Esto implica que las medidas de seguridad que se tomen deben tener un entendimiento holístico de las necesidades de todos los actores, y que no deberían ser tan férreas que impidan el uso del ambiente digital abierto requerido para generar capital. Este nuevo enfoque de política para Colombia es más entendible cuando se conocen las cifras nacionales. Los sectores más afectados en Colombia por los incidentes digitales para el año 2015, son también los que más aportan al Producto Interno Bruto (PIB) nacional: ciudadanía (42.4%), gobierno (23.9%), educación (9.2%), financiero (9%), sector privado e industria (5.8%) y sector defensa (5.8%) (CONSEJO…, 2016, p. 41). Se estima que la digitalización de estos representó entre los años 2005 y 2013 un 6.12% de crecimiento acumulado del PIB de Colombia, mientras que los costos de los incidentes fueron sólo para el 2013 aproximadamente USD $ 464 millones o 0,14% del PIB (CONSEJO…, 2016, p. 36-41).

Para generar el nivel de confianza requerida, la 'Política Nacional de Seguridad Digital en Colombia' dispone de cinco dimensiones y objetivos estratégicos, todos soportados en cuatro principios fundamentales. El primero de estos principios es salvaguardar los derechos humanos y valores fundamentales de los individuos,

lo cual gira en torno a temáticas tan complejas como garantizar la libertad de expresión, confidencialidad, y protección de la intimidad (CONSEJO…, 2016, p. 69). El segundo principio es la adopción de un enfoque influyente y colaborativo que involucre a los actores que hacen uso del entorno digital. El tercer principio se refiere a la corresponsabilidad de estos actores para proteger el entorno, mientras que el último principio enfatiza la necesidad de contar con un enfoque basado en la gestión de riesgos. Las cinco dimensiones estratégicas que encaminan la formulación de los objetivos son fortalecimiento del marco legal y regulatorio, gobernanza, gestión sistémica del riesgo, cultura ciudadana, y capacidades para la gestión del riesgo (CONSEJO…, 2016, p. 69- 70).

Se espera que el CONPES 0000 (CONSEJO…, 2015), otorgue una visión estratégica a Colombia que le permita vincular integralmente las partes interesadas para gestionar los riesgos de la seguridad digital, maximizar las oportunidades en el desarrollo de actividades socioeconómicas (desarrollar las capacidades de ciberseguridad y ciberdefensa necesarias y fortalecer los esfuerzos de cooperación y colaboración nacional e internacional (CONSEJO…, 2016, p. 46 - 61).

La estrategia nacional hace especial énfasis en la necesidad de formación y capacitación como un pilar para la corresponsabilidad frente a la seguridad del entorno digital. Un claro ejemplo de este compromiso proviene de la Escuela Superior de Guerra de Colombia (ESDEGUE); institución de educación superior militar, que forma personal de las fuerzas militares, policiales y civiles en temáticas conexas a la seguridad y defensa nacional. La ESDEGUE es pionera en la región con la creación del programa de Maestría en Ciberseguridad y Ciberdefensa, y ha adelantado iniciativas como juegos de guerra cibernética, laboratorios de investigación para infraestructuras críticas SCADA y de análisis de *Malware,* proyectos de investigación de innovación y desarrollo de capacidades, y diplomados y seminarios internacionales en los ámbitos jurídicos y técnicos.

Dentro una visión técnica, se espera que el direccionamiento estratégico del CONPES 0000 (CONSEJO…, 2016), facilite la finalización de un catálogo de infraestructura crítica para los sectores de servicio esencial, y el desarrollo de una arquitectura de referencias para la implementación de los ciberactivos que correspondan a la infraestructura crítica ligada a sistemas SCADA. De igual forma, se espera contar con una gestión de incidentes de ciberseguridad operativa y coordinada, y una plataforma de ciberinteligencia funcional para todos los sectores de servicios esenciales.

Estos logros son particularmente importantes en el actual punto de inflexión que se encuentra el país. Un acuerdo para la finalización del conflicto entre el Estado y las Fuerzas Armadas Revolucionarias de Colombia (FARC) tiene la facultad de

modificar el contexto estratégico nacional. Dentro de ese nuevo contexto estratégico, se visualiza un aumento de las nuevas amenazas y una mutación de las antiguas; principalmente, la criminalización de las disidencias del grupo insurgente FARC. Considerar que las bandas criminales son ajenas a las Tecnologías de la Información y Comunicación para el desarrollo de actividades ilícitas es ingenuo, estas les usan en detrimento de la confianza de los usuarios del ambiente digital (CHAMBERS-JONES, 2013; ETGES; SUTCLIFFE, 2008). En este sentido, la ciberseguridad y ciberdefensa se vuelven componentes indispensables para garantizar el escenario propicio que garantice la transición de Colombia hacia una paz estable y duradera.

3 Conclusiones

El nivel de digitalización de Colombia le ha permitido adquirir muchos beneficios, causando a la vez la aparición de diferentes tipos de retos en materia. Se estima que la digitalización entre los años 2005 y 2013 representó un crecimiento acumulado del 6.12% del Producto Interno Bruto (PIB) nacional. A la par, ocurrieron incidentes como *botnet* 'Mariposa', diferentes delitos cibernéticos (ej. *phishing, smishing, defacement*, entre otros), filtraciones de *Wikileaks*, ataques del grupo hacktivista Anonymous, que obligaron a Colombia desarrollar y potenciar capacidades de ciberseguridad y ciberdefensa. Para poderlo hacer, se necesitó de una política pública que diera direccionamiento estratégico, razón por la cual se creó el CONPES 3701 (CONSEJO…, 2011).

El CONPES 3701 es, sin duda alguna, la política que marcó el comienzo de Colombia en el ámbito de la seguridad y defensa en el ciberespacio. Los lineamientos e iniciativas que allí se propusieron, cumplidas a la fecha en un 90%, facilitó la creación del Grupo de Respuestas Cibernéticas de Colombia (ColCERT), Comando Conjunto Cibernético de las Fuerzas Militares (CCOC), Centro Cibernético Policial (CCP), y los Comandos Cibernéticos de cada una de las Fuerzas. Adicionalmente, permitió que las demás entidades del Estado ingresaran en la dinámica de la protección de la información, y que los diferentes sectores desarrollaran *Computer Security Incident Response Teams* (CSIRT) para la protección de la infraestructura crítica de la nación.

Colombia ha tenido avances significativos en términos operativos, jurídicos, estratégicos, y diplomáticos, que han permitido endurecer al país como un objetivo de las amenazas que rondan en el ciberespacio, y garantizar a los ciudadanos e instituciones un ambiente digital con unas condiciones de seguridad suficientes para una certeza mínima en los sistemas. El camino a recorrer por Colombia sigue siendo largo, principalmente por el nivel de dinamismo de los retos, y la velocidad

de mutación de las amenazas. Para equiparar el ritmo entre iniciativas estratégicas y amenazas, los Estados deben actualizar constantemente sus políticas públicas; esta es la razón por la cual Colombia decidió realizar una nueva política sectorial en el marco del CONPES CONSEJO…, 2015).

El nuevo CONPES toma la lógica de la OCDE de la gestión del riesgo, aproximación aceptada por diferentes autores en la academia (BRECHBÜHL; BRUCE; DYNES; JOHNSON, 2010; BAKER, 2014). El argumento que los riesgos del ambiente digital no pueden ser tomados como algo aislado, sino que son transversales para todos los actores y, como tal, deben tener una respuesta coordinada y corresponsable es lógico según una visión red-céntrica (BRECHBÜHL; BRUCE; DYNES; JOHNSON, 2010, p. 83-86). Para fortalecer la coordinación entre todos los actores, el Estado colombiano implementó una cuantificación en términos socioeconómicos de los riesgos digitales. En la medida que el entorno sea percibido más seguro por los actores, y se genere mayor certeza sobre su uso, habrá mayor disposición para emprender actividades con capacidad de formación de riqueza.

Una gestión del riesgo digital en términos socioeconómicos requiere que las medidas de seguridad sean desarrolladas teniendo en consideración a todos los actores involucrados, y que se desarrollen bajo una lógica realista de costo-beneficio. Las medidas de seguridad deberán diseñarse para hacer del riesgo algo aceptable, de forma tal que los beneficios percibidos sean mucho mayores. En este sentido, Colombia se acoge a las recomendaciones de OCDE plasmando una estrategia conciliadora entre la seguridad y defensa, y los objetivos económicos y sociales del Estado.

El futuro contexto estratégico de Colombia está permeado por una mutación en las fuentes de amenaza, principalmente por una tendencia de criminalización de la insurgencia. Pensar que las estructuras criminales no harán uso de las tecnologías de la información y comunicación para el desarrollo de actividades ilegales es erróneo. En torno a esto, se espera que el CONPES 0000 permita a Colombia no sólo desarrollar las capacidades necesarias, sino fortalecer los esfuerzos de cooperación y colaboración nacional e internacional. El futuro ideal que se espera alcanzar a través de la estrategia es uno donde se cuente con un catálogo de infraestructura crítica para los sectores de servicio esencial y una arquitectura de referencia para la implementación de los ciberactivos que corresponden a la infraestructura crítica ligada a sistemas SCADA. De igual manera, se espera que la gestión de incidentes de ciberseguridad sea operativamente efectiva y coordinada, siempre bajo la guía de una plataforma de ciberinteligencia completamente funcional.

REFERENCIAS

ANDERSON, G. South Korea and Colombia agree to enhance defence ties. *IHS Jane's 360*, London, 2015. Disponible en: <http://www.janes.com/article/49907/south-korea-and-colombia-agree-to-enhance-defence-ties>. Fecha de acceso: 30 oct. 2015.

ASÍ cogieron al mayor pornógrafo infantil de Colombia, alias 'gemido ruidoso'. *Noticias Caracol*, [S.l.], 9 oct. 2015. Disponible en: <http://www.noticiascaracol.com/colombia/cayo-uno-de-los-mayores-distribuidores-de-pornografia-infantil-en-colombia>. Fecha de acceso: 15 oct. 2015.

BAKER, Elizabeth White. A model for the impact of cybersecurity infrastructure on economic development in emerging economies: evaluating the contrasting cases of India and Pakistan. *Information Technology for Development*, [S.l], v. 20, n. 2, p. 122-139, abr. 2014.

CHAMBERS-JONES, Clare. Virtual world financial crime: legally flawed. *Law and Financial Markets Review*, [S.l.], v. 7, n. 1, p. 48-56, enero 2013.

COLECTIVO 'ataca' a páginas web del Gobierno. *El Tiempo*, [S.l.], 15 abr. 2011. Disponible en: <http://www.eltiempo.com/archivo/documento/CMS-9172423>. Fecha de acceso: 19 nov. 2015.

COLOMBIA. Congreso Nacional. Proyecto de Ley n° 241, de 2011. Por la cual se Regula la Responsabilidad por las Infracciones al Derecho de Autor y los Derechos Conexos en Internet. 2011. *Imprenta Nacional*, Bogotá, DC, 04 abr. 2011. Disponible en: <http://flip.org.co/sites/default/files/archivos_publicacion/Texto%20aprobado%20en%20primer%20debate_20.doc>. Fecha de acceso: 08 abr. 2016.

_____. Departamento Nacional de Planeación. *Bases del Plan Nacional de Desarrollo 2014-2018*: todos por un nuevo país. Bogotá, DC, 2014. Disponible en: <https://colaboracion.dnp.gov.co/cdt/prensa/bases%20plan%20nacional%20de%20desarrollo%202014-2018.pdf>. Fecha de acceso: 02 abr. 2016.

_____. Ministerio de Defensa. *Política de Defensa y Seguridad (MINIDEFENSA)*: todos por un nuevo país. Bogotá, DC, 2016. Disponible en: <https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Documentos_Descargables/espanol/politica_defensa_deguridad2015.pdf >. Fecha de acceso: 04 feb. 2016.

COLOMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones. *Colombia firma un memorando de entendimiento con Microsoft en temas de ciberseguridad, educación e innovación*. Bogotá, DC, 2013. Disponible en: <http://www.mintic.gov.co/portal/604/w3-article-5037.html>. Fecha de acceso: 06 enero 2016.

_____. Ministerio de Tecnologías de la Información y las Comunicaciones. *Boletín trimestral de las TIC*: cifras primer Trimestre de 2015. Bogotá, DC, 2015a. Disponible en: <http://colombiatic.mintic.gov.co/602/articles-11128_archivo_pdf.pdf>. Fecha de acceso: 6 enero 2016.

_____. _____. *Informe de Gestión al Congreso de la República*. Bogotá, DC, 2015b. Disponible en: <http://www.mintic.gov.co/portal/604/articles-13320_doc_pdf.pdf>. Fecha de acceso: 20 dic. 2015.

COMANDO GENERAL DE LAS FUERZAS MILITARES (Colombia). *Informe de Gestión 2015*. Bogotá, DC, 2015-2016. 4 trim. Disponible en: <http://cgfm.mil.co/informes-de-gestion>. Fecha de acceso: 14 abr. 2016.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL (Colombia). *Política Nacional de Seguridad Digital*. Bogotá, DC, 2016. (Documento CONPES 0000). Disponible en: <http://www.mintic.gov.co/portal/604/articles-14481_recurso_1.pdf>. Fecha de acceso: 10 nov. 2015.

_____. *Lineamientos de política para ciberseguridad y ciberdefensa*. Bogotá, DC, 2011. (Documento CONPES 3701). Disponible en: <http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf >. Fecha de acceso: 20 nov. 2015.
ETGES, Rafael; SUTCLIFFE, Emma. An overview of transnational organized cyber crime. *Information Security Journal*: A Global Perspective, [S.l.], v. 17, n. 2, p. 87-94, mayo 2008.

FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS . *About First*. [S.l., 2015?]. Disponible en: <https://www.first.org/about>. Fecha de acceso: 08 dic. 2015.

LEÓN, Juanita. Este es el 'dossier' de Wikileaks sobre Colombia. *La Silla Vacía*, [S.l.], 9 dic. 2010. Disponible en: <http://lasillavacia.com/historia/este-es-el-dossier-de-wikileaks-sobre-colombia-20507>. Fecha de acceso: 17 enero 2016.

MCAFEE LABS. *McAfee threats report*: fourth quarter 2009. Santa Clara, CA, 2010. Disponible en: <http://www.federalnewsradio.com/wp-content/uploads/pdfs/2009Q4ThreatsReportfinal.pdf>. Fecha de acceso: 13 marzo 2016.

_____. *McAfee threats report*: fourth quarter 2010. Santa Clara, CA, 2011. Disponible en: <http://www.redteamusa.com/PDF/McAfee/McAfee-quarterly-threat-q4-2010.pdf>. Fecha de acceso: 13 marzo 2016.

_____. *McAfee threats report*: fourth quarter 2011. Santa Clara, CA, 2012. Disponible en: <http://www.intel.com/content/dam/www/public/us/en/documents/reports/mcafee-threats-quarterly-report.pdf >. Fecha de acceso: 13 marzo 2016.

MEDINA C., María Alejandra. La hoja de ruta para la ciberseguridad. *El Espectador*, Bogotá, DC, 3 agosto 2015. Disponible en: <http://www.elespectador.com/noticias/economia/hoja-de-ruta-ciberseguridad-articulo-576914>. Fecha de acceso: 13 nov. 2015.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Digital Security Risk Management for Economic and Social Prosperity*: OECD Recommendation and Companion Document. Paris: OECD Publishing, 2015. Disponible en: <http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf>. Fecha de acceso: 25 nov. 2015.

OVER 13 million users in 190 countries and 31,901 cities affected by the Mariposa botnet. *Panda Security*, [S.l.], 10 marzo 2010. Disponible en: <http://www.pandasecurity.com/mediacenter/news/over-13-million-users-in-190-countries-and-31901-cities-affected-by-the-mariposa-botnet>. Fecha de acceso: 12 dic. 2015.

PÁGINAS web del Gobierno, víctimas de 'anonymous'. *El Tiempo*, [S.l.], 16 agosto 2011. Disponible en: <http://www.eltiempo.com/archivo/documento/MAM-4755365>. Fecha de acceso: 23 feb. 2016.

RICON-CÁRDENAS, Erick . Instrumentos normativos de Ciberseguridad. *Certicámara*, [S.l.], 01 marzo 2014. Disponible en: <https://web.certicamara.com/media/58493/normativa-colombiana-en-materia-de-ciberseguridad-y-ciberdefensa-1-marzo-2014.pdf>. Fecha de acceso: 15 enero 2016.

SANTOS-CALDERÓN, Guillermo . El Enigma de WikiLeaks. *El Tiempo*, [S.l.], 6 dic. 2010. Disponible en: <http://www.eltiempo.com/archivo/documento/MAM-4291136>. Fecha de acceso: 10 feb. 2016.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA. *Informe de operaciones*: primer semestre de 2015. [S.l.], 2015. Disponible en: <https://www.superfinanciera.gov.co/descargas?com=institucional&name=pubFile1014571&downloadname=informetransacciones0615.docx>. Fecha de acceso: 02 abr. 2016.

EL CIBERESPACIO Y LA SEGURIDAD NACIONAL EN EL SALVADOR

Roberto Artiga Chicas*

1 Introducción

En un periodo corto de tiempo suceden cosas extrañas en nuestro entorno, hay cortes y sobrecargas de energía en sectores del país que destruyen elementos importantes en las principales plantas potabilizadoras de agua los cuales requerirán semanas para volverlos a poner en línea; estas fallas suceden al mismo tiempo que inexplicablemente las compuertas de las presas hidroeléctricas se activan dejando salir grandes cantidades de agua que inundan las cosechas que estaban a punto de ser recolectadas afectando el 60 % de las tierras cultivables, casi al mismo tiempo cientos de usuarios de la banca reciben sus Estados de cuentas en donde reflejan pagos o compras realizadas en diferentes partes del mundo.

Para agravar más la situación el sistema de radar principal y control aéreo del aeropuerto nacional arroja datos erróneos al personal de la torre de control, provocando el mayor desastre aéreo hasta la fecha en donde dos aeronaves chocan en vuelo con decenas de muertos como resultado de ese accidente; y si esto fuera poco los sistemas de telefonía celular y de comunicaciones públicos y privados dejan de funcionar en su totalidad. Generando un caos sin precedentes al perder por completo el Estado su capacidad de coordinación y articulación de respuesta para solventar estos problemas. Al pasar los días nuestro gobierno se da cuenta por informes de organizaciones internacionales que la causa de tales eventos ha sido una serie de accesos no autorizados a sistemas informáticos, una agencia denomina que en su gran mayoría se ha recibido un ataque a los sistemas SCADA (*Supervisory Control And Data Acquisition*) que controlan los procesos en los centros hidroeléctricos, distribución de agua, controladores aéreos entre otros. Accesos que, tras una manipulación de datos, cambio de programación y otros que van surgiendo como resultado del peor incidente en el ciberespacio sufrido hasta la fecha en el país. Lo

* Diplomado en Administración de Instituciones Educativas en la Pontificia Universidad Católica de Chile en 1995, Curso Superior de Desarrollo Nacional en el Colegio Fu Hsing Kang en Taipéi Taiwánen 2009, Seminario Internacional para América Latina en el Instituto de Altos Estudios de la Defensa Nacional en Paris Francia en 2011, Curso sobre Ciberespacio y su impacto en la Seguridad Nacional en el Center for Hemispheric Defense Studies (CHDS) United States of America el 2013, II Curso de Ciberseguridad para Oficiales Superiores Iberoamericanos el 2016y Curso de Post Grado en Planificación Estratégica y Administración de Recursos Nacionales en el Colegio Industrial de las Fuerzas Armadas de la Universidad de Defensa en Estados Unidos (ICAF Class -2006).
Director de CAEE de El Salvador. Contacto: <artiga.roberto@caee.edu.sv>

peor de todo, la identidad y ubicación geográfica de donde proviene el ataque y quiénes son los autores del mismo sigue siendo un total misterio. Por supuesto que este es un escenario probable que pudiese llegar a suceder y que de alguna forma afecte la capacidad de funcionamiento de nuestro País.

De la misma forma resulta paradójico el que hace más de 30 años este término de ciberespacio o lo que sucede en ese entorno no era conocido en la escala global, mucho menos nacional, en la cual se comenta en la actualidad. Cuando en 1984 se comienza a utilizar el término ciberespacio se da inicio a un desarrollo sin precedentes en las Tecnologías de Informática y Comunicaciones (TIC) en el cual las ficciones con la realidad han llegado a converger en determinados momentos. Aun en la actualidad seguimos refiriéndonos al ciberespacio como algo puramente abstracto y que no tiene realidad propia y que es de difícil comprensión, por lo tanto, lo catalogamos de cualquier manera y de acuerdo a la interpretación que el ente político o especialistas en la materia le asignen. En cualquier caso, lo que sucede o deja de suceder en ese mundo desconocido y nuestro país de no tomar las medidas necesarias para actuar en ese medio, podemos vernos frente a algo que se convertirá en un serio peligro para la Seguridad Nacional.

En nuestro país, la Ley de la Defensa Nacional del 2002 establece que la Seguridad Nacional es:

> […] un conjunto de acciones permanentes que el Estado propicia para crear las condiciones que superan situaciones de conflictos internacionales, perturbaciones a la tranquilidad pública, catástrofes naturales y aquellas vulnerabilidades que limiten el desarrollo nacional y pongan en peligro el logro de los objetivos Nacionales. (EL SALVADOR, 2002).

Por consiguiente, el Estado debe de realizar acciones permanentes en todos los ámbitos incluyendo (aunque se desconozca su naturaleza real en este momento) el ciberespacio a efecto de salvaguardar los intereses y objetivos nacionales que velan por la permanencia del Estado, el bienestar nacional y la concordia internacional. Por otro lado, la Seguridad propiamente dicha se convierte en una percepción de la realidad que nos envuelve, ya que casi siempre los individuos o sociedades en general se hacen siempre la misma pregunta ¿qué tan seguros nos sentimos ante las amenazas que tenemos? Y en el caso del ciberespacio al desconocer lo que es ese entorno por completo, la sensación de seguridad es muy incierta.

En caso de llegar a suceder una situación de catástrofe nacional como la "ficción" anteriormente descrita nos lleva a plantearnos una serie de interrogantes a efecto de tomar las medidas preventivas y correctivas necesarias para afrontar esos

riesgos y amenazas: ¿qué es en realidad el ciberespacio y cuáles son sus características principales?, ¿cuáles son las amenazas que encontramos en este entorno que puedan afectar las infraestructuras estratégicas y críticas, y por ende afectar la Seguridad Nacional?, ¿cómo medimos la afectación de los objetivos nacionales?, ¿Qué nos preocupa?, ¿Cuáles son los tipos de ataques y atacantes?, ¿qué acciones se deben de tomar?, ¿qué tipo de organización que se requiere y el marco legal necesario?, ¿Quiénes son los responsables de protegernos? en fin, la lista de cuestionamientos podría seguir y seguir, especialmente cuando se desconoce por completo a que nos enfrentamos y que es lo que se puede hacer o no hacer en ese entorno de actuación "nuevo".

El presente artículo se orienta a describir una posible respuesta a esas interrogantes antes planteadas sobre el ciberespacio, tomando en consideración la afectación a la Seguridad Nacional de El Salvador, esto con el objeto de establecer una idea de cómo académicamente llegaremos a materializar una adecuada Política y Estrategia de Ciberseguridad, tomando en consideración que no poseemos aún una Estrategia De Seguridad Nacional que oriente los esfuerzos del Estado a contrarrestar cualquier tipo de amenazas, no se tiene tampoco una organización acorde permanente que esté dando seguimiento y prevea el accionar futuro, ni tampoco el marco legal y/o normativa correspondiente nacional e internacional (tratados y acuerdos ratificados) que guíe el actuar de estas organizaciones.

2 ¿Qué es el Ciberespacio? y ¿Cuáles son sus Características Principales?

Buscando una definición ampliamente aceptada en El Salvador dentro de algún tipo de legislación nacional sobre el tema (la cual no existe hasta el momento), o algún diccionario académico de uso regular en nuestras escuelas; no hemos encontrado una definición adecuada, por no decirlo existente sobre lo que es el ciberespacio. La real academia española de la lengua española lo define como "ámbito artificial creado por medios informáticos"; por otro lado, el diccionario Merriam-Webster nos da otra aproximación "el mundo en línea de las redes informáticas y de internet". Podemos seguir buscando definiciones de ciberespacio y la mayor parte se refiere a ese espacio artificial y abstracto (casi siempre relacionado a internet) el cual ha sido creado por el hombre.

Allí es donde radica un serio problema cuando orientamos el enfoque hacia la Seguridad Nacional, ya que, al ser un espacio artificial y abstracto, no se percibe o no se tiene una concientización sobre lo que es y representa para el funcionamiento adecuado del Estado; y, por ende, no captamos o sabemos si estamos o no seguros en ese ambiente. Esto debido a que tradicionalmente estamos acostumbrados a

interactuar en entornos creados por la madre naturaleza o creados con poca participación humana, dejando por fuera al ciberespacio y que muy a pesar del grado de penetración de los medios tecnológicos y las TIC´s, seguimos sin toma conciencia sobre los riesgos y amenazas en ese entorno.

Un enfoque militarista sobre el ciberespacio lo estableció en el 2010 William J. Lynn III, *Deputy Secretary of Defense de USA*, quien publicó un artículo en la prestigiosa revista *Foreign Affairs*, donde expuso los cinco principios básicos de la estrategia de la guerra del futuro: siendo la primera en donde […] "el ciberespacio debe ser reconocido como un territorio de dominio igual que la tierra, mar y aire" (LYNN III, 2010) y de allí otros países de la Unión Europea adoptaron el mismo concepto del quinto entorno de actuación en donde se pueden desarrollar operaciones militares. De allí muchas de las estrategias nacionales de ciberseguridad que se fueron desarrollando, decantaron en estrategias militares que generaron la creación de Comandos de Ciberdefensa o con nombres similares y otras organizaciones orientadas a desarrollar acciones dentro de la denominada "ciberguerra"

Por otro lado, cuando incluimos en esta ecuación en la cual se pretende el definir ciberespacio, surge una pregunta al respecto ¿Quién ejerce soberanía sobre el ciberespacio? Pues si consideramos a este ciberespacio como parte del Global Commons que de acuerdo con lo que establece el derecho internacional "son aquellos espacios que no forman parte de ningún Estado concreto y sobre los que, por tanto, ningún Estado puede ejercer derechos soberanos"(NEBRERA, 2015) ya que existe la creencia de que el ciberespacio se considera como de dominio público; pero por otro lado sabemos que si bien es cierto los medios que se utilizan para intercambiar o transmitir los datos y las comunicaciones (cables u ondas) cruzan áreas que se catalogan dentro del *Global Commons*. Estos medios son propiedad de alguna corporación o de un País en particular SARAIVA, 2007); pero además pueden ser utilizados y mejorados por cualquiera que disponga la tecnología y conocimientos adecuados. Otro aspecto que se determina en los *Global Commons*, es lo concerniente a soberanía, pues otro aspecto es lo siguiente que: "La característica común a todos ellos, aparte del hecho de no estar bajo la soberanía de ninguna nación concreta, es que constituyen los espacios de tránsito de bienes, servicios e información."GLOBAL…, 2010). ¿Quién ejerce soberanía en el ciberespacio?, en nuestro país la Constitución de la República establece que la "soberanía reside en el pueblo" (EL SALVADOR, 1983). Pero la soberanía dentro de tantas definiciones que encontramos emplearemos la siguiente:

> La independencia internacional de un Estado combinada con el derecho y el poder que le asiste para regular sus asuntos in-

> ternos sin imposiciones exteriores… y que esa soberanía tiene tres elementos importantes el primero es el Territorio donde el Estado protege los espacios donde ejerce jurisdicción, el otro es el aspecto Funcional que es la capacidad de ejercer con autonomía y efectividad su acción de gobierno; y por último la Identidad donde están los recursos intangibles que cohesionan a la población en torno a sus valores, historia, cultura, derechos y deberes legales, sistema económico, etc.(SANZ-ALSEDO, 2010, p. 82).

Y si nuestro estado no tiene los medios y capacidad de ejercer su poder nacional en ese entorno, entonces difícilmente ejerceremos soberanía sobre el mismo. Otra aproximación para definir el ciberespacio lo hace el Departamento de Defensa de los Estados Unidos (país que tiene los medios suficientes y adecuados para ejercer "soberanía" en el ciberespacio) en su Diccionario de términos militares en donde establecen que es: "Un dominio creado por la interacción de tres diferentes componentes el hardware, el virtual y el cognitivo" (UNITED STATES OF AMERICA, 2001):

> […] en donde "La realidad física del ciberespacio está compuesta por la red de infraestructuras interdependientes de tecnología de la información. Esto incluye todo el hardware de sistemas de telecomunicación e informáticos, desde los routers, fibra óptica y cables transatlánticos, torres de telefonía celular, y los satélites, a las computadoras, los teléfonos inteligentes, y, en definitiva, cualquier dispositivo que contiene procesadores integrados. De la misma forma también tiene un componente virtual que abarca el software, firmware, y de datos de la información residente en el hardware. Esto incluye los sistemas operativos, las aplicaciones y los datos almacenados en el disco duro o la memoria de un sistema informático; y el tercer componente cognitivo que el ser humano. Mientras que otros dominios son únicamente parte del entorno físico, el ciberespacio como el único dominio hecho por el hombre, se forma y se utiliza por los seres humanos y son las personas que interactúan con el entorno virtual y entre sí. (TRUJILLO, 2014).

Aunque la definición anterior menciona en un punto el uso de internet, no amplía o establece la importancia de este canal de comunicaciones sin el cual no existiría probablemente el ciberespacio. Entonces si el ciberespacio es otro dominio de actuación en donde podemos ejercer "soberanía", no podemos limitarnos al concepto abstracto de este como se pretende visualizar en tantas definiciones, que por regla general se "cree" que el ciberespacio es el sinónimo de internet.

De esta forma adoptaremos una definición más amplia y que es utilizada en el Colegio de Altos Estudios Estratégicos de El Salvador (en adelante CAEE) para las clases, investigaciones y demás actividades y que, en el presente artículo, cuando nos refiramos a ciberespacio será en estos términos:

> El ciberespacio es el conjunto de medios y procedimientos basados en las Tecnologías de la Información y Comunicación, configurados para la prestación de servicios. Y está constituido por hardware, software, Internet, servicios de información y sistemas de control que garantizan la provisión de aquellos servicios esenciales para la actividad socioeconómica de cualquier nación, y en especial aquellos ligados a sus infraestructuras críticas. (SANZVILLALBA; CHAMORRO, 2011, p. 45-46).

Ya no estamos limitándonos solamente a ese ámbito artificial o mundo en línea descrito en las definiciones de Webster y de la RAE, sino que a un sistema formado por componentes claramente establecidos y donde se identifica claramente una capa lógica, una capa física y una capa social. En donde internet juega un rol muy importante ya que es la carretera de múltiples vías para conectarse y comunicarse entre esos servicios de información establecidos; pero hay otros componentes de los cuales debemos de prestar la atención adecuada a efecto de formular las políticas y estrategias de ciberseguridad.

3 ¿Qué Características Tiene este Entorno?

Si bien es cierto es sumamente problemático el construir una definición ampliamente aceptada de lo que es el ciberespacio, el CAEE al utilizar y ajustar a nuestro enfoque particular la que establece Sanz Villalba e Chamorro (2011) también buscamos darles una descripción más adecuada a las características de ese entorno. Sabemos que hay una gran infinidad de características diferenciadoras; pero como se mencionaba anteriormente, el CAEE utiliza las siguientes para tomar un poco más de conciencia sobre los riesgos y amenazas a la Seguridad Nacional en el ciberespacio.

La primera característica principal que establecemos es la de que “no hay fronteras físicas” y ese concepto de frontera está en un cambio siempre continuo, ya que, de acuerdo al planteamiento de los Doctores García, Beltran y Núñez en su artículo Una Aproximación al Concepto de Frontera Virtual (JIMÉNEZ; ORENES; PUENTE, 2010), hay que tomar en cuenta varios aspectos para el establecimiento de las fronteras, aspectos que van desde la dimensión histórica, de espacio cultural,

de aspectos normativos hasta lo que conlleva a demarcar la dimensión económica, material y humana. El ciberespacio nos presenta la faceta de tener esa característica que engloba lo que determina una frontera física; pero al profundizar en su análisis vemos ese aspecto intangible del canal de comunicaciones llamado internet, en el cual según Jiménez, Orenes e Puente (2010):

> El espacio aparece como un concepto infinito y el tiempo como infinitesimal, es decir que por un lado se comprime infinitamente hasta llegar al tamaño infinitesimal (todo está al alcance de la mano) y, al mismo tiempo, se expande infinitamente (hay una infinidad potencial de interacciones e informaciones posibles que crece exponencialmente). (JIMÉNEZ, ORENES; PUENTE, 2010).

Con el establecimiento del Ciberespacio surge la diferenciación entre una frontera física o tradicional Y el otro tipo de frontera que es la virtual. La tradicional como la conocemos en sus diferentes modalidades; pero que es palpable, está demarcada en el ámbito terrestre, marítimo, aéreo y espacial, y que puede ser fácilmente identificable utilizando sistemas de posicionamiento global u otros métodos de medición. La segunda característica es sobre la "frontera virtual", ya que con el Ciberespacio todo está al alcance de la mano y en el momento que sucede; por ejemplo, el recién terremoto de Ecuador del 2016, el terremoto y Tsunami en Japón en el 2011, o los atentados terroristas en Bélgica el 2016. Estos son ejemplos de que en el ciberespacio no necesitamos un medio de transporte terrestre, aéreo o marítimo, ni mucho menos de pasaporte para viajar a cualquier parte del mundo y enterarnos o influir en algún evento que esté sucediendo.

Es así como ese desaparecimiento de fronteras físicas, tiene una consecuencia que es el del aparecimiento de comunidades virtuales relacionadas a las redes sociales que llegan en algunos casos a ser más numerosas que la mayoría de los 193 Estados reconocidos y que forman parte de las Naciones Unidas ([20--?]).

Nuestro país no es inmune a este tipo de creación a comunidades virtuales que como se mencionaba anteriormente asemejan a los componentes de una nación y si le agregamos el componente territorial "virtual" pues se convertiría en un Cibereestado. La penetración de Internet en El Salvador al 2015 con una población de alrededor de 6.1 millones de habitantes era del 47.2%, una cantidad de 2.9 millones de usuarios de las redes sociales y con una tasa de crecimiento del 2000 al 2015 del 7,1500% muy por encima de otros países de la región INTERNET…, 2016) Y si a esto le sumamos lo que mencionamos anteriormente que el 80 % del software que se utiliza es pirata, los riesgos que tenemos ante las amenazas en el ciberespacio son sumamente elevados.

Una tercera característica es la "pérdida de identidad o agrupación por afinidades" que se da en las redes sociales o cualquier comunidad virtual que se crea y organiza; la creación de grupos o seguidores en cualquiera de estos sistemas de comunicación y organización social, presentan un serio reto al control del Estado y el establecimiento de normativas para el funcionamiento de lo que denominamos "las redes sociales". La quinta característica muy interesante que es la del "uso de un lenguaje común y diferenciado" del resto de otros grupos, el uso de abreviaturas no catalogadas en ningún diccionario, esta característica la describe ampliamente Romero(2012) en su artículo sobre Ciberlenguaje Juvenil en las Redes Sociales "Entre las regularidades discursivas generales se encuentran: la adecuación lingüística, la competencia comunicativa (en especial, la pragmática y tecnológica), el registro coloquial (la variedad coloquial escrita), la nueva oralidad, la construcción de la imagen, los participantes y las temáticas. El discurso es acción".

La sexta característica que enfocamos y que representa una particularidad muy importante dentro del ciberespacio es el "uso de monedas y transacciones económicas diferentes" a las anteriormente establecidas. Si bien es cierto se llevan a cabo las consideradas normales como pago por medio de tarjetas de créditos, transacciones bancarias, uso de medios como PayPal (2016) que permite "crear una forma fácil y segura de pagar y recibir pagos por medio de internet sin compartir información financiera. Estos datos bancarios estarán a salvo gracias a un sistema de encriptación automática y a avanzados sistemas contra el fraude." (NIETO, 2014). Estos medios permiten emplear las monedas en curso legal u otro tipo de medios tradicionales de intercambio monetario; pero es el uso de BITCOIN el que hace al ciberespacio único en su forma de efectuar transacciones financieras sin la intervención de bancos, gobiernos u otro medio de control establecido en tratados internacionales y legislación local.

Bitcoin por ende es:

> […] una moneda que no depende de ningún órgano central, ya sea este un banco, un Estado o una institución política. Lo que su intercambio sea de los más seguros en el mundo, ya que se basa en que todos y cada uno de los usuarios que tiene el programa Bitcoin en su ordenador compartiendo datos". (BOICOINS, 2015) .

Esto representa un serio riesgo al no tener un control adecuado se puede prestar para comprar y vender prácticamente cualquier cosa, y al utilizar sitios web no indexados o colocados de tal forma que no se puedan accesar tan fácilmente y se encuentren en lo que se le llama la internet profunda o *Deep Web* en inglés,

hacen posible que Estados, organizaciones o simples individuos puedan representar amenazas hacia la Seguridad Nacional de cualquier Estado.

El hablar de individuos, organizaciones o Estados, nos plantea la sexta característica más significativa del ciberespacio y esta es la Asimetría, es un *Dejá* vu de David contra Goliat, donde el más pequeño y menos preparado vence al rival más organizado, equipado, y con gran cantidad de recursos. De esta forma un simple individuo puede causar serios problemas a una organización u otro Estado. Y un Estado u Organización puede emplear a un individuo o grupo pequeño para causar serios daños a su adversario sin llegar a verse involucrado directamente en ese hecho, por lo tanto, el determinar la fuente de origen de un ciberataque y vincularla a un Estado en particular es sumamente complicado y difícil de establecer.

4 ¿Qué nos Preocupa? ¿Cuáles son los Tipos de Ataques y Atacantes?

Para una persona o para la sociedad en general, es difícil identificar un problema o peligro si no lo vemos o percibimos. Diferente es cuando nos ubicamos frente a frente con algo que pueda colocarnos en riesgo o amenazar nuestra integridad física o en una mayor magnitud aspectos fundamentales y necesarios para el adecuado funcionamiento de nuestro Estado. Un dato importante es el crecimiento de usuarios que accesan a internet, ya que en el 2002 solo 1.9 personas de cada 100 contaban con ese recurso, al 2013 la cantidad de usuarios se incrementó a 23 por cada 100 habitantes USUÁRIOS…, 2015). En el 2016 en una serie de preguntas a los estudiantes de nuestro Curso de Seguridad y Desarrollo Nacional, sobre ¿quiénes tienen acceso a internet en sus casas?, ¿quiénes tienen o utilizan *Smartphones?*, ¿quiénes comparten información en las redes sociales?, ¿quiénes llevan trabajo a casa o llevan sus propios equipos al trabajo?, ¿quiénes comparten la computadora en casa o la red doméstica de internet con sus hijos o familiares?; la respuesta es del 100%, todos los alumnos tienen esas prácticas y todos los alumnos tienen acceso a internet. Pero solo 3 de cada 10 toma medidas de seguridad como compra de antivirus, utilización de contraseñas adecuadas, etc., por lo que los riesgos a que se ven confrontados es muchísimo más grave; y si tomamos en cuenta que esta es una práctica casi normal en nuestro medio, la concientización sobre la seguridad en el ciberespacio es bastante deficiente.

El gobierno de El Salvador ha implementado también una iniciativa para establecer una red de gobierno electrónico (Ministerios, autónomas, semiautónomas y otras dependencias gubernamentales) la cual se ubica dentro de la Red de Gobierno Electrónico de América Latina y del Caribe, en donde muchas de las transacciones y tramites serán llevados a cabo en línea; esto abre la posibilidad de fortalecer la re-

lación gobierno-ciudadano, gobierno-empresa, gobierno-gobierno y gobierno-empleado. Al establecer este nivel de interconexión y no existir los adecuados sistemas de protección que van desde el marco legal hasta las organizaciones que se crean para proteger los componentes del ciberespacio, la vulnerabilidad a los ataques que se llevan a cabo en ese dominio crece exponencialmente.

Por lo general creemos que las amenazas en el ciberespacio son solamente:

> […] los virus que son programas diseñados a efecto de copiarse a sí mismos con la intención de infectar otros archivos o ficheros, el código dañino conocido también como código malicioso o malware que es capaz de realizar un proceso no autorizado sobre un sistema, las bombas lógicas que se activa al cumplir ciertas condiciones de acceso o fecha, los troyanos que son programas que se ven como no dañinos pero en realidad permiten intrusiones y borrado de datos y los gusanos que son similares a los virus pero se diferencia en la forma que actúa este es el caso del famoso gusano Stutnext. (BEJARANO, 2010, p. 71-72).

Pero estos son solamente algunas de las herramientas o medios que utilizan los atacantes. Y estos agresores son los que se ubican o trabajan en diferentes entornos que pueden afectar la Seguridad Nacional, ya sean estos ataques patrocinados por Estados, servicios de inteligencia estratégica, terroristas o extremistas político/ideológico, delincuencia organizada, hasta individuos que por curiosidad o algún tipo de reto efectúan acciones de intrusión o de otro tipo. Innotec, empresa especializada en seguridad del Grupo Entelgy, analiza las ciberamenazas más frecuentes de 2013. (ESTAS..., 2014):

> Ciberespionaje industrial que es el robo de información a empresas con el fin de acceder a sus datos más valiosos (propiedad intelectual, desarrollos tecnológicos, estrategias de actuación, bases de datos de clientes, etc.). Ciberespionaje gubernamental: robo de información a organismos gubernamentales como la operación Octubre Rojo en la que se infiltraron en las redes de comunicaciones diplomáticas, gubernamentales alrededor de 40 países. Ciberataques a infraestructuras críticas: accesos no autorizados para manipular, alterar datos que provoquen daños debido a mal funcionamiento de los sistemas de agua, luz, transporte, salud, etc. Cibermercenarios o grupos de hackers con conocimientos avanzados, contratados para desarrollar ataques dirigidos contra un objetivo concreto, con el objetivo de conseguir la información deseada. Ciberdelincuencia contra servicios financieros, y muy especialmente, los denomi-

> nados troyanos bancarios, diseñados para el robo de datos de tarjetas de crédito y cada vez más, centrados en los dispositivos móviles. Ciberdelincuentes aislados que venden la información obtenida al mejor postor. Ciberdelincuentes organizados o mafias que han trasladado al mundo virtual sus acciones en el mundo real. Infección a través de páginas web. En 2013 se detuvo al autor de Blackole, un exploit-kit (paquete que contiene programas maliciosos) que permitía explotar vulnerabilidades de webs legítimas e infectar a los usuarios que accedían a dichas páginas, millones en todo el mundo. Ciberhacktivistas: personas o grupos que, movidos por alguna ideología, intentan socavar la estructura del oponente, ejemplo de Anonymous. Cibersabotaje que busca dañar la reputación de una organización y por ende su funcionamiento. Y la lista de amenazas ira creciendo con el paso del tiempo, por lo que al desconocer cuales y de qué tipo podrían ser; lo más conveniente es desarrollar capacidades para poder enfrentarlas en mejores condiciones que las actuales para enfrentar las ya existentes o conocidas.

Todas estas amenazas pueden tener efectos diversos y perturbar en diferentes formas el normal funcionamiento de las diferentes organizaciones gubernamentales, privadas y de diferente índole; pero el gran reto para un Estado es el de establecer un parámetro de medición a efecto de determinar ¿Cuándo una acción en el ciberespacio afecta a la Seguridad Nacional? Pues al fin de cuentas establecer el origen de los ataques o intrusiones es sumamente difícil; pero el efecto de esas acciones se puede medir con el objeto de determinar en primer lugar ¿cuándo se produce una alteración del orden constitucional? y en segunda instancia ¿cuándo hay una afectación significativa a la paz interna, estos dos planteamientos nos pueden determinar un parámetro más adecuado y aceptable para establecer cuando un ataque o intrusión es o no una amenaza a los Objetivos o Intereses Nacionales del Estado Salvadoreño. Pero a manera de ejemplo, si en una casa no se tienen detectores de humo para alerta temprana de incendios ni mecanismos de control sobre los mismos como aspersores automáticos, cierre de conductos de ventilación, etc., lo que nos queda después es apagar el fuego como sea; pero de que se apaga se apaga. De la misma forma en nuestro país al carecer de un sistema adecuado de alerta, de prevención y de control, estamos abiertos completamente a cualquier tipo de atacante y ataques que se puedan suscitar; y lo que nos queda al igual del fuego, es el solucionar el problema, pero ya después que ha causado los destrozos correspondientes.

A esto le sumamos otra característica muy peculiar y de carácter endémico en nuestro país, y este es el que se genera por el uso de *software* adquirido sin licencia,

ya que de acuerdo al estudio realizado por Business Software Alliance en el 2013 (BUSSINESS, 2014) el 80% del software utilizado es pirata, esto significa que, de cada 10 computadoras, 8 tienen en uso *software* adquirido ilegalmente, arrojando a las compañías productoras de *software* pérdidas económicas de cerca de los 72 millones de dólares al año. El Salvador se coloca en el 4º lugar del "ranking" latinoamericano en uso de software pirata, detrás de Nicaragua con el 82%, Paraguay con el 84% y en primer lugar Venezuela con el 88%. En este caso el uso masivo de programas ilegales o sin licencia, conlleva uno de los más grandes riesgos de seguridad al no contar con las actualizaciones correspondientes para enfrentar las temibles amenazas denominadas *exploit* de día cero en donde "tiene lugar el mismo día en que se descubre una debilidad en el *software*. En ese momento, el ataque se produce antes de que el creador del software encuentre una solución al problema" (KASPERSKY LAB, [20--?]) , y otro tipo de respaldo técnico del fabricante. Las vulnerabilidades son significativas en este punto siendo un caldo de cultivo idóneo para que puedan ser utilizados como computadoras zombies, acceso no autorizado, manipulación o secuestro de datos etc.

5 ¿Qué protegemos?

"Quien defiende todo, no defiende nada" decía Federico II, y si establecemos que el ciberespacio tiene cinco componentes principales *hardware, software,* servicios de información, sistemas de control e Internet, lo difícil es determinar qué es lo que hay que proteger y cómo hacerlo de una forma más eficiente. Allí radica uno de los problemas principales en el tema de la ciberseguridad ya que por nuestra parte debemos de salvaguardar todos los accesos hacia y desde nuestros sistemas lógicos, físicos y sociales; sin embargo, el atacante solo debe de encontrar un punto de entrada en todo ese entorno y poder realizar cualquier tipo de acción que desee o tenga la capacidad de llevar a cabo. Por lo tanto, es necesario el establecer ¿Cuál es el principal objetivo de los *hackers?*; y considerando que lo que se mueve en el ciberespacio son *bytes* en un conjunto ordenado de *bites* y estos son el componente principal de los "datos". Por lo tanto, los datos se convierten en el principal objetivo a defender y a atacar; allí surgen dos términos de uso muy común que son el ciberataque y la ciberdefensa, no necesariamente relacionados al concepto tradicional de ataque o defensa que se describe en la doctrina de la guerra tradicional librada en la tierra – mar – aire - espacio.

De acuerdo a lo descrito por Chamorro y SanzVillalba:

> Hasta fechas recientes, la ciberseguridad respondía a la exigencia de tutelar la información (Information Security), lo que determinaba un enfoque legislativo destinado a sancionar los

> accesos, usos, revelaciones, o daños ilícitos no autorizados. Sin embargo, en la actualidad, la evolución conduce hacia la gestión de riesgos del ciberespacio (Information Assurance), en la que los riesgos para la seguridad se encuentran vinculados al uso, procesamiento, almacenamiento y transmisión de información o datos, y los sistemas y procesos utilizados. Hoy la ciberseguridad requiere de ambos enfoques, diferentes pero complementarios. (CHAMORRO; SANZ VILLALBA, 2010).

Tomando en consideración lo planteado anteriormente, podemos establecer que los datos son el objetivo principal a proteger y estos datos son los que se encuentran en toda aquella instalación o infraestructura crítica, y que su afectación o mal funcionamiento puede impactar en la estabilidad, tranquilidad y normal desarrollo del país, así como la relación de nuestro Estado con la comunidad internacional.

Pero esos datos se encuentran en diferentes áreas, desde el sector gubernamental, pasando por las organizaciones internacionales radicadas en nuestro país, empresa privada, individuos, etc.; pero si consideramos aquellas áreas cuyo adecuado y normal funcionamiento depende la estabilidad y/o permanencia del Estado, el bienestar nacional y una conveniente y adecuada relación de convivencia internacional. Pasamos a un área que no ha sido establecida aún en nuestro país, y esta es la de establecer cuáles son el tipo de infraestructuras que son vitales para la Seguridad Nacional de El Salvador. Estas se deberían de clasificar al igual que en otros países de la forma siguiente: las infraestructuras estratégicas: que son instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales. Y las infraestructuras críticas: que son aquellas infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales (salud, energía, sistemas tributarios, transporte, agua entre otros). (ESPAÑA, 2011).

Como se mencionaba en el párrafo anterior, en El Salvador todavía no se clasifican de esta forma las infraestructuras, considerando los parámetros establecidos por la Unión Europea o por el Departamento de Homeland Security de los Estados Unidos (DEPARTMENT, 2015) en donde agrupan en diferentes sectores aquellos componentes que son parte de esa infraestructura estratégica y sus componentes que son parte también de esa infraestructura crítica. Estos sectores que comprenden: facilidades TIC del gobierno y empresa privada, sector de energía, agua, salud, comunicaciones, comercio, sector financiero, transporte, servicios de emergencia, seguridad pública y la defensa nacional.

Algunos ejemplos de estas infraestructuras estratégicas en nuestro país comprenden los sistemas de producción, distribución nacional e interconexión centroamericana de energía eléctrica de la Comisión Ejecutiva Hidroeléctrica del rio Lempa (CEL), los centros de captación, purificación, bombeo y distribución del sistema nacional de acueductos y alcantarillados (ANDA), El sistema de control y comunicaciones de la Comisión Ejecutiva Portuaria Autónoma (CEPA), Todos los sistemas de manejo de datos relacionados a identificación de personas del Registro Nacional de las Personas Naturales (RNPN) y el registro de propiedades desde intelectuales, catastrales, de comercio por el Centro Nacional de Registros (CNR), todos los sistemas de comunicaciones privados (CLARO, TIGO, DIGICEL, MOVISTAR, SALNET etc.) y los sistemas de comunicaciones estratégicas del Estado, especialmente las de la Fuerza Armada.

De la misma forma, a pesar de que se cuenta con esos elementos de infraestructuras vitales para el funcionamiento del Estado, no se cuenta con una organización centralizada o una planificación estratégica que contemple lo que debe ser protegido y que acciones se deben de realizar en caso de ser atacados a efecto de defender esas instalaciones que pueden resultar afectadas. A nivel del órgano Ejecutivo que tiene como misión fundamental la Seguridad Nacional, cuentan con la Dirección de Innovación Tecnológica e Informática de la Presidencia de la República (EL SALVADOR, 20?), la cual asesora sobre el uso de las TIC, velando por la seguridad e infraestructura de los equipos y de la información, articulando esfuerzos con las instituciones del Órgano Ejecutivo para la consecución de proyectos que se alineen a las actividades de la Presidencia. Esta Dirección no coordina esfuerzos con otras Organizaciones Gubernamentales, No Gubernamentales, Públicas, Privadas, Nacionales o Internacionales. De la misma forma no se cuenta aún con otro tipo de organismo que diseñe y ejecute una estrategia adecuada de ciberseguridad y tampoco se tienen funcionando Centros de Respuesta a Incidentes Informáticos que protejan esas infraestructuras estratégicas y críticas del Estado o cualquier otra acción intrusiva en contra de los datos que deben de ser protegidos.

6 ¿Cómo nos protegemos?

Un adagio popular nos da la guía para encontrar la respuesta a esta interrogante “Si copias la idea de una persona se llama plagio, si copias las ideas de varias personas se llama Inspiración” . Esos refranes provenientes de la sabiduría popular nos dan como resultado el que no hay ninguna necesidad de inventar la rueda en lo que a ciberespacio respecta. Muchos Estados, Organizaciones e individuos ya han recorrido el camino que vamos a trazar para desarrollar los medios

de protección necesarios en el ciberespacio. ¿Qué nos enseña lo mencionado anteriormente?, Pues en definitiva a los países como el nuestro que tenemos un incipiente desarrollo tecnológico, y que existe una indiferencia marcada por el estamento político y por qué no decirlo también, por la ciudadanía en general sobre lo que es el ciberespacio. No nos queda más que seguir en un inicio la hoja de ruta exitosa trazada por otros Estados que tienen ya un nivel de desarrollo organizacional, legal, así como de investigación y desarrollo adecuados para enfrentar las amenazas actuales y prepararse en mejor forma para enfrentar las amenazas futuras.

Pero a pesar de que podemos aprender de otros, efectuar acuerdos de cooperación, firmar tratados, asistir a un sinfín de conferencias y escribir ríos de tinta al respecto; es responsabilidad de nuestros gobernantes el definir qué camino es el que deberemos de seguir, una ruta complicadísima con una disyuntiva a escoger entre lo reactivo o lo proactivo. Este dilema clásico para los gobernantes implica el tomar decisiones menos políticas (algo muy difícil por supuesto) e inclinarse por soluciones más técnicas, ya que el ciberespacio no tiene muy buena relación con las decisiones que toman algunos políticos. Si no veamos lo que sucedió con la acción desarrollada por Tariq Tayyib Mohamed Bouazizi (2016) quien por medio de su acción de protesta personal causó la reacción política denominada la primavera árabe NAVARRO, 2011). Por otro lado, corremos el riesgo de caer como lo menciona Carrasco (2014) que "en la era de la información, que, de forma paradójica, se toman decisiones utilizando muy poca información, sin realizar un análisis crítico o sin contrastarla; más que una era de información es una era de datos", segundo Carrasco (2014). Tomando en cuenta lo mencionado por Carrasco, la tendencia a tomar decisiones coyunturales sin ver el horizonte estratégico es un común denominador en muchas de las leyes creadas, organizaciones que se anuncian con bombo y platillo y otras acciones llevadas a cabo por el Estado en general para apagar un fuego o querer solucionar un problema mediático que afecta intereses que no son siempre relacionados al Interés Nacional u Objetivos Nacionales.

Trazar una ruta reactiva o proactiva, esa es la interrogante más crítica a responder. No podemos limitarnos a estar actuando en base a reacciones tomadas a problemas que van surgiendo en el camino, por tal razón debemos de aprender de aquellos que ya han iniciado ese recorrido y se están preparando para afrontar las amenazas que surgen a diario en ese entorno. Por el momento nuestro país NO dispone de una estructura gubernamental o en combinación con la empresa privada para afrontar este tipo de amenazas, de la misma forma el marco legal adecuado. Por ejemplo, podemos citar la misión que rige el funcionamiento de la Superinten-

dencia General de Electricidad y Telecomunicaciones SIGET (SUPERINTENDENCIA..., 2015), máxima organización gubernamental que tiene que ver con lo pertinente a comunicaciones, esta misión solo le da funciones reguladoras, y su visión es también solamente la de regular los servicios TIC.

De la misma forma, siempre a nivel del órgano Ejecutivo que tiene la responsabilidad fundamental de la Seguridad Nacional, cuentan con la Dirección de Innovación Tecnológica e Informática de la Presidencia de la República (EL SALVADOR, [20—¿]), la cual asesora sobre el uso de las TIC, velando por la seguridad e infraestructura de los equipos y de la información, articulando esfuerzos con las instituciones del Órgano Ejecutivo para la consecución de proyectos que se alineen a las actividades de la Presidencia. Esta Dirección no coordina esfuerzos con otras Organizaciones Gubernamentales, No Gubernamentales, Públicas, Privadas, Nacionales o Internacionales. Y así buscamos en toda la orgánica del Estado Salvadoreño las responsabilidades de los diferentes Ministerios, organismos Autónomos, Semiautónomos, Instituciones, etc. Sin encontrar en alguno de ellos quien es el encargado de planificar, coordinar, o de al menos defendernos de estos riesgos y amenazas; queda mucho camino que recorrer y debemos de aprender de esos países que ya tienen desde sus Políticas y estrategias de ciberseguridad, hasta las organizaciones que están involucradas en todo lo concerniente a la defensa de los Intereses y Objetivos Nacionales que se pueden ver afectados por las acciones provenientes desde el ciberespacio.

Por consiguiente, si bien es cierto en El salvador no hay acciones coordinadas u organizaciones que ya están realizando en otros países como Estados Unidos, Brasil, Colombia, Chile, España y otros en la Unión Europea y el mundo (la rueda ya fue inventada en esos lugares). Los cuales cuentan con los medios adecuados para defender el quinto dominio o que cuentan con legislación, organización y recursos para contrarrestar los riesgos y amenazas a la Seguridad Nacional; riesgos y amenazas que provienen del ciberespacio. Podríamos mencionar que en nuestro país volvemos al paradigma de la "Polis Griega" cuando nos referimos a las acciones que se debería de estar tomando para enfrentar las ciberamenazas o prepararnos a reaccionar ante cualquier situación que se nos presente en el ciberespacio. La "Polis Salvadoreña" en donde cada organización gubernamental, no gubernamental, nacional e internacional, empresa privada y ciudadanos. Todos levantan murallas al igual que esas ciudades Estado para resguardarse de los riesgos y amenazas proveniente del entorno ciber; pero si bien es cierto esas murallas defienden parcialmente a determinada organización, siempre existirá un punto débil donde los atacantes lograran penetrar y después seguir con las siguientes polis hasta tomar el control de todo.

7 ¿Quiénes son los responsables?

En caso de suceder algún tipo de acontecimiento, por regla general en un sistema reactivo que no dispone de procedimientos claramente establecidos para incidentes informáticos, lo que se buscan son culpables y después si queda tiempo las soluciones (patrón de la cultura organizacional en nuestro entorno). Pero al carecer de un entorno adecuado en el que se vislumbre un horizonte en el mediano y largo plazo para la búsqueda de soluciones; partiremos de la premisa en que se requiere el contar no solamente con el marco legal correspondiente, una organización, recursos humanos, materiales y financieros. Si no que se requiere contar con una "ciber-concientización" a efecto de que todos reconozcan y tomen un nivel de responsabilidad y conocimiento de la problemática ante las vulnerabilidades en el ciberespacio.

Buscando una analogía con el entorno del ciberespacio y cómo se comportan nuestras diversas organizaciones gubernamentales, no gubernamentales, empresa privada y demás estructuras organizacionales dentro del entorno del ciberespacio. Podemos relacionar referidas organizaciones a la "polis" griega en donde "Cada una de estas ciudades-Estado se consideraba como una especie de nación separada e independiente y denominaba «extranjeros» a los habitantes de las demás polis" (CONCEPTO…,[20--]). Algunas de las características de estas Polis como una extensión territorial reducida, independencia económica e independencia política pueden darnos la idea del comportamiento de las organizaciones que tenemos en este momento que independientemente del tema ciberespacio; actúan en todo ámbito como esas "polis" griegas presentando por lo tanto un serio problema de coordinación y articulación de acciones para proteger al Estado salvadoreño de las amenazas que se presentan en el ciberespacio.

En El Salvador la responsabilidad principal en el marco de la Seguridad Nacional, corresponde a los Órganos de Gobierno, Ministerio Público y demás Instituciones permanentes al servicio del Estado; pero los que participan en los procesos de planificación y ejecución de las estrategias de ciberseguridad son todos los sectores de la misma sociedad inclusive organizaciones internacionales ya sean gubernamentales o privadas. Por lo tanto, la creación del marco legal, organizacional, y demás elementos necesarios; involucra el construir un esquema que, a la vez de complicado, será sumamente complejo y el aprender a manejar la complejidad es algo que el aparato gubernamental nunca ha Estado muy bien preparado que se diga, esto debido al sin fin de intereses y agendas particulares que prevalecen al momento de tomar decisiones.

Por ende, al final del día, las decisiones son eminentemente políticas y dejan de lado en muchas ocasiones los resultados de estudios, análisis, y otros docu-

mentos en donde equipos multidisciplinarios recomiendan las medidas adecuadas a tomar; pero que por lo general no son políticamente viables, o no satisfacen los intereses políticos de las organizaciones. El entorno se mantiene similar al de las "polis" que describíamos anteriormente, en donde cada estructura indistintamente de la función que desempeñe; se mantiene aislada creando sus propios sistemas de defensa, en esfuerzos que consumen recursos que pueden ser aprovechados con otras organizaciones. En el Siglo XXI en donde la globalización crea una serie de nuevos paradigmas sobre gobernanza y gobernabilidad, ya no es posible estar desconectados o actuando separadamente. El ciberespacio es un nuevo entorno que afecta transversalmente a los demás que ya conocemos de tierra – mar – aire – espacio, es por lo tanto una necesidad imperiosa el de crear nuevos patrones de comportamiento colectivo y que a la vez sirvan para protegernos antes las amenazas crecientes en ese para algunos considerado como "Global Commons" y para otros considerado como un quinto dominio de actuación.

La pregunta se mantiene entonces ¿quién está a cargo en nuestro país?, seguiremos actuando como lo hemos hecho siempre, o crearemos algo nuevo tomando en consideración la experiencia de los países que ya cuentan con estrategias de ciberseguridad y sus correspondientes organizaciones, marco legal, etc. Nos remontaremos al pasado reciente en 1963 cuando el control de las comunicaciones era responsabilidad única del Estado, cuando funcionaba solamente la Administración Nacional de Telecomunicaciones (ANTEL):

> […] tendrá el control exclusivo del espectro electromagnético, de acuerdo a los adelantos técnicos, a los tratados o convenios internacionales ratificados por El Salvador; su utilización en el territorio nacional, se regulará de conformidad a esta ley y a los reglamentos que se dicten para los servicios de telecomunicación. (EL SALVADOR, 1963).

El monopolio estatal era evidente y no existía otro ente regulador del espectro electromagnético, por lo que, las ventajas y desventajas de ese modelo de control estatal son evidentes tomando en cuenta sus características centralizadoras, burocráticas y de difícil capacidad de transformación y modernización de un campo que requiere la participación del ente privado.

Fue hasta 1996 cuando se privatizan las telecomunicaciones y se crea un ente gubernamental diferente al anterior para regular los procesos de funcionamiento. Es así como surge la Superintendencia General de Telecomunicaciones (SIGET) (SUPERINTENDENCIA…, 2013) , a la cual se le asignan las responsabilidades de representar oficialmente a nuestro país ante las diversas organizaciones a las que

estamos suscritos, tales como la Unión Internacional de Telecomunicaciones (UIT), la Comisión de Telecomunicaciones Centroamericanas (COMTELCA), la Comisión Interamericana de Telecomunicaciones (CITEL) y el Foro Latinoamericano de Entes Reguladores de Telecomunicaciones (REGULATEL).

La SIGET a pesar de que se han realizado varias reformas a su ley de creación hasta la del Decreto Legislativo No. 086 del 18 de agosto de 2012, Diario Oficial N° 154, Tomo 396 del 22 de agosto de 2012. Como se describió en párrafos anteriores, sus funciones son estrictamente de regulación y de ejercer cierto grado de control y coordinación entre los que prestan diferentes servicios de comunicaciones, sin considerar la inclusión de regulación de internet ya que esta se encuentra como parte de las comunicaciones telefónicas. Atribuciones tales como aplicar tratados, aprobar tarifas, dictar normas y estándares técnicos, informar a las autoridades sobre acciones que atenten a la libre competencia, publicar información estadística, establecer, mantener y fomentar relaciones de cooperación, representar al país ante organismos internacionales; pero nada que la convierta en el ente rector de las comunicaciones en El Salvador. Por otro lado, a la fecha no se cuenta con una ley que regule directa y efectivamente el ciberespacio ni el uso que se le da a este medio para la transmisión de datos.

A pesar de que los Estados miembros de la OEA aprobaron en el 2004 la Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética en la resolución AG/RES. 2004 (XXXIV-O/04), proporcionando un mandato que permite a la Secretaría del CICTE trabajar en asuntos de Seguridad Cibernética en coordinación con los Ministerios de Seguridad de los países miembros. Y tomando como referencia datos obtenidos del observatorio de la ciberseguridad en América Latina y el Caribe (ORGANIZACIÓN…; BANCO…, [2016?]),

en el 2016 nuestro país adolece del marco legal, la o las organizaciones adecuadas y la política o estrategia de ciberseguridad que nos brinde en cierta medida las condiciones necesarias de enfrentar las amenazas en ese entorno representado por el ciberespacio.

Si bien es cierto se está trabajando en ese sentido, de parte de algunas instituciones del gobierno y empresa privada. La falta de regulaciones y conciencia sobre la ciberseguridad, hace que el trabajo se desarrolle en una forma diametralmente opuesta a la velocidad a que se desarrollan los eventos en ese quinto dominio al que se refieren los militares. En nuestro país, a pesar de que las iniciativas a nivel internacional sobre legislación en el área del ciberespacio dan en el 2001 con el Convenio sobre la Ciberdelincuencia en Budapest o en otros años siempre relacionado al mismo entorno. Ya en 1997 al decretar el Código Penal se hacen referencias a delitos en forma general que también se utilicen “medios electrónicos”

(EL SALAVADOR, 1997),). Es hasta el 2006 que se da uno de los primeros pasos en ese sentido al señalar directamente el delito informático cuando se decreta la ley especial contra actos del terrorismo

(EL SALAVADOR, 2006), en donde en su Artículo 12 establece una pena de prisión a quien "utilizare equipos, medios, programas, redes informáticas o cualquier otra aplicación informática para interceptar, interferir, desviar, alterar, dañar, inutilizar o destruir datos… de servicios públicos, sociales, administrativos, de emergencia o de Seguridad Nacional" […]. (EL SALVADOR, 2006).

Otro ejemplo es el de la Ley contra delitos informáticos que se comenzó a gestar en el 2010, cuando el entonces Diputado Douglas Avilés presentó una noción para dar inicio al estudio de que se llevaran a cabo reformas a la ley penal de ese entonces, no se propuso entonces una creación de ley sobre ciberespacio o delitos informáticos; sino que, solamente reformas aisladas en diferentes componentes de la legislación penal. Y así fue transcurriendo el tiempo y generándose un debate continuo por muchos años en la Asamblea Legislativa dentro de la Comisión de Seguridad Pública y Combate a la Narcoactividad. El 2012 se genera otra discusión alrededor del como castigar las actividades delincuenciales que se cometen en el ciberespacio; pero no se llega a ninguna propuesta en concreto. Para el 2013 sigue la discusión política y que a pesar de haber tenido ya ataques de tipo de denegación de servicio (que son los más evidentes) a los sitios web de Casa Presidencial, Policía Nacional Civil en el 2011, y el 2012 las del Ministerio de Trabajo, Asamblea Legislativa y la del Presidente de ese Órgano de Gobierno. (MÓRAN, 2013).

Así ha venido evolucionando la discusión sobre una nueva ley, y en octubre del 2014 se crea un equipo interinstitucional conformado por: El Ministerio de Justicia y Seguridad Pública, la Fiscalía General de la República, la Superintendencia General de Electricidad y Telecomunicaciones, la Dirección Ejecutiva del Consejo Nacional de la Niñez y Adolescencia, las empresas privadas de telecomunicaciones CLARO, DIGICEL, RED-INTELFON, TELEMOVIL y TELEFONICA. Equipo que revisa la propuesta final de redacción del anteproyecto de ley presentando su recomendación en marzo del 2015; sin embargo, a pesar de la revisión anterior continúa otro proceso de consultas con la Fundación Salvadoreña para el Desarrollo Económico, la Asociación Bancaria Salvadoreña, la Cámara Americana de Comercio de El Salvador, Departamento de Asuntos Jurídicos de Casa Presidencial, Consejo Nacional de Publicidad, La Prensa Gráfica. Y es así que, en febrero del 2016, después de seis años de consultas, estudios, y vueltas a consultar y a estudiar, se aprueba el acuerdo al decreto 260 la "Ley Especial Contra los Delitos Informaticos y Conexos (LDIC)"

A pesar de que esta ley fue aprobada el 2016, estos casos de iniciativas de ley y/o creación de normativas relacionadas al ciberespacio son señalados por FUSA-

DES en el 2015, como un error que se ha venido cometiendo al no enfocar o tomar la importancia que tiene el ciberespacio, generando una multiplicidad de normativas relacionadas a ese entorno.

> Se considera problemático que el Anteproyecto de la LDIC incluya delitos que están tipificados en el Código Penal, en el caso que se realicen por medio de las TIC, puesto que ello podría derivar en una duplicidad de tipificación, falta de proporcionalidad en las penas y una regulación diferenciada para una conducta similar. (FUNDACIÓN, 2015).

El enfoque unilateral hacia la seguridad pública que se le da a la ley sobre "delitos informáticos", si bien es cierto es un primer paso a elaborar el entramado jurídico, organizacional tan necesario para contrarrestar o tipificar algunas formas nuevas de delito a nivel nacional. Se queda corta en su enfoque estratégico de manejo en el mediano y largo plazo al dejar fuera en su Articulado, considerandos y definiciones que puedan ser utilizadas como referencia no solamente en la persecución del delito, sino que también para la futura conformación de políticas y estrategias en este sentido. De la misma forma, el encajonar en la seguridad pública algo que afecta todos los espacios de actuación nacional e internacional, se genera un paradigma peligroso en el que las ciberactividades orientadas a amenazar los objetivos nacionales o interés nacional del Estado, no son consideradas. Por otro lado, a pesar de haberse reunido una serie de organizaciones gubernamentales, no gubernamentales y privadas en el estudio de esta ley. Solamente se enfocaron al estudio de la ley de delitos informáticos, habiendo perdido una valiosa oportunidad para generar la creación de una normativa que diera pie a una política más amplia sobre el accionar multisectorial en el ciberespacio.

8 ¿Cuál es la hoja de ruta a trazar para establecer las políticas y estrategias de ciberseguridad más adecuadas a nuestras necesidades?

Es difícil el trazar una ruta considerando el marco legal actual, por lo tanto, en primer lugar, si vamos a desarrollar una Política y Estrategia para el Ciberespacio, lo más lógico es establecer una definición de lo que es el Ciberespacio. Para este fin adoptamos la siguiente:

> El ciberespacio es el conjunto de medios y procedimientos basados en las TIC, configurados para la prestación de servicios

> esenciales y el intercambio de datos de las actividades políticas, económicas, sociales y militares de El Salvador. Y está constituido por hardware, software, Internet, servicios de información y sistemas de control. (INSTITUTO…, 2015).

Son cinco los componentes que lo integran, así como cuatro los campos de acción en los cuales se organiza y articula el poder nacional de nuestro país y que ahora en el Siglo XXI se ven afectados por igual en cualquier situación que afecte el normal funcionamiento en el ciberespacio. De la misma forma se han establecido definiciones en el entorno académico del CAEE que son similares a las utilizadas por otros países, ya que consideramos importante que, si vamos a enfrentar una amenaza que es de carácter global, es recomendable el adoptar definiciones o al menos conceptos similares cuando nos refiramos a ciberconflicto, ciberguerra, ciberataque, ciberdefensa, infraestructura crítica, delito informático, dato informático, sistema informático, etc., como por ejemplo la taxonomía de soluciones de ciberseguridad empleada por INCIBE (INSTITUTO…, 2015) y las de la Unión Internacional de Telecomunicaciones.

Así mismo, de nuevo nos vemos confrontados a la analogía de "para que vamos a inventar la rueda si esta ya existe", pues podríamos decir que la respuesta a esto debería de ser sumamente fácil, y que con solo el adaptar lo que otros países ya están haciendo al respecto, tenemos asegurado el éxito en ese sentido. Bueno, la realidad es muy diferente pues El Salvador no ha dado grandes avances en lo concerniente a este punto, una muestra son los casi seis años que la Asamblea Legislativa tardó en aprobar una ley contra delitos informáticos. Y si a esto le sumamos las demás resoluciones dadas por diferentes organismos internacionales, así como tratados internacionales efectuados sobre el ciberespacio, cibercrimen, etc.; por ejemplo, que desde el 2004 en que la OEA aprueba la Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética en la resolución AG/RES. 2004 (XXXIV-O/04) (ORGANIZACIÓN…, [20--?])

También como efecto de esta resolución donde se involucran igualmente otras tres organizaciones CICTE, CITEL y REJMA a efecto de asesorar a las diferentes organizaciones gubernamentales y no gubernamentales sobre los aspectos pertinentes al ciberespacio.

Es así como, nuestro país continúa sin lograr ese grado de concientización especialmente en el estamento político, para dar inicio a procesos transformadores y de modernización orientados al ciberespacio. Es así que a la fecha no hemos realizado ningún tipo de pronunciamiento o adhesión a los mismos por medio de ratificaciones siguiendo los procesos constitucionales vigentes en nuestro país. Por consiguiente, hemos llegado a determinar que no hay continuidad en las iniciativas

no solamente de ley, sino que la creación de un proceso político y estratégico que genere el impulso necesario para la creación del marco legal, organizacional y de diferente índole orientado a contrarrestar las amenazas cibernéticas.

Ejemplos a seguir sobre procesos de creación de sistemas de ciberseguridad tenemos bastante en otros países, así como los desarrollados en forma conjunta por una serie de organismos internacionales mundiales y regionales. En ese sentido el Global Cybersecurity Índex (ITU, 2016) establece el Estado de ciberseguridad en los diferentes países del mundo, también la guía establecida por la ITU nos ayuda a comprender mejor el gran problema de Seguridad Nacional en el ciberespacio, y que servirán de soporte para utilizar adecuadamente la caja de herramientas para desarrollar o mejorar las estrategias nacionales de ciberseguridad (ITU, [2016?]) implementada por la misma organización. Esto, aunado a las resoluciones de la OEA y otros organismos que trabajan en esta área, nos da una pauta sobre lo que debemos de tratar de implementar. Esta lista de comprobación elaborada por la ITU en el Telecom World 2014 celebrado en Doha, consta de cinco puntos: medidas legales, medidas técnicas, medidas orgánicas, capacitación y cooperación. Estos puntos se dividen en 17 ítems que se convertirán en una lista de comprobación para determinar cómo estamos y marcar el punto de partida para llegar a crear el Sistema de Ciberseguridad Nacional con todos sus componentes y afrontar en una mejor condición las amenazas en el ciberespacio.

Ese punto de partida de establecer donde estamos en este momento, será la elaboración del diagnóstico adecuado. Diagnóstico en el que nos valdremos de varias herramientas y procesos desarrollados por esas organizaciones internacionales y países amigos. Lo primero que haremos es analizar los datos presentados sobre ciberseguridad de la ITU en el perfil de El Salvador (ITU, 2015), y las contrastaremos con un diagnostico a elaborar en otra investigación que se está llevando a cabo en este Colegio, tomando como referencia los procesos para establecer las Estrategias de Ciberseguridad y los sistemas que conllevan estas estrategias, los cuales han sido efectuados ya por España, Colombia y Chile.

Una referencia muy importante en esa ruta a trazar y que estamos utilizando son las "orientaciones y líneas de acción de aplicación general para la implementación y evaluación de diversas actividades tendientes a minimizar los riesgos y amenazas del ciberespacio en el país, las cuales se deberán implementar tanto respecto del sector público como del privado" materializadas en Las Bases para una Política de Ciberseguridad (CHILE, 2015) realizado por el Ministerio del Interior y Seguridad Pública en conjunto con el Ministerio de Defensa de Chile. Otros documentos que nos sirven como referencia son los Lineamientos de Política para Ciberseguridad y Ciberdefensa de Colombia CONSEJO, 2011) que "busca generar lineamientos de

política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas" y la Agenda Estratégica de Innovación en Ciberseguridad de Colombia (COLOMBIA, 2014) "que nos orientan sobre los vectores de desarrollo en este campo".

Por último, para desarrollar nuestra estrategia de ciberseguridad, debemos de tomar ejemplo dentro de la gran diversidad de estrategias de seguridad cibernética que encontramos en el repositorio de la ITU (20--?) y en el Centro de Ciberdefensa Cooperativa de la OTAN (NATO, 2015). Esto con el objeto de acomodar nuestra estrategia ciber; al proceso político, económico, social y militar de desarrollo del poder nacional de nuestro país y estar en mejor forma de defender los intereses y objetivos nacionales que se vean afectados por las acciones provenientes del ciberespacio. Elaborar el diagnóstico correspondiente, generar la concientización en todos los ámbitos, desarrollar las políticas y estrategias para alcanzar los objetivos, crear y sostener las organizaciones y darle la continuidad, así como, el nivel de importancia que merece a esta estrategia. Este es el modelo que estamos recomendando a seguir desde el ambiente académico del CAEE en nuestro país a efecto de realizar las investigaciones que conduzcan a generar la teoría y después del análisis debido, la doctrina necesaria para seguir adelante en el proceso de la creación de una estrategia de ciberseguridad más robusta y acorde a las capacidades y necesidades que poseemos.

9 Conclusiones

El presente artículo no se refiere al ciberespacio en el ámbito de ciberguerra o aspectos relacionados a las características intrínsecas de la guerra tradicional tal y como la conocemos y estudiamos los militares. Existe una tendencia a utilizar términos que se emplean en las acciones armadas; pero el ciberespacio es un campo o dominio que afecta transversalmente a otros entornos de actuación de manera transversal tierra-mar-aire-espacio. Por lo que , dentro de la dinámica de los conflictos, estas acciones de intrusión, ataque, o de cualquier índole que se oriente a afectar positiva o negativamente dentro del ciberespacio y que de acuerdo a lo planteado por Sánchez, (2012), los conflictos se manejan en seis fases diferentes, desde la primera que es la paz, siguiendo con la paz inestable, pasando a él tensionamiento entre los involucrados, decantándose en crisis que puede llegar a un conflicto armado y de allí convertirse en una guerra. Las ciberacciones llámense como se llamen, pueden emplearse en cualquier fase de esta dinámica y que a diferencia del ambiente de una guerra convencional o no convencional en donde se emplean medios cinéticos. Las ciberacciones como le hemos denominado se pueden llevar a

cabo en cada una de las etapas de un conflicto, sin llegar a declaraciones de guerra, atribuciones que conlleven represalias y ser prácticamente anónimas en procedencia o accionar de cualquier Estado, organización o individuos.

A pesar de que el término ciberespacio se viene utilizando desde 1984 como producto de la novela de William Gibson, 32 años después en el 2016 en nuestro país todavía se desconoce que es el ciberespacio y los riesgos y amenazas que encontramos en ese entorno. La percepción general es tomar como sinónimo de ciberespacio a internet, todo esto tomando en cuenta que, a pesar del constante crecimiento en la penetración de internet en el país, uso de redes sociales, smartphones, computadoras personales, tablets, laptops y cualquier otro equipo que tenga circuitos y procesadores integrados y que también corra programas que se conecten por cualquier medio entre ellos. Por ejemplo, del crecimiento de usuarios de internet que del año 2000 era apenas de 40,000 y se expande en quince años a 2.9 millones de usuarios registrados (INTERNET, 2016); y la cantidad de servidores conectados a la WWW que eran alrededor de 4,000 en el 2003 hasta llegar a un poco más de 24,000 en el 2012 (CUADROS, 2016). Otro aspecto crítico en la concientización hacia lo que es el ciberespacio, las amenazas y que debemos de hacer al respecto se muestra con el alto índice de piratería en software, ya que 8 de cada 10 computadoras corren programas piratas (CUADROS, 2016). Dejando un campo fértil para todos los que quieran utilizar esas computadoras para que los que deseen llevar a cabo cualquier tipo de intrusiones, o uso al margen de la ley de esos sistemas.

Las organizaciones internacionales ONU (mundial), OEA (Continental) y SICA (centroamericana-regional) respectivamente, tienen resoluciones, normativas, estructuras que se orientan a educar, capacitar, estructurar y/o coordinar los aspectos relacionados al ciberespacio. A nivel nacional en El Salvador, se carece de una organización adecuada, ya sea civil o militar que se encargue del diseño de políticas y estrategias de ciberseguridad, así como las diferentes normativas y/o regulaciones que administren organizaciones para atender asuntos específicamente en el ciberespacio. Y para proteger esa infraestructura estratégica y crítica se deben de crear las políticas y estrategias necesarias para crear el marco legal, las organizaciones y recursos necesarios a efecto de crear los sistemas que nos den la prevención y alerta temprana, detecten esas intrusiones, se tenga la capacidad de reaccionar ante estos eventos y lo más importante manejar las crisis que se presenten.

El decreto Legislativo No 948 del año 2002 donde se establece la Ley de Defensa Nacional de El Salvador, establece también la definición de Seguridad Nacional como el "Conjunto de acciones permanentes que el Estado propicia para crear las condiciones que superan situaciones de conflictos internacionales, per-

turbaciones a la tranquilidad pública, catástrofes naturales y aquellas vulnerabilidades que limiten el desarrollo nacional y pongan en peligro el logro de los Objetivos Nacionales". En este sentido y orientado al ciberespacio, se carecen de acciones permanentes en ese sentido y no se cuenta además con un sistema de medición o determinación cuando algo afecta la Seguridad Nacional, al no contar con el entramado legal y organizacional adecuado para enfrentar las amenazas que se presenten.

Este colegio establece dos situaciones para medir el grado de afectación y determinar si amenazan o no la Seguridad Nacional, estas son: en primer lugar ¿cuándo se produce una alteración del orden constitucional? y en segundo lugar ¿cuándo hay una afectación significativa a la paz interna?, estos dos planteamientos nos pueden determinar un parámetro más adecuado y aceptable para establecer cuando un ataque o intrusión es o no una amenaza a los Objetivos o Intereses Nacionales de nuestro país. Y puede tener un efecto negativo en la permanencia del Estado, el bienestar nacional y en la concordia internacional.

Referencias

BEJARANO, Maria José Caro. Alcance y ámbito de la Seguridad Nacional en el ciberespacio. In.: INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS. *Ciberseguridad*: retos y amenazas a la seguridad nacional en el ciberespacio. Madrid, 2010. p. 49-82. (Cuadernos de Estrategia, 149).

BITCOINS, una buena argumentación para principiantes. *Qué es Bitcon*, [S.l.], 24 dic. 2015. Disponible en: <https://www.queesbitcoin.info/argumentario-sobre-los-bitcoins/>. Fecha de acceso: 02 abr. 2016.

BUSINESS SOFTWARE ALLIANCE. *La brecha de cumplimiento:* encuesta global sobre software de BSA. Washington, DC, 2014. p. 7-10. Disponible en: <http://www.bsa.org/~/media/Files/Research%20Papers/GlobalStudy/2014/2013GlobalSurvey_Study_es.pdf>. Fecha de acceso: 12 abr. 2016.

CARRASCO, Luis de Salvador. Los problemas estructurales en el planteamiento de la ciberseguridad. *Documento Marco IEEE.ES,* [S.l.], n. 09/2014, jul. 2014.

CHAMORRO, Enrique Fojón; SANZ VILLALBA, Ángel F. Ciberseguridad en España: una propuesta para su gestión. *ARI:* Revista do Real Instituto Elcano, Madrid, n. 77, jul. 2010.

CHILE. Ministerio del Interior y Seguridad Publica; Ministerio de Defensa Nacional. *Bases para una política nacional de ciberseguridad.* Santiago, 2015. Disponible en: <http://ciberseguridad.interior.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf>. Fecha de acceso: 09 abr. 2016.

COLOMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones. Ciberseguridad. Bogotá, DC, 2014. Disponible en: <http://www.mintic.gov.co/portal/604/w3-article-6120.html>. Fecha de acceso: 11 abr. 2016.

CONCEPTO de polis o ciudad-estado. *Guía de Grecia,* [S.l., 20--]. Disponible en: <http://www.guiadegrecia.com/general/polis.html>. Fecha de acceso: 03 abr. 2016.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL (Colombia). *Lineamientos de política para ciberseguridad y ciberdefensa.* Bogotá, DC, 2011. (Documentos Copes, 3701). Disponible en: <http://www.mintic.gov.co/portal/604/w3-article-3510.html>. Fecha de acceso: 10 nov. 2016.

CUADROS de Datos Históricos Anuales. *Index Mundi,* [S.l.], 2016. Disponible en: <http://www.indexmundi.com/g/g.aspx?v=140&c=es&l=es>. Fecha de acceso: 12 abr. 2016.

DEPARTMENT HOMELAND SECURITY (United States of America). *Critical Infrastructure Sectors.* [Washington, DC], 2015. Disponible en: <https://www.dhs.gov/critical-infrastructure-sectors>. Fecha de acceso: 10 abr. 2016.

EL SALVADOR. Constitución de la República (1983). Art. 83. El Salvador es un Estado soberano. La soberanía reside en el pueblo, que la ejerce en la forma prescrita y dentro de los límites de la constitución. *[Diario Oficial de la República de El Salvador, San Salvador],* n. 234, tomo 281, 16 dic. 1983.

_____. Decreto Legislativo nº 370, de 27 de agosto de 1963. Creó la Administración Nacional de Telecomunicaciones (ANTEL). *[Diario Oficial de la República de El Salvador],* San Salvador, n. 163, tomo 200, 27 agosto 1963.

_____. Decreto nº 103, de abril de 1997. *Código Penal*, San Salvador, 1997.

EL SALVADOR. Decreto nº 108, de 21 de septiembre de 2006. Art. 12. Ley especial contra actos de terrorismo. *Diario Oficial de la República de El Salvador,* San Salvador, nº 193, Tomo 373, 17 oct. 2006.

_____. Ley de Defensa Nacional, Decreto Ley nº 948, de 03 de octubre de 2002. Art. 4. *[Diario Oficial de la República de El Salvador],* Ministerio de la Defensa Nacional, 03 oct. 2002. n. 184, tomo 357. Disponible en: <http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-de-la-defensa-nacional/archivo_documento_legislativo>. Fecha de acceso: 15 nov. 2015.

ESPAÑA. Ley nº8, de 28 de abril 2011. Establecen medidas para la protección de las infraestructuras críticas. *Boletín Oficial del Estado España,* Madrid, 29 abr. 2011.

ESTAS son las diez ciberamenazas más comunes. ABC Tecnología, Madrid, 07 abr. 2014. Disponible en: <http://www.abc.es/tecnologia/redes/20140404/abci-amenazas-ciber-201404031906.html>. Fecha de acceso: 03 abr. 2016.

GLOBAL Commons. *Pensamientos Estratégicos,* [S.l.], oct. 2010. Disponible en: <https://agdeagreda.wikispaces.com/GLOBAL+COMMONS>. Fecha de acceso: 22 nov. 2015.

FUNDACIÓN SALVADOREÑA PARA EL DESARROLLO ECONÓMICO Y SOCIAL. Una ley contra los delitos informáticos que respete la libertad de expresión, La Libertad: n. 91, 2015. (Estudios Legales) Disponible en: <http://fusades.org/sites/default/files/investigaciones/POSICI%C3%93N%20INST.%20NO.%2091%20UNA%20LEY%20CONTRA%20DELITOS%20INFORM%C3%81TICOS.pdf>. Fecha de acceso: 10 feb. 2016.

INTERNET usage and population in Central America. *Internet World Stats,* [S.l.], 2016. Disponible en: <http://www.internetworldstats.com/stats12.htm>. Fecha de acceso: 12 feb. 2016.

INSTITUTO NACIONAL DE CIBERSEGURID (España). *Taxonomía de soluciones de ciberseguridad.* Madrid, 2015. Disponible en: <https://www.incibe.es/extfrontinteco/img/File/empresas/guias/taxonomia_ciberseguridad_2015.pdf>. Fecha de acceso: 08 abr. 2016.

ITU. *Cyberwellness profile Republic of El Salvador.* [S.l.], 2015. Disponible en: <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/El_Salvador.pdf>. Fecha de acceso: 08 abr. 2016.

ITU. Global Cybersecurity Index. [S.l.]. 2016. Disponible en: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx. Fecha de acceso: 07 abr. 2016.

ITU. *National Cyber Security Strategy* (NCS) Toolkit. [S.l., 2016?]. Disponible en: <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf>. Fecha de acceso: 08 abr. 2016.

ITU. *National Strategies Repository.* [S.l., 20--¿]. Disponible en: <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx>. Fecha de acceso: 11 abr. 2016.

JIMÉNEZ, Antonio García; ORENES, Pilar Beltrán; PUENTE, Sonia Núñez. Una aproximación al concepto de frontera virtual: identidades y espacios de comunicación. *Revista Latina de Comunicación Social:* revista da Universidade de La Laguna, San Cristóbal de La Laguna, n. 65, p. 214-221, 2010.. Disponible en: <http://www.revistalatinacs.org/10/art2/894_Madrid/16_Antonio_Garcia_et_al.html>. Fecha de acceso: 12 abr. 2016.

KASPERSKY LAB. *¿Qué es un exploit de día cero?* [S.l., 20--?]. Disponible en: <http://www.kaspersky.es/internet-security-center/definitions/zero-day-exploit>. Fecha de acceso: 08 abr. 2016.

LYNN III, William J. *A conversation on cybersecurity.* Brussels: Security & Defence Agenda, 2010. (SDA Report).

MERRIAM-WEBSTER. *Merriam-Webster's collegiate dictionary.* 11. ed. Springfield, MA: Merriam-Webster, 2004.

MOHAMED Bouazizi. *Wikipedia*, [S.l.], 29 marzo 2016. Disponible en: <https://es.wikipedia.org/wiki/Mohamed_Bouazizi>. Fecha de acceso: 11 abr. 2016.

MORÁN, Otto. Preparan ley para castigar ciberdelitos. *La Prensa Gráfica,* [S.l.], 21 jul. 2013. Disponible en: <http://www.laprensagrafica.com/preparan-ley-para-castigar-ciberdelitos>. Fecha de acceso: 09 abr. 2016.

NACIONES UNIDAS. *Estados Miembros de las Naciones Unidas.* [S.l., 20--?]. Disponible en: <http://www.un.org/es/member-states/index.html>. Fecha de acceso: 12 abr. 2016.

NATO. Cooporative Cyber Defence Centre of Excellence. *Cyber Security Strategy Documents.* Tallinn, EE, 2015. Disponible en: <https://ccdcoe.org/strategies-policies.html>. Fecha de acceso: 11 abr. 2016.

NAVARRO, José María Blanco. Primavera Árabe, protestas y revueltas, análisis de factores. *Documento Opinión IEEE.ES,* [S.l.], n. 52/2011, jul. 2011.

NEBRERA, Alexander Kutt. La importancia de dominar los Global Commons en el Siglo XXI. *Documento Marco IEEE.ES,* [Madrid], n. 29/2012, nov. 2015.

NIETO, Nerea. ¿Cómo funciona PayPal? tutorial para principiantes. *Computer Hoy,* [S.l.], 13 feb. 2014. Disponible en: <http://computerhoy.com/paso-a-paso/internet/como-funciona-paypal-tutorial-principiantes-8733>. Fecha de acceso: 02 abr. 2016.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS; BANCO INTERAMERICANO DE DESARROLLO. *Observatorio de Ciberseguridad de América Latina y el Caribe.* [S.l., 2016?]. Disponible en: <http://observatoriociberseguridad.com/graph/countries/sv/selected/sv/0/dimensions/1-2-3-4-5>. Fecha de acceso: 14 abr. 2016.

PAYPAL. *Condiciones de uso del servicio de PayPal.* [S.l.], 2016. Disponible en: <https://www.paypal.com/es/webapps/mpp/ua/useragreement-full>. Fecha de acceso: 26 feb. 2016.

ROMERO, María Montserrat Vaqueiro. Ciberlenguaje juvenil en las redes sociales. In: CONGRESO IBEROAMERICANO DE LAS LENGUAS EN LA EDUCACIÓN Y EN LA CULTURA, 4., 2012, Salamanca. *Anais…* Salamanca: Leer.es, 2012. Disponible en: <http://www.oei.es/congresolenguas/comunicacionesPDF/Vaqueiro_Montserrat.pdf>. Fecha de acceso: 25 feb. 2016.

SÁNCHEZ, Javier López de Turiso y. La evolución del conflicto hacia un nuevo escenario bélico. In: CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL (El Salvador). *El Ciberespacio:* nuevo escenario de confrontación. Madrid, 2012. cap. 3. p. 117-166. (Monografás del CESEDEN, 126).

SANZ ALSEDO, Gonzalo. Intereses que afectan la soberanía nacional. In: MUNTALÂ, Jordi Marsal (Ed.). *Evolución del concepto de interés nacional.* Madrid: CESEDEN, 2010. (Monografías del CESEDEN, 115).

SANZ VILLALBA, Ángel Francisco; CHAMORRO, Enrique Fojón. Ciberespacio: la nueva dimensión del entorno operativo. In: *Documentos de Seguridad y Defensa*, 1 (44), 2011.

SARAVIA, Diego. Gobiernos e Internet. *Documentos de la UNAs,* [S.l.], 2007. Disponible en: <http://bo.unsa.edu.ar/docacad/softwarelibre/articulos/internetg/>. Fecha de acceso: 20 nov. 2015.

SUPERINTENDENCIA GENERAL DE ELECTRICIDAD Y TELECOMUNICACIONES (El Salvador). *Misión y Visión.* San Salvador, 2015. Disponible en: <http://www.siget.gob.sv/index.php/institucion/marco-institucional/historia>. Fecha de acceso: 11 abr. 2016.

_____. *Las telecomunicaciones en El Salvador.* San Salvador, 2013. Disponible en: <http://www.siget.gob.sv/index.php/component/content/article/115-telecomunicaciones/1955-las-telecomunicaciones-en-el-salvador>. Fecha de acceso: 03 abr. 2016.

TRUJILLO, Clorinda. Los límites de la disuasión en el ciberespacio. *Joint Force Quarterly,* Washington, DC, v. 75, 4. trim., sept. 2014.

UNITED STATES OF AMERICA. Department of the Army; Department of the Navy. *Department of Defense Dictionary of Military and Associated Terms.* Washington, DC: The Joint Staff, 2001. (Joint Publication 1-02). Disponible en: <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf> Fecha de acceso: 02 abr. 2016.

USUARIOS de internet por cada 100 habitantes. *Knoema*, [S. l.], 2015. Disponible en: <http://knoema.es/atlas/El-Salvador/Usuarios-de-internet-por-cada-100-habitantes>. Fecha de acceso: 15 dic. 2015.

CIBERDELINCUENCIA: DESAFÍOS PARA LA DEFENSA Y LA SEGURIDAD EN REPÚBLICA DOMINICANA

Francisco A. Ovalle Pichardo*

1 Introducción

No existen dudas sobre los grandes beneficios que el uso de las Tecnologías de las Informaciones y las Comunicaciones (TIC´s) han aportado a la sociedad, no obstante es justo reconocer, que las mismas han abierto las puertas a manifestaciones delictivas impensables. El aumento progresivo del ciberdelito en la República Dominicana durante los últimos años, el uso mutante de medios y métodos tecnológicos para su comedimiento, no es más que el reflejo del uso negativo que unos pocos dan a esta importante herramienta de desarrollo y que obliga a los Estados a ser cada vez más efectivos en la prevención, preparación y respuesta a esta nueva forma del delito.

Hay que destacar que las amenazas a la seguridad en los entornos virtuales son complejas, lo cual supone para los ciudadanos comunes y hasta para las mismas autoridades, nuevos retos que enfrentar para de esta forma garantizar la integridad individual y de las sociedades en un mundo que está cada vez más hiperconectado. En este sentido, el Estado Dominicano implementa y desarrolla importantes políticas y estrategias orientadas a mejorar la seguridad cibernética las cuales involucran a múltiples agencias que trabajan de forma coordinada a través de la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología (CICDAT), la cual tiene cinco funciones centrales. A saber:

- ✓ Asegurar la coordinación y cooperación entre las principales agencias nacionales de las Fuerzas Armadas, Policía Nacional, Ministerio Público y el poder judicial, comprometidas en prevenir, investigar y sancionar los actos de ciberdelincuencia;
- ✓ Coordinar y cooperar con las demás instituciones del gobierno nacional e instituciones internacionales para prevenir, reducir y sancionar las actividades cibercriminales en nuestro país y en el ámbito global;
- ✓ Definir políticas, establecer directivas y desarrollar estrategias y planes de seguridad cibernética para ser presentados a las autoridades nacionales;

* General de Brigada ERD, Francisco A. Ovalle Pichardo, MCS. Director de la Escuela de Graduados de Altos Estudios Estratégicos (EGAEE), Ministerio de Defensa de la República Dominicana (MIDE). Contacto: <faop24@gmail.com>

✓ Promover la adopción e implementación de los tratados, convenciones y acuerdos internacionales relacionados con el tema, de los cuales el Estado Dominicano es signatario;

✓ Asesorar al Estado Dominicano en cuanto a su representación y presentar ante las organizaciones internacionales involucradas en la lucha contra la cibercriminalidad y en la promoción de la seguridad cibernética de las cuales la República Dominicana es parte.

Ahora bien, en términos de investigaciones de actos de ciberdelincuencia, han sido creadas dos entidades específicas: la División de Investigación de Delitos Cibernéticos (DIDI) del Departamento Nacional de Investigaciones (DNI) y el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) en la Policía Nacional.

En tanto, la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología, tipifica las infracciones y sanciones a quienes las cometen utilizando recursos informáticos. Específicamente, hay penas contra quienes incurren en: atentado contra la vida de la persona, robos con uso de alta tecnología, obtención ilícita y transferencia electrónica de fondos (REPÚBLICA DOMINICANA, 2007; UN NUEVO…, 2015).

También figuran en esta Ley la estafa, chantaje, robo de identidad, falsedad de documentos y firmas, uso de equipos para invasión de privacidad, comercio ilícito de bienes y servicios, difamación e injuria, atentado sexual y pornografía infantil entre otros; destacándose estas últimas pues constituyen un cáncer que corroe la columna vertebral de la sociedad, como lo es la familia. En tal sentido, este importante documento se circunscribe en el respaldo legal que otorga el Estado Dominicano para prevenir y dar respuesta a la Ciberdelincuencia acorde a una política criminal holística y moderna.

Es precisamente que al hablar de estrategias, las medidas preventivas contra este preocupante delito se visualizan como la principal arma a tomar. Dentro de estas se destacan las Campañas de educativas frente a los riesgos cibernéticos, a través de instituciones educativas así como entidades privadas y públicas, que incluyen iniciativas de concientización en las redes sociales con el objetivo de identificar oportunamente y prevenir la ciberdelincuencia.

Existen también otras instituciones estatales que trabajan para informar a la población acerca de los riesgos cibernéticos y brindar asesoría y consejos sobre buenas prácticas, entre ellas se encuentra el Instituto Dominicano de las Telecomunicaciones (INDOTEL) el cual para esos fines, cuenta con un programa denominado “Internet Sano”[1]

1 Disponible en: <http://www.internetsano.do/>.

En líneas generales, se han establecido y optimizados en la práctica, los mecanismos judiciales para solicitar y compartir de manera oficial, todo tipo de información que ayude a detectar y combatir irregularidades asociadas a estos delitos incluso a través del desarrollo de sociedades colaborativas entre el Gobierno y el sector privado, producto de los importantes esfuerzos previos realizados para generar conciencia también a este nivel.

Como parte de las estrategias de capacitación continuada del recurso humano, los investigadores y técnicos responsables del análisis forense digital dentro de los organismos policiales y judiciales, reciben formación perenne para mantener y mejorar sus habilidades, dado que el entrenamiento y el desarrollo de las capacidades del personal, es una prioridad clave para enfrentar al ciberdelito que por su propia naturaleza, es complejo y muta constantemente.

En materia de cooperación internacional, existen investigaciones conjuntas con autoridades de gobiernos aliados, destacándose de manera reciente el éxito alcanzado en las recientes operaciones desarrolladas con España, Colombia y los Estados Unidos. Igualmente República Dominicana, como miembro del Convenio de Budapest y de varias de las redes 24-7 del G8, Interpol y la Organización de Estados Americanos, ha facilitado el intercambio de información constante y el acercamiento en términos de seguridad cibernética, con otros países también afectados por estos delitos.

No obstante, sigue siendo el mayor obstáculo a nivel de investigación e inteligencia, el acceso a información pertinente y oportuna especialmente de los proveedores de servicios de internet y de operadores de redes sociales.

Se recuerda que el Convenio Budapest fue el primer tratado internacional sobre delitos cometidos a través de la red de internet y otras redes informáticas, que trata en particular de las infracciones de derechos de autor, fraude informático, pornografía infantil y delitos de violaciones de seguridad de red. Contiene una serie de competencias y procedimientos, como la búsqueda de redes informáticas e interceptación legal y su principal objetivo 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 (COUNCIL OF EUROPE, 2001; Un NUEVO…, 2015).

Fue elaborado y aprobado junto a su Informe Explicativo, por el Consejo de Europa en Estrasburgo, por el Comité de Ministros del Consejo de Europa en su 109ª reunión, el 8 de noviembre de 2001 y con la participación activa de los Estados observadores de Canadá, Japón y China. Siendo el 23 de noviembre de

2001 cuando se abrió a la firma en Budapest y entró en vigor el 1 de julio de 2004; pero es solo a partir del 28 de octubre del año 2010 cuando 30 estados firmaron, ratificaron y se adhirieron, que la Convención pasó a ser conocida en el mundo.

El Convenio de Budapest (COUNCIL OF EUROPE, 2001) clasifica los delitos cibernéticos en cinco tipos penales de la siguiente manera:

- ✓ Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos;
- ✓ Infracciones informáticas;
- ✓ Infracciones relativas al contenido;
- ✓ Infracciones vinculadas a la propiedad intelectual y los derechos afines y;
- ✓ Otras formas de responsabilidad y sanción.
- ✓ Ahora bien, partiendo de la importancia de analizar la norma a la luz del bien jurídico tutelado por el derecho penal, es preciso clasificar los delitos de acuerdo con la afectación del bien jurídico protegido. En este sentido, el autor Roxin (1997) se refiere a la siguiente clasificación, siendo estos:

- Delitos de Internet que afectan la intimidad:
  - ✓ Delitos cibernéticos que afectan la privacidad;
  - ✓ Delitos cometidos por Internet y su afectación al honor y la dignidad humana;
  - ✓ Internet como instrumento de difamación e injuria.

- Delitos contra la libertad e indemnidad sexual:
  - ✓ La pornografía infantil y el interés superior del niño.
- La afectación del patrimonio por la comisión de delitos cibernéticos:
  - ✓ Daños a la "cosa objeto del patrimonio";
  - ✓ Delitos contra la propiedad intelectual y derechos afines.
- Delitos que atentan contra la seguridad nacional:
  - ✓ Sabotaje contra la seguridad nacional;
  - ✓ Ciberterrorismo;
  - ✓ Ciberespionaje;
  - ✓ Blanqueo de capitales.

De acuerdo al autor, todas estas categorías de delitos afectan directamente derechos que están protegidos constitucionalmente, lo que trae consigo mayores implicaciones tomando en consideración el deber estatal de garantizar la protección de los mismos a sus ciudadanos y la seguridad de la nación.

2 Ciberdelitos más Comunes en la República Dominicana

En parcial coincidencia con la clasificación planteada por Roxin (1997), en la República Dominicana los delitos que motivan todo tipo de esfuerzo por parte del Estado para combatirlos, son aquellos que atentan contra la *seguridad nacional*.

La Ley 53-07 no solamente se ha encargado de tutelar los delitos informáticos que pueden ser cometidos contra determinadas personas físicas o morales, sino que ha ampliado su campo de acción hacia aquellas infracciones que afectan la seguridad nacional (REPÚBLICA DOMINICANA, 2007).

La cobertura normativa ha sido tan amplia que los supuestos establecidos en el artículo 27, relativos a los crímenes y delitos contra la seguridad del Estado, poseen un carácter enunciativo y no taxativo. Esta conclusión se extrae de la expresión *"…tales como…"* contenida en este artículo, el cual se limita a señalar los delitos de espionaje, sabotaje y suministro de informaciones (REPÚBLICA DOMINICANA, 2007).

De igual modo, la precitada ley sanciona el terrorismo realizado a través de medios electrónicos con penas que van desde 20 a 30 años de reclusión y multa de trescientos a mil salarios mínimos, así como la destrucción y confiscación de los sistemas de información utilizados para la comisión de estos crímenes.

En el país, los ciberdelitos no discriminan a nadie: pueden victimar por igual a individuos comunes y corrientes, empresas y hasta al propio Estado dominicano. Entre los incidentes más comunes denunciados se encuentran: clonación de tarjetas de crédito, difamación mediante correos electrónicos y redes sociales, *phishing* (suplantación de identidad) y estafas telefónicas. También se han detectado numerosos ataques y actos de vandalismos de sitios gubernamentales llevados a cabo por grupos de *hacktivistas.*

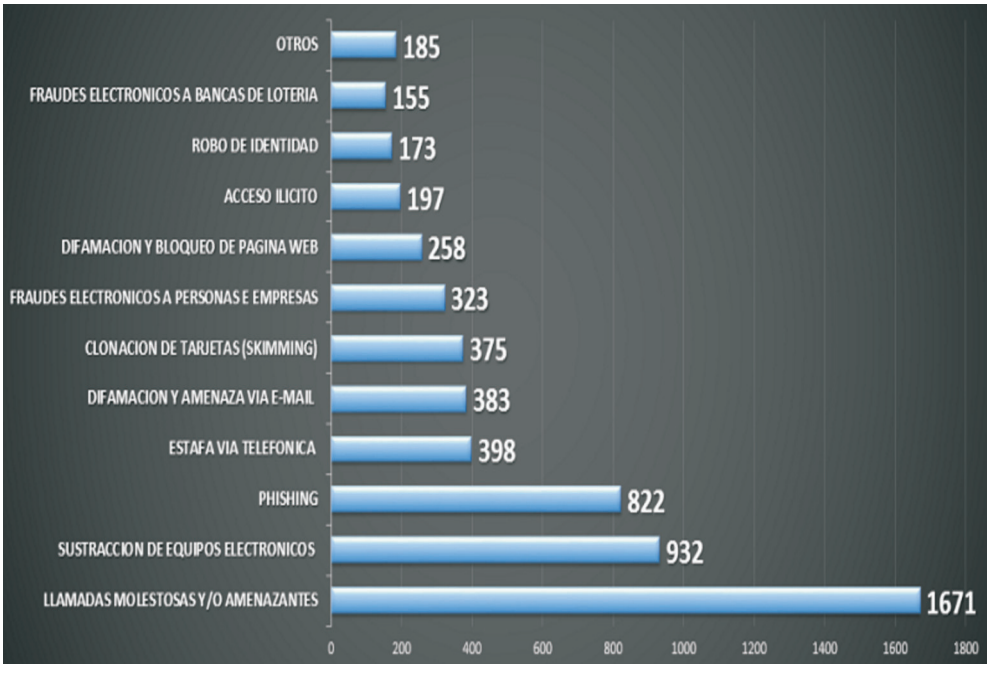
Durante los años 2014-2015, se abrieron 791 casos relacionadas con ciberdelincuencia, lo cual ha dado como resultado la apertura de más de 300 procesos judiciales. También se han desmantelado con éxito grupos de *hacktivistas* que operaban en el país, luego de una investigación conjunta de seis meses de duración realizada entre la Policía Nacional, el Ministerio Público, la Organización Internacional de Policía Criminal (Interpol) y las autoridades de otros cuatro países, que dio como resultado la detención de seis personas afiliadas a Anonymous Dominicana y a un anexo de Anonymous con asiento en la República Dominicana.

Es así como y de manera reciente, el Ministerio Público de la República Dominicana presentó ante los estamentos judiciales, a dos personas que intentaron "hackear" la página electrónica de la Junta Central Electoral (JCE) a dos días de la celebración de las elecciones generales del 2016; las investigaciones las emprendió el Departamento de Delito Electrónico de la Procuraduría General de la República, y evidencia el trabajo oportuno que vienen realizando las autoridades en este sentido (TRATARON…, 2016).

De acuerdo al Coronel de la Policía Nacional Licurgo Yunes, Director del Departamento de Investigaciones de Crímenes de Alta Tecnología (DICAT), desde la promulgación de la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología en el año 2007 a la fecha, han sido interpuestas más de 5 mil medidas de coerción contra personas involucradas en este delito o en operaciones de mafias electrónicas transnacionales (UN NUEVO…, 2015).

Cabe destacar que junto a la necesaria educación de los usuarios con relación a los riesgos de estos delitos, es igualmente importante la denuncia de estos hechos ante las autoridades correspondientes.

Gráfico 1 - Principales ciberdelitos en la República Dominicana



Fuente: DICAT, 2016.

Cuadro 1 - Estadística de montos recuperados producto de phishing en RD (2007-2015)

ENTIDADES BANCARIAS	MONTOS EN PESOS	MONTOS EN DOLARES	MONTOS EN EUROS
ENTIDAD BANCARIA A	24,894,066.84	/	/
ENTIDAD BANCARIA B	38,170,662.73	12,329,901.34	/
ENTIDAD BANCARIA C	24,610,851,99	2,329,901.34	1,000.00
ENTIDAD BANCARIA D	7,900,689.18	/	/
ENTIDAD BANCARIA E	1,975,972.54	24,784.19	/
ENTIDAD BANCARIA F	3,267,333.43	/	/
ENTIDAD BANCARIA G	/	/	2,036.67
ENTIDAD BANCARIA H	525,282.37	/	/
ENTIDAD BANCARIA I	/	/	5,777.00
ENTIDAD BANCARIA J	2,645,505.00	1,654,185.00	/
ENTIDAD BANCARIA K	/	/	35,952.00
ENTIDAD BANCARIA L	326,974	/	/
ENTIDAD BANCARIA M	170,957	/	/
ENTIDAD BANCARIA N	8,890	/	/
ENTIDAD BANCARIA O	916,382	/	/
TOTAL MONTOS	**105,413,567.41**	**4,020,870.53**	**44,765.67**

Fuente: DICAT, 2016.

En otro orden, el tema de blanqueo de capitales como delito nacional y transnacional es uno de los ilícitos penales que más estragos han causado en los países más vulnerables, por la flexibilidad en su legislación y mecanismos de control, los que se han convertido en foco para la comisión de esta infracción.

De acuerdo con la teoría jurídica que configura esta infracción, se trata de un fenómeno delictivo complejo, así la República Dominicana tipificó el lavado de activo en el año 2012 mediante la ley sobre Lavado de Activos Provenientes del Tráfico Ilícito de Drogas y Sustancias Controladas. Su artículo 3 la tipifica de la siguiente manera:

> Art. 3.- A los fines de la presente ley, incurre en lavado de activos la persona que, a sabiendas de que los bienes, fondos e instrumentos son el producto de una infracción grave.
> a) Convierta, transfiera, transporte, adquiera, posea, tenga, utilice o administre dichos bienes;
> b) Oculte, encubra o impida la determinación real, la naturaleza, el origen, la ubicación, el destino, el movimiento o la propiedad de dichos bienes o de derechos relativos a tales bienes;
> c) Se asocie, otorgue asistencia, incite, facilite, asesore en la comisión de algunas de las infracciones tipificadas en este artículo, así como a eludir las consecuencias jurídicas de sus acciones. (REPUBLICA DOMICANA, 2002).

Para comprender la complejidad aludida a blanqueo de capitales, es preciso presentarlo desde su plano conceptual.

De acuerdo con la Convención de las Naciones Unidas contra la Corrupción, surgida mediante Resolución 58-4 de la Asamblea General del 31 de octubre de 2003[2] se establece como responsabilidad de los Estados partes de este convenio, tomar las iniciativas legislativas o de cualquier otra índole, que sean necesarias para tipificar como delito, las siguientes conductas que configuran el blanqueo del producto del delito, tal como lo establece este instrumento internacional (NACIONES UNIDAS, 2004).

A saber:

> a) La conversión o la transferencia de bienes, a sabiendas de que estos bienes son producto del delito, con el propósito de ocultar o disimular el origen ilícito de los bienes o ayudar a cualquier persona involucrada en la comisión del delito determinante a eludir las consecuencias jurídicas de sus actos:
> b) La ocultación o disimulación de la verdadera naturaleza, el origen, a ubicación, la disposición, el movimiento o la propiedad de bienes o del legítimo derecho a estos, a sabiendas de que dichos bienes son producto del delito. (NACIONES UNIDAS, 2004).

Es así como la situación se complica más aún cuando el medio utilizado para el blanqueo son los avances tecnológicos, tal como la Internet. La doctrina[3] ha alertado acerca de esta situación al indicar que:

2 Ratificada por República Dominicana mediante resolución 33.06, aprobada por el poder legislativo el 18 de julio del 2006 y promulgada el 6 de agosto del mismo año.

3 Citado por Orts Berenguer, obra citada, página 160. Figura alojada en los artículos 298 a 304 del Código penal de España.

> […] Son imaginables las maquinaciones encuadrables en la receptación y otras conductas afines, realizadas aprovechando las ventajas que brinda la Internet, para traficar con los efectos provenientes de delitos contra el patrimonio o el orden socioeconómico…particularmente, para el blanqueo de dinero […]. (BERENGUER; TORRES, 2001, p. 160)

Ahora bien, en medio de esta análisis de los ciberdelitos que afectan al país, existen planteamientos importantes, como los expresados por la Jueza de la Suprema Corte de Justicia de la República Dominicana Esther Agelán Casasnovas (2011), quien afirma el gran reto para la efectiva protección de los derechos de las personas, en especial de niñas y adolescentes, es enfrentar nuevos tipos delictivos caracterizados por la inexistencia de límites temporales y espaciales para su materialización, y realizados con sofisticados medios tecnológicos como los cometidos por Internet.

Estas ideas contenidas en la Constitución, suponen por parte del Estado Dominicano, a través de sus principales instituciones, la creación de una política criminal encaminada al combate efectivo de la delincuencia en sus distintas formas. Generándose entonces la necesidad de que el aparato persecutorio también se tecnifique y modernice a fin de ampliar su campo de acción para la tutela de los bienes jurídicos constitucionalmente resguardados.

Tal y como ella lo señala, en el preámbulo de la actual Carta Magna, los legisladores en su calidad de representantes del pueblo dominicano por el hecho de haber sido elegidos por el mismo, señalan que:

> […] regidos por los valores supremos y los principios fundamentales de la dignidad humana, la libertad, la igualdad, el imperio de la ley, la justicia, la solidaridad, la convivencia fraterna…el progreso y la paz…" estos entendidos como factores esenciales para la cohesión social"… adoptamos y proclamamos la siguiente Constitución […] (REPÚBLICA DOMINICANA, 2010).

Este preámbulo del Pacto Político dominicano, proclamado el 26 de enero del año 2010, sirve de parámetro para evaluar que la intención legislativa –Congreso Nacional- se concretiza al convertir ese documento guía supremo, en el principal instrumento de tutela de los bienes jurídicos entendidos como fundamentales, y categorizados de forma organizada en el cuerpo de ese texto. Así, la dignidad del ciudadano, su intimidad y derecho de propiedad, son bienes especialmente

regulados y protegidos por la constitución, y que dentro del fenómeno delictivo denominado "delito informático o cibernético" constituyen los principales supuestos vulnerados por los infractores o sujetos activos en las distintas maneras en que este fenómeno se manifiesta.

Es por esto que para la Jueza Casasnovas (2011), al momento de la interpretación de la norma penal y procesal es imprescindible tomar en cuenta el rango supra normativo de los derechos vulnerados. El aparato estatal garantiza la salvaguarda de los derechos ciudadanos antes indicados, a través del efectivo combate de la "ciberdelincuencia", logrando así la legitimización como Estado democrático. Esta afirmación es corroborada por la doctrina científica constitucional al indicar que: "[…] el problema pasa a ser de la legitimización democrática del poder del Estado, es decir, el de la reconducción de la voluntad del Estado única y exclusivamente a la voluntad de la sociedad." (RAYO, 2014, p. 12)[4].

Es así como asevera que el sistema de protección de los derechos ciudadanos sujetos a normatividad o "bienes jurídicos protegidos", por parte del ordenamiento jurídico de un determinado país, ha sido entendido como una de las características principales de las denominadas "sociedades de derechos". Así lo confirma la doctrina:

> Las sociedad occidentales actuales pueden ser caracterizadas como sociedades de derechos, (énfasis original) lo que quiere decir –entre otras cosas- que están sustentadas por un duro y generalizado esqueleto de leyes, especialmente de leyes destinadas a garantizar, definir y proteger una red de derechos individuales. (BERENGUER; TORRES, 2001, p. 4).

De modo pues, que entre los bienes jurídicos constitucionalmente protegidos que pueden verse afectados por la comisión de cualquier delito, incluyendo los de Internet, están los delitos contra el honor, tal como la difamación e injuria, igualmente consagrados en el artículo 44 de la Constitución dominicana. En el caso de ciberdelitos como la publicación o tenencia de fotografías no consentidas; vale la pena destacar que no existen límites temporales o espaciales para su materialización y se trata de hechos que no siempre son denunciados por sus propias víctimas.

4 Constitución y Justicia Constitucional, jornadas de derecho Constitucional en Centroamérica.

A juicio de la magistrada, es preocupante el auge creciente de la Ciberdelincuencia o delitos electrónicos como el robo de identidad, plagios de cuentas bancarias, la difamación e injuria, el blanqueo de capitales y la pornografía infantil, porque a través de ellos se violenta la intimidad de las personas y se trastorna la paz de las sociedades. Casasnovas (2011) detalla que cuando se hace alusión a la afectación de la intimidad, ha de entenderse aquellos delitos que de alguna manera afectan la vida privada de la persona.

Desde el punto de vista de Constitución dominicana, el artículo 44 establece lo siguiente: "Toda persona tiene derecho a la intimidad. Se garantiza el respeto y la no injerencia en la vida privada familiar, el domicilio y la correspondencia del individuo.". En lo relativo al derecho a la intimidad y consecuentemente, de la privacidad, existe una prohibición expresa de violentar "la correspondencia y documentos privados", salvo la obediencia al debido proceso en casos de investigación, esto sometido a control judicial.

De igual manera el numeral 3 del artículo 44 de la Constitución establece que:

> Se reconoce la inviolabilidad de la correspondencia, documentos o mensajes privados en formatos físico, digital, electrónico o de cualquier otro tipo. Sólo podrán ser ocupados, interceptados o registrados, por orden de una autoridad judicial competente, mediante procedimientos legales en la substanciación d asuntos que se ventilen en la justicia y preservando el secreto de lo privado, que no guarde relación con el correspondiente proceso. Es inviolable el secreto de la comunicación telegráfica, cablegráfica, electrónica, telemática o la establecida en otro medio, salvo las autorizaciones otorgadas por juez o autoridad competente de conformidad con la ley. (REPÚBLICA DOMINICANA, 2010, p. 14).

De modo pues que resulta preocupante, la facilidad con la que a través de la Internet pueden obtenerse datos personales de ciudadanos, muchos de ellos comprometedores, que pueden dar lugar a chantajes o extorsiones con la utilización de esas informaciones. Para autores como Orts Berenguer y Roig Torres, el derecho a la intimidad deriva de la dignidad. Estos autores colocan el bien jurídico dignidad como una subcategoría de la intimidad. Pero podría colocarse la dignidad como un bien jurídico particular, por el grado de afectación que esta implica.

En este sentido, resulta interesante la distinción realizada por la jurisprudencia entre el derecho "al control" de los datos personales y el derecho a la intimidad. Entendiéndose estos como dos derechos fundamentales diferentes, tomando en cuenta su función, objeto y contenido (BERENGUER; TORES, 2001)[5].

De acuerdo con esa distinción, el derecho a la intimidad protege "cualquier invasión al ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno. Un punto central para el tipo de delito que afecta el derecho a la intimidad, es la forma como se proyecta, que según diversos autores, los delitos que afectan la intimidad pueden proyectarse desde dos vertientes: desde el exterior o desde el interior. Desde el exterior, hace referencia a la protección de bienes como lo es la inviolabilidad del hogar la correspondencia u otro tipo de documentación personal; y, desde el interior, abarca la protección de "los bienes propiamente inmateriales" como por ejemplo: el derecho al honor, a al honra y la propia imagen (BERENGUER; TORES, 2001).

En este sentido, la Jueza Casasnovas (2015, información verbal) propone el reforzamiento de las políticas criminales locales para que el trabajo de prevención sea más efectivo y no se centre solo en la persecución del delito como lo establece la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología y su Reglamento de aplicación. Según ella, la violación de la intimidad a través de la exposición de imágenes o un video en los medios electrónicos, es un delito poco perseguido.

El perfil y los patrones de conducta del victimario, es muy particular. En muchos de los casos, son jóvenes con acceso a educación, a una formación académica incluso universitaria y con destrezas informáticas. Es por esto que Casasnovas (2015, información verbal) plantea como prioridad la educación de la ciudadanía "Porque mientras más personas tienen acceso a la internet más peligro viene en consecuencia y si no tienen el conocimiento de cómo usar ese instrumento y protegerse de sus peligros o amenazas, el fenómeno sigue devorando su seguridad personal, familiar y hasta económica", subraya.

Tomando en cuenta factores como la desigualdad social, que limita el acceso al Internet de una gran parte de la población dominicana y la poca comprensión que se tiene sobre los ciberdelitos, la Jueza recomienda la inclusión en los pensum universitarios de materias electivas concernientes a los delitos de alta tecnología y la creación de planes o campañas educativos para adultos, también en las Universidades.

5 STC. 111/1998, de 13 de enero.

Foto 1 – Montaje. Entrevista a la Dra. Agelán Casasnovas, Jueza de la Suprema Corte de Justicia República Dominicana, durante el programa radial de la EGAEE "Hacia una Cultura de Defensa"

Fuente: RELACIONES PÚBLICAS EGAEE, 2015.

3 ¿Es considerado en República Dominicana, el Envío de Correos Electrónicos Masivos un Ciberdelito?

La Ley Nº. 310-14 que regula el envío de correos electrónicos comerciales no solicitados (SPAM) o Ley "Antispam" tiene contemplado un protocolo a través del cual puede notificarse primero de la acción invasiva de terceros a las cuentas personales, por ante el Instituto Nacional de Protección de los Derechos del Consumidor (PRO CONSUMIDOR), organismo estatal creado mediante la Ley General de Protección de los Derechos del Consumidor o Usuario (358-05), que tiene por objetivo de establecer y reglamentar las políticas, normas y procedimientos necesarios para la protección efectiva de los derechos de los consumidores en la República Dominicana.

Luego de este paso, el usuario querellante solicita a quien le envía los "correos molestosos" lo saque de sus listas de destinatarios y si la acción continúa, puede abrirse en su contra, un proceso legal que al igual se está aplicando en otros países como Estados Unidos y España, donde se han obtenido muy buenos resultados. Es una realidad, que una gran parte de los usuarios de móviles en la República Dominicana, han sido víctimas de estos envíos masivos de SMS o mensajes de texto sin consentimiento. Esto pasa por la venta de la base de datos

de los clientes que hacen las diferentes telefónicas para las empresas, marcas y profesionales, a personas o empresas que desean llegar a un número importante de usuarios de una manera más rápida.

Sin embargo, ahora con la promulgación de la Ley AntiSpam en la República Dominicana, ya las empresas telefónicas que vendan la base de datos para el envío masivo de SMS, tendrán que obligar a estas a que coloquen un nombre o número al cual los usuarios afectados puedan llamar, esto para que nunca más le vuelvan a llegar estos mensajes de textos que tan molestos resultan (UN NUEVO...., 2015).

4 ¿Cómo prevenir los Ciberdelitos y no Claudicar en el Intento?

El ingeniero Jimmy Rosario, director de informatización de la Universidad Autónoma de Santo Domingo (UASD) la casa de altos estudios más importante de la República Dominicana, considera que solo en la prevención reposa la clave de cualquier acción que intente ser efectiva en materia de seguridad. Recuerda que líderes mundiales han reconocido que los ciberdelitos con el tiempo, se han constituido en uno de los mayores desafíos que ha llevado a los gobierno del mundo, a redoblar los esfuerzos para garantizar la seguridad, producto de los constantes ataques a sus bases de datos y las intromisiones de desaprensivos en la vida pública individual y nacional (LICURGO; ROSARIO, 2015, información verbal).

El hecho de que terceras personas invadan la privacidad de una persona o del mismo Estado a través de sus instituciones, puntualizó Rosario, puede afectar su seguridad económica, la salud mental de las familias, y el bienestar en general de la población. Son comunes los robo de información sobre todo en las redes sociales; la sustracción de las contraseñas de las tarjeta de crédito o débito y las estafas cuando se compra a través del internet si no se toman las medidas de lugar. Unos de los delitos más comunes es el *Pishing* que ocurre cuando el usuario hace *click* en ventanas falsas en las cuales se le pide coloque sus datos personales, bajo la promesa de que podrá obtener un producto con precios muy por debajo de los existentes en el mercado.

De allí la importancia de verificar la autenticidad de la procedencia de los correos electrónicos, enlaces que redireccionan a otras webs, archivos descargados; hay que procurar tener softwares licenciados en los equipos y vigilar el acceso que tienen los niños a ciertos portales, hablar con ellos, advertirlos y hasta hacerse amigo de sus amigos.

Foto 2 – Montaje. Entrevista al Coronel Licurgo Yunes, Director del Departamento de Investigaciones de Crímenes de Alta Tecnología (DICAT) y al ingeniero Jimmy Rosario de la UASD, durante el programa radial de la EGAEE "Hacia una Cultura de Defensa"

Fuente: RELACIONES PÚBLICAS EGAEE, 2015.

5 Conclusiones

Al momento, no existe una estrategia o política nacional sobre seguridad cibernética a gran escala en la República Dominicana, ni se ha establecido un centro o CIRT (*Computer Incident Response Team*) que cuente con capacidades de respuesta ante incidentes similares. El Estado como parte de su estrategia de ciberseguridad necesita integrar medidas de protección en Internet en todos los niveles; ya que aunque inicialmente esto podría elevar los costos de los servicios ofertados, los beneficios a largo plazo para evitar los costos y los daños causados por delitos informáticos, son mayores y superan con creces los gastos iniciales de medidas técnicas y de protección y de salvaguardas de la red.

Es preciso resaltar que una estrategia nacional de la ciberseguridad requiere una amplia concertación entre todos los actores de la sociedad. Por citar un ejemplo, una estrategia de ciberseguridad debe prever desde el desarrollo de sistemas técnicos de protección de las infraestructuras críticas del Estado y del sector privado, hasta la educación de los usuarios para evitar que se conviertan en víctimas de la ciberdelincuencia.

Como recomendaciones para el desarrollo de un plan educativo efectivo se consideran viables:

- ✓ La inclusión en los pensum de universitarios de materias electivas concernientes a los delitos de alta tecnología, especialmente la Internet.
- ✓ La creación de un plan educativo dirigido también a adultos, donde estos tengan la oportunidad de alfabetizarse en un doble sentido, la alfabetización básica y la digital.

- ✓ La realización de campañas preventivas desde las universidades, pues aunque no se cuenten con datos estadísticos específicos, un alto porcentaje de ciberdelincuentes son estudiantes universitarios o profesionales, lo que contribuye a sensibilizar acerca de los hechos que constituyen delitos y sobre la gravedad de las sanciones que conlleva la comisión de los mismos. La factibilidad de esta campaña radica en que se trata de grupos que se encuentran focalizados en universidades y a nivel de bachilleratos.

Referencias

BERENGUER, Enrique Orts; TORRES, Margarita Roig. Delitos informáticos y delitos comunes cometidos a través de la informática. Valencia: Tirant lo Blanch, 2001.

CASASNOVAS, Esther E. Agelán. *Ciberdelincuencia y política criminal*: Internet: nuevo reto jurídico penal. Santo Domingo: [s.n.], 2011.

_____. Entrevista sobre 'Ciberdelitos y seguridad en la República Dominicana: Programa Radial Hacia una Cultura de Defensa'. *EGAEE* [en línea], Santo Domingo, nov. 2015. Disponible en: <http://www.egae.mil.do/index.php?option=com_content&view=article&id=204:2015-11-24-20-30-13&catid=14:entrevistas&Itemid=43>. Fecha de acceso: 30 marzo 2016.

COUNCIL OF EUROPE. *Convenio de Budapest*. Budapest, 2001. Disponible en: <http://www.coe.int/pt/web/conventions/full-list/-/conventions/treaty/185>. Fecha de acceso: 15 marzo 2015.

LICURGO, Yunes; ROSARIO, Jimmy. Entrevista sobre 'Ciberdelitos y seguridad en la República Dominicana: Programa radial Hacia una cultura de Defensa'. *EGAEE* [en línea], Santo Domingo, junio 2015. Disponible en: <http://www.egae.mil.do/index.php?option=com_content&view=article&id=148:un-nuevo-desafio-para-la-seguridad-ciudadana-combatir-los-ciberdelitos&catid=13:noticias&Itemid=40>. Fecha de acceso: 30 marzo 2016.

NACIONES UNIDAS. Oficina contra la Droga y el Delito. *Convención de las Naciones Unidas contra la corrupción*. Nueva York, 2004.

RAYO, Javier Pérez. *Curso de Derecho Constitucional*. 14. ed. [S.l.]: Marcial Pons, 2014.

REPÚBLICA DOMINICANA. Constitución de la República Dominicana. *Gaceta Oficial*, Santo Domingo, nº 10561, 26 enero 2010.

_____. Ley nº 53, de abril de 2007. Crímenes y Delitos de Alta Tecnología. *Gaceta Oficial*, Santo Domingo, 23 abr. 2007.

_____. Ley 72, de jun. 2002. Contra el lavado de activos provenientes del tráfico ilícito de drogas y sustancias controladas y otras infracciones graves. [*Gaceta Oficial*], Santo Domingo, 02 jun. 2002.

ROXIN, Claus. *Derecho Penal*: parte general. Fundamentos: la estructura de la Teoría del Delito. 2. ed. Madrid: Thompson Civitas, 1997. Tomo 1. p. 62-63.
TRATARON de 'hackear' la página electrónica de la JCE. *El Caribe*, Santo Domingo, 13 mayo 2016. Disponible en: <http://www.elcaribe.com.do/2016/05/13/trataron-pagina-electronica-jce#sthash.EC9bgJzm.dpuf>. Fecha de acceso: 13 mayo 2016.

UN NUEVO desafío para la seguridad ciudadana: combatir los Ciberdelitos. *EGAEE*, Santo Domingo, 18 jun. 2015. Disponible en: <http://egae.mil.do/index.php?option=com_content&view=article&id=148:un-nuevo-desafio-para-la-seguridad-ciudadana-combatir-los-ciberdelitos&catid=14:entrevistas&Itemid=43>. Fecha de acceso: 20 enero 2016.

EL MODELO DE CIBERSEGURIDAD Y CIBERDEFENSA EN ESPAÑA

Ángel Gómez de Ágreda*

1 La Estrategia Nacional de Ciberseguridad

La Estrategia de Ciberseguridad Nacional de España (ESPAÑA, 2013a) se aprobó en la reunión del Consejo de Ministros del día 5 de diciembre de 2013 (PORTAL..., 2013) con la intención de "responde(r) a la creciente necesidad de preservar la seguridad del ciberespacio por su enorme repercusión en cuestiones que afectan a la seguridad nacional, así como a la competitividad de nuestra economía y, en general, al progreso y prosperidad de nuestra sociedad.".

La elaboración de la Estrategia se llevó a cabo bajo la coordinación del Departamento de Seguridad Nacional (DSN) del Gabinete del Presidente del Gobierno y contó con la participación de diversos ministerios y organismos públicos con responsabilidades en la definición de su alcance y en la futura implementación de las medidas recogidas en la misma.

2 Orígenes

La Estrategia Nacional de Ciberseguridad deriva de la 'Estrategia de Seguridad Nacional: un proyecto compartido' (ESPAÑA, 2013b), del 31 de mayo del mismo año. Este documento marco identifica en el tercer lugar de entre los riesgos y amenazas para la Seguridad Nacional, las ciberamenazas. La tercera línea de acción que propone es, en justa correspondencia, la de la ciberseguridad. A pesar de que se afirma que el orden en que son enunciadas no pretende primar unas sobre otras o privilegiar su acometimiento, este parece responder a criterios de gravedad potencial de cada una.

Además, la Estrategia de Seguridad Nacional refleja el carácter claramente trasversal del ámbito ciberespacial con respecto al resto de las amenazas que señala. El ciberespacio se describe como un ámbito con influencia en el resto de los entornos de actividad y con una creciente influencia en los riesgos y oportunidades que presentan estos.

Al mismo tiempo, la Estrategia aboga por la elaboración de "[…] una legislación armonizada en materia de ciberseguridad […]" – cuya inexistencia reconoce – para

* Ángel Gómez de Ágreda. Teniente Coronel del Ejército del Aire. Jefe de Cooperación del Mando Conjunto de Ciberdefensa. https://es.linkedin.com/in/angelgdeagreda

mitigar los ataques a nuestras infraestructuras y servicios y para evitar "la pérdida de confianza de los ciudadanos en unos sistemas que, en la actualidad, resultan críticos para el normal funcionamiento de la sociedad." (ESPAÑA, 2013b, p. 27).

La Estrategia reconoce de una forma inequívoca la existencia de un entorno virtual que resulta clave para el desarrollo económico de la sociedad, para su capacidad industrial y tecnológica, para la seguridad de sus ciudadanos y de la nación en su conjunto y, no menos importante, para permitir el impulso de un nuevo modelo de sociedad basado en las tecnologías de la información y las comunicaciones.

Así, cada una de las otras amenazas que identifica la Estrategia de Seguridad Nacional, desde la Defensa Nacional hasta la vulnerabilidad de las infraestructuras y servicios críticos, se encuentra íntimamente vinculada con la necesidad de establecer un ciberespacio seguro y, al mismo tiempo, ágil y transparente en el que se puedan llevar a cabo las actividades de los actores públicos y privados sacando el máximo partido posible a las oportunidades que ofrece y minimizando el impacto de las vulnerabilidades a las que está sometido.

Para conseguir la finalidad anterior, se establece como objetivo el "garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques." (ESPAÑA, 2013b, p. 42).

Este incremento de capacidades debe basarse en un "[…] marco jurídico operativo y eficaz." (ESPAÑA, 2013b, p. 42) y su desarrollo normativo, a través de la cooperación público-privada, la promoción de la formación y la I+D+i en España, la concienciación de ciudadanos, profesionales y empresas a través de una sólida cultura de ciberseguridad, y de la cooperación internacional.

Estas líneas de acción se verán recogidas y desarrolladas en la Estrategia de Ciberseguridad Nacional unos meses más tarde. Posteriormente, darán lugar a un Plan Nacional de Ciberseguridad (el 31 de octubre de 2014) [LÓPEZ, 2015) y a los distintos Planes Derivados que lo concretan.

La Estrategia de Ciberseguridad Nacional es, por lo tanto, la pieza central que pone en relación la visión del Gobierno de España con la Seguridad Nacional y los planes concretos para que los distintos organismos responsables de cada una de las áreas acometan la tarea de garantizar un ciberespacio libre y seguro para todos los españoles.

A pesar de su papel central, la Estrategia no es sino un acuerdo del Consejo de Ministros, es decir, la expresión de la voluntad de un Gobierno, y no forma parte de la legislación española como tal. Resulta especialmente importante tener en cuenta este extremo ya que la adopción de las medidas que propugna la estrategia requiere de una legislación que las cree y desarrolle.

3 Contenido de la Estrategia

Los cuatro primeros capítulos de la Estrategia de Ciberseguridad Nacional están dedicados a la descripción del entorno ciberespacial, y a definir los objetivos a alcanzar y las líneas de acción que habrán de seguirse para alcanzarlos.

En el quinto y último capítulo se describe la estructura y organización de la ciberseguridad en España sentando las bases para la creación de nuevos organismos y para las relaciones entre todos ellos. De esta estructura y su implementación se hablará en el siguiente capítulo de este trabajo.

La Estrategia define el ciberespacio como el "dominio global y dinámico compuesto por las infraestructuras de tecnología de la información –incluida Internet–, las redes y los sistemas de información y de telecomunicaciones." (ESPAÑA, 2013a, p. 9).

La utilización del término 'dominio', presente en otras estrategias nacionales en todo el mundo, se presta a distintas interpretaciones que pueden ir desde la mera definición de un ámbito de actuación hasta la de un espacio de soberanía restringido a la jurisdicción de una autoridad. El debate actual sobre la soberanía en el ciberespacio no está presente, sin embargo, en el espíritu de la Estrategia, que no adopta ninguna posición respecto de la soberanía concreta de continente ni contenido del ciberespacio.

El propósito explícito de la Estrategia es la fijación de directrices para la utilización segura del ciberespacio, sin entrar en consideraciones jurídicas ni políticas sobre el ejercicio de la soberanía en el mismo.

En cuanto a limitar el ciberespacio a las "[…] redes y los sistemas de información y telecomunicaciones […]", la Estrategia precisa más adelante que estos están compuestos por una infraestructura física y por una "vertiente inmaterial" que incluiría programas informáticos, modelos o procedimientos. No asocia, por consiguiente, ciberespacio con los componentes físicos en los cuáles basa su funcionamiento (ESPAÑA, 2013a, p. 9).

A continuación, el documento enumera las principales características del espacio cibernético y su diferenciación con los ámbitos físicos. El bajo coste de su operación y la relativa facilidad de su utilización lo convierten en un instrumento al alcance de la práctica totalidad de la población mundial con acceso a las telecomunicaciones. Esta característica, unida a la ubicuidad de su alcance, incrementa el número de actores con los que se tiene contacto directo de una manera sin precedentes.

No solo cualquier Estado, con independencia de su ubicación geográfica, puede convertirse en un potencial adversario en un ciberespacio sin fronteras

físicas, sino que su coste y simplicidad extienden la amenaza a grupos más o menos organizados, delincuenciales o terroristas, y a individuos particulares con conocimientos avanzados.

A ello se unen las otras dos características que identifica la Estrategia, la efectividad del impacto de las operaciones desarrolladas en el ciberespacio y el reducido riesgo que corre el atacante, para hacer del entorno virtual un aspecto oblicuo en relación con todas las posibles amenazas a la seguridad de un Estado.

Poco ha variado la situación desde la redacción de la Estrategia en este sentido. La dificultad para la atribución de la autoría de los hechos en el ciberespacio sigue siendo una de las asignaturas pendientes para las fuerzas de seguridad y para los servicios de inteligencia de los países. Esto es especialmente cierto cuando se trata de conseguir identificar al autor en tiempo útil para la adopción de las medidas que permite el Derecho Internacional en cuestión de legítima defensa o de medidas defensivas de carácter activo o disuasorio.

En cuanto al impacto de las operaciones, estos dos años largos no han hecho más que confirmar la capacidad disruptiva de los ataques cibernéticos. En el momento de escribir estas líneas sigue de actualidad el ataque sobre las redes de distribución de energía eléctrica de Ucrania en vísperas de la Navidad de 2015. Otros ataques, como el perpetrado por Corea del Norte contra la compañía japonesa *Sony Pictures*, demuestran tanto este potencial destructor como el tipo de simetría en la que se mueve el mundo cuando Estados, corporaciones, grupos organizados e individuos se atacan entre sí de forma indiscriminada.

Más adelante, la Estrategia retomará este postulado para argumentar en favor de la necesidad de cooperación entre todos los actores nacionales interesados en una red segura y eficiente. En este primer capítulo, no obstante, ya hace mención específica de la necesidad de garantizar el funcionamiento de las Administraciones Públicas, y de las infraestructuras y servicios críticos.

Para alcanzar sus objetivos, la Estrategia define cuatro principios rectores:

✓ liderazgo nacional y coordinación de esfuerzos, asumiendo dicho liderazgo desde la misma Presidencia del Gobierno como director de la Política de Ciberseguridad Nacional;

✓ la responsabilidad compartida, tanto entre las distintas partes de la Administración como entre esta y los actores privados;

✓ la proporcionalidad, racionalidad y eficacia, gestionando los riesgos dentro de la legalidad nacional e internacional y de una forma dinámica[1], y

1 Concepto que se recoge mucho después en el documento publicado por el Atlantic Council: Dynamic Stability: US Strategy for a World in transition. (PAVEL; ENGELKE; WARD, 2016).

✓ la cooperación internacional, como elemento clave en un ámbito de alcance global.

Finalmente, la Estrategia acomete la necesidad de equilibrio entre la privacidad y la seguridad privada, por un lado, y la seguridad pública y estatal, por el otro. En el último párrafo del capítulo:

> El Gobierno de España se compromete a desarrollar políticas que, mejorando la seguridad de los Sistemas de Información y Telecomunicaciones que emplean los ciudadanos, profesionales y empresas, preserven los derechos fundamentales de todos ellos, especialmente en los sectores más desprotegidos. (ESPAÑA, 2013a, p. 17).

Este equilibrio, de plena actualidad con la disputa entre el FBI norteamericano y la empresa Apple, también debe ser acometido de forma progresiva y dinámica[2].

El capítulo 3 enumera los objetivos que pretende alcanzar la Estrategia. El objetivo genérico redunda en la idea de que España haga un uso seguro de los sistemas de información y telecomunicaciones y en el fortalecimiento de las capacidades de prevención, defensa, detección y respuesta de los ciberataques.

En este sentido, la Estrategia se diferencia de otras más modernas, como la holandesa, que incorpora un uso eficiente de estos mismos sistemas entre sus objetivos en lo que es una aproximación más amplia, aunque menos centrada en la seguridad.

Los objetivos concretos que fija la Estrategia no hacen sino definir los distintos ámbitos de actuación en que debe desarrollarse el objetivo principal. Así, el primero fija el foco en la Administración Pública; el segundo en el sector empresarial en general y en las infraestructuras y servicios críticos en particular; el tercero en la lucha contra la delincuencia y el terrorismo que hacen uso de las redes; el cuarto hace referencia a la necesidad de concienciación del conjunto de los usuarios; el quinto a la formación y especialización del personal técnico y, en fin, el sexto a la contribución a la ciberseguridad del ciberespacio internacional, como contribución nacional y como medida necesaria para asegurar el propio.

2 El acceso a los datos del teléfono móvil de uno de los terroristas del atentado de San Bernardino de diciembre de 2015 ha supuesto la elevación a sede judicial del debate entre la seguridad que proporcionan la compañías privadas y la que debe proporcionar el Estado. Este será un asunto que deberá continuar debatiéndose en sede parlamentaria en su momento. Por ahora, aparentemente, la intervención de un tercero ha evitado la confrontación entre el Estado norteamericano y la empresa Apple pero la decisión de retirar la demanda solo supone una dilación en el establecimiento de unos nuevos límites en la interpretación del contrato social que deberán clarificarse próximamente (SANDOVAL, 2016).

En consonancia con estos objetivos, la Estrategia establece ocho líneas de acción para su desarrollo.

La materialización de la Estrategia, como queda dicho, se recoge en el Plan Nacional de Ciberseguridad y en los Planes Derivados que se han elaborado en los dos últimos años por sendos grupos de trabajo[3]. No procede discutir el detalle de su contenido en estas líneas, pero el mismo carácter dinámico de la defensa del ciberespacio demanda la constante renovación de las ideas sobre las cuales se basa esta y, por lo tanto, la revisión de la Estrategia misma y los documentos que de ella se derivan.

4 Relaciones y Organización de la Ciberseguridad en España

4.1 El Consejo Nacional de Ciberseguridad

El quinto capítulo de la Estrategia de Ciberseguridad Nacional describe la integración de la ciberseguridad dentro del Sistema de Seguridad Nacional. Su implementación, sin embargo, no se ha ajustado a la literalidad del contenido del capítulo, muy genérico y conciso, por otro lado (ESPAÑA, 2013a).

La Estrategia preveía un Comité Especializado en Ciberseguridad y un Comité Especializado de Situación genérico (un Gabinete de Crisis), ambos dependientes del Consejo de Seguridad Nacional, creado de forma simultánea a la publicación de la Estrategia de Seguridad Nacional y máximo órgano asesor del Presidente del Gobierno. En el Consejo de Seguridad Nacional se reúnen los ministros más relacionados con la seguridad y con la situación concreta a tratar junto con el Secretario de Estado Jefe de Estado Mayor de la Defensa y el Director del Centro Nacional de Inteligencia (CNI).

La implementación práctica de este apartado supuso la creación, el 14 de febrero de 2014, de un Consejo Nacional de Ciberseguridad (EL GOBIERNO..., 2014). Se establecía que su presidencia debía ser rotatoria entre sus miembros con carácter anual, con un primer periodo liderado por el Secretario de Estado del CNI.

4.2 Organismos implicados en la ciberseguridad en España

El desarrollo de la Estrategia no podía sino seguir un esquema similar al de sus capítulos, y divide la responsabilidad de la seguridad de las redes y sistemas

3 Aunque los Planes Derivados han sido aprobados, no constituyen un documento público que pueda consultarse sin la debida autorización.

informáticos y de telecomunicaciones entre distintos organismos en función de su ámbito de actuación. Esta responsabilidad abarca, en ocasiones, más aspectos que la simple defensa e implica la explotación de las oportunidades que proporciona la capacidad para hacer un uso eficaz del ciberespacio.

De una forma muy esquemática, España ha dividido las responsabilidades de la defensa entre tres CERT (*Computer Emergency Response Team*) principales. El ámbito de la Administración Pública, recogido de forma separada en los objetivos y en las líneas de acción como se recordará, se asignó al CCN-CERT, equipo de respuesta del Centro Criptológico Nacional (CENTRO CRIPTOLÓGICO..., [20--?]), colocado junto al Centro Nacional de Inteligencia. La seguridad de empresas – especialmente las infraestructuras y servicios críticos – y ciudadanos, tanto en la protección de los mismos respecto del terrorismo como de la delincuencia, caen dentro de la tutela del CERT-SI (Seguridad e Industria)[4], establecido por el Ministerio de Industria, y que sirve también al Ministerio del Interior y a las Fuerzas y Cuerpos de Seguridad del Estado. Finalmente, el Ministerio de Defensa es de la exclusiva responsabilidad del Mando Conjunto de Ciberdefensa (ESPAÑA, [20--?]a) y su ESPCERTDEF (CERT de Defensa de España), y tiene dependencia directa del Jefe de Estado Mayor de la Defensa.

Los responsables de los tres organismos que gestionan los CERT principales son vocales del Consejo Nacional de Ciberseguridad y, por lo tanto, se coordinan entre ellos y con los representantes del resto de los organismos afectados (por ejemplo, los ministerios de Justicia, de Asuntos Exteriores y Cooperación, de Economía o de Educación) en el ámbito del Consejo. De esta manera queda cubierta la relación vertical superior hacia el nivel estratégico-político y se facilitan los mecanismos para la coordinación horizontal entre los tres CERT.

Evidentemente, existen otros muchos CERT, organismos y agencias de menor entidad que también asumen responsabilidades en la gestión de la ciberseguridad en España. Todos ellos, sin embargo, deben coordinar sus acciones con alguno de los tres CERT principales. De este modo, el resto de los organismos de la Administración, tanto a nivel nacional, como autonómico y local, dependerán del CCN-CERT. Las organizaciones públicas – como el Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC) o las organizaciones de la Policía Nacional[5]

4 El CERT-SI (INSTITUTO..., [201-?]a) está gestionado por INCIBE, Instituto Nacional de Ciberseguridad (INSTITUTO..., [201?]b) empresa de titularidad pública creada ex profeso para esta tarea en el año 2006.

5 El Cuerpo Nacional de Policía encuadra sus unidades de lucha contra los delitos cibernéticos dentro de la Brigada de Investigación Tecnológica (BIT) (CUERPO..., 2016).

y la Guardia Civil[6] y privadas encargadas de proporcionar seguridad ciudadana y protección a la propiedad intelectual de las empresas y ciudadanos, se relacionan con el CERT-SI. Finalmente, el ESPCERTDEF tiene la responsabilidad de coordinar la actuación de los ejércitos y las operaciones nacionales e internacionales del ámbito de la Defensa Nacional (CENTRO NACIONAL..., [20--?]; CUERPO..., 2016; ESPAÑA, [20--?]c; ASR, [20--?]).

Se argumentará, con razón, que existen numerosas zonas de solape entre las responsabilidades de las distintas administraciones y organismos encargados de la ciberseguridad a nivel nacional. Esta es una circunstancia que se repite en la implementación de la práctica totalidad de los casos a lo largo y ancho del mundo. De hecho, las zonas de solape, si bien pueden ocasionar algunos inconvenientes a la hora de delimitar responsabilidades y competencias, permiten asegurar que no se mantienen zonas de impunidad, zonas grises en las que nadie tenga asignada la capacidad para actuar.

En el caso español, como en la mayoría, la protección de las infraestructuras críticas, por su carácter estratégico para la Seguridad Nacional, podrían constituir un espacio de intersección de competencias entre los tres CERT principales. En tanto estructuras que suponen una vulnerabilidad estratégica, su protección más allá de la propia responsabilidad de las empresas privadas a quien pertenecen, podría interpretarse como competencia del Centro Criptológico Nacional. En tanto que afectan a la Defensa Nacional, podrían ser asignadas al Mando Conjunto de Ciberdefensa en función de su misión subsidiaria, según veremos más adelante. Naturalmente, como empresas que son, también caen dentro del ámbito del CERT de Seguridad e Industria.

El legislador fue, evidentemente, consciente de esta múltiple dependencia potencial que, por otro lado, enfatiza la prioridad que se concede a la protección de estas infraestructuras y servicios críticos. Reforzando aún más este carácter, se crea el Centro Nacional de Protección de las Infraestructuras Críticas, dependiente del Ministerio del Interior y, por lo tanto, en el entorno del CERT-SI, con la expresa tarea de elaborar las normas de autoprotección de estas industrias y servicios.

La casuística irá decantando responsabilidades y estableciendo el *modus operandi* para cada caso. El ámbito de la ciberseguridad es lo suficientemente amplio como para satisfacer las aspiraciones de todos los organismos y, probablemente, para saturar sus capacidades de actuación.

6 La Guardia Civil dispone de una unidad especializada en el combate contra la delincuencia común en las redes, el Grupo de Delitos Telemáticos de la Unidad Central Operativa (ESPAÑA, [20--?]c), y con una unidad especializada en la lucha contra las actividades terroristas que aprovechan las capacidades de internet, la Unidad Central Especial número 3 del Servicio de Información de la Guardia Civil (ASR, [20--?]).

Es más, sería inconsistente con la misma naturaleza permanentemente evolutiva del ciberespacio pretender fijar unas estructuras orgánicas y unos procedimientos operativos que sirvan de una forma permanente para acometer los retos que se vayan presentando en este campo. La resiliencia, más que la mera resistencia, debe ser el objetivo de las estructuras que se creen. Esta resiliencia se basa en la flexibilidad de los mecanismos y en su capacidad de adaptación a circunstancias novedosas. Dotar de soluciones unívocas a retos polimorfos y evolutivos sería una receta infalible para el fracaso.

5 El papel del Ministerio de Defensa en la Ciberseguridad Nacional: el Mando Conjunto de Ciberdefensa

Ciertamente, la protección de las redes y sistemas del Ministerio de Defensa – la misión principal del Mando Conjunto de Ciberdefensa – es una tarea mucho más amplia de lo que puede parecer a simple vista[7] (MANDO..., [20--?]).

Para empezar, el mero tamaño de las redes es considerable. Tanto en España como en la mayor parte de los países, Defensa es uno de los ministerios clave y uno de los que mayor cantidad de personal emplea. Si a ello le sumamos la dispersión geográfica de dicho personal, no solamente en territorio nacional, sino también en los destacamentos en las misiones internacionales, en los buques de la Armada o en las representaciones ante las Organizaciones Internacionales y en las Embajadas, la complejidad se ve incrementada notablemente.

Cualitativamente, la protección de la información que se mueve por las redes de Defensa es también de alto valor estratégico y, por lo tanto, a la complejidad física se añade la trascendencia de la misión de protección de dichos recursos. Esta información debe, en muchos casos, estar disponible en tiempo real en ubicaciones muy distintas. Por lo común, es la información más sensible la que resulta más urgente.

Es esta multiplicidad de actores y sensibilidades lo que obliga al mantenimiento de numerosas redes diferenciadas en función de los distintos grados de confidencialidad de las mismas y de los socios con los que se comparte la información en las mismas. Cada red implica el diseño de una arquitectura y la protección de un perímetro distinto y, en muchos casos, con requerimientos específicos.

Además de las redes propias, el Mando Conjunto de Ciberdefensa también está encargado de la protección de aquellas otras que se le puedan asignar *ad hoc*

7 El concepto se desarrolla algo más en el video sobre el Mando Conjunto de Ciberdefensa que publicó el diario El Mundo (MANDO..., [20--?]).

en función de su importancia para la Defensa Nacional y de las vulnerabilidades que presenten sobre la base de sus recursos defensivos propios.

Dos circunstancias convierten esta misión -aparentemente secundaria- en crítica para la Defensa. En primer lugar, la dependencia del entorno militar respecto de las infraestructuras y servicios que prestan compañías civiles de servicios públicos. La misma operatividad de las Fuerzas Armadas depende, en casi todas las ocasiones, del funcionamiento adecuado de los servicios civiles para la provisión de energía, comunicaciones y buena parte de la logística. La protección de las redes de estos servicios y la implementación de medidas para la mitigación de su afectación por una avería o por un ataque son vitales para asegurar la continuidad de la disponibilidad de los propios servicios.

En segundo lugar, la pérdida de la asimetría, el efecto igualador, que se ha alcanzado en el ciberespacio y que supone que los ataques contra cualquier red puedan proceder de sus equivalentes o de otro actor público o privado. Una muestra de este último extremo es el ataque contra la compañía Sony, una entidad privada, a cargo de un gobierno estatal, o los ataques contra los gobiernos que proceden de *hackers* particulares o de grupos delincuenciales o terroristas. Los ataques de Estados contra empresas pueden requerir de la implicación de las organizaciones públicas en la protección de los intereses nacionales, como se ha visto ya en algunas ocasiones como el mencionado caso de Sony.

En este escenario complejo, el Ministerio de Defensa no puede permanecer ajeno a las tácticas, técnicas y procedimientos comunes en ataques en otros ámbitos y niveles. Alrededor de los servicios esenciales se teje una suerte de defensa perimetral por capas en las que todos los recursos deben estar disponibles.

6 Origen y Misión

El Mando Conjunto de Ciberdefensa se crea en 2013 de forma prácticamente simultánea al proceso de elaboración de la Estrategia Nacional de Ciberseguridad.

La creación del Mando no parte de la nada, sino que se basa en servicios preexistentes en el Ministerio de Defensa y que venían asumiendo la protección de las redes desde su creación. La aparición de una estructura de carácter conjunto, en la que todos los distintos servicios aportaban personal, permitía asumir otras funciones adicionales a la mera protección de redes corporativas y centralizaba labores comunes de carácter trasversal.

De este modo, el Mando Conjunto de Ciberdefensa pretendió desde su creación dotarse de las capacidades de Defensa, Explotación y Respuesta, con el objetivo de ir alcanzando la plena competencia en cada una de ellas de forma

escalonada y en el mismo orden mencionado, pero con el desarrollo simultáneo de las tres. Cumplidos los tres primeros años desde su creación, esta meta sigue siendo perfectamente vigente y el grado de consecución de los objetivos coherente con la idea inicial.

Es justo recordar aquí el difícil escenario en el que se desarrollan las actividades del Mando y de sus equivalentes en otros países. Además del cumplimiento de la misión establecida de la protección de las redes, se está en el proceso de diseñar el mismo entorno del ciberespacio, de las leyes que lo regulen, y de sus modos y modelos de utilización. En una figura muy gráfica de su primer Jefe de Estado Mayor, es como invitar a almorzar a un amigo y emplear como mantel los mismos planos – a medio desarrollar – del diseño de la casa en la que se está comiendo.

Es, en parte, motivado por esta circunstancia por lo que el Ministerio de Defensa en España ha mantenido descentralizada la protección de las redes específicas de cada uno de los ejércitos, de modo que el Mando Conjunto de Ciberdefensa solo sea responsable directo de la protección de las redes y sistemas corporativos y de los conjuntos. Es decir, mientras que el Mando asume la protección de la *web* de Ministerio y del Estado Mayor de la Defensa, las redes empleadas de forma conjunta en operaciones y sus sistemas asociados, cada uno de los ejércitos mantiene la competencia sobre sus sistemas específicos, sean logísticos, administrativos u operativos.

La solución adoptada permite, además, una mayor implicación de los ejércitos en la función de ciberdefensa y una mayor sensibilización respecto de los retos y oportunidades que presenta el ciberespacio.

7 Formación y Adiestramiento

Esta misma labor de sensibilización o concienciación es una de las tareas trasversales que sí recae entre las responsabilidades del Mando. Criterios de eficiencia aconsejaron retenerla, junto con la formación del personal, en un nivel centralizado. Así, la determinación de los perfiles de egreso de los alumnos que configuran a su vez los planes y programas de estudios relacionados con la ciberdefensa son competencia exclusiva del Mando de Ciberdefensa. El Centro Superior de Estudios de la Defensa Nacional (CESEDEN)[8], como responsable de los cursos de carácter conjunto que se imparten en el Ministerio, coordina la impartición de los cursos cuya implementación corre a cargo de los Centros Universitarios de la Defensa (CUD) adscritos a cada uno de los ejércitos (ESPAÑA, [20--?]b).

8 CESEDEN. Disponible en: <http://www.defensa.gob.es/ceseden/>.(CENTRO SUPERIOR..., [20--?])

Siguiendo este criterio, la Armada había asumido la organización, con el CUD de la Universidad de Vigo[9], del Curso Básico de los que componen el programa FORCIBE (Formación en Ciberdefensa). El Ejército de Tierra desarrollará, junto al CUD de Zaragoza[10], el Curso Avanzado y el Ejército del Aire, a través del CUD de Cartagena[11], los cursos de especialización de más alto nivel y grado de concreción.

En el momento de escribir estas líneas, la solución adoptada pasa por impartir el Curso Básico en la Escuela de Especialidades de la Armada "Antonio de Escaño", el Curso Avanzado en la Academia del Arma de Ingenieros, en Hoyo de Manzanares, Madrid, y los cursos de especialidades en la Escuela de Técnicas Aeronáuticas de Torrejón de Ardoz, también en Madrid. Todos los cursos se impartirían, en un principio, por parte de profesores del conjunto de los CUD[12].

De nuevo, se reproduce el modelo anterior en el que la política se determina en el Mando Conjunto mientras que la ejecución corre a cargo de los ejércitos en un modelo colaborativo que hace uso de la estructura de los CUD para garantizar la homogeneidad de la enseñanza.

A un nivel académico superior, el Mando Conjunto de Ciberdefensa coopera activamente con varias universidades españolas en la elaboración de currículos y en la impartición de materias concretas de varios títulos de Máster. Los convenios establecidos con la Universidad Politécnica de Madrid y con la Universidad Carlos III de Madrid han facilitado la colaboración con estas y otras instituciones académicas sin limitar por ello la capacidad ni el deseo del Mando por colaborar con otros centros.

Fruto de esta colaboración es la presencia del Mando en el Máster Universitario en Ciberseguridad de la Universidad Carlos III (UNIVERSIDAD..., [20--?]), en el Máster Internacional en Ciberdefensa de la Universidad de Alcalá (MÁSTER..., [20--?]), o en el Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen, de la Universidad Autónoma de Madrid (UNIVERSIDAD..., 2016), entre otros.

8 Cooperación

La cooperación ha sido bandera del Mando Conjunto de Ciberdefensa desde sus inicios. No solo en el ámbito público-privado, ni solamente en el mundo

9 CUD de Vigo, asociado a la Escuela Naval Militar: Disponible en: <http://cud.uvigo.es/>. (CENTRO SUPERIOR..., [20--?]).

10 CUD de Zaragoza, asociado a la Academia General Militar: Disponible en: <http://cud.unizar.es/>. (CENTRO SUPERIOR..., [20--?]).

11 CUD de Cartagena, asociado a la Academia General del Aire: Disponible en: <http://www.cud.upct.es/>.(CENTRO SUPERIOR..., [20--?])

12 También es un CUD el implantado en la Universidad de Alcalá de Henares para dar servicio a los Cuerpos Comunes de la Defensa: Disponible en: <https://cud.uah.es/>.

académico. En ese mismo contexto, el Mando colabora con otros centros de enseñanza, y de investigación y desarrollo, buscando potenciar el mismo para conseguir una sólida base industrial de vanguardia que garantice un cierto grado de autonomía nacional en el desarrollo de productos y servicios. Ejemplo de esta colaboración es la presencia del MCCD en las Jornadas Nacionales de Investigación en Ciberseguridad (JNIC)[13].

En el ámbito institucional, la cooperación es también muy amplia. Además de las relaciones derivadas del papel asignado al Mando por la Estrategia Nacional de Ciberseguridad y que implican una coordinación horizontal y vertical con los demás miembros del Consejo Nacional de Ciberseguridad, el Mando ha buscado estrechar relaciones con la sociedad civil nacional.

Internacionalmente, el papel del Mando Conjunto de Ciberdefensa y la implicación de España en la materia queda de relieve en los numerosos compromisos adquiridos y en los foros en los que se participa. Como miembro fundador del Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN (CCD CoE)[14], el Mando mantiene dos posiciones permanentes en Tallin, una civil y una militar – como Jefe de la División de Formación y Entrenamiento – y es uno de los principales contribuidores al Centro.

El MCCD participa también en distintos foros en el ámbito de la Unión Europea, principalmente con la Agencia Europea de Defensa (EDA) (EUROPEAN…, 2015), y con la Alianza Atlántica. Dentro de la OTAN, el Mando está presente tanto en las labores de planeamiento y generación de doctrina, como en las misiones operativas y en la creación de la Red Federada de Misión (*Federated Mission Network*) (NORTH…, 2015).

Por lógicas razones históricas, culturales y de interés mutuo, Iberoamérica constituye un foco de atención preferente en la cooperación del Mando Conjunto de Ciberdefensa. En este sentido, el lanzamiento este mismo año 2016 del Foro Ciberoamericano de Defensa, en el marco de las Jornadas de Ciberdefensa desarrolladas en Madrid en el mes de mayo, constituye un paso fundamental para alinear las doctrinas y políticas cibernéticas en los países de habla hispana y lusa, contribuir a una formación homogénea en este campo y cimentar los intercambios de información operativa que permitan mejorar la seguridad colectiva contra ataques cibernéticos.

13 La segunda edición de las JNIC se celebra en 2016 bajo la coordinación de la Universidad de Granada <http://ucys.ugr.es/jnic2016/>, después de su puesta en marcha en 2015 por iniciativa de INCIBE y de la Universidad de León <http://jornadasciberseguridad.riasc.unileon.es/>.

14 Página del inicio: <https://ccdcoe.org/>.

9 Capacidades: Defensa, Explotación y Respuesta

Mientras que la función defensiva está descentralizada, como queda dicho, en los ejércitos para sus redes y sistemas específicos, las funciones de explotación y respuesta se mantienen en el Mando debido a su especial sensibilidad y a la especificidad de la formación que requiere el personal que las ejecuta. En este sentido, con independencia de la intención y de los efectos buscados por cualquier acción de este tipo, las repercusiones tienen -como en el caso de la aviación en el mundo físico- muchas veces consecuencias operacionales o estratégicas.

Como se apuntó más arriba, las capacidades de explotación y respuesta están siendo desarrolladas de forma simultánea, aunque con un cierto decalaje temporal respecto de la de defensa. Las características de todas ellas se estudian en mayor profundidad en el siguiente apartado.

Para el desempeño de la función defensiva de las redes corporativas y conjuntas, y para el apoyo a los ejércitos en sus labores en las redes específicas -incluida la certificación de las redes en territorio nacional y en destacamentos- el Mando Conjunto de Ciberdefensa se ha dotado de una serie de capacidades que incluyen la de análisis de *malware*, el análisis forense avanzado y la gestión de redes y sistemas.

Además de todo lo anterior, el Mando ha desarrollado un Kit Desplegable (CDK - *Cyber Deployable Kit*) con capacidad para complementar o suplir las necesidades de un destacamento militar. Adicionalmente, se ha dotado también de un campo de maniobras, *Cyber Range*, adaptado a los requerimientos de su operación.

10 La Integración de los Aspectos Cibernéticos en las Operaciones Militares

Al observar los distintos modelos de integración de los organismos encargados de la ciberseguridad en las estructuras de las Fuerzas Armadas de los distintos países se ve una tendencia a insertar estos dentro del contexto organizativo preexistente, preferiblemente dentro de las áreas de la división de tecnologías de la información y comunicaciones, o dentro de la rama de inteligencia.

Al igual que ocurre en la traslación de los postulados del Derecho, particularmente del Derecho Internacional, al ámbito del ciberespacio, los gobiernos adecúan un ámbito trasversal a las orgánicas verticales tradicionales en lo que

parece una apreciación muy parcial de las características que presenta el entorno digital (DÍAZ, 2013)[15].

La creación de un Mando de Ciberdefensa – o sus equivalentes – en numerosos países no termina de permitir la integración directa de las capacidades que ofrece la ciberseguridad en el espectro completo de las operaciones militares. Además de crear un instrumento capaz de llevar a cabo operaciones, es necesario contemplar, como hace la doctrina española, el dominio digital como una línea más dentro de los recursos disponibles para el cumplimiento de la misión.

En este sentido, el reconocimiento del ciberespacio como quinto entorno operacional se ve fortalecido con la creación en España de un quinto Mando Componente, en igualdad de condiciones teóricas con los otros cuatro – terrestre, marítimo, aeroespacial y de las operaciones especiales – e independiente de todos ellos.

La traslación posterior a las operaciones militares de estos conceptos implica, no obstante, la necesidad de evitar las diferenciaciones entre las acciones cinéticas y las cibernéticas, no ya por su naturaleza jurídica, todavía no establecida formalmente, sino por su capacidad para apoyar la consecución de una situación final deseada.

Esta afirmación, aparentemente de sentido común cuando se sigue el razonamiento que se venía exponiendo, tiene todavía un difícil encaje en los diseños operacionales de la mayor parte de los países. Las personas, más que las estructuras, condicionan muchas veces la capacidad de integración de conceptos como este en el ciclo de planeamiento.

Así, frecuentemente se busca limitar el ámbito de actuación de las actividades del ciberespacio a determinadas actividades relacionadas con su naturaleza tecnológica o a la explotación de la información que fluye, de forma preferente, por el ciberespacio. De ahí la tendencia a hacer depender los organismos encargados de la ciberseguridad de segundas, sextas o novenas secciones, en función de que el interés principal sea la generación de inteligencia, la protección de las comunicaciones propias o el apoyo a las operaciones de influencia.

15 De hecho, incluso dentro de la diversidad de visiones que los Estados tienen de la ciberseguridad, se pueden distinguir tres grandes grupos nacionales. Por un lado, la aproximación ciberliberal defensiva, propia de los países europeos continentales – entre los que está España – y que prima la capacidad de utilización de las redes propias. En segundo lugar, la visión ciberliberal ofensiva, de corte anglosajón, especialmente norteamericano, y que tiene un carácter más expansivo. Finalmente, la cibernacionalista-aislacionista, que se identifica con Rusia o China, que fomenta un ciberespacio enfocado hacia dentro, conectado con el resto a través de pasarelas controlables por el Estado.

Esta aproximación supone una utilización ineficiente de los medios cibernéticos, tanto como lo sería una interpretación de las fuerzas navales circunscrita a labores de apoyo logístico o de interdicción de rutas. Al contrario, igual que cualquier fase y aspecto del planeamiento incluye las capacidades que pueden aportar el resto de los mandos componentes, se impone que las capacidades digitales puedan estar presentes de la misma manera.

Esta deficiente visión conjunta de las operaciones en lo que respecta al ciberespacio es tanto más miope cuanto que la dualidad de funciones cívico-militar es más acusada todavía en este entorno que en cualquiera de los otros y, por lo tanto, permite una integración en el esfuerzo global del Estado para la consecución de sus objetivos más real y cotidiana.

11 Guerra Híbrida y Permanente

Los conflictos actuales se libran en lo que ha dado en llamarse un modelo de guerra híbrido, que combina actos de fuerza con otros de mera presión, intimidación o, incluso, seducción. No existen declaraciones de guerra ni, al menos de forma necesaria, crisis diplomáticas que anuncien un cambio de estado. Es más, la distinción entre Estados amigos y enemigos se traduce, a efectos prácticos, en una cuestión de intereses nacionales y en un respeto de ciertas líneas rojas en el grado de competición que va asociado a la necesaria cooperación entre países.

La teoría de Thomas P. Barnett de un mundo conectado e interdependiente en el cual no pueden darse conflictos abiertos por las graves consecuencias económicas que implican para los contendientes y para la economía mundial se traduce en un estado permanente de agresión por debajo del umbral del uso de la fuerza. En estas agresiones participan amigos y adversarios, actores estatales y privados, incluso hasta el extremo de producirse agresiones internas provocadas por grupos de presión o de interés.

Son estas guerras híbridas, permanentes y deslocalizadas las que tienen que combatir las Fuerzas Armadas modernas. Es para este tipo de conflictos, tanto o más que para los bélicos cinéticos tradicionales, para los que se debe ser capaz de integrar el mundo digital en las operaciones cotidianas.

Cabe, por lo tanto, identificar dos tipos de misiones fundamentales que pueden llevar a cabo los miembros del componente cibernético de las Fuerzas Armadas. Por un lado, dentro de la guerra híbrida y de carácter permanente, los guerreros cibernéticos tienen la importante misión de asegurar que las redes y sistemas de información y telecomunicaciones se encuentran disponibles para su utilización eficiente por parte del Estado y los ciudadanos. Al mismo tiempo, es de primordial

importancia que las percepciones y, por ende, las narrativas que se construyen sobre los contenidos del ciberespacio respondan a los intereses propios o, al menos, no sean contrarias a los mismos. Esta segunda misión, si bien no corresponde en cuanto a su planeamiento y dirección al componente cibernético, se basa en sus capacidades y en las infraestructuras de cuya seguridad es responsable.

En segundo lugar, dentro del contexto de las operaciones militares, los medios digitales deben ser utilizados como una capacidad más, equivalente a las cinéticas que proporcionan los otros mandos componentes. Se trata de medios distintos de conseguir efectos equivalentes y, por lo tanto, deben utilizarse en función de los condicionantes que imponga la misión pero partiendo de un conocimiento profundo de las posibilidades que ofrecen. Las oportunidades serán tanto más claras y evidentes cuanto mayor sea el grado de sofisticación y dependencia del adversario respecto del uso de sus propias redes produciéndose la paradoja de que capacidades y vulnerabilidades mantienen una correlación directa en lugar de minimizarse unas cuando las otras están más ampliamente desarrolladas.

12 Percepciones y Narrativas

La sociedad del siglo XXI es fundamentalmente distinta de la del siglo XX por el alcance de la globalización. Un concepto *demodé* y "gastado", la globalización ha afectado, no obstante, a la forma en que las personas viven y se relacionan. Es imprescindible comprender en profundidad las implicaciones de estos cambios para ser conscientes de cuáles son las oportunidades que ofrece el ciberespacio y, por justa correspondencia, cuáles sus vulnerabilidades.

Algunos autores, como Jeremy Rifkin (RIFKIN, 2014), ilustran los cambios que a nivel sociológico y geoeconómico trae consigo la última revolución tecnológica. Se trata de cambios cualitativos significativos y no de meras actualizaciones o variaciones en la magnitud de los fenómenos de la era anterior. Despreciar la magnitud y el alcance de estos cambios supondría la incapacidad para reconocer cuál es el nuevo terreno elevado que hay que ser capaz de defender para conseguir la ventaja estratégica.

Un vistazo siquiera casual a la génesis de los conflictos contemporáneos en los que están implicadas las grandes potencias mundiales revela la importancia de la opinión pública y las percepciones sobre las que se construyen las narrativas en las que se basan las decisiones de los líderes políticos. La permeabilidad de la sociedad a los mensajes -instantáneos e interactivos- que se difunden por los medios digitales convierte a estos en verdaderas armas de generación de influencia.

La obsesión de los técnicos por la protección de los números, de los datos contenidos en las redes y sistemas hace que, en ocasiones, se pierda de vista el poder de las ideas, de las letras, que se difunden por esas mismas redes. Con los cambios en los modelos sociales y económicos se producen también alteraciones en los basamentos de la sociedad. Los ataques que recibe el sistema financiero occidental en general, y norteamericano en particular procedente de países de Oriente Medio revelan una diferencia en el patrón ofensivo de un adversario global. Ya no se toma como objetivo el núcleo duro del rival, sus Fuerzas Armadas o su Gobierno, sino que se intentan minar los valores y las estructuras basales del sistema productivo.

En las operaciones marco, en aquellas que responden a la necesidad de defender los mismos fundamentos de nuestra sociedad, los círculos concéntricos que describía John Warden III (ALVAREZ, 2014) en su libro '*The Air Campaign: planning for combat*' (WARDEN III, 1988), es necesario fortalecer las narrativas propias. Mientras que en Irak en 1991, Warden abogaba por incidir sobre los círculos interiores, el liderazgo y su capacidad de comunicarse, en 2016 la opinión pública y la sociedad civil se han posicionado como aspectos clave en la voluntad de vencer de las naciones.

Los mismos fundamentos de la economía colaborativa muestran la resiliencia que presentan los sistemas basados en nodos dispersos e invitan a identificar los elementos clave y los vínculos más sensibles a la hora de planificar un ataque.

La incorporación de agentes o agencias no estatales a la ejecución de operaciones tendentes al mantenimiento de una narrativa favorable, sea basadas en la protección de los mensajes propios o en la desinformación o en desvirtuar los contrarios, es un campo que presenta opciones especialmente atractivas por la especificidad del mismo, por la inadecuación de los instrumentos propios de las Fuerzas Armadas para acometer la tarea y por los réditos que pueden obtenerse de este tipo de operaciones.

13 La integración de los Aspectos Cibernéticos y los Cinéticos en Operaciones

El ciberespacio ofrece un amplio abanico de posibilidades en cuanto a la actuación en las operaciones militares. Se identifican al menos cuatro modos de uso de la fuerza en las confrontaciones (CARRILLO, 2015):

1. El uso subrepticio de las herramientas digitales implica su actuación clandestina y anónima (Estonia 2007, donde no se ha podido demostrar la implicación estatal).

2. La utilización paralela coadyuva a la ejecución de las operaciones pero sin mantener una ilación con sus equivalentes físicos (Georgia 2008).

3. El empleo conjunto, en cambio, se realiza en apoyo de las operaciones cinéticas o siendo apoyado por estas para la consecución de los objetivos (Operación Huerto, de supresión de defensas aéreas por medios cibernéticos).

4. Finalmente, el uso alternativo del elemento cibernético se lleva a cabo en lugar del empleo de medios convencionales y obteniendo los mismos efectos que aquellos habrían logrado (como en el caso Stuxnet) (ÁGREDA, 2012)[16].

De este modo, las actuaciones en y desde el ciberespacio abarcan la totalidad del espectro de las operaciones clásicas y añaden a las mismas la posibilidad de usurpar sus funcionalidades actuando desde un espectro distinto para obtener efectos similares a los que se habrían logrado con una acción cinética.

Con la excepción del tercer caso la actuación de las herramientas informáticas se produce con relativa independencia de la acción o la operación conjunta y, por lo tanto, la necesidad de coordinación no tiene lugar más que a un nivel estratégico o, a lo sumo, operacional. Esta circunstancia no obsta para que el proceso de planeamiento militar pueda -y deba- llevarse a cabo siguiendo las mismas o similares pautas que en las operaciones cinéticas. La determinación de una situación final deseada, las diferentes líneas de acción a seguir para ir alcanzando puntos decisivos sucesivos y la consideración de variantes alternativas sigue siendo perfectamente aplicable al planeamiento de las operaciones específicas, incluyendo en este apartado a las cibernéticas.

En cualquier caso, un planeamiento conjunto debería preceder a la decisión de una utilización autónoma de los medios digitales -o de cualesquiera otros, para estos efectos- tras alcanzar la conclusión de que se trata del modo más eficiente de resolver el problema y alcanzar los objetivos finales.

Cabría deducir del ejemplo aportado que las acciones subrepticias tienen necesariamente un carácter estratégico y que se llevan a cabo contra los poderes del Estado en su conjunto. Muy al contrario, la capacidad disruptiva de los medios cibernéticos sobre la logística o la capacidad de mando y control del adversario puede proporcionar también una ventaja operacional desvinculada, en principio de cualquier acción táctica concreta (en cuyo caso nos encontraríamos en el tercer supuesto).

Por descontado, no tiene sentido llevar a cabo una operación subrepticia, por simple y barata que resulte, si no lleva asociada esa ventaja operacional. Más allá del coste de oportunidad asociado al uso de unos recursos sin beneficio alguno, la especificidad de las herramientas digitales hace que, en muchas ocasiones,

16 Para una descripción más detallada sobre cada una de estas operaciones y para bibliografía adicional puede consultarse Ágreda (2012).

su utilización efectiva dependa de la falta de conciencia por parte del adversario respecto de una vulnerabilidad de su sistema. El valor de las herramientas cibernéticas estriba en su carácter específico y no en el coste de su elaboración. Mientras que una bomba de 500 libras mantiene su capacidad destructiva en cualquier momento dadas unas circunstancias concretas, sus equivalentes digitales pueden resultar inertes una vez descubierto su modo de operación.

Las operaciones paralelas a las cinéticas vienen siendo una realidad desde hace ya unos años. De hecho, la afirmación de que podrá haber operaciones cibernéticas sin su contraparte cinética, pero que lo contrario no ocurrirá se ha convertido en un axioma en los cuarteles generales de todo el mundo.

El caso concreto de la guerra de Georgia muestra claramente la diferencia entre las operaciones cibernéticas paralelas a las cinéticas con la convergencia de líneas de acción cibernéticas y cinéticas hacia un mismo objetivo. Como ya habían aparentemente demostrado previamente (ROBERTSON; RILEY, 2014)[17], las capacidades del Ejército ruso le permitían acometer acciones contra sistemas SCADA[18] que habrían tenido un efecto cinético directo sobre Georgia en apoyo a las operaciones cinéticas clásicas. Sin embargo, la operación paralela que llevan a cabo las fuerzas digitales durante el conflicto se limita a actuar sobre la capacidad de Tiblisi para enviar y recibir noticias, con el consiguiente desgaste moral y de la voluntad de vencer de sus fuerzas.

El uso alternativo de las fuerzas cibernéticas respecto del empleo de vectores cinéticos queda perfectamente ilustrado en el ejemplo de Stuxnet, en el que se estima que los efectos del gusano informático fueron equivalentes a los de un ataque aéreo *en masse*. El grado de protección ante ataques convencionales que poseía la central de Natanz aconsejaron al o a los agresores – cuya identidad sigue sin confirmarse oficialmente – la utilización de medios cibernéticos para cumplir el mismo objetivo.

Se ha hablado mucho sobre el elevado coste de compilación del Stuxnet, en el cual habría que incluir toda la recopilación de inteligencia previa y otros factores.

17 Unas semanas antes del comienzo de las hostilidades en Georgia se produjo un siniestro en el gasoducto Bakú-Tiblisi-Ceyhan, probablemente el más importante de la región, cuyas causas aparentes son una sobrepresión en una de las válvulas del sistema producida por un fallo informático inducido (ROBERTSON; RILEY, 2014). Este ataque, atribuido a Rusia y que ha pasado desapercibido para muchos analistas, constituiría un ejemplo de utilización subrepticia del ciberespacio en apoyo a una configuración geoeconómica regional que semanas más tarde se vería reforzada por una operación cinética, la invasión de parte de Georgia.

18 Control de Supervisión y Adquisición de datos (Supervisory Control and Data Adquisition), sistemas informáticos que gestionan procesos industriales al tiempo que adquieren y muestran los datos extraídos de los mismos. Estos sistemas están cada día más presentes en la mayor parte de los procesos industriales modernos y, concretamente, en las infraestructuras críticas de carácter energético.

Sin embargo, incluso para un programa de la sofisticación que tenía este, el coste en términos económicos fue varios órdenes de magnitud menor de lo que habría supuesto un ataque con medios convencionales. Por descontado, el coste en términos humanos, e incluso políticos, se reduce hasta casi hacerse irrelevante.

Una de las principales causas por las que es razonable esperar un incremento sustancial en la frecuencia con la que se producirán ataques cibernéticos como método alternativo al convencional es, sin embargo, el asociado con las consecuencias jurídicas en Derecho Internacional. En absoluto quiere esto decir que los ataques y los actos de fuerza realizados por medios cibernéticos no estén considerados ilícitos. Sin embargo, las dificultades en la atribución de estos ataques y, en último extremo, las de su atribución a un Estado hacen que sea muy difícil su sanción internacional o, incluso, el recurso a la legítima defensa ante los mismos.

Se ha dejado para el final la integración de las operaciones cibernéticas junto con las cinéticas en operaciones conjuntas por su especial complejidad, no ya en su ejecución sino en su gestión al mezclarse disciplinas diferentes y por la trasversalidad de los efectos de las herramientas o armas cibernéticas.

La primera circunstancia que tiene que tener en cuenta el Comandante a la hora de integrar las capacidades ciber en las operaciones es que no existe una correlación directa entre la intencionalidad y los efectos que pueden derivarse de su uso. El ciberespacio es un universo hiperconectado y, por lo tanto, las acciones que se aplican sobre cualquiera de sus nodos pueden reverberar en cualquier otro punto, en sentidos imprevisibles y en momentos muy distintos. Igual que es casi imposible determinar audiencias objetivo para un mensaje en las redes sociales ya que su alcance va a ser global, también es muy difícil determinar el alcance y respuesta que provocará cualquier acción en el ciberespacio operacional. Es por eso que las acciones de este tipo deben estar imbricadas en el conjunto de las operaciones y estar consensuadas con el consejo de un grupo multidisciplinar que considere, en la medida de lo posible, todos los ángulos de la acción.

A partir de esta precaución inicial, las capacidades ciber deben estar presentes en todos los niveles de planeamiento, desde el político (marcado normalmente por la Directiva Política en el entorno OTAN) hasta el táctico (con el Concepto de Operaciones del Componente) pasando por el estratégico (Directiva Militar Inicial) y el operacional (Concepto de Operaciones). El alcance estratégico-político de las operaciones cibernéticas refuerzan la necesidad de esta aproximación multinivel.

En el plano operacional, las capacidades cibernéticas se integran en el planeamiento tanto en los Planes Permanentes y Planes de Contingencia de carácter permanente desde tiempo de paz como en los Planes de Operaciones elaborados para responder a crisis concretas.

En todos los casos y a todos los niveles, el componente digital no debe entenderse como equivalente a las funciones desempeñadas por las Operaciones Especiales, o la Inteligencia, o las Transmisiones sino como un conjunto de capacidades que forma parte de todas ellas y de muchas otras. La tendencia que existe en algunos casos a entender la ciberdefensa como una capacidad en lugar de como un componente aboca a la infrautilización de sus posibilidades y a un pobre entendimiento de las del enemigo. A la falta de eficiencia en la operación propia se puede sumar, por consiguiente, la insuficiente preparación ante las acciones de un adversario más versátil.

En este sentido, hay que abandonar la idea de que el ciberespacio será siempre un mando que desarrollará funciones de apoyo a la acción de otros. El caso contrario ocurre con frecuencia, tanto en las operaciones conjuntas, como en las operaciones de influencia. Del mismo modo que nadie duda de la criticidad de mantener abiertas las rutas logísticas físicas, tampoco debería infravalorarse la importancia de nodos, servidores, satélites de comunicaciones o cables submarinos.

La forma de integrar las capacidades ciber no difiere básicamente de las del resto de los componentes, pero puede requerir de unas consideraciones específicas. Mientras que el *tempo* al que se desarrollan las operaciones digitales es mucho más elevado que, incluso, el de las operaciones aéreas, la fase de preparación es considerablemente más compleja en tanto en cuanto no existen "cargas de pago" estandarizadas que puedan utilizarse en cualquier momento y lugar.

El armamento cibernético ofensivo es difícilmente reutilizable y pocas veces aplicable en distintas situaciones, su tasa de caducidad es muy elevada y su viralización altamente imprevisible.

Por contra, la capacidad de penetración en las redes de un *malware* correctamente elaborado es prácticamente ilimitada, las probabilidades de que se pueda efectuar una trazabilidad del ataque para atribuir autorías son muy remotas y el coste económico de su compilación es marginal respecto de los sofisticados equivalentes cinéticos.

Todas estas características positivas y negativas permitirán al Comandante determinar la idoneidad del uso de las capacidades del componente ciberdefensivo en una fase concreta de una operación. Igual de peligroso y erróneo sería omitir de forma negligente el uso del ciberespacio en el contexto general de las operaciones como esperar que este, por sí mismo, sea capaz de solucionar todos los problemas[19].

Ya en el nivel táctico, la escasa experiencia acumulada en operaciones conjuntas de envergadura y en ejercicios en que ha participado el componente

19 La guerra de Kósovo fue la demostración evidente de que el arma aérea, si bien puede llegar a ganar un conflicto actuando – en determinadas circunstancias – por sí sola es más eficiente utilizada en conjunción con el resto de los componentes.

cibernéticos apunta a la posibilidad de que sea necesario establecer algunos elementos equivalentes a los que ya existen en las operaciones aéreas: una Autoridad de Control de las Operaciones Ciber, un Centro de Mando y Control de Ciberdefensa, una *Tasking Order* ciber (equivanlente al ATO aeronáutico) y un proceso de *targetting* en tiempo real.

14 Estado actual de la Ciberseguridad y la Ciberdefensa en España

España es uno de los países de mundo que mayor talento acumula en las disciplinas relacionadas con la ciberseguridad. Con la mera canalización adecuada de ese potencial humano, España está en condiciones de convertirse en uno de los referentes en estas disciplinas.

Como se ha visto más arriba, la universidad española se está posicionando a nivel internacional como un referente, España es sede de algunas de las empresas punteras en las tecnologías de la información y las comunicaciones, y a nivel institucional, tanto las Fuerzas y Cuerpos de Seguridad del Estado como las Fuerzas Armadas llevan años construyendo los vínculos necesarios para tener una conciencia situacional adecuada y actuar en consecuencia ante las amenazas. La empresa privada también ha adoptado iniciativas en este sentido, aprendiendo muchas veces según el método de ensayo-error.

Si se toma como referencia lo conseguido por otros países, se puede comprobar cómo España mantiene una progresión similar a la del resto de los de su entorno. En muchas ocasiones, siguiendo modelos similares a los establecidos por los que le precedieron, en otras tantas marcando la pauta que después están empezando a adoptar otras naciones y organizaciones internacionales.

En cualquier caso, en un entorno en el que las normas internacionales están todavía en vías de desarrollo y en el que la evolución de la tecnología a un ritmo de crecimiento exponencial marcan el camino a seguir en cada momento, no es ni fácil ni necesariamente deseable marcar siempre el ritmo. No resulta eficiente llevar una delantera significativa en el desarrollo de conceptos cuando no están aún clarificadas las reglas de juego o cuando las posibilidades que ofrece la tecnología permiten vías más rápidas o cómodas, o simplemente cierran puertas que estaban abiertas apenas unos meses antes.

15 La Estrategia Nacional de Ciberseguridad

La Estrategia de Ciberseguridad Nacional ha cumplido ya tres años, tiempo que algunos consideran más que razonable para remozarla (ORGANISATION…,

2012). Con sus virtudes y sus defectos (CHAMORRO, 2014), ha servido como guía para la construcción *ex novo* de todo el sistema de seguridad cibernética tal y como hoy lo conocemos. A pesar de ser un ámbito nuevo, la de ciberseguridad ha sido la segunda estrategia nacional sectorial que se ha finalizado, tras la de Seguridad Marítima, todo un logro teniendo en cuenta que se partía de un folio en blanco.

No se puede desdeñar el esfuerzo realizado en la elaboración del Plan Nacional de Ciberseguridad y de los Planes Derivados de cada uno de los sectores. En muchos casos, las soluciones a las que se ha llegado resultan únicas y han sido posibles gracias a la falta de referencias anteriores que condicionasen el trabajo. En otras, este condicionamiento venía de la mano de instituciones y organismos que desarrollaban su labor en campos distintos del de la ciberseguridad.

Se puede argumentar que no se ha seguido el modelo previsto en el capítulo cinco de la Estrategia *ad litteram*, o que el Consejo Nacional de Ciberseguridad no es un instrumento suficiente para la coordinación de todos los organismos implicados en el día a día. Siendo ambas afirmaciones ciertas, no lo es menos que buena parte de las organizaciones previstas en dicho capítulo y representadas en el Consejo nacieron de forma simultánea o posterior a la Estrategia y que han requerido de un periodo de tiempo prolongado para su puesta en marcha y para la definición de su funcionamiento interno en ausencia de antecedentes válidos.

A día de hoy se está en condiciones de acometer la siguiente evolución en el esquema relacional entre los distintos organismos respetando la idiosincrasia propia de la Administración española y las sensibilidades de cada uno de ellos. Las soluciones se han ido imponiendo durante estos años por la vía de los hechos y la tozudez de la lógica del sentido común.

16 Ciberseguridad

Desde la Fiscalía General y el Ministerio de Justicia, así como desde la sociedad civil, no se ha perdido ocasión para avanzar en la clarificación de los conceptos y de las ideas que deben guiar la generación de legislación y la interpretación misma de las leyes. A ese esfuerzo han contribuido de forma notable las Fuerzas y Cuerpos de Seguridad del Estado, como no podía ser de otro modo.

Estas mismas fuerzas policiales se han dotado de estructuras y de instrumentos altamente eficaces, como demuestran los resultados obtenidos en los ámbitos de la lucha contra el fraude, delitos económicos y de blanqueo de capitales, el terrorismo, los delitos de carácter sexual en internet, los atentados contra la propiedad intelectual y la piratería, y otros ilícitos.

Mención aparte merece la labor de concienciación desarrollada por el Cuerpo Nacional de Policía y por la Guardia Civil, tanto presencial en las aulas de los colegios y en otros foros, como virtual a través de las redes sociales[20]. Como se ha comentado, la concienciación y la "higiene" en las redes son la base para la consecución de una sociedad segura en el entorno cibernético (NATIONAL..., [20--?])[21]. Vistos con algo de perspectiva, los avances conseguidos en este campo son realmente notables en los últimos años en España. Tampoco puede dejar de mencionarse, en este aspecto, la tremenda labor desarrollada por el INCIBE (CONSEJOS..., [2014])[22]

La otra labor asignada a las Fuerzas y Cuerpos de Seguridad del Estado es la de la protección de las infraestructuras críticas. El CNPIC, partiendo de un núcleo reducido de personal y medios, ha conseguido aglutinar en torno a sí a las principales infraestructuras y servicios críticos, y elaborar protocolos y normativas que mejoren la seguridad de estos elementos esenciales para la sociedad.

A pesar de todo, la creciente conectividad asociada al internet de las cosas y a las iniciativas de varias ciudades de adoptar modelos de *smart cities* introduce cada día nuevos riesgos en la sociedad española y mundial. El grado de implicación de los españoles en las redes sociales y el altísimo índice de penetración de los dispositivos móviles en España, mientras que suponen todo un mundo de oportunidades para el desarrollo de las ideas y de la sociedad civil (cuyo aprovechamiento real sigue siendo cuestionable en el caso concreto español) también suponen vectores avanzados para las amenazas a la seguridad de la ciudadanía.

El grado de concienciación de la población varía grandemente en función de parámetros como la edad, la extracción social y cultural, y la digitalización de su actividad cotidiana. En general, no obstante, se tiende a infravalorar la amenaza y, sobre todo, sus consecuencias. Incluso para aquellos que son conscientes de vivir en la burbuja de cristal que es internet, Europa en general y España en particular carecen del grado de concienciación de otros países sobre la importancia de la

20 La cuenta de Twitter del Cuerpo Nacional de Policía mantiene más de 2,25 millones de seguidores, aventajando en más de medio millón a otros cuerpos policiales de mucha mayor entidad como el FBI en más de medio millón de seguidores <https://twitter.com/policia?lang=es>.

21 En este sentido, la Estrategia de Ciberseguridad Nacional de los Países Bajos ha considerado llegado el momento de evolucionar hacia una segunda versión (NATIONAL..., [20--?]) . En la primera se ponía el foco en la concienciación de la población, al entenderla como punto de partida fundamental. La segunda estrategia, probablemente una de las más avanzadas del mundo, incide ya en el desarrollo de capacidades.

22 El Instituto Nacional de Ciberseguridad ha puesto en marcha numerosas iniciativas de concienciación tanto entre empresas como entre particulares. Quizás una de las más llamativas sea la protagonizada por el monologista Leo Harlem (CONSEJOS..., [2014]).

preservación de la identidad digital y la criticidad de la preservación de la propiedad intelectual en el desarrollo de un modelo de negocio.

17 Ciberdefensa

La ciberdefensa en España ha sufrido una transformación radical en los últimos tres años, pasando de una mera gestión de la seguridad de la información a un desarrollado concepto de operaciones en el ciberespacio. Esta metamorfosis, liderada por el General Carlos E. Gómez López de Medina, Comandante del Mando Conjunto de Ciberdefensa desde su creación hasta el momento de escribirse estas líneas, ha contado en todo momento con el decidido apoyo del Ministro de Defensa y del Jefe de Estado Mayor de la Defensa, que han apostado por situar a la ciberdefensa en la mesa de planeamiento de las operaciones como un actor más.

En estos tres años no solo se han creado estructuras, acometido amenazas, establecido relaciones, habilitado infraestructuras, formado personal,... sino que también se ha generado doctrina, e incluso un léxico unificado del cual se carecía. Es difícil para cualquiera que llegue ahora al mundo de la ciberdefensa hacerse una idea del estado de la misma hace tan solo tres años.

18 Conclusiones

Más allá de las capacidades concretas de las que dispone el Mando -y que habrán evolucionado significativamente para cuando estas líneas se publiquen-, lo más importante es la integración permanente en el proceso de planeamiento de las operaciones que se ha conseguido. La interiorización de esta inclusión y su visualización como algo natural todavía llevará su tiempo. No obstante, el proceso está en marcha y es irreversible. Se ha conseguido erradicar la idea de que la ciberdefensa forma parte exclusiva del ámbito de las comunicaciones, o de la inteligencia, o de la comunicación pública, para imbuir a los mandos de las Fuerzas Armadas de la idea de que se trata de un arma combatiente más y que, como tal, debe estar integrada en el área de las operaciones, pero también tenida en cuenta en todas las demás.

Hoy España es uno de los países de referencia en cuanto a la doctrina, y la formación y adiestramiento en ciberdefensa. La presencia del Mando en foros nacionales e internacionales y la amplitud de su red de “amigos del Mando” le permiten no solo actuar decisivamente en tiempo de paz o de conflicto de forma decisiva, sino también generar sinergias con otros actores para aprovechar, en un modelo colaborativo, las capacidades de todos ellos.

En el mundo digital, no obstante, las capacidades obtenidas hoy no son garantía de nada para mañana. La necesidad de evolución es constante y el ritmo al que debe hacerse, equivalente al de la misma tecnología sobre la cual se basa su actividad.

La coyuntura socioeconómica en la cual tiene lugar el nacimiento del Mando Conjunto de Ciberdefensa dista mucho de ser la más favorable para la obtención de todos los recursos que le son necesarios. A pesar del esfuerzo que se ha hecho por parte del Jefe de Estado Mayor de la Defensa y del conjunto de las Fuerzas Armadas para dotar de personal y medios a este nuevo área, queda todavía un largo camino hasta que sus recursos estén a la altura de la importancia de su misión.

Por el momento, con recursos limitados, pero con una provisión inagotable de "lealtad, constancia, ingenio y destreza", como reza el logo de su escudo, el Mando ha conseguido colocar los cimientos de la ciberdefensa en España y contribuir activamente a la de su entorno aliado.

Referencias

ÁGREDA, Ángel Gómez de. El ciberespacio como escenario del conflicto: identificación de las amenazas. In: CENTRO SUPERIOR DE ESTUDIOS DDE LA DEFENSA NACIONAL (España). *El ciberespacio, nuevo escenario de confrontación.* [Madrid], 2012. Cap. 4. p. 167-204. (Monografías del CESEDEN, n. 126). Disponible en: <http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_CIBERESPACIO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf >. Fecha de acceso: 11 feb. 2016.

ALVAREZ, Darío Aurelio Abilleira. Teoría de los Cinco Anillos de John Warden. *Estrategia Uruguay*, [S.l.], 21 jun. 2014. Disponible en: <https://estrategiauruguay.wordpress.com/2014/06/21/teoria-de-los-cinco-anillos-de-john-warden-es-imposible-no-atacar-objetivos-civiles-se-trata-entre-otras-cosas-de-matar-muy-rapidamente/>. Fecha de acceso: 11 feb. 2016.

ASR. Organización del Servicio de Información de la Guardia Civil. *La pagina de ASR*, [S.l., 20--?]. Disponible en: <http://www.intelpage.info/organizacion-del-servicio-de-informacion-de-la-guardia-civil.html>. Fecha de acceso: 24 feb. 2016.

CARRILLO, Margarita Robles. Las Fuerzas Armadas ante el reto de la ciberseguridad. In: ENCABO, Sofía Olarte (Diret.); Linares, Ramón María Orza (Coord.). *Estudios sobre derecho militar y defensa*. Madrid: Thomson Reuters Aranzadi, 2015. p. 431-439.

CENTRO CRIPTOLÓGICO NACIONAL (España). *CCN-CERT*. Madrid, [20--?]. Disponible en: <https://www.ccn.cni.es/index.php?option=com_content&view=article&id=18&Itemid=22>. Fecha de acceso: 12 marzo 2016.

CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS (España). *CNPIC*: inicio. [S.l : 20--?]. Disponible en: <http://www.cnpic.es/>. Fecha de acceso: 05 marzo 2016.

CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL (España). Ministerio de Defensa. Madrid, [201-?]. Disponible en: <http://www.defensa.gob.es/ceseden/>. Fecha de acceso: 15 nov. 2015.

CHAMORRO, Enrique Fojón. Año I de la Estrategia de Ciberseguridad Nacional. *Real Instituto Elcano*, Madrid, 11 dic. 2014. Disponible en: <http://www.blog.rielcano.org/ano-de-la-estrategia-de-ciberseguridad-nacional/>. Fecha de acceso: 20 enero 2016.

CONSEJOS ciberseguridad con Leo Harlem. Produção INCIBE. [S.l., 2014]. 1 vídeo (2 min), color. Disponible en: <https://www.youtube.com/watch?v=nhDBD6UTDtM>. Fecha de acceso: 13 enero 2016.

CUERPO NACIONAL DE POLÍCIA (España). *Brigada de Investigación Tecnológica*. [S.l], 2016. Disponible en: <http://www.policia.es/org_central/judicial/udef/bit_alertas.html>. Fecha de acceso: 05 marzo 2016.

DÍAZ, Emilio Sánchez de Rojas. Cooperación internacional en temas de ciberseguridad. In: CENTRO SUPERIOR DE ESTUDIOS DDE LA DEFENSA NACIONAL (España). *Necesidad de una conciencia nacional de ciberseguridad*: la ciberdefensa, un reto prioritario. [Madrid], 2013. Cap. 5. p. 255-301. (Monografías del CESEDEN, n. 137). Disponible en: <http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/137_NECESIDAD_DE_UNA_CONCIENCIA_NACIONAL_DE_CIBERSEGURIDAD_LA_CIBERDEFENSA_UN_RETO_PRIORITARIO.pdf>. Fecha de acceso: 22 marzo 2016.

EL GOBIERNO constituye el Consejo de Ciberseguridad Nacional. *El País*, Madrid, 14 feb. 2014. Disponible en: <http://politica.elpais.com/politica/2014/02/14/actualidad/1392367698_347430.html>. Fecha de acceso: 12 marzo 2016.

ESPAÑA. Estado Mayor de La Defensa. *Mando Conjunto de Ciberdefensa*. Madrid, [20--?]a. Disponible en: <http://www.emad.mde.es/CIBERDEFENSA/>. Fecha de acceso: 02 marzo 2016.

_____. Ministerio de Defensa. Portal de Tecnología e Innovación. *Centros Universitarios de la Defensa*. Madrid, [20--?]b. Disponible en: <http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Presentacion/OrganizacionID/Paginas/CentrosUniversitarios.aspx>. Fecha de acceso: 15 nov. 2015.

_____. Ministério del Interior. Grupo de Delitos Telemáticos. *Home*. [S.l., 20--?] c. Disponible en: <https://www.gdt.guardiacivil.es/webgdt/home_alerta.php>. Fecha de acceso: 06 marzo 2016.

_____. Presidencia del Gobierno. *Estrategia de Ciberseguridad Nacional*. [Madrid], 2013. Disponible en: <http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf>. Fecha de acceso: 02 marzo 2016.

_____. Presidencia del Gobierno. *Estrategia de seguridad nacional*: un proyecto compartido. [Madrid], 2013. Disponible en: <http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf>. Fecha de acceso: 02 marzo 2016.

EUROPEAN DEFENCE AGENCY. *Activities Search*. [S.l.], 2015. Disponible en: <http://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence>. Fecha de acceso: 03 marzo 2016.

INSTITUTO NACIONAL DE CIBERSEGURIDAD (España). *Alerta temprana*. [S.l., 201-?] a. Disponible en: <https://www.incibe.es/CERT/Alerta_Temprana/>. Fecha de acceso: 15 marzo 2016.

_____. *Home*. [S.l., 201-?]b. Disponible en: <https://www.incibe.es/home/instituto_nacional_ciberseguridad/>. Fecha de acceso: 16 marzo 2016.

LÓPEZ, María del Mar. Plan nacional de ciberseguridad. In: JORNADA DE CIBERSEGURIDAD EN ANDALÚCIA, 2., 2015, Sevilha. *Anais*... Sevilla:
Ingeniería e Integración Avanzadas, 2015. Disponible en: <http://es.slideshare.net/Ingenia_es/mara-del-mar-lpezcibersegand15>. Fecha de acceso: 10 marzo 2016.

MANDO Conjunto de Ciberdefensa. Coprodução de El Mundo. Madrid, [20--?]. 1 vídeo (4 min), color. Disponible en: <http://videos.elmundo.es/v/0_1j7zvvnt-ciberdefensa?count=0>. Fecha de acceso: 24 feb. 2016.

MÁSTER en Ciberdefesa. Fundación In-Nova, Castilla-La Mancha, [20--?]. Disponible en: <http://masterciberdefensa.in-nova.org/>. Fecha de acceso: 23 feb. 2016.

NORTH ATLANTIC TREATY ORGANIZATION. *Federated Mission Networking (FMN)*. [S.l.], 2015. Disponible en: <http://www.act.nato.int/fmn>. Fecha de acceso: 03 marzo 2016.

NATIONAL COORDINATOR FOR SECURITY AND COUNTERTERRORISM (Nederland). *National Cyber Security Strategy 2*: from awareness to capability. Den Haag, [20--?]. Disponible en: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf >. Fecha de acceso: 20 marzo 2016.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Cybersecurity policy making at a turning point*: analysing a new generation of national cybersecurity strategies for the Internet economy. [S.l], 2012. Disponible en: <https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf>. Fecha de acceso: 23 marzo 2016.

PAVEL, Barry; ENGELKE, Peter; WARD, Alex. *Concepto que se recoge mucho después*. Washington, DC: Atlantic Council, 2016. (Atlantic Council Strategy Paper, n. 1). Disponible en: <http://www.atlanticcouncil.org/publications/reports/dynamic-stability-us-strategy-for-a-world-in-transition>. Fecha de acceso: 05 marzo 2016.

PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. *Aprobada la Estrategia de ciberseguridad nacional*. [S.l], 2013. Disponible en: <http://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2013/Diciembre/Noticia_2013-12-10_Estrategia_Ciberseguridad_nacional.html#.VtxJNZzhCCg>. Fecha de acceso: 02 marzo 2016.

ROBERTSON, Jordan; RILEY, Michael. Mysterious ’08 turkey pipeline blast opened new cyberwar. *Bloomberg*, [S.l.], 10 dic. 2014. Disponible en: <http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar >. Fecha de acceso: 23 marzo 2016.

SANDOVAL, Pablo Ximénez de. El FBI logra entrar en el iPhone de San Bernardino sin ayuda de Apple. *El País*, Los Angeles, 29 marzo 2016. Disponible en: <http://internacional.elpais.com/internacional/2016/03/29/estados_unidos/1459204906_761502.html>. Fecha de acceso: 10 marzo 2016.

UNIVERSIDAD AUTÓNOMA DE MADRID. *Programas de títulos propios*. Madrid, 2016. Disponible en: <http://www.uam.es/ss/Satellite/es/1242654675830/1242683206845/estudiopropio/estudioPropio/Master_en_Analisis_de_Evidencias_Digitales_y_Lucha_contra_el_Cibercrimen.htm>. Fecha de acceso: 23 feb. 2016.

WARDEN III, John A. *The air campaign*: planning for combat. [Washington, DC]: National Defense University Press Publication, 1988. Disponible en: <http://www.au.af.mil/au/awc/awcgate/warden/ward-toc.htm>. Fecha de acceso: 15 enero 2016.

LA CIBERSEGURIDAD Y CIBERDEFENSA EN EL CONTEXTO DE MÉXICO

Jesús García García*
Julio Cesar Mondragón Pérez**

1 Introducción

En todos los países del mundo, los sistemas y equipos informáticos se han convertido en una herramienta indispensable para el desarrollo; sin embargo, los ataques a los portales de internet en redes, sistemas y equipos informáticos, por parte de los denominados "hackers", quienes actúan individualmente o formando parte de alguna organización delictiva, siendo en este sentido las empresas, los bancos, el sector industrial, las fuerzas armadas y el gobierno, los más susceptibles de sufrir ciberataques; por lo cual las naciones han tenido la necesidad de establecer medidas de protección a su infraestructura cibernética dando origen a la creación de la ciberseguridad como mecanismo de protección del ciberespacio.

De tal manera que escuchamos cada vez con mayor frecuencia hablar de ciberespacio, de ciberseguridad, de ciberinteligencia y otros términos relacionados con la seguridad informática, al mismo tiempo que vemos en los medios de comunicación diversas noticias sobre el incremento de *hackeos*, fugas de información, robos de identidad y otros ataques a las redes informáticas.

Hoy en día las amenazas cibernéticas han evolucionado siendo que aquellas consideradas anteriormente como poco probables han empezado a ocurrir con mayor regularidad, este aumento en la tendencia se debe a la creación de herramientas y técnicas de ciberataques más maduras y complejas.

Los ataques recientes sucedidos han aumentado la preocupación sobre temas de amenazas avanzadas, por mencionar algunos casos ocurridos, tenemos:

✓ En marzo de 2011, Intento de hackeo a los sistemas de la empresa *Lockheed Martin* que desarrolla armamento para los EE.UU, y otros países. En enero de 2014, 110 millones de datos de tarjetas de crédito son robados a las tiendas departamentales Target.

* Militar Egresado del Colegio Militar y Escuela Superior de Guerra. Maestro en Ciencias Políticas con diversos estudios de especialización en los EE.UU. y Uruguay, ha participado en Congresos Y Seminarios Relativos a temas de Ciberseguridad Y Ciberdefensa. Contacto: <odinpazer@gmail.com>
** Profesor de la asignatura de Mando y Control del Centro de Estudios Superiores Navales de la Armada de México, egresado de la Maestría en Ingeniería en Aeronautica del Instituto Polititecnico Nacional (IPN) y de la Heroica Escuela Naval Militar. Contacto: <jcmpmara@gmail.com>

✓ En junio de 2014, la operación *dragonfly*, comprometió sistemas de empresas de los Estados Unidos de América, Francia, Italia y Alemania.

✓ En agosto de 2014, el banco J.P. Morgan, perdió *gigabytes* de información sensible de sus clientes, durante un ciberataque.

✓ En septiembre de 2014, en una forma de ataque muy similar al de Target, la cadena de tiendas Home Depot, reconoce el robo de información de 56 millones de tarjetas de crédito de sus clientes.

✓ En noviembre de 2014, se suscita un ataque informático a la empresa Sony, como reacción a la trama de una película, supuestamente efectuado por Corea del Norte.

✓ En Febrero de 2106, un grupo de hackers, efectuaron transacciones a cuentas privadas por un monto de US $101 millones de las reservas de divisas del Banco Central de Bangladesh.

✓ Por lo que se refiere a los ciberataques a instancias gubernamentales y militares tenemos:

✓ 1968, Alemania. La policía detiene un ciudadano de origen alemán oriental espiando una subsidiaria de International Business Machines (IBM) considerándose de los primeros casos de ciberespionaje.

✓ 1990, Robert Tappan Morris, pasante de ciencias de la computación, fue condenado de perpetrar un ataque a gran escala en sitios corporativos, universitarios y militares.

✓ 2007, Estonia. Alcanza gran desarrollo y dependencia del uso del internet, estableciendo en su población el uso de tarjetas de identidad con firma digital, votación electrónica municipal y federal, entre otras. Al reubicarse un monumento de la era soviética, surge una inconformidad de la minoría rusófona tras las cual hubo ataques cibernéticos de negación de servicio (D.O.S.) a los bancos, gobierno, servicios básicos e inhabilitación de los servicios críticos nacionales, creando caos en la población, se presume como perpetrador a Rusia.

✓ En agosto 2007. Reino Unido, Francia y Alemania acusan públicamente a China de diferentes ciberataques a su infraestructura cibernética.

✓ En noviembre 2007. Israel hackea los sistemas de defensa antiaérea de Siria y efectúa un ataque aéreo a la construcción de una planta nuclear retrasando su construcción.

✓ 2008, Irán. El virus Stuxnet ataca su planta nuclear en Natanz, la mayor ciberarma hasta entonces usada, atacó a la centrifugadora con software Siemens usada para enriquecer uranio, ocasionando el retraso en su construcción por más de dos años.

✓ En agosto 2008. Georgia, primera ciberguerra entre Georgia vs Rusia.

Ataque a los servidores gubernamentales del gobierno de Georgia en coordinación con el despliegue militar de Rusia.

✓ En junio 2013. Caso Snowden, Edward Snowden, exanalista de seguridad informática, reveló sobre las actividades de ciberespionaje o vigilancia electrónica de la *Agencia de Seguridad Nacional* (N.S.A.).

Del contenido de la información anterior podemos destacar algunos aspectos significativos: Primero, los países que se encuentran en conflicto, al realizar un ataque armado, lo anteceden y acompañan de ciberataques a sus sistemas o redes de armas y a la infraestructura estratégica del país objetivo; Segundo, los países que se encuentran en algún tipo de conflicto están constantemente realizando ciberataques entre ellos; los países potencia tienen grupos, algunos no reconocidos y otros reconocidos como cibercomandos, que elaboran y accionan ciberarmas con diferentes fines.

De lo anterior, se infiere que algunos Estados, a través de grupos reconocidos o no , se encuentra espiando y robando información significativa de países que consideran clave para sus intereses económicos, tecnológicos, geopolíticos y militares; por lo que el desarrollo de ciberarmas requiere de grandes inversiones, personal o grupos especializados y de objetivos específicos.

Todo ello obliga a países como México a desarrollar y fortalecer mecanismos de protección en el ámbito del ciberespacio, que conlleven a estar mejor preparados, anticiparse y en su caso atender en forma adecuada posibles ataques cibernéticos. ¡Estamos viviendo la era del Ciberespacio!

2 Normatividad en Materia del Ciberespacio

Internacionalmente hay esfuerzos por parte de algunos países y organismos internacionales de regular o legislar en relación al ciberespacio, en este ámbito tenemos que:

En 1980, la Organización para la Cooperación y Desarrollo Económico (OCDE) emitió directrices sobre política internacional de protección de la privacidad y los flujos transfronterizos de datos personales (ORGANIZACIÓN…, 2002).

En 2001, se firmó el convenio de Budapest, que trata sobre la ciberdelincuencia ante la necesidad de aplicar una política penal común con objeto de proteger a la sociedad frente a los ciberdelitos, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional (COUNCIL OF EUROPE, 2001).

En 2003, auspiciada por las Naciones Unidas se realiza en Ginebra, ac ogida por el gobierno de Suiza, la Primera Cumbre Mundial Sobre la Sociedad de la Infor-

mación (CMSI) con el propósito de construir la sociedad de la información como desafío global para el nuevo milenio.

En 2004, la Organización de Estados Americanos (OEA), estableció una Estrategia Interamericana Integral de Seguridad Cibernética, promoviendo a través del Comité Interamericano Contra el Terrorismo (CICTE) y del Programa de Seguridad Informática, Estrategias Nacionales Sobre Seguridad Cibernética, quedando plasmadas en la resolución AG/RES. 1939 (XXXIII-O/03), referida al desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética.

En 2005, igualmente auspiciada por las naciones unidas se realiza en Túnez, acogida por el gobierno de Túnez, la Segunda CMSI con el propósito de dar continuidad a la primera CMSI.

En 2014, se firma el Convenio Iberoamericano de Cooperación Sobre Investigación, Aseguramiento y Obtención de Prueba en materia de ciberdelincuencia y de la recomendación de la conferencia de los ministros de justicia de los países iberoamericanos relativa a la tipificación y sanción de la ciberdelincuencia.

En 2015, nuevamente auspiciada por las naciones unidas, se realizó la Tercera Cumbre Mundial Sobre la Sociedad de la Información, logrando definir la sociedad de la información que se convino internacionalmente con líneas para la creación de capacidad, diversidad cultural y la creación de confianza y seguridad en la utilización de las TIC (ZHAO, 2015).

Actualmente La Unión Europea, está legislando en materia de ciberespacio en lo relacionado al comercio en línea, dejando sin atender los aspectos que comprende a los campos social, político y militar [1].

Respecto a la normatividad aplicable en México, se tienen los fundamentos siguientes:

La Constitución Política de los Estados Unidos Mexicanos (CPEUM), establece atribuciones, funciones y responsabilidades para que el gobierno federal a través de sus dependencias promueva leyes que establezcan la normatividad para operar, controlar y supervisar las comunicaciones terrestres, marítimas, aéreas y de comunicaciones. (MÉXICO, 2014a)

La Ley Orgánica de la Administración Pública Federal (LOAPF), establece que a la Secretaría de Comunicaciones y Transportes (SCT) le corresponde, entre otras funciones: formular y conducir programas para el desarrollo de las comunicaciones; conducir la administración de los servicios federales de comunicaciones eléctricas y electrónicas, así como el procesamiento remoto de datos; otorgar concesiones y permisos para establecer y explotar sistemas de comunicación y procesamiento

1 Estrategia de ciberseguridad de la Unión Europea de 2013.

remoto de datos, así como vigilar el aspecto técnico del funcionamiento de tales sistemas; fijar las normas técnicas del funcionamiento del servicio público de comunicaciones; fomentar la organización de sociedades cooperativas cuyo objeto sea la prestación de servicios de comunicaciones (MÉXICO, 2014c).

Dentro del contexto de la Ley Federal de Telecomunicaciones y Radiofusión (LFTR), en su artículo 9, se reconoce al internet como medio de comunicaciones y obliga a la SCT a:

> Promover, en el ámbito de sus respectivas atribuciones, el acceso a las tecnologías de la información y comunicación y a los servicios de radiofusión y telecomunicaciones, incluido el de banda ancha e internet, en condiciones de competencia efectiva;
> Realizar las acciones tendientes a garantizar el acceso a internet de banda ancha en edificios e instalaciones de las dependencias y entidades de la Administración Pública Federal y coadyuvar con los gobiernos de la Ciudad de México, Estatales y Municipales para el cumplimiento de este objetivo;
> Establecer programas de acceso a banda ancha en sitios públicos que identifiquen el número de sitios a conectar cada año de manera progresiva, hasta alcanzar la cobertura universal. (MÉXICO, 2014b).

La Ley de Seguridad Nacional (LSN), en su artículo 5, considera como amenazas en contra de la seguridad nacional los actos tendentes a consumar espionaje, sabotaje, terrorismo, interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado mexicano; los actos que impidan a las autoridades actuar contra la delincuencia organizada y aquellos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada; que atenten en contra del personal diplomático, con la intención de consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva; en contra de la navegación marítima; financiamiento de acciones y organizaciones terroristas; dirigidos a obstaculizar o bloquear actividades de inteligencia o contrainteligencia, y los tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos (MÉXICO, 2005), los actos señalados indiscutiblemente que pueden ser perpetrados a través de ciberataques.

El Código Penal Federal (CPF), contempla los delitos informáticos que aun sin aludir específicamente al ciberespacio resulta aplicable, de igual manera la ley Federal de acceso a la información pública gubernamental, reglamenta sobre las medidas que deben seguirse en la Administración Pública federal para preservar la

confidencialidad, disponibilidad e integridad de la información.

Las metas nacionales y las estrategias transversales del Plan Nacional de Desarrollo (PND) son la base que fundamenta la actuación gubernamental para lograr "Un México en Paz", de acuerdo al objetivo 1.2 del mismo, garantizar la seguridad nacional; y de la estrategia 1.2.3, fortalecer la inteligencia del Estado mexicano para identificar, prevenir y contrarrestar riesgos y amenazas a la seguridad nacional; de las líneas de acción diseñar e impulsar una estrategia de seguridad de la información y la de fortalecer las operaciones de seguridad del ciberespacio y ciberseguridad (MÉXICO, 2013, p. 107).

De la misma manera el programa para un gobierno cercano y moderno del mismo PND, establece una estrategia digital nacional que acelere la inserción de México en la sociedad de la información y del conocimiento, así como impulsar la seguridad de la información dentro de los sistemas y aplicaciones de las dependencias y entidades, para fortalecer la seguridad cibernética y la gobernanza en internet (MÉXICO, 2013).

El Programa para la Seguridad Nacional 2014-2018 (PSN), considera a la ciberseguridad como una amenaza a la seguridad nacional, indicando que el incremento de los ataques en contra de la infraestructura crítica, los intereses económicos, las redes de información y las capacidades de defensa de naciones específicas, demuestra que existen gobiernos, grupos criminales y organizaciones terroristas dispuestas a explotar el ciberespacio con propósitos hostiles. Señalando que para hacer frente a este tipo de amenazas, es necesario que México redoble sus esfuerzos en materia de ciberseguridad.

La Agenda Nacional de Riesgos 2013-2018, contempla atender la vulnerabilidad cibernética del Estado mexicano, definiendo la Estrategia Nacional de Seguridad de la Información establecida por la presente administración federal, la cual se encuentra aun en desarrollo y tiene como objetivo: garantizar la integridad, confidencialidad y disponibilidad de la información de las personas e instituciones públicas y privadas de México; asignando responsabilidades a las instancias de Seguridad Nacional en el sentido de proteger la gestión de la información vinculada de manera directa o indirecta con el mantenimiento de la integridad, estabilidad y permanencia del Estado mexicano. Referida Estrategia contempla las siguientes líneas de acción al interior de las dependencias de Seguridad Nacional:

- Implementación y/o fortalecimiento de un sistema de gestión de seguridad de la información.
- Crear y en su caso desarrollar un área responsable de la seguridad de la información.

- Desarrollar un equipo de respuesta a incidentes de seguridad cibernética.

En repuesta a la vulnerabilidad cibernética que hoy en día está presente en todos los niveles de gobierno y de la sociedad en general, las fuerzas armadas mexicanas han realizado acciones en materia de seguridad de la información, ciberseguridad y ciberdefensa con el fin de consolidar las actividades que se desarrollan empleando como medio el ciberespacio, por lo que en sus programas sectoriales han definido estrategias y líneas de acción para fortalecer sus capacidades en materia de ciberseguridad y ciberdefensa.

El Programa Sectorial de Defensa Nacional 2013-2018 (PSDN). En la línea de accion 2.1.10, y la meta No. 6, manifiesta la necesidad de fortalecer la infraestructura y las TIC, que permitan materializar cada fase del ciclo de la información de manera ágil y segura. Adicionando que se requiere continuar promoviendo mecanismos de intercambio de información con organismos castrenses de países amigos, en un ámbito de respeto para generar confianza y seguridad mutua.

El PSDN refiere que la seguridad en el ciberespacio en México debe ser abordada desde el punto de vista de la defensa nacional, ya que inicialmente solo se ha atendido desde el ámbito de la seguridad institucional y persecución del delito.

El Plan Sectorial de la Secretaría de Marina (PSM), contempla una estrategia enfocada a consolidar y modernizar el sistema integral de seguridad de la información y fortalecer la seguridad de las infraestructuras críticas de la información, con prioridad a incrementar las capacidades de ciberseguridad y ciberdefensa a través de la construcción de un centro de control de ciberdefensa y ciberseguridad; adquirir la infraestructura tecnológica para implementar acciones de ciberseguridad en el ciberespacio; e implementar una estrategia de ciberdefensa.

3 Marco Conceptual

3.1 El Ciberespacio

El glosario de términos homologados SEDENA-SEMAR 2014 (MÉXICO, 2014e), define al ciberespacio como el dominio intangible soportado por las tecnologías de la información y comunicación (TIC), que con programas informáticos, utilizando el espectro electromagnético, se comunican, intercambian datos e información a través de sus redes, ya sea entre personas, computadoras o sistemas.

Sergio Castro Reynoso, en su libro “Principios de la Ciberguerra. Una Guía para Oficiales Militares”, contextualiza el ciberespacio como un campo de batalla

para las guerras modernas, donde se tiene que aplicar las doctrinas de guerra, su planeamiento, métodos, técnicas y tácticas pero adecuadas a este nuevo dominio. Lleva desde la ubicación del centro de gravedad del enemigo en el ciberespacio, pasando por describir de manera general a lo particular de la arquitectura, las fases, y tácticas hasta llegar a la creación de un cibercomando para hacer frente a las ciberamenazas (REYNOSO, 2015).

Podemos considerar al ciberespacio como el conjunto de redes de comunicaciones y ordenadores existentes a nivel mundial que se encuentran interconectados directa o indirectamente entre sí. En ocasiones, este término se suele acotar y centrar en internet, pero durante el análisis del mismo, el término se ha utilizado en el sentido más amplio; Según la compañía especializada en integración de sistemas (SISCO), se considera al ciberespacio como un dominio universal, en el que se encuentran conectados actualmente 8.7 billones de aparatos, estimándose que, para el 2020, estén conectados 40 billones de dispositivos.

Hay que tomar en cuenta que en los conflictos tradicionales normales existen fronteras y límites, mientras que en el ciberespacio no, para realizar un ciberataque no es necesario desplazarse, moverse o tener que pasar una frontera. Esta 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 fácilmente clandestino.

En el ámbito de la defensa se tenían claras las tres dimensiones en las que se realizaban las operaciones: tierra, mar y aire añadiendo el espacio exterior como una cuarta dimensión para algunos países desarrollados. En los últimos tiempos ha surgido una nueva dimensión donde pueden materializarse diversas amenazas. Hoy en día debemos hablar de una dimensión adicional y más intangible que las anteriores… ¡El ciberespacio!

3.2 La ciberseguridad

El PSDN, señala que a fin de alcanzar el objetivo final que es un “México en paz” para lograrlo entre otros aspectos, se requiere considerar la inteligencia como centro de gravedad de las operaciones, comprendiendo el uso de la ciberseguridad como elemento fundamental del ciberespacio.

En tanto que el PSM, establece la definición de ciberseguridad como 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 ciberespacio.

El glosario de términos homologados SEDENA-SEMAR 2014, refiere a la ciberseguridad como el conjunto de controles, procedimientos y normas del Estado para proteger y asegurar sus activos en el ciberespacio (MÉXICO, 2014e). Es decir comprende la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o riesgos provenientes del ciberespacio.

El Centro de Inteligencia para la Seguridad Nacional (CISEN), define el ciberespacio como 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 se utilizan para proteger lo que se resguarda o interactúa en el ciberespacio; el CISEN establece que es la protección de datos, información y sistemas conectados a Internet (ACOSTA et al., 2009, p. 149).

Por lo anterior, podemos concluir que la ciberseguridad puede ser conceptualizada como la habilidad de proteger o defender el uso del ciberespacio de ciberataques, con el objeto de evitar el acceso, uso, alteración modificación, extracción o destrucción no autorizada de la información almacenada electrónicamente. Mencionados actos indiscutiblemente que pueden ser perpetrados a través de ciberataques, tipificándose como ciberdelitos. Tomando en cuenta que la ley en la materia, considera como seguridad nacional las acciones destinadas a la protección del Estado mexicano frente a las amenazas o riesgos que enfrente nuestro país. Por lo cual se debe considerar el uso del ciberespacio como asunto de seguridad, desarrollo y defensa nacionales.

3.3 La ciberdefensa

En el nuevo concepto de Ciberdefensa de la OTAN, se define la protección de las redes de la OTAN como una responsabilidad fundamental de los aliados, por lo que la OTAN utilizará los procesos de planeamiento de la defensa para promover el desarrollo de las capacidades de Ciberdefensa de los aliados (IEEE 2011) (NEWCOM-BE, 2011).

La OTAN ha conceptuado la ciberdefensa como la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques (MC0571-NATO Cyber Defence Concept) (LUII-JF, 2012). En donde el propósito y prioridad de la ciberdefensa es mantener fuera de los sistemas a los intrusos que pretenden realizar ciberataques en contra de la infraestructura crítica.

El glosario de términos homologados SEDENA-SEMAR 2014, considera a la Ciberdefensa, como el conjunto de acciones, recursos y mecanismos del Estado en

materia de seguridad nacional para prevenir, identificar y neutralizar toda ciberarma o ciberataque que afecte la infraestructura crítica nacional (MÉXICO, 2014e). El grupo de ciberdefensa de la SEDENA, considera que la ciberdefensa es un tema de seguridad nacional, debido a que las acciones que se realizan en este marco, buscan proteger infraestructuras críticas, datos, e información cuya afectación puede impactar seriamente a las actividades sustantivas del país.

Estadísticamente, según *Kaspersky*, las estrategias de ciberdefensa están distribuidas de la siguiente manera: forensia [2] de ataques para ganar inteligencia en prevención de ataques 14%; obtención de nueva tecnología para identificar y entender ataques en progreso 18%; renovar los procesos internos, estrategias y acercamientos 19%; educación y entrenamiento del personal 19%; y obtención de nueva tecnología defensiva para evitar intrusos 25% (KASPERSKY LAB, 2015).

En tal sentido se debe considerar que no existe la protección de la información y/o datos al 100% ya que se tendrían que sacar en su totalidad de la red y con esto no estarían disponibles, constituyendo esto como una característica del ciberespacio, la disponibilidad; el diseño de la ciberdefensa estriba en lograr el equilibrio entre las tres características principales del ciberespacio, la confidencialidad, integridad y disponibilidad que se quiere para esa información. Otra variable a tomar en cuenta para la ciberdefensa es el presupuesto que se asigna para implementar las medidas de ciberdefensa, ya que de este dependerá la calidad del mismo, dicho de otra manera, se puede dar más seguridad a la red, no al 100% pero si más que otras compañías, así el tiempo y esfuerzo de un hacker es menos eficiente en comparación con otras empresas además de que estas últimas, al presentar objetivos más fáciles para el hacker, preferirán hacerlo con las que facilitan el intento (REYNOSO, 2013, p. 47-48).

Los ciberataques se concretan en el ciberespacio con la intención de denegar el servicio, espiar, tomar el control de una computadora, dispositivo de comunicación (celular), sistema, comunicación o control, se realizan con base a estrategias y tácticas que involucran procesos de planeamiento para, dentro de un sistema, seleccionar sus debilidades para la implantación de una ciberarma eficiente, que logre los resultados buscados.

3.4 La ciberguerra

Se considera la ciberguerra, por analogía, como el empleo del ciberespacio como teatro de operaciones de guerra (MÉXICO, 2014e).

2 Técnica digital para proteger a las empresas, entidades gubernamentales, etc., de la mala utilización de sus sistemas informáticos.

La ciberguerra se caracteriza por ser de bajo costo, evolución tecnológica con constante, no tiene fronteras por actuar en el ciberespacio, dificulta el manejo de su percepción, tiene deficiente inteligencia estratégica, dificultad de alerta táctica y evaluación del ataque y posee dificultad para el establecimiento y mantenimiento de coaliciones con otros países y vulnerabilidad del territorio del Estado.

A partir de la postguerra fría se plantea una nueva tipología de batalla que se describe por el empleo de computadoras y la comunicación en red para atacar a un enemigo mediante el empleo de información con fines psicológicos y de desarticulación logística, o bien, hacer uso de las tecnologías de la información para la organización estratégica, operacional y logística de los diversos componentes.

Richard Clarke menciona que la ciberguerra son las acciones llevadas a cabo por un Estado para penetrar las computadoras, redes o sistemas de otro país con el propósito de causar daño o disrupciones (CLARKE; KNAKE, 2011, p. 6) o componente de las operaciones en el ciberespacio que extiende el poder cibernético más allá de los límites de la defensa del ámbito cibernético propio, para detectar, detener, denegar, y nulificar a los adversarios.

La ciberguerra también crea disrupciones en los sistemas vitales del enemigo con el fin de anular sus capacidades de acción. El blanco principal de los ciberataques son los servidores, un blanco secundario de los ciberataques son las computadoras personales (PC) por carecer estas de las medidas de seguridad apropiadas por parte de los usuarios y por no seguir las reglas básicas de seguridad informática; otro blanco lo constituyen los sistemas de supervisión, control y adquisición de datos *(SCADA, Supervisory Control And Data Adquisitión)*, por ser estos parte de los sistemas que son controlados remotamente por computadoras para la administración de sistemas de control industrial, máquinas y sistemas eléctricos, en otras palabras son interfaces entre el ciberespacio y el mundo físico considerándose los blancos más valiosos en una ciberguerra y por último, los celulares que se han convertido en dispositivos esenciales para la comunicación de todo tipo de personas.

Esta nueva forma de enfrentamiento solo requiere una computadora conectada a internet y un objetivo. En este sentido se aleja de la concepción moderna de guerra tradicional. En la ciberguerra no es fundamental ni el tiempo, ni el espacio, ni el clima, ni el arsenal, ni el número de tropas, ni la movilización, ni las pérdidas de vidas humanas.

Estos hechos, nos demuestran una realidad, hoy los ciberataques, son más intensos, los ciberatacantes tienen más recursos y nuevas motivaciones, ya no son solamente *hacker´s* y grupos activistas, se les ha unido el crimen organizado trasnacional, grupos extremistas terroristas, e incluso simpatizan con gobiernos de algunas naciones.

Las estrategias que utilizan son más complejas y de largo plazo, utilizan múltiples pasos previos para llegar a su objetivo, combinan diversas técnicas de exploración y de evasión, emplean *malware* avanzado, así como diversos mecanismos cibernéticos para pasar desapercibidos.

3.5 Las ciberamenazas

Causa potencial en el ciberespacio con capacidad de provocar un efecto adverso (MÉXICO, 2014E), mediante un ciberataque, usualmente perpetrado por hackers, delincuentes comunes, *malware* de propagación (*gusanos, bots etc*.), atacantes internos, personal descontento, personal realizando actividades no autorizadas (acceso a Internet), inteligencia corporativa, contratistas, servicio de inteligencia extranjero, crimen organizado, terroristas, manifestantes, activistas (medioambientalistas, políticos, pro derechos de los animales) que a través del ciberespacio, con motivos específicos, buscan causar daño a la infraestructura.

3.6 El Ciberterrorismo

Para México no existe un término legal específico que tipifique el delito de ciberterrorismo; sin embargo los capítulos VI y VI BIS del Código Penal Federal, establecen el delito de terrorismo donde este puede quedar encuadrado.

Son los ataques y amenazas en contra de computadoras, redes e información con el propósito de intimidar o coaccionar a un gobierno o a una población en favor de un propósito político, ideológico o religioso (DENNING, 2000). Tomado de la exposición de Dorothy E. Deening para el *Special Oversight Panel on Terrorism*, Committe on Armed Services de la cámara baja de los EE.UU.

3.6.1 El Hacker

Es un individuo con conocimientos especiales en informática capaz de crear *software y hardware* para computadoras o acceder y manipularlas, para que realicen nuevas funciones o acondicionarlas, aprovechando las vulnerabilidades de las computadoras para tener dominio sobre ellas (ACOSTA et al., 2009, p. 149).

3.6.2 .El Cracker

Es un individuo que con fines ilegales, conocimientos especiales en informática capaz de crear *software y hardware* para computadoras o acceder ilegalmente y manipularlos,

para que realicen nuevas funciones o acondicionarlas, aprovechando las vulnerabilidades de las computadoras para tener dominio sobre ellas (ACOSTA et al., 2009, p. 149).

4 Retos y Desafíos a la Ciberseguridad y Ciberdefensa

4.1 Las nuevas amenazas [3].

Una de las ciberamenazas más sofisticadas hoy en día son las amenazas persistentes avanzadas (A.P.T. Advanced Persistant Threats) cuyo objetivo es robar, por un tiempo prolongado, información valiosa de una organización determinada. Los ataques utilizan múltiples métodos para vulnerar a la organización objetivo, uno de ellos es el *spearphishing* dirigida a un blanco específico, que a través de enviarle un correo con un contexto los vuelve muy creíble y con un alta probabilidad de que el usuario lea el correo en cuestión y abra el anexo que previamente ha sido contaminado.

Una vez que el blanco es vulnerado se crean puertas traseras (*backdoors*) que permiten al atacante tener acceso continuo hacia los sistemas comprometidos. El atacante, a continuación, busca expandir su alcance tomando control de más equipos para afianzar su permanencia, con lo cual, si es exitoso, logra mantener el acceso a los sistemas del cliente por largos períodos, con el fin de recolectar más información sobre el blanco, realizar más ataques (movimientos laterales) hasta que logre tener acceso a la información objetivo y la extraiga (exflitración).

Estos ataques típicamente se organizan a través de "campañas", las cuales pueden estar conformadas, a su vez, por una o más operaciones, y cada operación suele tener las siguientes fases:

- ✓ Preparación.
- ✓ Infección.
- ✓ Expansión y consecución de la persistencia.
- ✓ Búsqueda y extracción de información.
- ✓ Limpieza.
- ✓ Mayores vulnerabilidades [4]

Las vulnerabilidades son las debilidades de seguridad de nuestro sistema, entendiendo por sistema desde una P.C. o SMARTPHONE, hasta toda una organización junto con su infraestructura de cómputo y comunicaciones, aplicativos y servicios del negocio, así como la información involucrada en lo anterior.

3 Informe anual de ciberseguridad del Centro de ciberseguridad SCITUM-TELMEX, 2013.
4 Ibid.

Hoy tenemos muchos más elementos de *hardware y software* que proteger para evitar intrusiones. Dado que casi todas las vulnerabilidades tecnológicas están asociadas con el *software*, ahora:

Se tienen más piezas de *software* ejecutándose en servidores, PC., Laptops, Tabletas, teléfonos inteligentes, automóviles y crecientemente en las cosas (lo que se ha llamado el internet de las cosas, refrigerador, sistemas inteligentes y sensores en distintos dispositivos u objetos incluyendo relojes y ropa inteligente).

Todo está interconectado y es muy difícil, a veces imposible, distinguir dónde termina una red y empieza la otra, algo que se ha llamado el "PERÍMETRO BORROSO" de las nuevas redes.

La complejidad de las tecnologías ha crecido: servidores (virtualizados y no) con distintas naturalezas (base de datos, aplicaciones, servicios como DNS, directorio activo, etc.), *routers*, *switches*, balanceadores, aceleradores de tráfico (distintos tipos), arquitecturas de nubes privadas y públicas, *software* intermediario (middleware de diversas aplicaciones), aplicaciones móviles, etc.

Los ciberataques más comunes son:

✓ La denegación de servicios, siendo el activo más preciado los sistema *SCADA* (Supervisión Control y Adquisición de Datos), por el daño que a través de estos se puede lograr en la infraestructura crítica;

✓ El ciberespionaje para obtener información de tecnología, militar, económica y política;

✓ El ciberterrorismo para realizar actos de sabotaje;

✓ La ingeniería social para el robo de identidad, información o introducción de *bots*; el lavado de dinero, extorsión, presión, disuasión;

✓ El fraude financiero. Las ciberarmas más comunes para realizar ciberataques son: las consideradas de bajo costo *Xtunet, malware,* gusanos, troyanos, bots, DOD, pishing/pharming para robo de identidad y fraude, *script*, chantaje, *spam*, URL maliciosos y *ransomware/cryptoLocker*.

El ataque dirigido. Comienza cuando un atacante inicia un phishing contra un usuario, este se hace a través de archivos contaminados, el usuario inadvertidamente abre los archivos adjuntos, el sistema objetivo es invadido y comprometido, es extraída la información del sistema objetivo y, a la vez, una herramienta de administración remota (RAT) es descargada en el sistema objetivo, haciendo una red contaminada, el RAT es utilizado para atacar otras computadoras del sistema; los datos son extraídos de las demás computadoras contaminadas.

Los principales desafíos que la actual administración tiene que enfrentar en materia de ciberseguridad comprenden: adoptar acciones para la fusión de inteligencia convenientes, mediante un ente que articule la información gubernamental, que le dé sentido

y dirección a la actividad de inteligencia y que coadyuve en las decisiones que tienen que ver con las ciberoperaciones, y sobre todo la creación de un CERT-NACIONAL.

La creación de un Centro de Respuesta a Incidentes en Cómputo (CERT) Nacional, con la participación de las instancias que tienen responsabilidades en la seguridad nacional del Estado mexicano, con base en una organización que brinde seguridad a todos los elementos y sus interconexiones.

El desafío del ciberespacio esta manifiesto en el actual momento mexicano en una serie de activos y retos en donde se requiere otorgar el lugar que corresponde a lo ciber, una nueva dimensión de lo estratégico prioritario, considerando que: En el diseño de la Ciberseguridad requerimos de políticas públicas de Estado, estrategias para recolección, análisis y contrainteligencia de la información, para instrumentar operaciones, abiertas o encubiertas, acordes a las políticas de seguridad nacional. (ROSALES, 2014a, 2014b).

La posición estratégica de México está vinculada y condicionada por la relación con Estados Unidos, no obstante, México debe desarrollar políticas de desarrollo y seguridad autárquicas, como las que en su momento Japón o Alemania implementaron y actuar de manera racional y estratégica en la realidad mundial. Atender sus comunicaciones, por ejemplo, aun cuando sea en 20, 30 ó 50 años, es prioritario. (ROSALES, 2014a).

Fomentar visiones estratégicas y regionales y así enfrentar la idea de que Latinoamérica no sabe qué quiere y cómo lograrlo, que no se halla aún. Mirar el horizonte como futuro promisorio. No voluntarista, sino realistamente.

Afianzar una política exterior que sin estar subordinada ni enajenada en contenido y futuro a los EE.UU., se complemente fortaleciendo nuestros objetivos estratégicos, con nuestros intereses vitales mutuos, de común Defensa Estratégica en todos los campos de la producción humana. Así, con la estrategia en el ámbito del ciberespacio, atendemos de lo local a lo global.

Dadas las características relevantes de nuestras instalaciones estratégicas, en la cuenca mexicana del Golfo de México y en los centros de telecomunicaciones, es importante considerar un Centro de Gravedad estratégico. La ciberdefensa en plenitud.

Asistimos a la competencia por mercados, batalla anticipada de futuras guerras comerciales, antesala a conflictos bélicos. Cibercompetencia geoestratégica.

No solo los recursos que se tienen, sino también de lo que se carece, debe estar en una visión Geoestratégica, para dar impulso a una posición Geopolítica. La ciberdefensa y la ciberseguridad alcanzan estos campos.

Como elementos condicionantes de negociación y coacción, de conflictos latentes y manifiestos en el mundo. El petróleo y el gas siguen siendo elementos de inobjetable valor estratégico, determinantes en el desarrollo industrial y la geo-

política mundial, seguidos de los productos agrícolas y el agua. Sin embargo, cada segundo, el dominio de la tecnología, del conocimiento, va colocando la primacía en un saber basado en la idea, el diseño, la innovación, dejando la producción en otros países, con la consecuencia del costo en empleos de maquila e ingresos bajos, contaminación ambiental y limitación al desarrollo. Revalorar la ciberestrategia nacional.

Toda decisión beneficia a unos y perjudica a otros. Hay riesgos probables o posibles, el primero es cuantificable, el segundo puede o no puede aparecer, aunque las circunstancias hacen que lo posible o latente se vuelva manifiesto y lo probable se acerca a lo necesario.

5 Centros de Ciberseguridad

5.1 Infraestructura con la que cuenta la iniciativa privada como instancia a la vanguardia en materia de ciberseguridad.

Dentro de la iniciativa privada (IP), Teléfonos de México (TELMEX), creó una empresa denominada Centro de Ciberseguridad de TELMEX designado (SCITUM-TELMEX), el cual ofrece servicios de protección cibernética contra ciberataques que pudieran afectar a los organismos denominados "cliente" (CERT´s públicos y privados, centros de inteligencia de amenazas de fabricantes especializados, entidades para el cumplimiento de la ley, universidades, Bolsa de valores y banca de organismos tanto nacionales como internacionales).

Como parte de su estrategia de este Centro, cuenta con tres ejes principales que permiten a la empresa ofrecer a los clientes servicios altamente especializados: personal certificado y especializado, laboratorios avanzados (SCILabs® -Scitum Cyber Intelligence Laboratories-) y un ciberecosistema para la colaboración. Su portafolio consta de varios grupos de servicios tales como: Diagnóstico y Protección contra Amenazas Avanzadas, Servicios Forenses Avanzados, Gestión Continua de Ciberriesgos basada en Inteligencia y Ciberinteligencia. En este Centro de Ciberseguridad se realizan:

- ✓ El monitoreo 24x7 de los distintos componentes tecnológicos habilitados en las redes de los clientes de Telmex, así como de aquellos habilitados dentro del propio Centro.
- ✓ Procesos de investigación y análisis de información para el envío de alertas tempranas y la prevención sobre posibles ciberamenazas.
- ✓ Se coordinan los esfuerzos de los diversos grupos involucrados en la contención y remediación en su caso de una contingencia cibernética.

✓ Se realizan análisis avanzados con el fin de identificar y entender los rastros y comportamientos del *malware* así como sus mecanismos de infección, persistencia, evasión y comunicación C&C (Command & Control).

Además de ello y como consecuencia del avance en las tecnológicas de la información se han creado empresas que ofrecen servicios y soluciones en internet mediante la implementación de centros de fusión de datos cuya función es la de recibir, analizar, ordenar y normalizar datos, imágenes y videos provenientes de diferentes fuentes e instancias.

Entre estas empresas destaca Postech, de México, empresa 100% mexicana cuya función principal es la construcción de centros de monitoreo y seguridad cibernética, ofreciendo soluciones a empresas y dependencias gubernamentales y de la iniciativa privada en México, Centro y Sudamérica, entre las que se cuentan instituciones financieras, fuerzas armadas, sistemas de ciberseguridad para gobiernos de diferentes países a fin de fortalecer su sistema de seguridad gubernamental de los países.

5.2 Estructura y acciones por parte de las autoridades para el fortalecimiento de la ciberseguridad

Diversos países cuentan o bien están estructurando, dentro de sus gobiernos, cibercomandos, agencias o centros especializados en el ámbito del ciberespacio para fortalecer su ciberdefensa Con el fin de proteger sus infraestructuras críticas, previendo ataques, denegación de servicio, espionaje, *hackeo*, robo de información y afectación a sus redes sociales; regular el uso del ciberespacio; analizar y recuperar su infraestructura ante ciberataques; fomentar la ciberseguridad y cibercultura en todo su contexto; así como el desarrollar métodos, técnicas e instrumentos para estar en capacidad de efectuar ciberataques a naciones o grupos antagónicos, considerando en ellos la multidimensionalidad así como los diferentes campos de poder.

De acuerdo al reporte de *Symatec*[5] 2013, México se encuentra en el lugar 25 del *ranking* mundial, como de los países más susceptibles a recibir ciberataques. En los reportes de *Symatec* se muestra que en el 2013 los ciberataques en México crecieron 113% respecto al 2012, y que en el 2014 crecieron un 300% con respecto al año anterior, distribuidos de la siguiente manera: 39% a las organizaciones académicas, 31% contra instituciones gubernamentales, 26% contra entidades del sector privado, y 4% contra otras entidades (NORTON SEGURID, [2014?]).

5 Corporativo internacional, con base en California EE.UU., diseña y vende software informático dirigido a la ciberseguridad.

Los factores que más influyen en estos ataques por la vulnerabilidad cibernética son: legislación inadecuada, falta de estrategias nacionales e interinstitucionales que integren al gobierno, iniciativa privada, academia y sector público en una doctrina de ciberseguridad y ciberdefensa, así como accesos indiscriminados a recursos informáticos.

Para prevenir los ciberataques constituidos a su vez por los ciberdelitos, según *Kaspersky*, internacionalmente se tiene la estadística de que, el costo del ciberdelito asciende a 113 MMD, de los cuales les corresponde a México 3 MMD de costo del ciberdelito con una afectación de 10 millones de habitantes. De estos el 83% de estos corresponde al fraude y robo de información, sumando el fraude 38%, robo 21%, reparaciones 24% y otros 17%, los bancos han reportado pérdidas anuales de 93 millones de dólares (KASPERSKY LAB, 2015).

Con el fin de regular el uso del ciberespacio, en 2010, el Consejo de Seguridad Nacional (C.S.N.), creo un Comité Especializado en Seguridad de la Información con la participación de las dependencias que integran el mismo.

Como parte de la ciberdefensa, para contener los ciberataques de diferente índole; se implementó un Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX) al interior de la Policía Federal (PF).

En tanto que la Universidad Nacional Autónoma de México dispone del Centro de Respuesta a Incidentes de Seguridad en Cómputo (UNAM-CERT). Localizado dentro de la estructura de la Coordinación de Seguridad de la Información de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM. Está conformado por personal profesional especialista en seguridad en cómputo. Este equipo da respuesta a ciberataques, difunde información y alertas de vulnerabilidades cibernéticas e investiga para fortalecer la seguridad en el ciberespacio. Coordina con CERT-MX, SEDENA y SEMAR en lo relativo a incidentes e información cibernética

Se encarga de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de un ciberataque, así como publicar información respecto a vulnerabilidades de ciberseguridad, alertas de la misma índole y realizar investigaciones de la amplia área cibernética y así ayudar a mejorar la seguridad de los sitios.

De igual forma en las diversas instancias del gobierno federal se han puesto en marcha diversos esquemas de capacitación y formación de cuadros especializados en materia de ciberseguridad y ciberdefensa, enfatizando que durante la presente administración se trabajará activamente en el desarrollo y actualización del marco jurídico en materia de la seguridad de la información y ciberdefensa, así como en la prevención, investigación y sanción de delitos cibernéticos a fin de responder a estándares de excelencia y mejores prácticas internacionales.

6 El desarrollo de las Capacidades de Ciberdefensa de las Fuerzas Armadas

Al inicio de la presente administración como una preocupación del Alto Mando del Ejército y Fuerza Aérea para determinar y desarrollar las capacidades de ciberdefensa de la Secretaría de la Defensa Nacional (SEDENA), se integró un grupo de trabajo para la "Integración de un Programa General para el Desarrollo de la Ciberdefensa en el Ejto- Y FAM" con funciones adicionales de gestión y coordinación de los proyectos, del programa se desprendieron las siguientes líneas de acción:

- ✓ Promover políticas públicas para la defensa del Estado mexicano en el ciberespacio.
- ✓ Determinar la forma en que las fuerzas armadas cumplirán sus misiones generales en el ciberespacio, como nueva dimensión de la guerra.
- ✓ Definir el tipo de operaciones militares en base a las actividades relacionadas a al ciberespacio
- ✓ Identificar su relación con la actuación de las otras armas y servicios.
- ✓ Crear o reestructurar organismos para la ejecución de las operaciones en el ciberespacio
- ✓ Dotar a los organismos encargados de las operaciones de ciberdefensa que se definan, con la capacidad técnica y capital humano para la materialización de las nuevas operaciones militares.

En el 2014 fue creado el grupo de ciberdefensa como un organismo que centralizaba el esfuerzo en materia de ciberdefensa, con personal capacitado y material adecuado, buscando generar las bases de defensa y seguridad de las actividades que lleva a cabo a través del ciberespacio.

Actualmente el Grupo de Ciberdefensa se está empeñando en la gestión y coordinación de las siguientes cuatro estrategias en materia de cibernética:

- ✓ Capacitación de personal en las áreas de tecnologías de la información y seguridad de la información, enfocados a la ciberdefensa y ciberseguridad.
- ✓ Generación de doctrina en materia de ciberespacio.
- ✓ Coadyuvar en las políticas públicas para la defensa del Estado mexicano en el ciberespacio.
- ✓ Creación a corto plazo del Centro de Operaciones del Ciberespacio (COC).

Tanto en el Sistema de Adiestramiento Militar, como en el Sistema Educativo Militar0, como es el caso del Colegio de Defensa Nacional, La Escuela Superior de Guerra y El Centro de Estudios del Ejército y Fuerza Aérea, se contemplan como parte de sus planes y programas de estudios, aspectos relativos a la Ciberseguridad y Ciberdefensa.

Por lo que respecta al C.O.C., este estará enfocado a desarrollar las capacidades de defensa y seguridad en el Ciberespacio, con instalaciones, equipo y personal adecuados, con el objeto de proteger y asegurar las Tecnologías de la Información y Comunicaciones de la SEDENA y en su caso coadyuvar en la seguridad de la red de la infraestructura crítica nacional, con las capacidades siguientes:

Operaciones Defensivas

- ✓ Respuesta a incidentes de seguridad en cómputo.
- ✓ Operaciones de monitoreo de redes.
- ✓ Operaciones de protección de sistemas.

Doctrina Militar y Educación

- ✓ Generación de doctrina y adiestramiento especializado.
- ✓ Investigación y desarrollo para la obtención de herramientas de ciberdefensa bajo propiedad de la SEDENA

- ✓ Colaboración Nacional e Internacional
- ✓ Impulso del marco jurídico nacional, mediante propuestas de políticas públicas en materia de ciberdefensa.
- ✓ Coordinación interinstitucional (nacional e internacional) con organismos de fuerzas armadas, gobierno, iniciativa privada, academia, entre otros.

Lo anterior, permitirá crear una doctrina relativa al ciberespacio, además de impulsar acciones para promover políticas públicas y una armonización normativa que proporcione sustento jurídico a las actividades en este ámbito, además de ello se está elaborando un "Manual de Operaciones en el Ciberespacio", "Un prontuario de Ciberdefensa" un "Compendio de Ciberdefensa y Ciberseguridad para ser integrados a la Doctrina Militar"

Por su parte La Secretaría de Marina Armada de México en 2004, creo la Comisión de Seguridad de la Información la cual se constituyó en el ente rector sobre este tema y hoy en día en atención al Plan Nacional de Desarrollo a través de su plan sectorial ha definido estrategias y líneas de acción con las que se buscó:

- ✓ Consolidar y modernizar el Sistema Integral de Seguridad de la Información.
- ✓ Fortalecer la seguridad de las infraestructuras críticas de información.
- ✓ Incrementar las capacidades de ciberseguridad y ciberdefensa mediante:

- ✓ El establecimiento de un centro de control de Ciberdefensa y Ciberseguridad.
- ✓ Adquirir la infraestructura tecnológica necesaria para implementar acciones de seguridad en el ciberespacio.
- ✓ Implementar una estrategia de ciberseguridad y ciberdefensa.

El Centro de Control de Ciberdefensa y Ciberseguridad (C4), que tiene la misión de planear y ejecutar acciones en materia de seguridad de la información, ciberseguridad y ciberdefensa, para salvaguardar las infraestructuras críticas de la SEMAR, así como coadyuvar con el esfuerzo federal para gestionar la vulnerabilidad cibernética que afecte a la seguridad nacional, con las siguientes capacidades:

- ✓ Seguridad y defensa de las infraestructuras de información institucionales.
- ✓ Detección preventiva de amenazas.
- ✓ Análisis y pruebas de seguridad a la infraestructura tecnológica.
- ✓ Análisis de vulnerabilidades y de Malware.
- ✓ Detección de posibles fugas de información.
- ✓ Apoyos a las operaciones de Inteligencia y Contrainteligencia.
- ✓ Apoyo a otros centros de respuesta a incidentes de seguridad cibernética como el CERT-MX a cargo de la Policía Federal.

La Secretaría de Marina conforme a su programa sectorial reestructuró el área responsable de la seguridad de la información y se estableció la Subsección de Protección de Infraestructuras de Información la cual depende del Estado Mayor General y cuya misión principal es:

> Planear y ejecutar acciones en materia de seguridad de la información, ciberseguridad y ciberdefensa, para salvaguardar las infraestructuras críticas de información de la Secretaría de Marina – Armada de México, así como coadyuvar con el esfuerzo federal para gestionar la vulnerabilidad cibernética que afecte a la seguridad nacional. (MÉXICO, 2015).

De acuerdo a su misión y atribuciones, dentro del contexto del ciberespacio, las fuerzas armadas de México dirigen sus estrategias y esfuerzos operativos en dos vertientes:

La primera en organizar, adiestrar, equipar y operar a las fuerzas armadas para la defensa nacional, lo cual implica acciones en el ciberespacio. Dentro de

esta vertiente, también se realizan operaciones de ciberdefensa de los sistemas de armas propios y de la infraestructura estratégica de la nación.

La segunda está enfocada a la seguridad interior, para la cual la Secretaria de la Defensa Nacional y la de Marina tienen la misión de "garantizar la seguridad interior" (MÉXICO, 2014d) y la de "[…] emplear el poder naval de la federación para coadyuvar en la seguridad interior […]" (MÉXICO, 2002) respectivamente, enfocando estas acciones a la ciberseguridad y ciberdefensa de la infraestructura propia, así como la de la infraestructura estratégica de los diferentes campos, ya que por misión y atribución legal y dentro de las funciones como integrantes del consejo de seguridad nacional, se tiene el ordenamiento de coadyuvar para preservar la seguridad interior de la nación.

Los pasos esenciales para la ciberdefensa en las fuerzas armadas, inician con una cultura de seguridad cibernética, en el personal militar y naval, estas son la actualización de software e instalación de parches, eliminar los correos electrónicos masivos o desconocidos, evitar acceder a páginas web no seguras o desconocidas, establecimiento de contraseñas fuertes y con modificación periódica así como instalar antivirus y firewalls; de manera institucional compartimentar la red interna de la institución, no usar USB ni dispositivos no autorizados por el área especializada de informática de la unidad.

Es importante señalar que existe una gran coordinación entre SEDENA Y SEMAR, ambas dependencias participan activamente en el Comité Especializado en Seguridad de la Información, el cual está integrado por las diferentes instituciones que forman parte del Consejo de Seguridad Nacional. Además, entre SEMAR y SEDENA, se llevan a cabo reuniones de trabajo que tienen como fin, homologar la visión conjunta de las Fuerzas Armadas Mexicanas mediante la elaboración de una Estrategia Conjunta en materia de Ciberseguridad y Ciberdefensa y que tiene como objetivo definir el marco de actuación de las fuerzas armadas en este ámbito para coadyuvar con el Estado mexicano ante amenazas y ataques provenientes del ciberespacio que afecten a la seguridad nacional.

También se elaboró ya entre ambas dependencias un catálogo de conceptos homologados en el dominio del Ciberespacio con el fin de disponer de un vocabulario común que permita hacer más efectivas las coordinaciones en materia de respuesta a incidentes en el ciberespacio.

Asimismo, en forma coordinada se han diseñado líneas de acción para ser incorporadas a la Estrategia Nacional de Seguridad de la Información y se han

establecido procedimientos, protocolos y canales de comunicación en materia de Respuesta a Incidentes de Seguridad en el Ciberespacio.

6.2 Ciberdelitos, Ciberespionaje y las Redes Sociales

Comúnmente se enfrentan diferentes tipos de ciberamenazas; en el caso de México, se tienen identificadas tres tipos: la primera es en el sector económico en las finanzas a través del fraude; la segunda es en el sector político a través del espionaje, robo, denegación de servicios, robo de tecnología; y por último, una combinación de ellas. Estas ciberamenazas no solamente se circunscriben al entorno nacional por lucha política sino también al internacional. Con países interesados en obtener información política, económica y tecnológica que les dé ventaja; el tercer lugar lo presentan las actividades de los grupos *hacktivistas* como *Anonymous*, *Safety Last Group*, Resistencia Cibernética, Raza Mexicana, Insurgencia Digital y *Mexican Hacker Mafia*, entre otros; grupos que tienen la capacidad de sabotear las plataformas de empresas e inclusive algunas entidades, sistemas o redes (ESPINOSA, 2015).

De acuerdo con el concepto dado por la UIT[6] y por el convenio sobre criminalidad del consejo de Europa, mejor conocido como Convenio de Budapest, la ciberdelincuencia comete sus crímenes de cuatro maneras: la primera son las ofensas contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos (*hackeo*, *phishing*, espionaje, intercepción y DOS); segunda las ofensas relativas a los contenidos (pornografía infantil, extremismo, apuestas, *spam*); la tercera, son las ofensas mediante el uso de computadoras (fraude, falsificación, robo de identidad); la cuarta, son las ofensas contra los derechos de autor y la propiedad intelectual (piratería). Anteponiendo a esto que solo son intentos para regular o tipificar, sin que haya aún un consenso nacional o mundial que los establezca.

De acuerdo a los antecedentes, el internet surge como un recurso inventado por los E.U.A. para proporcionar un medio alterno de comunicación en caso de guerra, pero una vez que se implementó y se proliferósu uso de manera mundial y multidimensional, pasó a ser un dominio global sin dueño, pero con países que tienen servidores y otorgan dominios para su utilización.

La cantidad de actividades financieras, contratos, almacenamiento e intercambio de información, redes sociales, control de infraestructura crítica y estratégica, información mediática, comando y control de sistemas de armas, con las vulnerabilidades y fallas que presentan los diseños de sus programas, los hacen blanco del cibercrimen, creando una relación del ciberespacio vs seguridad y defensa nacional.

6 Unión Internacional de Telecomunicaciones.

La importancia del internet, de acuerdo a su penetración, es porque mundialmente son 378 millones de víctimas anuales, México es el segundo lugar en Latinoamérica que más sufre ciberataques aumentando hasta un 400% en el 2014. Los usuarios del internet se incrementaron de 12.8 a 53.9 millones en 2014 y en 2015 se incrementó a 71.9 millones de usuarios de internet, que sitúa a México en el lugar 11 entre las naciones con más internautas del mundo, el impacto de la red es tan fuerte que el 27 por ciento de los cibernautas mexicanos convive menos con su familia y 9 de cada 10 pasa más tiempo en las redes sociales.

La importancia del internet por su penetración en la sociedad ha creado de él una dependencia imprescindible por la exponencial cantidad de usuarios que crecen día con día, y por la importancia de las actividades financieras, políticas, sociales, militares, tecnológicas y diplomáticas que en él se realizan, dando oportunidad a que grupos, países o hacker, realicen actividades delictivas que ponen en riesgo la seguridad nacional.

7 Conclusiones

Dentro del aspecto jurídico, como ya se mencionó anteriormente, no hay un organismo internacional que tome la iniciativa de normar, regular, controlar y supervisar las actividades que se desarrollan en el ciberespacio. Como medio de comunicación y transporte de datos en todas sus versiones, corresponde de manera internacional a la UIT. Aunado a que se observa un desinterés por normalizar su uso y tipificar los ciberdelitos; también se observa a grupos u organizaciones, como la OTAN y la CEE que realizan reuniones e iniciativas para regular el uso del ciberespacio, sin lograr consolidar integralmente sus esfuerzos en algo oficial.

La falta de una regulación internacional relacionada al uso del ciberespacio, así como el no estar debidamente conceptuadas y tipificadas las actividades que se consideran como criminales, es aprovechado por países o grupos con un gran desarrollo en cuestión de cibercomandos, ciberguerra y ciberespionaje, para que desde el anonimato y a través del ciberespionaje o ciberataques, tomen información sensible de países u organismos antagónicos o causen daño en sus infraestructura crítica para obtener o incrementar su poder económico, tecnológico o militar.

El ciberespacio se ha convertido en un campo de batalla, donde las naciones o grupos realizan actividades de ciberataques, ciberespionaje y ciberterrorismo, escudándose en la falta de una legislación que lo regule, controle, supervise y actúe contra esos actos delictivos. Ante la perfidia y naturaleza humana de tomar ventajas económicas, políticas o militares a través de la guerra, declarada o no declarada, se busca ser potencia cibernética para agregar valor al poder nacional y así tener

ventaja y poder explotar las vulnerabilidades y fallas en los sistemas de defensa de los países objetivo de los ciberataques en los sistemas de los diferentes campos del poder, pueden causar severos daños y obstaculizar el desarrollo y la seguridad de un Estado, con mayor repercusión en los países desarrollados, ya que entre mayor desarrollo tecnológico se tenga, mayor será la dependencia de los sistemas de información y comunicación en el uso del ciberespacio.

Los conflictos actuales se han caracterizado por el uso del ciberespacio como campo de batalla. Se han formado agencias, centros o cibercomandos dentro de su aparato gubernamental o fuerzas armadas. Destacando que al realizar ataques militares, estos están antecedidos y/o a la vez se realizan ciberataques a los sistemas, redes, comunicaciones o controles de las fuerzas armadas enemigas y paralelamente a la infraestructura estratégica del país enemigo, doblegando su voluntad de pelear y su capacidad militar. De igual manera se realiza continuamente ciberespionaje contra países enemigos o amigos para obtener ventaja económica, política, militar o tecnológica.

El marco jurídico nacional fundamenta la actuación de las fuerzas armadas y demás dependencias que integran el C.S.N. en el ciberespacio para mantener la seguridad interior y la defensa nacional ya que en su contexto, se realizan actividades que pueden escalar en antagonismos a la seguridad nacional, así como también tomar acciones para la defensa nacional a través de un CERT-Nacional, en caso de ciberataques a la infraestructura crítica nacional. Lo cual da como consecuencia que, de acuerdo a la misión y atribuciones de las fuerzas armadas, estas realicen actividades de ciberseguridad y ciberdefensa en el ámbito del ciberespacio por desarrollarse en el mismo actividades consideradas como factores de amenaza que pueden escalar y afectar el desarrollo y a la seguridad nacional. Aunque partiendo de los principios de legitimidad y legalidad se requiere promover reformas jurídicas que fortalezcan la legislación en materia de ciberseguridad y ciberdefensa.

Debido al incremento de riesgos por el uso y desarrollo de las tecnologías de información y comunicaciones (TIC), El Estado mexicano proyecta la creación de un CERT unificado a nivel nacional, se buscará consolidar mecanismos de planeación que coordinen a todas las instancias generadoras de inteligencia, a fin de garantizar la coordinación a través de un efectivo intercambio de información, con estrictos controles en su secrecía, difusión y explotación. Tomando en consideración que cada instancia del C.S.N. utiliza diferentes procesos para la generación de inteligencia y su empleo, buscando al mismo tiempo unificar dichos procesos y crear una doctrina nacional que guie esta actividad, en la defensa del Estado mexicano en el ciberespacio.

Las redes sociales se integraran más a nuestra sociedad, y su capacidad de convocatoria crecerá en un futuro cercano, afectando directamente a los campos del poder, aunado a que con la reciente reforma en telecomunicaciones y radiodifusión se ha incrementado la conectividad en 18 millones de usuarios de internet haciendo un total de 77, 200,000 usuarios, lo cual sin duda coadyuva en incrementar el potencial económico del país, pero sobre todo genera mayor bienestar en los mexicanos, pero al mismo tiempo constituye una mayor vulnerabilidad y se convierte en una amplia gama de acción de los ciberdelincuentes. Por lo que en este sentido se requiere incorporar acciones de trabajo conjunto de los diferentes niveles de gobierno, de la iniciativa privada, de la academia y de la ciudadanía en general para que juntos se establezcan acciones que permitan fortalecer la protección del ciberespacio en el ámbito que a cada uno le compete.

Esta nueva realidad nos obliga a actuar en forma distinta, donde se requiere colocar en el centro de la geopolítica en el ámbito cibernético a México y desarrollar una visión geoestratégica que contemple este ámbito y que mapee con claridad y precisión las acciones estratégicas y los actores-factores relevantes. Implica repensar la idea de seguridad nacional mexicana, que incluya diagnosticar a fondo y tomar decisiones para una estrategia de ciberseguridad en las instituciones e instancias de seguridad y justicia, para el desarrollo nacional.

Conformar un sistema con bancos de datos e información, muchas veces incompletos y desarticulados, podría subsanarse con la propuesta de fusión de inteligencia, que rompa el trabajo de campo limitado, con una estrategia para la ciberseguridad y una Inteligencia para la ciberdefensa, que permita romper la estrechez formal de una estrategia de combate a la delincuencia organizada parcial y limitada. Incluyendo la corrupción e impunidad. Trascender el límite de la legislación actual. Revalorar el papel de la ciberdefensa, en aspectos de los delitos cibernéticos, digitales y o en redes sociales.

Impulsar el conocimiento pleno del ciberespacio, en las condiciones actuales del mundo globalizado, en las situaciones críticas existentes, bajo una estrategia mínima de riesgos o de seguridad, análisis y contrainteligencia. Considerando que es el momento de México, pero sin inteligencia, no habrá desarrollo ni seguridad que hagan viable un futuro promisorio. La conformación de una estrategia en el ámbito cibernético contribuirá a la seguridad de la Nación, la capacidad profesional y recursos suficientes, fortalecerán la seguridad y el desarrollo nacionales.

Finalmente se enfatiza que Las Fuerzas Armadas Mexicanas, se continuarán preparando para enfrentar los nuevos retos de seguridad derivados del extendido uso de las tecnologías de la información; asimismo se modernizan y se adaptan a las nuevas condiciones de su entorno implementando estrategias que le permitan desarrollar

sus capacidades en materia de ciberdefensa y ciberseguridad, mediante: un proceso constante de concienciación sobre los aspectos de seguridad de las tecnologías de la información, en este sentido el recurso humano es la piedra angular de cualquier estrategia y al mismo tiempo, el eslabón más débil de la cadena de la seguridad.

Referencias

ACOSTA, Oscar Pastor et al. *Seguridad Nacional y Ciberdefensa*. Madrid: Fundetel, 2009. (Cuadernos Cátedra ISDEFE-UPM, 6).

CLARKE, Richard A.; KNAKE, Robert K. *Guerra en la Red:* los nuevos campos de batalla. Barcelona: Ariel, 2011.

COUNCIL OF EUROPE. *Convenio de Budapest.* Budapest, 2001. Disponible en: <http://www.coe.int/pt/web/conventions/full-list/-/conventions/treaty/185>. Fecha de acceso: 15 nov. 2015.

DENNING, Dorothy E. *Special Oversight Panel on Terrorism.* [S.l.]: Committe on Armed Services, 2000.

ESPINOSA, Edgar Iván. Hacia una Estrategia Nacional de Ciberseguridad en México. *Revista de Administración Pública,* Ciudade de México, n. 136, enero/ abr. 2015. Disponible en: <http://www.juridicas.unam.mx/publica/rev/indice.htm?r=rap&n=136>. Fecha de acceso: 14 feb. 2016.

KASPERSKY LAB. What is flame malware? [S.l., 2015]. Disponible en: <http://www.kaspersky.com/flame>. Fecha de acceso: 21 feb. 2016.

LUIIJF, Eric. Understanding cyber threats and vulnerabilities. In: LOPEZ, Javier; SETOLA, Roberto; WOLTHUSEN, Stephen D. (Ed.). *Critical Infrastructure Protection*. Heidelberg: Springer, 2012. p. 52-67.

MÉXICO. Constitución Politica de los Estados Unidos Mexicanos (1917). Actualización 2014. *Diario Oficial de la Federación,* Ciudad de México, 2014a.

_____. Ley de Seguridad Nacional, de 31 de enero de 2005. Última reforma publicada DOF en 26 de diciembre de 2005. *Diario Oficial de la Federación,* Ciudad de México, 26 dic. 2005.

MÉXICO. Ley Federal de Telecomunicaciones y Radiodifusión, de 8 de julio de 2014. Decreta se expiden la ley federal de telecomunicaciones y radiodifusión, y la ley del sistema público de radiodifusión del estado mexicano; y se reforman, adicionan y derogan diversas disposiciones en materia de telecomunicaciones y radiodifusión. Diario Oficial de la Federación, Ciudad de México, 14 jul. 2014b. Disponible en: <http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014>. Fecha de acceso: 19 dic. 2015.

_____. Ley Organica de la Armada de México, de 30 de diciembre de 2002. Artículo reformado DOF en 31 de diciembre de 2012. *Diario Oficial de la Federación*, Congreso de la Unión, Ciudad de México, 31 dic. 2012.

_____. Ley Organica de la Administración Pública Federal, de 29 de diciembre de 1976. Última reforma publicada DOF en 11 de agosto de 2014. *Diario Oficial de la Federación,* Ciudad de México, 11 agosto 2014c.

_____. Ley Organica del Ejército y Fuerza Aérea Mexicanos, de 26 de diciembre de 1986. Última reforma publicada el 6 de noviembre de 2014. *Diario Oficial de la Federación,* Ciudad de México, 6 nov. 2014d.

_____. Plan Nacional de Desarrollo 2013-2018. *Diario Oficial de la Federación,* Poder Ejecutivo, Ciudad de México, mayo 2013.

_____. Secretaría da Marina. La ciberseguridad y el Estado Mexicano. Ciudad de México, 2015. Disponible en: <www.derecho.unam.mx/ciberseguridad2015/UNAM.pptx>. Fecha de acceso: 20 marzo 2016.

_____. Secretaría de la Defensa Nacional; Secretaría da Marina. *Glosario de Términos homologados SEDENA-SEMAR.* Ciudade de México, 2014e.

NEWCOMBE, Richard A. et al. KinectFusion: Real-time dense surface mapping and tracking. In: IEEE INTERNATIONAL SYMPOSIUM ON MIXED AND AUGMENTED REALITY (ISMAR), 10., 2011, Basel. IEEE ISMAR. Basel: IEEE, 2011. p. 127-136.

NORTON SEGURID. *2013 Norton Report.* [S.l.]: Symantec, [2014?]. Disponible en: <http://www.symantec.com/es/mx/about/news/resources/press_kits/detail.jsp?pkid=norton>. Fecha de acceso: 13 enero 2016.

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO. *Directrices OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales.* Paris, 2002.

REYNOSO, Sergio Castro. *Principios de ciberguerra:* una guía para oficiales militares. Ciudad de México: Instituto Catenari, 2015.

_____. *Arquitectura de Seguridad Informatica.* Ciudad de México: Alianza de Seguridad Informática, 2013.

ROSALES, Emilio Vizarretea. Inteligencia y Seguridad Nacional en México: una visión estratégica. In: CONFERENCE CYBER SECURITY AND CYBER DEFENCE, 2014a, Cancún. [Anais…] Cáncun: [s.n.], 2014.

_____. *Poder y Seguridad Nacional.* Ciudad de México: CESNAV, 2014b. 582 p.

ZHAO, Houlin. La Cumbre Mundial sobre la Sociedad de la Información y la brecha de la banda ancha: obstáculos y soluciones. *Crónica ONU*, [S.l.], v. 48, n. 3, oct. 2011. Disponible en: <http://unchronicle.un.org/es/article/la-cumbre-mundial-sobre-la-sociedad-de-la-informaci-n-y-la-brecha-de-la-banda-ancha-obst/>. Fecha de acceso: 11 enero 2016.

CIBERDEFENSA, CIBERSEGURIDAD Y ECONOMÍA

Roberto Vizcardo Benavides *

1 Introducción

Cuando el ser humano se vio en la necesidad de diseminar sus ideas, tuvo que buscar una "herramienta tecnológica" para controlar y disponer de la información con el propósito de crear, preservar y compartir sus pensamientos con sus congéneres.

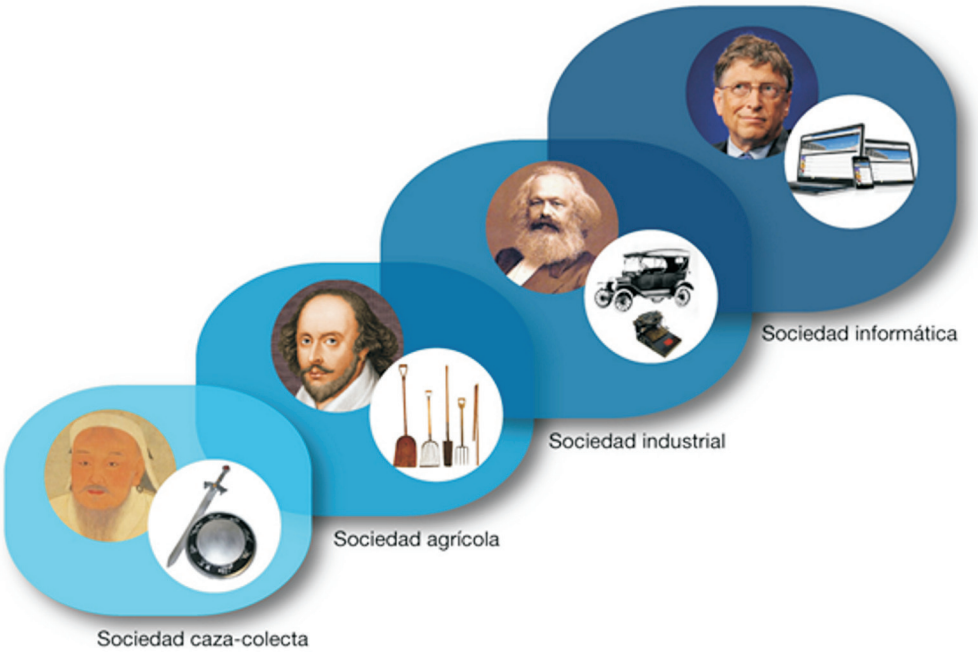
Indistintamente de que se haya transmitido estos pensamientos por medio de herramientas tales como los mensajes en piedra (jeroglifos), papiro, varas de bambú, vitela, papel, imprenta, máquinas de escribir, telégrafo, teléfono, fax, computadora, y actualmente, por la internet; cada una de estas "herramientas tecnológicas" ha tenido impacto trascendental en la sociedad del momento, a lo largo de la historia de la humanidad. Por ende, podemos inferir que el desarrollo de la sociedad humana, desde sus orígenes, ha sido determinado por las herramientas de la información y comunicación.

El proceso revolucionario que desencadenó cada una de estas "herramientas tecnológicas", a su turno, dependió del cambio trascendental que produjo en términos de creación y diseminación del pensamiento. De esta manera, la profundidad del impacto político, económico y social que produjo la imprenta o el teléfono no tiene comparación con el impacto que causó en su entonces el papiro o el papel.

De igual manera, la informática y la Internet han desencadenado en un proceso de transición donde no solo ha afectado, sino que ha revolucionado, la esencia misma de nuestra sociedad.

* Coronel EP ® del arma de Artillería, Magister en Economía por la Universidad San Martín de Porres, Doctor en Ciencia Política y Relaciones Internacionales por la Universidad Ricardo Palma, Graduado en Desarrollo y Defensa Nacional por el CAEN. Ha realizado estudios en Argentina, EEUU, Corea del Sur y Taiwán. Actualmente ejerce la docencia en universidades e instituciones militares de nivel superior y es Secretario General del Centro de Altos Estudios Nacionales (CAEN).
Contato: <roberto.vizcardo@caen.edu.pe>

Figura 1 - Recursos de internet



Fuente: ELABORACIÓN PROPIA, 2016.

Es fácil constatar que estos avances se han dado con mayor rapidez que los anteriores, y han afectado las formas tradicionales de generar y aprovechar el valor socioeconómico de los pueblos. En especial destaca la *Internet*, que permite que individuos y organizaciones compartan información, desarrollen y estructuren el conocimiento en una dimensión totalmente nueva. La *Internet* ha permitido establecer relaciones inter e intra organizacionales que eran consideradas como imposibles hace algunas décadas.

Sin embargo, ese salto cuántico revolucionario también ha creado una nueva dimensión en la problemática mundial. Así, a la par de estos avances en la tecnología informática y de comunicación, también han aparecido nuevos desafíos para la humanidad, tales como la brecha digital, el ciberterrorismo y la excesiva dependencia en esta tecnología.

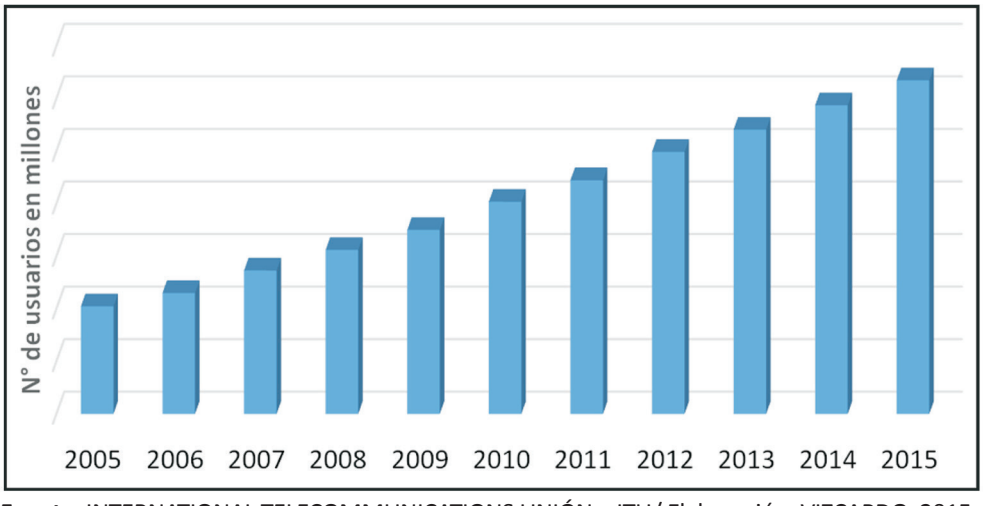
De manera que los últimos cincuenta años de desarrollo de la humanidad, tal vez sean los más sorprendentes e impresionantes en comparación con otros períodos de la historia, a juzgar por la vertiginosidad de los desarrollos científicos, sociales, humanísticos y políticos que la era de la globalización ha traído consigo. Se puede constatar que, a este punto de la globalización, queda claro y ratificado que el hombre

jamás perderá esa característica intrínseca que lo diferencia como ser humano: el conflicto. La historia nos documenta de manera recurrente y casi cotidiana la ocurrencia de conflictos por casi todo el planeta, (¿existe alguna *isla de paz*?), desde la creación hasta nuestros días; conflictos que van desde las riñas domésticas, enfrentamientos tribales, combates, guerras mundiales, batallas terrestres, marítimas y aéreas y, en nuestros tiempos, la ciberguerra o ciberconflicto.

La construcción de ingenios aéreos capaces de romper la barrera del sonido; submarinos guiados a propulsión atómica, transbordadores espaciales, aviones diseñados para transportar 800 personas en un vuelo continuo de 18 horas, son simplemente impresionantes. Hoy en día, un desarrollo tecnológico relativamente reciente, como lo es el teléfono celular, se innova cada año, y en cada presentación o lanzamiento de la nueva versión, se incrementan las prestaciones y las características, habiéndose convertido en un accesorio fundamental para la vida diaria.

Se estima que para el año 2025, el número de usuarios de los llamados teléfonos celulares "Smart" o teléfonos inteligentes, alcanzará la cifra de ocho mil millones en todo el mundo. Signo del vertiginoso avance de la tecnología, además de representar un indicador de la calidad de vida. Ya estamos viviendo el mundo de la "Internet de las cosas" (IoT), es muy probable que en poco menos que el mediano plazo se masifique o generalice su uso; es decir la automatización de la vida diaria pasando por el *e-commerce, la telemedicina, las operaciones financieras desde el teléfono celular* y la construcción, a gran escala, de los vehículos sin conductor.

Gráfico 1 - Usuarios de Internet en el Mundo



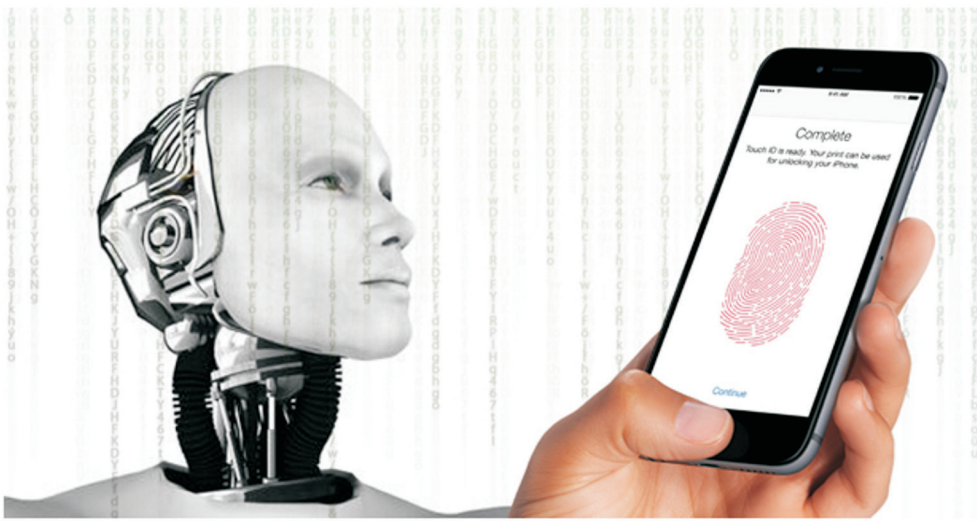
Fuente: INTERNATIONAL TELECOMMUNICATIONS UNIÓN – ITU/ Elaboración: VIZCARDO, 2015.

Todo lo descrito, aparentemente se ha desarrollado y diseñado para facilitar la vida de los ciudadanos, de hecho, esa es la intención, por ejemplo de las impresoras "3D", revolucionario invento que permite construir o replicar prácticamente todo, lo cual constituye una maravillosa innovación tecnológica. En fin, sería larga la lista de las aplicaciones, usos y bondades que la tecnología informática nos permite en la vida cotidiana, en la ciencia y el desarrollo humano, acceder a niveles de comunicación, interrelación y soluciones nunca antes vistos en la historia de la humanidad. Pues en buena hora, el ingenio humano, gracias a Dios, no tiene límite.

Solo en el campo de las aplicaciones (*App*), que se cuentan por miles, podríamos decir metafóricamente que somos "appdependientes" (si vale la pena acuñar un término nuevo), pues en el caso de los "Smartphone", o teléfonos celulares *Smart,,* estos pequeños ingenios tecnológicos, contienen todo tipo de aplicaciones que facilitan o coadyuvan a la vida diaria; las hay para todos los usos, están aquellas diseñadas para medir la presión arterial, para el "jogging", para determinar la ubicación con relación al globo terrestre, reconocer al usuario, llevar la agenda diaria, entre muchas otras.

El escenario es más elevado si de alta tecnología se trata (*high tech*). Pues esta se aplica a las centrales nucleares, satélites, sistema financiero, y todo tipo de actividades que se inscriben dentro del campo de los secretos de Estado, como aquellos programas de desarrollo de nuevos equipos para la defensa, el ámbito industrial o de las patentes denominadas críticas.

Figura 2 - Revolución en la Tecnología Informática



Fuente: EL AUTOR, 2016.

Igualmente los distintos idiomas se han visto "enriquecidos", a consecuencia de la nueva tecnología, con términos y acrónimos hasta hace poco desconocidos, tales como *ramsonware, DDOS, phishing, malware, trojans, hacker, hacktivismo* (que pueden ser aplicativos maliciosos utilizados por personas, estados o mafias), etc. todos ellos asociados a la cibercriminalidad, al delito informático y que configuran un amplio espectro de modalidades como la multiplicación de las prácticas de extorsión, el chantaje, la intrusión en los correos electrónicos de las personas e instituciones, robo de información de las bases de datos, modificación de *software* de aquellas infraestructuras críticas de carácter estratégico; pues bien a todo lo anterior habría que agregar la posibilidad de ejecutar estas acciones a distancia, tan remotas como aquellas de continente a continente.

Y consecuente con lo anterior, existen personas (Hacker, piratas etc), estados (como Corea del Norte) y grupos organizados, que por razones pecuniarias, ideológicas o simplemente figuración, se han constituido como las amenazas modernas del Siglo XXI, capaces de causar daños de magnitudes tales que podrían paralizar el funcionamiento de una empresa, las actividades de una persona (key person), estado o grupo de interés. Entonces aparecen el cibercrimen, el ciberterrorismo, los ciberataques; dejando atrás el enfrentamiento armado en el terreno de los campos de batalla. Un ciberataque en masa, podría destruir un estado y someterlo, por ejemplo.

Con mucha frecuencia se conoce los múltiples ataques cibernéticos a los que son sometidos las empresas en todo el mundo, así como las personas (hay otro tanto, de mayor magnitud, que no se da a conocer, sea por preservar la imagen, el prestigio, o simplemente por no incrementar el daño ocasionado); se pueden señalar como ejemplos el publicitado, notorio y escandaloso ataque que el año 2015 sufrió la transnacional SONY, cuya autoría se llegó a determinar proveniente de un Estado; la exposición pública de la información supuestamente "confidencial" de los miembros del portal de citas ASHLEY MADISON; las continuas exposiciones públicas de las fotografías "íntimas" de actrices de Hollywood; o el último escándalo de alcance global de los llamados PANAMA PAPERS, que involucra a políticos, empresarios, actores, deportistas, etc. En el año 2014, el banco norteamericano JP MORGAN CHASE informó a sus clientes (unos 70 millones de personas y 7 millones de pequeños negocios) que la información cliente-banco se había visto comprometida a causa de un ataque cibernético.

Otros casos emblemáticos y relativamente recientes, que ilustran la capacidad del ciberatacante (*hacker* o estado) sobre blancos determinados deliberadamente son:

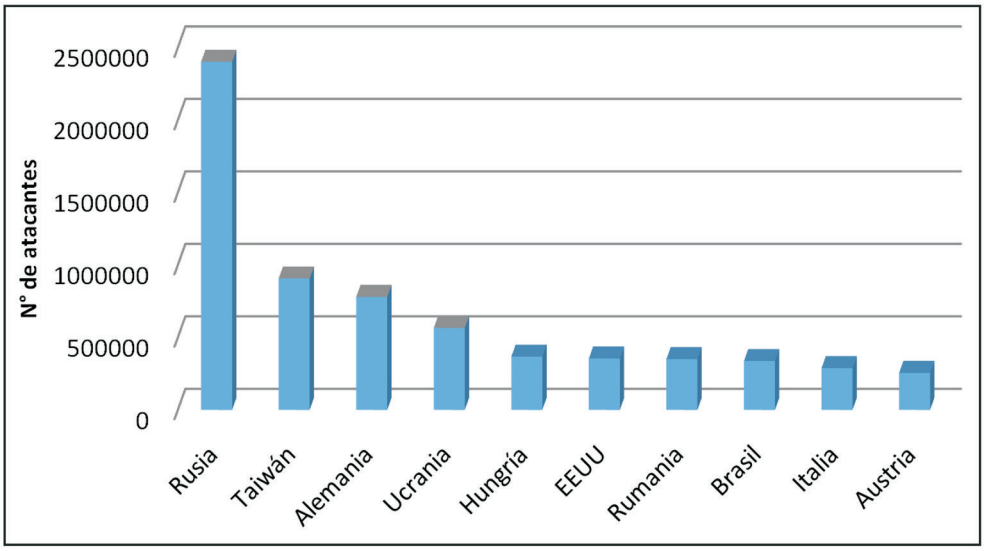
- ✓ El ataque DDOS (*distributed denial of service*), contra un estado: Estonia, producido del 27 de abril al 18 de mayo del 2009 (¡21 dias¡), sobre la estructura del gobierno, bancos, portales y páginas *web* corporativas. El daño causado produjo la paralización del 97% de las transacciones por internet; inoperatividad de la infraestructura gubernamental, sistema bancario, medios de comunicación, etc. ocasionando decenas de millones de dólares americanos en pérdidas.
- ✓ En Julio del año 2010 se descubrió la "infección" viral a las plantas nucleares del Estado de Irán, ocasionando daño a las usinas de enriquecimiento de uranio de *Natanz* (ciudad ubicada al sureste de Teherán); se paralizaron 1000 centrifugadoras nucleares que a la postre significaron el alargamiento del Programa Nuclear Iraní a por lo menos 5 años más. Extraoficialmente se atribuyó la responsabilidad a EEUU e Israel.
- ✓ El caso del exempleado de la CIA Edward Snowden que desveló numerosos programas de vigilancia a líderes mundiales y gobiernos aliados de EEUU, constituye un caso de uso de la cibernética tanto como de la vulnerabilidad y desafección del elemento humano.
- ✓ En diciembre del año 2012, se descubrió la fuga de información de 110 millones de operaciones de pago de una famosa cadena norteamericana de *retail;* nombres de los clientes, número de tarjeta de crédito, fecha de expiración, CVC/CVV. El método utilizado por los ciberdelincuentes fue el *malware* KAPTOXA, proveniente de un hacker ruso que había logrado "infectar" el POS (*point of sale*), es decir el punto de venta donde se registra el pago con tarjeta de crédito. El daño aproximado: 18 mil millones de dólares considerando los daños colaterales.
- ✓ El 23 de diciembre del año 2015, en lo que se podría considerar el primer apagón de gran magnitud causado por un ciberataque, las plantas de energía de Ucrania dejaron de funcionar dejando a más de 225,000 habitantes en la oscuridad. El ciberataque fue conducido a distancia mediante un "reconocimiento extensivo" para identificar las redes de energía, sustraer las credenciales de los operadores y conocer la manera en que se operan los controles de apagado de las plantas. Funcionarios de Ucrania responsabilizaron del hecho a Rusia. Este incidente causó gran alarma en Estados Unidos, al punto que la administración del Presidente Obama, cursó una circular de preventiva a los operadores norteamericanos de plantas generadoras de energía y agua, a fin de que tomen las debidas precauciones.

Figura 3 - Algunas Empresas Transnacionales que Han Sido Objeto de Ciberataques

Fuente: EL AUTOR, 2016.

Recientemente un vocero de la empresa norteamericana VARONIS, cuyo *core business* es brindar soluciones de seguridad de la información y el diseño de aplicaciones informáticas, aseguró que si un hacker o pirata cibernético interviniese las bases de datos o la información almacenada en los teléfonos inteligentes de los aspirantes y sus entornos, a la Presidencia de los EEUU de NA, las consecuencias serían desastrosas: expondría las estrategias de campaña, donantes, número de tarjetas de crédito etc.

Gráfico 2 – Dez Países con Mayor Número de Atacantes



Fuente: EL AUTOR, 2016.

Algunas expresiones y hechos relevantes, a tener en cuenta:

> Con la llegada de ciberamenazas ejecutadas por nuevos o distintos delincuentes o estados, es posible que observemos más ataques basados en *hardware* destinados a generar caos o producir la denegación de servicio a una organización. —Steven Grobman, Director de Tecnología (CTO), Intel Security. (MCAFEE LABS, 2015).
>
> En febrero de 2016, se llevó a cabo la Cumbre sobre Ciberseguridad y Protección del Consumidor en la Casa Blanca, Washington DC, organizada por la Universidad de Stanford; en dicho evento el Presidente Barack Obama firmó un Decreto por el cual se dispone compartir información e inteligencia entre todas agencias norteamericanas incluyendo al sector privado, a fin de detectar y actuar rápidamente ante los ciberataques.

2 Evolución Tecnológica de la Defensa

En lo que concierne al campo de la Defensa, los avances tecnológicos son también impresionantes, la "guerra de las galaxias" renovada en la realidad, misiles "inteligentes", el uso de "*drones*", han reemplazado a las armas y complejos militares tradicionales, que paradójicamente ha dado lugar a la ciberguerra y el ciberespionaje; el siguiente cuadro ilustra de manera resumida la evolución de la guerra:

Cuadro 1 - Evolución de la guerra

ETAPA	PERIODO	CARACTERISTICAS	ELEMENTOS
1ª. y 2da. Generación	1914 – 1917	Carácter global	- Masa - Poder de fuego - Maniobra
3ra. Generación	1918 - 1999	Evolución tecnológica	Poder aeronaval
4ª. Generación	2000 -	Netwar	Tecnología+información

Fonte: EL AUTOR, 2016.

Como se puede apreciar, desde fines de la década de los 90, se constata una verdadera revolución tecnológica aplicada al campo de la Defensa, convirtiendo en obsoletos el parque militar de la mayoría de países del globo. Desde entonces, hablamos de la NETWAR, asociada a la tecnología e información; ello ha traído como consecuencia lo que se ha dado en llamar la Revolución de los Asuntos Militares (RAM), fenómeno que implica una transformación en todos los vectores intervinientes, cuyos desafíos son: investigación y desarrollo de alta tecnología; interoperabilidad de armamentos y equipos; definición de la capacidad defensiva; requerimiento de infraestructura crítica; reformulación de la doctrina; financiamiento del cambio e identificación de las amenazas asimétricas, entre otros aspectos.

En relación a este último aspecto, premonitoriamente uno de los más importantes diarios del planeta comentó lo siguiente: "[…] en el día de hoy, Estados Unidos se asemeja inconfortablemente a Goliat, arrogante en su poderío, armado hasta los dientes e ignorante de su debilidad. En una guerra informática, Goliat podría ser derribado con una honda de alta tecnología […]" (LOHR, 1998).

Al respecto en la obra "The next world war: computers are the weapons and the frontline is everywhere", se consigna la siguiente frase: *"una persona armada solo con una computadora y un modem, literalmente podría chantajear a un país".* (ADAMS, 2001). Hablamos entonces de las amenazas asimétricas, como el ciberterrorismo, ciberataques, ciberespionaje etc.

Como propone Adams (2001):

> […] se trata de un silente, invisible y mortífero sistema de armas, capaz de paralizar una nación sin siquiera enviar un solo soldado al campo de batalla, lo hemos apreciado en la televisión durante la Guerra del Golfo, los ataques quirúrgicos sobre los sitios de radares, plantas de energía y puestos de comando. Ahora, un nuevo capítulo de la historia militar se está escribiendo: la era de la información ha llegado al campo de batalla…..la tecnología ha trazado su camino al campo de batalla: soldados equipados con tecnología "*Smart",* aparatos que pueden detectar la presencia enemiga, por el calor que emite el cuerpo; o el uso de pequeños robots para observación y sabotaje, monitoreados por satélite […]
>
> Pero el más importante y significativo uso de la información no está en el campo de batalla. Las armas más devastadoras serán aquellas que tienen como objetivo la infraestructura del

> enemigo: sistemas de control aéreo, líneas de distribución de energía y comunicaciones, solo por nombrar algunos blancos potenciales……"un caballo troyano" o virus especialmente diseñado para aceptar y responder a comandos de la inteligencia militar de Estados Unidos puede ser instalado en los computadores que se comercializan en el mundo haciéndolos vulnerables a ataques de toda naturaleza ….incluyendo la desinformación….este tipo de combate expone a los ciudadanos a mayores riesgos que nunca antes se ha visto […].

En mayo del 2015, el Secretario de Justicia de EEUU informó que acusaría formalmente a cinco Oficiales del Ejército de Liberación Popular de China de robo de secretos corporativos (muchos de ellos ligados a la industria de la defensa) por medios cibernéticos, en lo que constituyó la primera vez que el gobierno norteamericano levanta cargos contra agentes extranjeros por este tipo de delitos.

Según fuentes informadas del caso, se determinó que el medio utilizado habría sido el *malware Blackshade*, que permite controlar una computadora a distancia. El asunto ha comprometido secretos militares y de propiedad intelectual, protegidos por la legislación norteamericana. El tema fue objeto de discusión entre los líderes de EEUU y China en la cumbre de San Petersburgo en el año 2013.

El mapa desvelado por la NBC hace referencia a los casos de espionaje informático llevados a cabo desde un país asiático sobre objetivos norteamericanos, tanto privados como públicos, mostrándonos lo vulnerable que puede ser cualquier país a los ataques cibernéticos o al ciberespionaje.

Como es de suponer sin temor a errar, el blanco más atacado es la zona de Silicon Valley (California) y alrededores, donde se ubican las grandes empresas tecnológicas estadounidenses. También se observa ataques densos en la zona noroeste de la Costa del Pacífico, donde se concentra gran parte de la industria aeronáutica y militar norteamericana.

La información difundida por la NBC News recalca que además de los objetivos obvios, (empresas tecnológicas, militares y aeronáuticas), los ataques también han ido enfocados a espiar y obtener información secreta acerca de la industria del automóvil híbrido y sus especificaciones, la industria farmacéutica y el sector del control del tráfico aéreo, tanto civil como militar.

Figura 4 - CIBERATAQUES SOBRE EEUU.

Fuente: NBC/NSA, 2015.

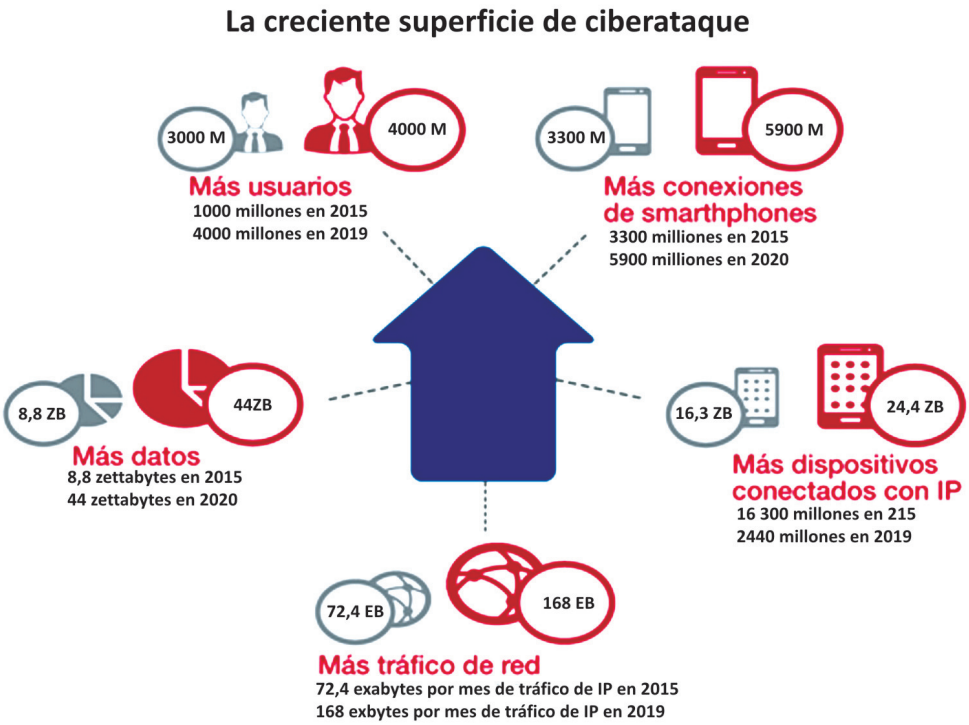
3 Situación actual ante la amenaza

Ciberguerra, ciberconflicto, cibercrimen, ciberespionaje etc., sobre el tema aún está pendiente homogenizar los conceptos. Lo cierto es que estamos frente a una amenaza real que desafía a la sociedad en su conjunto, sin ninguna clase de distinciones; de una manera general estamos hablando de ataques cibernéticos a sistemas e infraestructuras críticas que dependen justamente de la cibernética, que se encuentran en el campo industrial, comercial, militar, espacial, gubernamental etc., a los que debemos enfrentar.

Se conoce que más de 100 países en el mundo han implementado sistemas de ciberseguridad, incluyendo en la mayoría de ellos los comandos cibernéticos; de otro lado existe ya un cuerpo doctrinario desarrollado por los países líderes en ciberseguridad, como Israel, Corea del Sur, etc. En América Latina, la mayoría de naciones han establecido los llamados CERT (Computer Emergency Response Team – Equipos de Respuesta ante Emergencias Informáticas) que son centros

de respuesta a incidentes de seguridad que afecten los sistemas informáticos; operados por expertos en tecnologías de la información, los CERT tienen por función implementar las medidas preventivas y de respuesta ante incidentes cibernéticos; también, de acuerdo con la magnitud y nivel de equipamiento de la infraestructura puede proporcionar alertas relativas a amenazas y vulnerabilidades que puedan constituir peligros potenciales a la infraestructura crítica y la información tanto pública como privada.

Figura 4 - La Superficie del Ciberataque



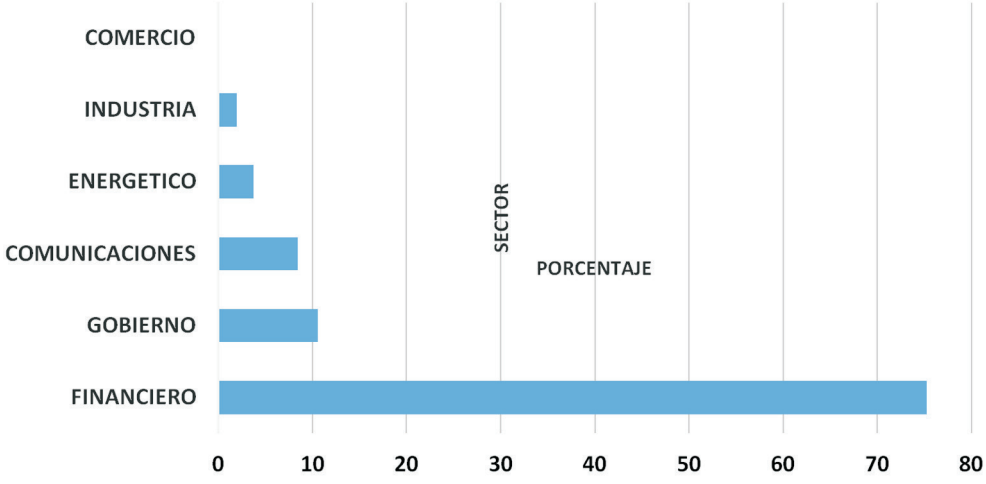
Fuente: MCAFEE LABS, 2015.

Sin embargo, no obstante que el quinto escenario, el ciberespacio, es el campo de batalla de la actualidad, comprobadamente no se ha tomado conciencia de la importancia y la gravedad de la amenaza cibernética, se valora muchísimo más las bondades que nos brinda la tecnología informática (pronto se estará masificando el internet de las cosas – *internet of things* IOT- , que nos permitirá el control doméstico de cuanta actividad se desarrolle en el hogar, desde un teléfono

inteligente); por ejemplo, ya es una realidad realizar operaciones financieras desde el *smartphone,* (¿para qué ir al banco?). En fin, maravillosa tecnología, que cada vez nos hace *TICdependientes* (si cabe acuñar un nuevo término, acorde con la situación).

Tal vez la euforia por la tecnología no nos haga ver que así como la *internet* y la PC, la tableta o el teléfono inteligente han revolucionado la vida moderna, al mismo tiempo se ha desarrollado todo un cuerpo de riesgos potenciales (se estima que existen unas 280,000 aplicaciones maliciosas) que afectan la cultura, la política, la economía, el gobierno, las empresas y los ciudadanos, y que en nuestras realidades, es una verdad insoslayable que no le concedemos la importancia que debería dársele, no obstante que el mundo ha sido y es testigo de la guerra silenciosa que en estos momentos se viene librando en el ciberespacio, que como se ha indicado anteriormente es una guerra permanente, de larga duración con beligerantes que no dan la cara.

Gráfico 3 - Ataques Cibernéticos en el Mundo



Fuente: DIGIWARE – EL AUTOR, [20??].

Algunas consideraciones dignas de tener en cuenta: las empresas del sector financiero acusan la mayoría de ataques, siendo las más vulnerables. De manera global, las empresas son reticentes a invertir en seguridad cibernética. Sin embargo, el factor recurso humano es el que representa la vulnerabilidad número uno, puesto que sus descuidos representan oportunidad para los delincuentes cibernéticos. En general los ciudadanos (usuarios) comprobadamente no tienen una visión sobre los

riesgos cibernéticos. También se debe destacar que en el caso de las empresas, los ataques cibernéticos no solo van dirigidos a la comisión de crímenes, sino también tienen como objetivo dañar la reputación de la marca o causar una disminución en el valor de las acciones.

Hace unos años, el hacker más famoso del mundo Kevin Mitnick, a quien se le recuerda por haberse introducido de manera ilegítima en los sistemas informáticos de empresas como MOTOROLA, NOVELL, NOKIA y SUN MICROSYSTEMS, para realizar llamadas de larga distancia y obtener información secreta a través de archivos almacenados en servidores. Por ello fue condenado a 3 años de prisión; ya en libertad, actualmente Mitnick es un hombre reformado y dedicado a enseñar a empresas y expertos en informática como protegerse de la ingeniería social (se denomina así, en el contexto de la ciberseguridad, al arte de la manipulación de personas para que realicen acciones o divulguen información confidencial –en la mayoría de los casos, el atacante nunca conoce a las víctimas). Su teoría es que muchas veces son las personas y no las tecnologías quienes presentan un punto débil en la seguridad de una organización. Según MITNICK, la gente que labora en las grandes compañias tiene poco cuidado al elegir el lugar para guardar *passwords* (claves) y desecha las libretas o apuntes confidenciales sin mayor cuidado, en la basura. Otro riesgo es revelar datos privados durante las conversaciones telefónicas que se realizan en lugares públicos. (MITNICK; SIMON, 2002)

La agenda global para enfrentar el problema se refleja en los siguientes tópicos: normatividad de ciberseguridad; medidas de confianza y capacidad de respuesta.

Para el desarrollo de esta agenda se han constituido cuatro foros: el Grupo de Expertos Gubernamentales de Naciones Unidas (UN-GGE); la Organización Europea para la Cooperación en Seguridad (OSCE); el Foro Regional de ASEAN (ARF) y el Foro de la Organización de Estados Americanos (OAS). Está claro que el trabajo que desarrolla la UN-GGE tiene implicancias en todas las regiones del mundo hasta el nivel nacional. Para el caso de la región latinoamericana, el último Reporte emitido por el Observatorio de Ciberseguridad de la OEA y el BID, señala lo siguiente:

> […] Los elementos generales de una estrategia regional se pueden describir brevemente como sigue. Los países necesitan establecer un organismo de coordinación en el nivel presidencial o de primer ministro, con capacidad de implementar y supervisar los esfuerzos de agencias, y a veces resolver disputas. La estrategia debe asignar responsabilidades entre los Ministerios relevantes; estos ministerios deberán establecer fuertes lazos con el sector privado a fin de crear una aproximación colaborativa, particularmente con el sector

> eléctrico, telecomunicaciones y financiero. Los gobiernos necesitan establecer organismos de ciberseguridad que incluyan como mínimo un equipo CERT (Computer Emergency Response Team), y una policía especializada en ciberdelitos. (LEWIS, 2016, p. 5). James A. Observatorio de Ciberseguridad – Reporte 2016, p. 5)

Por cierto, a nivel regional, enfrentar el reto requiere de la cooperación internacional, porque si algo se ha aprendido es que ningún país por sí mismo, actualmente, posee la capacidad de asegurar sus redes. La cooperación es esencial.

4 La dimensión Económica de la Ciberseguridad

En el pasado la conclusión de los megaconflictos como la I y II Guerra Mundial, la Guerra de la Península Coreana, de Vietnam, el Golfo o las varias guerras árabe-israelíes, trajeron como consecuencia etapas de depresión económica, principalmente para el bando perdedor y en general para la economía global.

Es muy ilustrativo el caso de la península de Corea. Cuando en 1953 concluye la guerra fraticida con la división del territorio; Corea del Sur inició el proceso de reconstrucción nacional desde las cenizas. Enormes sacrificios tuvieron que ser asumidos por los coreanos ante la devastación y pobreza. Es admirable el grado de resiliencia de esta cultura que actualmente es uno de los paradigmas del desarrollo y la tecnología, fundamentalmente de la electrónica y la informática, habiendo alcanzado la categoría de líder global en ciberseguridad.

Pues bien, hace ya varios años que asistimos al fin del conflicto en su versión tradicional, de ocupación y devastación de territorios enemigos (ciudades y pueblos) y destrucción de la infraestructura crítica ocasionando sufrimientos y dolor en poblaciones enteras. La recuperación y reconstrucción suponía grandes sacrificios económicos y por largo tiempo, cuando no las reparaciones económicas impuestas al perdedor. El beneficio económico que se irrogaba el vencedor generalmente estaba asociado a la captura de recursos y territorios estratégicos vía la ocupación o anexión geográfica; onerosas indemnizaciones pecuniarias entre otras condiciones humillantes.

Como se ha dicho anteriormente, con el advenimiento de la era digital, literalmente ha desaparecido el factor violento de la guerra, lo cual ha revolucionado la teoría del conflicto en tiempos de paz, tanto como la teoría de los asuntos militares. La destrucción física se ha reducido ostensiblemente al igual que el derramamiento de sangre y el número de víctimas fatales directas e indirectas.

A los escenarios terrestres, marítimos, aéreos y espaciales se ha sobrepuesto el escenario cibernético con sus características aquí expuestas.

Sin embargo, lo que no han desaparecido, con el advenimiento del quinto escenario – el ciberespacio- son las consecuencias económicas que se desprenden de un enfrentamiento o de un ataque cibernético sea cual fuera la modalidad empleada: invasión electrónica, ciberespionaje, *ransomware* etc. El daño económico que se puede ocasionar puede superar al de un enfrentamiento convencional, con el añadido de que se enfrenta a un enemigo invisible, difícil de ubicar (al menos que se cuente con la tecnología más avanzada) y de sancionar obviamente.

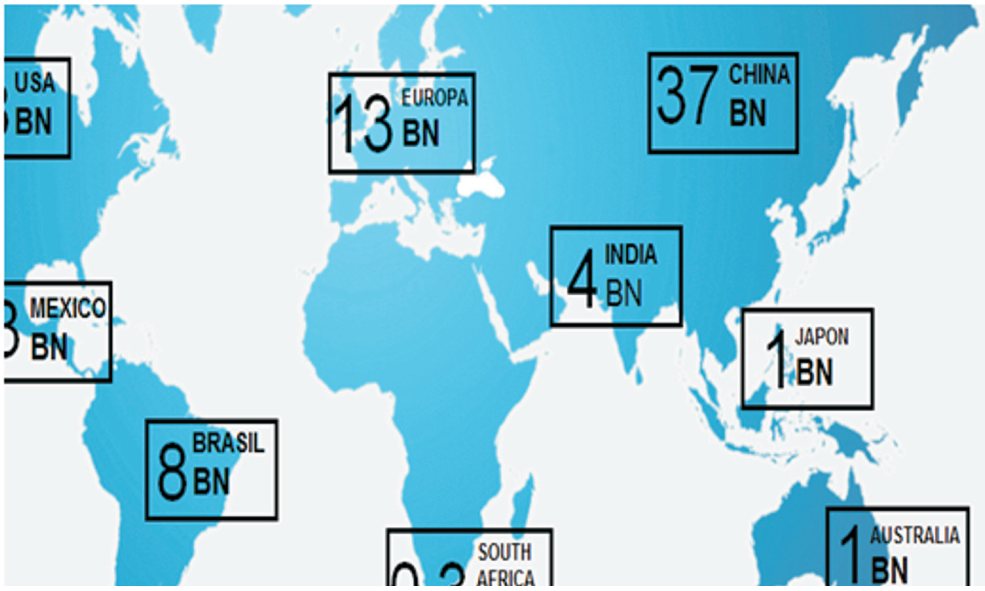
Pero, ¿qué que motivaciones pueden esgrimir el o los atacantes cibernéticos? Pues hay muchas. Van desde las motivaciones estrictamente comerciales, industriales y de seguridad nacional (sustracción de información privilegiada, confidencial, propiedad intelectual, desarrollos estratégicos y secretos así como conocer y vigilar los movimientos del competidor); también están las motivaciones ideológicas, aquellas llevadas a cabo por personas o grupos terroristas, fundamentalmente ligados a doctrinas violentas. No se puede perder de vista que en esta guerra moderna del S XXI, los intereses de los Estados quedan a salvo en tanto ahora se dispone de las herramientas cibernéticas para lograr sus objetivos.

Sea cual fuere la motivación y las herramientas cibernéticas utilizadas, la realidad es que la sociedad global de naciones está viviendo la primera guerra mundial en el ciberespacio, de carácter silencioso, permanente, multidireccional, intencional, enfrentando a enemigos aparentemente desconocidos, no cuantificables (van desde una persona hasta una organización, corporación o estado), y que por supuesto suponen ataques y defensas (muchas veces débiles, como es el caso de los países en vías de desarrollo), cuyas consecuencias económicas son inconmensurables y muchas veces no divulgadas por diversas razones.

Todo ello supone enorme costo económico, empezando por la implementación de las estrategias preventivas para proteger todo aquello que se encuentra digitalizado en todos los campos de la actividad humana: gobierno, industria, banca, comercio, educación, salud, seguridad, defensa, propiedad intelectual, propiedad privada, información personal, etc. Todo lo cual supone una organicidad o estructura relevante.

A la luz de los hechos, está claro que nadie (ninguna persona, empresa, corporación o estado sea este del primer mundo o no) está exento o se encuentra a salvo de los ataques cibernéticos de cualquier naturaleza. Todos son vulnerables, aquí y en el primer mundo. De lo que se conoce, al mensurar el daño e impacto económico, las cifras resultan sencillamente aterradoras alrededor del planeta: 378 millones de víctimas por año; más de un millón de víctimas por día; 12 víctimas por segundo (NORTON SEGURID, [2014?]).

Figura 6 - Impacto Económico del Cibercrimen (en miles de millones US$)



Fuente: NORTON REPORT, 2013.

5 La Ciberseguridad y la Ley

Las características del ciberespacio se pueden resumir en tres variables: tiempo (siempre disponible); espacio (sin límites ni fronteras); y, objeto (multicomunicación). En este contexto, para entender el marco legal de la ciberseguridad se tiene que considerar el efecto negativo de internet en nuestras vidas, la sociedad en su conjunto y la comunidad global. El hecho de que las comunicaciones por esta vía muchas veces no implican una relación cara a cara, ha generado desconfianza y la consecuente aparición del cibercrimen, la guerra cibernética, la invasión de la privacidad y el correo electrónico no deseado.

De acuerdo con el estado o nivel de ciberdefensa alcanzado por una organización o nación, los efectos negativos de internet o tecnología de la información, en su vertiente criminal, puede ocasionar: en el usuario: daño mental y financiero; en la empresa: pérdida de productividad; en el país: declive de la competitividad.

De ahí la necesidad de contar con un Sistema Legal de Ciberseguridad, el cual debería proporcionar las medidas de protección de los objetivos o infraestructuras críticas y los activos de información. Este cuerpo legal debe ser aplicable a los sistemas,

redes, hardware e información; en el caso de las personas se aplica a todo el recurso humano que forma parte del sistema de redes, incluyendo los terminales, la gestión técnica de los procesos de manejo de información y las medidas de seguridad.

En el ámbito del derecho internacional, existe consenso que el *jus ad bellum* (derecho sobre el empleo de la fuerza) y el *jus in bello* (derecho de la guerra), se aplican al escenario del ciberespacio. Diversas resoluciones de Naciones Unidas sobre la ciberseguridad han sido emitidas con la finalidad de crear una cultura global de ciberseguridad. Estas resoluciones identifican nueve elementos:

- ✓ Tomar conciencia del tema
- ✓ Responsabilidad
- ✓ Respuesta
- ✓ Ética
- ✓ Democracia
- ✓ Evaluación del riesgo
- ✓ Diseño de las medidas de seguridad y su implementación
- ✓ Gestión de la ciberseguridad
- ✓ Reevaluación.

Resulta interesante reseñar el Sistema de Leyes de Ciberseguridad de la República de Corea del Sur, uno de los países que se encuentra a la vanguardia, a nivel global en el desarrollo cibernético. El mencionado cuerpo de leyes tiene alcances bien definidos, producto de la experiencia y permanente enfrentamiento con sus vecinos del norte. Así, considera:

1. Prevenir la pérdida de información crítica.- Prevenir la divulgación indebida de la tecnología industrial y protegerla a fin de potenciar la competitividad de la industria coreana y contribuir al desarrollo y economía nacional.
2. Firma Digital.- Establecer un marco de referencia para el sistema de firmas digitales a fin de otorgar seguridad y confianza en las transacciones electrónicas y promover su uso.
3. Protección de la información de la infraestructura crítica.- Formular e implementar medidas que garanticen la gestión y operación de la información crítica y la infraestructura de comunicaciones, evitando el espionaje.
4. Prohibición de la intrusión.- Sancionar penalmente este tipo de actividad realizada por cualquier persona que ocasione molestias o paralizaciones de terminales informáticos o sistemas.
5. Protección de la información personal y la privacidad.- Prescribe reglas concernientes a la gestión de la información personal, a fin de proteger los derechos e intereses de los ciudadanos.

Este cuerpo de leyes, que reitero, es uno de los más avanzados en

ciberseguridad a nivel global, ha sido implementado con legislación ad-hoc, como se detalla a continuación:

- ✓ Ley para la promoción y utilización de las redes de información y comunicación, así como para su protección - (emitida en 1987).
- ✓ Ley para la protección de la información personal - (del año 2011).
- ✓ Ley para la protección de la información y la infraestructura de comunicaciones - (2001).
- ✓ Ley sobre las transacciones financieras electrónicas- (2006)
- ✓ Ley sobre la divulgación y protección de la tecnología industrial- (2007).
- ✓ Ley de protección del consumidor en el comercio electrónico - (2002).
- ✓ Ley sobre la firma electrónica o digital - (1999).
- ✓ Ley sobre la promoción de la información de seguridad industrial - (2015).
- ✓ Ley específica que promueve la seguridad industrial en los campos de la tecnología, el mercado, los recursos humanos y las inversiones.

Otro importante marco de referencia legal sobre el cibercrimen está constituido por el Tratado 185 del Consejo Europeo (CoE) sobre el cibercrimen, producto de la Convención de Budapest del año 2001 y puesto en vigor en el 2004. Este marco legal tiene como objetivo la protección de la comunidad contra el cibercrimen, estableciendo procedimientos y políticas comunes para enfrentarlo. Este tratado es de libre adhesión por los países que reúnan ciertos requisitos. Al momento, se conoce que unos 130 países alrededor del mundo lo han utilizado como guía para establecer sus propias estrategias.

6 Conclusiones

El vertiginoso desarrollo de las comunicaciones a partir de la era de internet, ha revolucionado el acceso a la información así como a la tecnología que la sustenta. Desde la creación de los primeros programas operativos para las computadoras, el *software* parece no tener límites; hoy en día se crean para toda necesidad de la vida diaria, desde los aspectos más domésticos hasta los de alta seguridad de las personas, empresas o estados. Desde luego, hay también *software* creado especialmente con fines delictivos para cometer fraude en el sistema financiero, robar información, bloquear sistemas o simplemente lograr notoriedad. Es cada vez más frecuente en el mundo el llamado CIBERCRIMEN, asunto que Naciones Unidas ya ha asumido como amenaza a la seguridad.

El rápido desarrollo de la tecnología de la información y comunicaciones va a la par con la expansión del cibercrimen; a su vez la innovación tecnológica crea nuevas vulnerabilidades en todo orden de cosas, en el IoT de los hogares, las empresas,

el gobierno, la defensa nacional; de una manera general en todos los campos de actividad humana, sin distinguir si los blancos corresponden a una empresa grande o pequeña, a un estado o nación desarrollada o en vías de desarrollo, o simplemente a un ciudadano. Una característica transversal a todo ello es la falta de toma de conciencia de la amenaza, en todo nivel.

La guerra mundial en el ciberespacio está teniendo lugar, las consecuencias potenciales pueden ser desastrosas y enfrentar poderes que deterioren las relaciones internacionales y ocasionen pérdidas económicas a los beligerantes. De otro lado, el fraude, robo de información y bases de datos protegidas, la extorsión y la amenaza, teniendo como protagonistas desde una persona o mafia organizada para el delito, tienen un impacto tremendo sobre la confianza y moral del blanco atacado.

A nivel regional, todavía no se ha homogenizado una plataforma común para enfrentar la amenaza; los esfuerzos que los países vienen realizando, son todavía dispersos. Si bien es cierto la ONU y la OEA han tomado la iniciativa para hacer frente a esta amenaza, la agenda está cargada de temas pendientes, como por ejemplo la legislación ad-hoc (una buena base constituye los lineamientos de la Convención de Budapest), tanto como la implementación de la infraestructura adecuada que permita asumir la tarea de brindar ciberseguridad a la nación.

Está claro que la ciberseguridad contribuye al crecimiento y al desarrollo de un país, su descuido puede acarrear graves consecuencias al gobierno, el aparato productivo, la generación de energía y agua, la operación de aeropuertos, puertos, la bolsa de valores, el sistema financiero, la propiedad intelectual, los secretos militares o de estado, y a los ciudadanos. No olvidemos que en el ciberespacio hay francotiradores (piratas, hackers etc.), ejércitos bien apertrechados (bandas criminales dedicadas al ciberdelito), países competidores y beligerantes. Afortunadamente, por otro lado, también existen cada vez más herramientas para enfrentar estas amenazas.

Referencias

ADAMS, James. The next world war: computers are the weapons and the front line is everywhere. New York: Simon and Schuster, 2001.

LOHR, Steve. War Games. *New York Times*, New York, 1 nov. 1998. Disponible en: <http://www.nytimes.com/1998/11/01/books/war-games.html>. Fecha de acceso: 18 feb. 2016.

MCAFEE LABS. *Predicciones sobre amenazas para 2016*. Madrid: Intel Security, 2015. Disponible en:<http://www.mcafee.com/es/resources/reports/rp-threats-predictions-2016.pdf>. Fecha de acceso: 17 dic. 2015.

MITNICK, Kevin D.; SIMON, William L. *The art of deception*: controlling the human element of security. John Wiley & Sons, 2002.

NORTON SEGURID. *2013 Norton Report*. [S.l.]: Symantec, [2014?].

ORGANIZATION OF AMERICAN STATES; INTER-AMERICAN DEVELOPMENT BANK. *Cybersecurity*: are we ready in Latin America and the Caribbean? Washington, DC, 2016. Disponible en: <https://publications.iadb.org/handle/11319/7449?locale-attribute=en&locale-attribute=pt&locale-attribute=es&>. Fecha de acceso:10 abr. 2016.

WEGENER, Henning. Los riesgos económicos de la ciberguerra. *Cuadernos de estrategia*, [S.l.], n. 162, p. 177-227, 2013. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=4276097>. Fecha de acceso: 15 nov. 2015.

CONTRIBUTO PARA O ESTUDO DA CIBERSEGURANÇA EM PORTUGAL

João Manuel Assis Barbas*

1 Introdução

A informação é um elemento social do poder nacional conjuntamente com a diplomacia, economia e o poder militar. Desde a década de 1990, que se diversificou o papel das tecnologias de informação nas relações internacionais, bem como a sua importância política, principalmente devido à proliferação das Tecnologias de Informação e Comunicação (TIC).

A capacidade de dominar a produção, gestão, utilização e manipulação da informação tornou-se num ambicionado recurso definidor de poder, pois o controle do conhecimento, crenças e ideias são consideradas cada vez mais como um complemento ao controle dos recursos tangíveis, tais como as matérias-primas,os recursos econômicos e as capacidades militares.

É pois neste contexto de interdependência entre as sociedades e as TIC que surge a temática da cibersegurança, associada nomeadamente à ciberdefesa, proteção das infraestruturas críticas e, em especial, à resiliência cibernética ou das infraestruturas de informação críticas.

Este artigo procura dar visibilidade à experiência do Instituto da Defesa Nacional de Portugal no domínio da sensibilização para a temática da cibersegurança e gestão de crises no ciberespaço, essencialmente no domínio da formação, procurando enquadrá-la no espaço das iniciativas da União Europeia, no quadro legislativo nacional e em relatórios internacionais de referência como, por exemplo: *Global RisksReport, CyberPowere UK 2015 Cyber Information Security Breaches Survey*. É, acima de tudo, um ponto de passagem para uma reflexão mais profunda sobre alguns dos temas aflorados.

2 O que é a Cibersegurança

É uma disciplina relativamente nova e que não tem uma definição amplamente aceita. Muitas pessoas acreditam que a cibersegurança ou segurança cibernética

* Coronel de Artilharia. Assessor de Estudos do Instituto da Defesa Nacional de Portugal. Responsável pela unidade curricular de Tecnologias de Informação e Plataformas Internet no Mestrado em Guerra de Informação da Academia Militar. Licenciado Ciências Militares e em Engenharia de Sistemas Decisionais. Mestre em Administração de e Gestão de Empresas (MBA) com especialização em Gestão da Informação. Possui ainda uma pós-graduação em Investigação Operacional e Análise de Sistemas. Contato: jmabarbas@clix.pt>. Site: <jmab.planetaclix.pt>

é algo que se pode adquirir incrementalmente como uma *commodity*. Outros acreditam que a cibersegurança refere-se exclusivamente a questões técnicas, como a utilização de *passwords* ou a instalação de *firewalls* para proteger uma rede de computadores. Ainda assim, outros acreditam que se trata de uma capacidade técnica e administrativa da exclusiva responsabilidade dos profissionais de TI.

Uma possível definição de cibersegurança está disponível no *site* da União Internacional das Telecomunicações como: "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." (INTERNATIONAL TECHNOLOGY UNION, 2016).

Desta definição decorre que a cibersegurança integra um conjunto holístico de atividades e recursos que visam proteger os ativos, físicos e virtuais das organizações e dos utilizadores, dos riscos do ambiente cibernético envolvente. É ainda de realçar que uma qualquer capacidade de cibersegurança eficaz preserva os principais atributos da informação[7] protegendo-a do ataque de *hackers*, danos e acesso não autorizado.

No ambiente empresarial de hoje, a segurança cibernética não é apenas uma questão técnica, mas um imperativo de negócio, que requer de cada decisor uma abordagem multidisciplinar de gestão de risco.

Desse modo, a cibersegurança permite acautelar a proteção das atividades das organizações, os investimentos dos acionistas e os ativos da organização, assegurando condições para que possam manter vantagem competitiva.

Mas tal proteção da normal atividade das organizações requer uma capacidade de identificação, prevenção e, no pior dos casos, mitigação dos riscos que sobre elas recaem. Três publicações têm-se debruçado na análise destes riscos: o *Global RisksReport*, o *CyberpowerIndex* e o *UK 2015 Information Security Breaches Survey*.

3 Os *Global Risks Report*

As primeiras nove edições dos *Global Risks Reports* do Fórum Económico Mundial realçaram os riscos globais mais significativos, numa perspetiva de longo prazo. Os últimos dois relatórios – 2015 e 2016 – identificam igualmente as interconexões entre os riscos e os seus efeitos, potencialmente em cascata e introduzem uma nova distinção entre riscos e tendências. (WORLD ECONOMIC FORUM, 2015; 2016)

7 Confidencialidade, integridade, disponibilidade, autenticidade, não-repúdio e conformidade.

No *Global Risks Report 2016* os riscos são agregados em cinco categorias (econômicos, ambientais, geopolíticos, sociais e tecnológicos), onde os riscos tecnológicos compreendem:

- ✓ Colapso de infraestruturas críticas de informação e redes: falhas sistémicas de infraestruturas de informação crítica e das redes de comunicação, afetando de forma adversa a indústria, os serviços públicos e as comunicações;
- ✓ Ataques cibernéticos em larga escala: ciber-ataques patrocinados por Estados, atores não-estatais, organizações criminosas ou terroristas, visando ao colapso das infraestruturas e/ou a perda de confiança nainternet;
- ✓ Incidentes em grande escala ou fraude/furto de dados: obtenção ilícita de dados oficiais ou privados, patrocinada por Estados ou organizações criminosas;
- ✓ Consequências adversas da evolução tecnológica: situação adversa intencional ou acidental decorrente de tecnologias como a inteligência artificial, geo-engenharia (ou engenharia climática) e biologia sintética, com danos humanos, ambientais e económicos.

Das treze tendências identificadas, realça-se o crescimento da ciberdependência, decorrente da progressiva digitalização da conetividade entre as pessoas, objetos e organizações.

Este relatório enfatiza o contributo dos avanços tecnológicos da Quarta Revolução Industrial (SCHWAB, 2016), a digitalização para a transformação das sociedades e das economias, e o seu impacto não só em novas oportunidades, mas igualmente no aumento das desigualdades na distribuição de riqueza e na ciberdependência, o que requererá um aprofundamento da capacidade de resiliência tecnológica.

Em resumo, as tecnologias emergentes promovem a produtividade, o crescimento e a inovação, suscitando a criação de novos modelos de negócio, processos e produtos. As tecnologias baseadas na internet como a internet móvel, trabalho colaborativo, internet das coisas (IoT) ou *cloud computing* são consideradas potenciadoras de benefícios econômicos, mas mais disruptivas. Os efeitos sistémicos dos riscos cibernéticos ou o colapso das infraestruturas de informação críticas colocam desafios que importará acautelar.

Os ataques ou incidentes cibernéticos têm sido considerados, nos últimos três relatórios, dos mais prováveis e com maior impacto, tendo mesmo sido registado um progressivo aumento da sua frequência e dimensão, se bem que de forma isolada em instituições ou países.

O aumento da conetividade promovida pela IoT, facilitadora da ligação de mais pessoas e equipamentos em rede, aumentará a dependência cibernética, a conectividade e interdependência e como tal, a probabilidade de ocorrência de ataques e a dificuldade de proteção dos mesmos, pelo que a resiliência cibernética ganhou relevância.

Apesar do reconhecimento dos benefícios das tecnologias, os riscos de segurança que lhe estão associadas não têm sido compreendidos pelas organizações, nem concretizados os investimentos que permitam diminuir o risco operacional.

O relatório realça ainda que é fundamental a integração da gestão das infraestruturas físicas e cibernéticas, reforçar a sua resiliência, os processos de negócio e as tecnologias de suporte.A médio prazo, as novas tecnologias e a sua integração terão impacto na segurança internacional, alterando os equilíbrios de poder, e a inovação tenderá a superar a capacidade de supervisão regulamentar.

Até agora, as capacidades de provocar destruição estavam reservadas aos detentores de poder letal, encontrando este poder apenas disponível para os Estados. Com a Quarta Revolução Industrial, essa capacidade ficou disponível a pequenos grupos ou indivíduos a partir dos seus computadores. A internet proporciona assim um novo horizonte para a guerra e, no futuro, todos os conflitos terão uma componente cibernética e alguns poderão mesmo ter lugar apenas no ciberespaço.

No ciberespaço é mais fácil atacar do que defender, pela facilidade no acesso a armas cibernéticas e à dificuldade de atribuição dos ciberataques, o que condicionará as arquiteturas de segurança dos Estados para fazer face a eventuais ataques ou violações. Nele, a distância física ao espaço de conflitualidade deixa de assegurar proteção, pois os ciberataques podem ser lançados a partir de locais remotos, fazendo uso de múltiplos equipamentos reféns de permeio e sem que os seus proprietários ou utilizadores se apercebam. As tecnologias *dual-use*, o controle privado da propriedade das infraestruturas críticas e as redes sociais são características indissociáveis deste novo ambiente virtual.

4 O *CyberpowerIndex*

O Índice de Poder Cibernético foi desenvolvido para obter uma melhor compreensão dos fatores que influenciam globalmente este poder e de que forma afeta as organizações. O índice é um modelo quantitativo e qualitativo dinâmico, construído a partir de 39 indicadores, medindo atributos específicos do ambiente cibernético através de quatro elementos orientadores do poder cibernético: quadro jurídico e regulamentar; contexto econômico e social; infraestruturas tecnológicas;

e aplicação industrial, que examinam o progresso digital em indústrias-chave (BOOZ ALLEN HAMILTON, 2013, p. 36).

Através de um exercício de *benchmarking* que abrangeu 19 países do G20, excluindo o seu último membro, a União Europeia (UE), cada país foi avaliado em relação aos outros, tendo-se concluído que:

- ✓ Apesar do forte desenvolvimento da sociedade digital permitir aumentar opoder cibernético potencial, o crescimento da dependência digital implica maiores riscos de segurança;
- ✓ As políticas abrangentes da Alemanha são a chave para o seu sucesso econômico e tecnológico, nomeadamente nos domínios jurídico e regulatório;
- ✓ Não existem Planos de Ação de Cibersegurança em algumas das grandes economias;
- ✓ O poder cibernético pressupõe sólidas fundações nos domínios das qualificações técnicas, educação, investigação e desenvolvimento, politicas comerciais e um ambiente empresarial inovador;
- ✓ Existe uma maior prioridade de acesso às tecnologias da informação e comunicações nos países desenvolvidos;
- ✓ Existe um limitado progresso tecnológico nas indústrias-chave dos países do G20.

5 O UK 2015 Information Security Breaches Survey

A recente publicação do governo britânico *UK 2015 Information Security Breaches Survey* (UNITED KINGDOM, 2015) representa uma fonte de informação estruturada sobre violações de cibersegurança no Reino Unido, segmentado por dimensão de organização[8]. Na ausência de informação nacional disponível e apesar das diferenças entre a realidade do Reino Unido e os demais países europeus em que se inclui Portugal, este relatório permite de forma objetiva visualizar alguns elementos que merecem a nossa reflexão, nomeadamente:

5.1 Intrusões e violações

- Aumento do número empresas e organizações, independentemente da sua dimensão, que reconheceram ter sofrido intrusões;

8 De acordo com a informação disponibilizada pelo relatório: as grandes organizações possuem mais de 250 colaboradores; as pequenas empresas possuem menos de 50 colaboradores; os resultados para as empresas de média dimensão (50-249 colaboradores) são semelhantes aos resultados para as pequenas, exceto quando indicado em contrário.

- Espectativa que os incidentes de segurançacontinuem a aumentar, requerendo um melhor alinhamento das defesas com as ameaças;
- Crescimento acentuado do custo-médio daciber-intrusão (cyberintrusion) mais grave sofrida para qualquer dimensão de negócio;
- Mudança do carácter dos ataques externos, passando a ser realizado por outsiders através de software malicioso (malware);
- Diminuição dos ataques de "negação de serviço" (denial of service - DoS), podendo indiciar a adoção de outros métodos de ataque mais sofisticados;
- As intrusões atribuídas ao pessoal das organizações, causadas por erro humano inadvertido, representam três quartos nas grandes organizações e quase um terço das pequenas organizações;
- Propensão do pessoal para causar ciber-violações através de vírus e outros tipos de software malicioso, apesar do aumento das ações de sensibilização;
- Aumento das violações de segurança da informação causadas ou potenciadas pela adoção de tecnologias destinadas a melhorar a produtividade ou a colaboração nomeadamente: acesso a redes sociais (13%), utilização de *smartphones* ou *tablets* (15%), adoção de serviços de *cloudcomputing* (7%) ou media portáteis (3%).

5.2 Normas, Sensibilizaçãoe Formação

- Aumento da percentagem de organizações que adotaram as normas de segurança promovidas pelo Governodo Reino Unido (Ten Steps to Cybersecurity) e a utilização de alertas governamentais sobre ameaças e vulnerabilidades;
- Quase metade das organizações auscultadas estão associadas ao programa Cyber Essentials apoiado pelo governo e pela indústria, visando orientar as empresas na sua proteção contra as ameaças cibernéticas (UNITED KINGDOM, 2014);
- A norma ISO270019 continua a ser o principal padrão adotado para a gestão de segurançada informação das organizações;
- Continuação da grande importância atribuída ao treino e sensibilização para a segurança;
- As administrações das organizações não estão suficientemente informadas sobre riscos de segurança (21%);

9 ISO/IEC 27001 - Information Security Management.

- Divergência quanto à atribuição de responsabilidade pela garantiada proteção de dados.

5.3 Políticas e Investimento

- As organizações cuja política de segurança foi mal compreendida tiveram violações de cibersegurança devido a ações do seu pessoal (75%);
- Aumento ligeiro do número de organizações onde a gestão de topo atribui uma prioridade "elevada" ou "muito elevada"à segurança da informação;
- Poucas organizações aumentaram os seus gastos em segurança da informação, e no futuro próximo, a tendência será reduzir ainda mais o número de instituições com a intenção de expandir os seus orçamentos neste domínio;
- Diferença substancial no perfil de despesa em segurança de informação em função da dimensão das empresas;
- Falta de avaliação da eficiência das despesas em segurança (25%);
- Não realização de qualquer forma de avaliação de risco de segurança (securityriskassessment) interno (32%);
- Intenção de investir em cyber-threatintelligence-i.e. na monitorização ativa das ameaças (32%);
- Proteção da informação dos clientes e a reputação da organização são os principais elementos 'motivadores' da despesa em segurança da informação;
- Mudança da natureza dos negócios como consequência de 'ciber-incidentes' (11%).

5.4 Recursos Humanos e Tecnológicos

- Tendência crescente para a contratação externa (outsourcing) de determinadas funções de segurança e o uso da computação e armazenamento na nuvem (cloudcomputing);
- Existência de recursos humanos qualificados em quantidade suficiente para gerir os riscos das organizações. Todavia, o relatório questiona até que ponto estas organizações possuem as qualificações e experiências adequadas às necessidades.
- Grande diversidade quanto aos níveis de maturidade da indústria no que respeita à gestão dos riscos de segurança, em consequência da diferença entre

os níveis mais elevados de absorção de *intelligence* sobre ameaças cibernéticas e a cobertura dos seguros de responsabilidade civil cibernética. O relatório conclui que, embora pareça existir uma quebra acentuada na cobertura de seguros, tal poderá decorrer de uma maior compreensão da cobertura fornecida por apólices de seguro *standard* para interrupções de negócios padrão, em casos de violação da segurança da informação.

6 A Situação na União Europeia

A União Europeia (UE) expressa na sua Estratégia para a cibersegurança (EUROPEAN COMMISSION, 2013a) uma visão articulada em cinco prioridades[10]. Para garantir a resiliência cibernética considera aconselhável que as instituições públicas e empresas do setor privado estreitem a sua cooperação de forma efetiva e desenvolvam capacidades específicas, podendo a UE favorecer a limitação dos riscos e ameaças cibernéticas transfronteiriças e colaborar na coordenação em situações de emergência cibernética.

As limitadas capacidades, recursos e processos indispensáveis à prevenção, deteção e resolução de incidentes cibernéticos são reconhecidas e continuam a ser uma das vulnerabilidades da Europa que importa obviar, pelo que a Comissão Europeia elaborou uma proposta de uma Política de Segurança das Redes e da Informação: *Network and Information Security – NIS*. (EUROPEAN COMMISSION, 2013b).

A Diretiva para as comunicações eletrônicas estabelece o dever dos operadores de comunicações na gestão do risco das respetivas redes bem como de informação sobre violações de segurança significativas (THE EUROPEAN PARLIAMENT AND THE COUNCIL, 2002). Por outro lado, no âmbito da legislação sobre proteção de dados da UE (EUROPEAN PARLIAMENT; CONCIL..., 1995) os "responsáveis pelo tratamento de dados"[11] devem assegurar os requisitos de proteção de dados, inclusive de

10 Resiliência cibernética, redução drástica da criminalidade cibernética, desenvolvimento da política e capacidades de ciberdefesa no âmbito da Política Comum de Segurança e Defesa (CSDP), desenvolvimento de recursos industriais e tecnológicos para a cibersegurança, estabelecer uma política internacional coerente para o ciberespaço para a União Europeia e promover os valores fundamentais da UE.

11 Na versão inglesa designam-se 'controllers' e representam "a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios do tratamento sejam determinados por disposições legislativas ou regulamentares nacionais ou comunitárias, o responsável pelo tratamento ou os critérios específicos para a sua nomeação podem ser indicados pelo direito nacional ou comunitário". (EUROPEAN PARLIAMENT; CONCIL..., 1995).

segurança e de notificação de incidentes com violações de dados pessoais às autoridades nacionais competentes.

A Estratégia da UE para a Cibersegurança refere ainda a elaboração de legislação visando:

- ✓ Ao estabelecimento de requisitos nacionais mínimos e comuns para asegurança das redes e da informação;
- ✓ À criação e coordenação de mecanismos de prevenção, deteção, atenuação e resposta, permitindo a partilha de informação e assistência mútua entre as autoridades nacionais competentes no domínio da segurança das redes e da informação;
- ✓ À melhoria da preparação e empenhamento do setor privado, através do desenvolvimento de uma adequada cultura de cibersegurança, capacidades técnicas próprias de resiliência cibernética, adequada gestão dos riscos e partilha das melhores práticas.

No âmbito da Política Comum de Segurança e Defesa, este documento realça que os esforços no domínio da cibersegurança também envolvem a dimensão da ciberdefesa, pelo que as capacidades de ciberdefesa se devem concentrar na deteção e resposta das e às ameaças cibernéticas sofisticadas por forma a assegurar a resiliência dos Sistemas de Informação e Comunicação (SIC) que apoiam as políticas de defesa dos Estados-membros e os seus interesses de segurança.

Na proteção dos recursos cibernéticos críticos, a UE entende existirem sinergias decorrentes do reforço da cooperação entre as abordagens civis e militares, apoiadas por Investigação e Desenvolvimento (I&D), cooperação intergovernamental, com o setor privado e as universidades.

Os recursos cibernéticos críticos, também designados por Infraestruturas de Informação Críticas (IIC), são sistemas de Tecnologias de Informação e Comunicação (TIC) considerados "críticos por si próprios ou essenciais para a operação de infraestruturas críticas (telecomunicações, computadores/*software*, internet, satélites, etc.)." (EUROPEAN COMMISSION, 2005).

Em 2005, a União Europeia designou a Proteção das Infraestruturas de Informação Críticas (PIIC) como o conjunto de: "[…] programas e atividades promovidas pelos proprietários das infraestruturas, operadores, fabricantes, utilizadores e autoridades reguladoras visando assegurar a performance das CII acima de um certo nível de serviço em caso de falha, ataque ou acidente, tendente a minimizar o seu tempo de recuperação e obviar a sua danificação". (EUROPEAN COMMISSION, 2005).

Ainda decorrente da Estratégia para uma Sociedade de Informação Segura (EUROPEAN COMMISSION, 2006b) cujo objetivo era reforçar a segurança e confiança

na Sociedade de Informação (NEVES, 2003), a Comissão Europeia produziu uma comunicação sobre a Proteção de Infraestruturas de Informação Críticas (EUROPEAN COMMISSION, 2009) para a prevenção, preparação e sensibilização, integrando um plano ação com um conjunto de medidas que visavam reforçar a segurança e resiliência das IIC e articuladas com as prioridades da política de SRI[12]. As propostas do plano complementavam ainda as ações no âmbito da prevenção, combate e repressão de atividades criminais e terroristas tendo por alvo as IIC, bem como outras iniciativas Europeias (ex. Segurança das Redes e Informação) ou internacionais.

Merecem ainda referência o Programa Europeu de Proteção de Infraestruturas Críticas (PEPIC) e a Diretiva sobre a Identificação e Designação das Infraestruturas Críticas Europeias (IDICE).

A versão inicial da IDICE, então considerado um primeiro passo no domínio da proteção das infraestruturas críticas europeias, considerava como críticos primariamente os setores da energia e transportes (EUROPEAN COMMISSION, 2006a). A referida Diretiva porém, já antecipava a necessidade de incluir outros setores, nomeadamente das tecnologias de informação e comunicação, e atribuía a responsabilidade primária pela sua proteção aos Estados-membros e seus proprietários ou operadores.

A atual versão do IDICE (COUNCIL OF THE EUROPEAN UNION, 2008) reconhece que a proteção e o aumento da resiliência das infraestruturas permitem minimizar o impacto sobre a perda de serviços pela sociedade e introduz a análise das interdependências entre infraestruturas críticas, indústria e atores estatais, tendo em consideração que:

- ✓ Uma única infraestrutura crítica pode ter um impacto significativo sobre múltiplos atores e infraestruturas;
- ✓ As interdependências podem ser transfronteiriças, multissetoriais e em diversos países dentro do mesmo setor.

O desenvolvimento da segurança e a estimulação da utilização de produtos, processos e serviços seguros carece de uma cultura de gestão de risco, capaz de responder às ameaças conhecidas e antecipar as desconhecidas, mas evitando reações excessivas.

Os desafios da proteção das infraestruturas de informação críticas foram identificados pela União Europeia como sendo decorrentes de estratégias nacionais heterogêneas e descoordenadas, da necessidade de um novo modelo europeu de governação para as infraestruturas de informação críticas, das limitadas capacidades de alerta rápido e de resposta a incidentes e da cooperação internacional.

12 Atendendo a que o documento é de 2009, presume-se que se trata de referência a proposta ou versão da Política de Segurança das Redes e Informação entretanto aprovada em 2013.

Da heterogeneidade e descoordenação das abordagens dos Estados-membros decorre o risco de fragmentação e ineficiência europeia, face à interconexão das infraestruturas de informação críticas e ao potencial impacto mutuo dos baixos níveis de segurança e resiliência de uns nas vulnerabilidades e riscos dos demais.

A segurança e a resiliência das infraestruturas de informação críticas, apesar de condicionadas pelas políticas dos Estados-membros, dependem da atuação, nomeadamente do investimento, do setor privado que detém a sua propriedade ou as controla. O modelo de parcerias público-privadas (PPP) nacionais que a União Europeia entendia poder obviar esta situação não teve até ao momento receptividade num plano mais abrangente de PPP Europeias.

Para obviar às diferenças de processos e práticas de monitorização e comunicação de incidentes entre os Estados-membros, que afetam a boa governação das infraestruturas de informação críticas e consequentemente a sua segurança e resiliência, é indispensável desenvolver mecanismos de cooperação e partilha de informação, simulação de incidentes e realização de exercícios para testar as capacidades de resposta.

A internet enquanto considerada como infraestrutura de informação crítica coloca fundadas preocupações relativamente à sua resiliência e estabilidade para lidar com perturbações e ataques cibernéticos, atendendo à contínua expansão dos seus serviços e ao crescimento da sua complexidade física e lógica, apesar da robustez da arquitetura distribuída e crescente redundância. Neste sentido, entende-se como essencial alcançar consenso no plano europeu relativamente às prioridades à sua estabilidade e resiliência no plano das políticas públicas e capacidades operacionais e a cooperação internacional visando ao desenvolvimento de um conjunto de princípios que reflitam os valores europeus.

Para obviar aos desafios da proteção das infraestruturas de informação críticas, a União Europeia propôs um plano de ação assente em cinco pilares: (1) preparação e prevenção: assegurar a preparação a todos os níveis; (2) deteção e resposta: criar mecanismos adequados de alerta rápido; (3) mitigação e recuperação: reforçar os mecanismos de defesa das CII na UE; (4) cooperação internacional: promover internacionalmente as prioridades da UE; e (5) estabelecimento de critérios para o sector das TIC: apoiar a aplicação da diretiva relativa à identificação e designação das infraestruturas críticas europeias (EUROPEAN COMMISSION, 2009).

Em 2011, na sequência de uma comunicação da Comissão Europeia sobre proteção de infraestruturas de informação críticas, intitulada *Achievements and Next Steps: Towards Global Cybersecurity* teve lugar uma Conferência Ministerial da UE[13].

13 Reunião organizada pela Presidência do Conselho Europeu em 14/15 de abril de 2011, em Balatonfüred, em colaboração com a Comissão, sobre Proteção de Infraestruturas de Informação Críticas (PIIC).

A comunicação da Comissão Europeia tomou em consideração o Plano de Ação de PIIC (EUROPEAN COMMISSION, 2009) enfatizando:

- ✓ A importância da cibersegurança e da proteção das infraestruturas de informação críticas para a confiança dos cidadãos e as empresas na internet e demais redes, e para a Agenda Digital para a Europa (EUROPEAN COMMISSION, 2009);
- ✓ A globalização dos desafios e a importância da cooperação entre os Estados-membros e o setor privado, ao nível nacional, europeu e internacional;
- ✓ A necessidade de envolvimento de todos os interessados na coordenação das iniciativas para prevenir, detetar, mitigar e reagir a todos os tipos de incidentes, mesmo naturais;
- ✓ A promoção de princípios orientadores para a resiliência e a estabilidade da internet; a materialização de parcerias estratégicas internacionais e esforços coordenados nas instâncias internacionais; e a melhoria da preparação da UE (estabelecimento de CERTs[14] nas instituições europeias) (EUROPEAN COMMISSION, 2009).

A declaração da Presidência do Conselho Europeu após a referida Conferência Ministerial reiterou a necessidade dos Estados-membros em "intensificarem os seus esforços no reforço das suas capacidades nacionais de segurança cibernética." (COUNCIL OF THE EUROPEAN UNION, 2011a). Na referida Conferência foram discutidas um conjunto de medidas, posteriormente acordadas no âmbito do "Working Party on Telecommunications and the Information Society" e submetidas para aprovação na reunião do Conselho da União Europeia que teve lugar em 27 de maio de 2011(COUNCIL OF THE EUROPEAN UNION, 2011b), incluindo um conjunto de elementos considerados de extrema importância para a proteção de infraestruturas críticas de informação, decorrentes da atuação dos Estados, da Comissão Europeia e da *European Union Agency for Network and Information Security* (ENISA), nomeadamente:

- ✓ A relevância estratégica das tecnologias de informação e comunicação e da indústria de segurança das redes bem como informação na proteção sustentada das infraestruturas de informação críticas europeias;
- ✓ O desenvolvimento de CERTs nacionais e governamentais;

14 Computer Emergency Response Teams.

- ✓ A conceção de planos de contingência para incidentes cibernéticos e o seu teste através da organização de exercícios nacionais;
- ✓ A promoção da cooperação europeia entre os Estados-membros no domínio cibernético através de mecanismos de articulação sobre incidentes, organização de exercícios à escala europeia , por exemplo, CyberEurope 2012, e o debate de temas relacionados com a segurança dos sistemas e tecnologias de informação e comunicação;
- ✓ Reforço da cooperação internacional nos domínios da segurança das redes e informação através do estabelecimento de parcerias estratégicas bilaterais e multilaterais15;
- ✓ Utilização e desenvolvimento de requisitos mínimos, princípios básicos e normas de segurança das redes e da informação, na promoção de security by design de produtos e serviços;
- ✓ Promoção de um "ambicioso" programa de investigação e desenvolvimento no domínio da segurança das redes, sistemas de informação e aplicações visando à sua articulação com a proteção de infraestruturas críticas de comunicação;
- ✓ Utilização de abordagens colaborativas para a segurança das redes e informação;
- ✓ Colaboração e responsabilização dos setor público e privado no desenvolvimento das suas capacidades e preparação para prevenir, detetar e responder aos desafios de segurança com potencial impacto sobre a disponibilidade de redes de comunicações eletrônicas e serviços;
- ✓ Desenvolvimento e produção de produtos de soluções de hardware, software e serviços TIC mais seguros e confiáveis;
- ✓ Promoção de uma cultura de gestão de risco e programas de educação, formação e investigação no domínio da segurança das redes e informação;
- ✓ Adoção de uma Estratégia Nacional de Cibersegurança, quando esta não exista;
- ✓ Assistência mútua e voluntária entre os Estados-membros em incidentes transfronteiriços;
- ✓ Acompanhamento das estratégias de governação das tecnologias emergentes com potencial impacto global , como cloudcomputing;

15 Por exemplo por meio do EU-U.S. Working Group on Cybersecurity and Cybercrime.

- ✓ Sensibilização dos cidadãos sobre as suas responsabilidades enquanto utilizadores de TIC, desafios e riscos de segurança das redes e da informação e melhores práticas na sua prevenção e/ou reação;
- ✓ Participação em PPP visando ao desenvolvimento de redes de comunicações seguras e confiáveis e o fortalecimento da indústria europeia de tecnologias de informação.

Posteriormente, o Conselho Europeu de 24/25 de outubro de 2013 solicitou a criação de uma rede de coordenadores digitais nacionais visando o desenvolvimento da *Cloud Computing*, *Big Data*e *Open Data*, bem como a adoção da *EU General Data Protection Framework' eda'EU Cyber-Security Directive,* consideradas essenciais para o 'Mercado Único Digital' a estabelecer em 2015 (EUROPEAN COUNCIL, 2013).

As conclusões do Conselho Europeu de 19/20 de dezembro de 2013 solicitavam a criação da *EU Cyber Defence Policy Framework* em 2014, tendo por base uma proposta de Alta Representante, em cooperação com a Comissão Europeia e a Agência Europeia de Defesa (AED) (EUROPEAN COUNCIL, 2013).O Conselho Europeu manifestou ainda o seu compromisso no apoio ao estabelecimento de capacidades e na minimização de deficiências cibernéticas críticas através de projetos concretos dos Estados-membros, apoiados pela AED.

As conclusões incluíram ainda uma referência à propriedade e à operação das capacidades cibernéticas pelos Estados-membrose ao desenvolvimento de um roteiro e projetos concretos visando ao desenvolvimento concorrente de iniciativas de exercício e treino, cooperação civil/militar na base da Estratégia de Segurança Cibernética da União Europeia – o que favoreceria uma iniciativa de educação e treino ciber, organizada por Portugal, como veremos – e a proteção dos ativos em missões e operações da UE.

No Conselho Europeu de 26/27 de junho 2014 (EUROPEAN COUNCIL, 2014), foi realçada a necessidade de apoiar os Estados-membros no desenvolvimento de uma abordagem abrangente para a cibersegurança e cibercriminalidade, através da mobilização de todos os instrumentos de cooperação judiciária e policial e reforço da capacidade de coordenação da Europol[16] e do Eurojust[17]. Entre as prioridades enunciadas destacam-se o combate ao crime cibernético e a proteção de dados pessoais e a segurança cibernética, nomeadamente através da cooperação com os parceiros estratégicos da UE.

16 Serviço Europeu de Polícia/European Union's Law Enforcement Agency.

17 Unidade Europeia de Cooperação Judiciária/European Union's Judicial Cooperation Unit.

A '*EU Cyber Defence Policy Framework*' (COUNCIL OF THE EUROPEAN UNION, 2014a) foi aprovada na sequência do Conselho da União Europeia de 17/18 de dezembro de 2014 (COUNCIL OF THE EUROPEAN UNION, 2014b), visando: ao apoio ao desenvolvimento das capacidades de defesa cibernética dos Estados-membros, empenháveis em operações e missões no âmbito da Política Comum de Segurança e Defesa e à proteção das redes de comunicação e informação do Serviço Europeu de Ação Externa (SEAE) relevantes para a PCSD.

Este documento identifica princípios facilitadores do desenvolvimento de capacidades de ciberdefesa com o setor privado, nomeadamente: através do reforço da I&D e da *European Defence Technological and Industrial Base* (EDTIB); iniciativas cooperativas multinacionais de "*poolingandsharing*" no âmbito do exercício e treino de ciberdefesa; e o reforço da cooperação com a NATO no domínio da ciberdefesa.

O quadro de referência apresentado enfatiza ainda que:

- ✓ Os exercícios devem permitir melhorar a capacidade de reação da União Europeia na reação a crises do ciberespaço no contexto da PCSD, melhorar o processo de decisão estratégica da UEe fortalecer a arquitetura das infraestruturas de informação;
- ✓ Os objetivos da ciberdefesa devem ser integrados de forma mais harmoniosa nos mecanismos de gestão de crises da União Europeia.

Relativamente a cada uma das prioridades da '*EU CyberDefencePolicy Framework*' é apontado:

- ✓ Que as capacidades de defesa cibernética dos Estados-membros disponíveis no âmbito da Política Comum de Segurança e Defesa requerem a garantia de resiliência das redes através da proteção das redes de comunicação geridas pelo Serviço Europeu de Ação Externa; o desenvolvimento de capacidades de ciberdefesa dos Estados-membros disponíveis para missões e operações; a avaliação contínua das vulnerabilidades das infraestruturas de informação associado ao conhecimento em tempo quase real da eficácia da proteção e a convergência dos requisitos de ciberdefesa da infraestrutura de Comando, Controlo, Comunicações e Computadores (C4).
- ✓ A necessidade de reforço da proteção das redes de comunicação e informação do Serviço Europeu de Ação Externa e demais instituições da UE suscita que o SEAE deverá desenvolver uma capacidade tecnológica de segurança e defesa autônoma que

permita aumentar a resiliência das suas redes da PCSD visando à prevenção, deteção, resposta a incidentes, conhecimento da situação, troca de informação e mecanismos de alerta precoce.

- ✓ A coexistência de sistemas de informação de diferentes atores institucionais da UE durante a condução das operações e missões da PCSD, implica a necessidade de simplificação das normas de segurançae uma cadeia de comando unificada que permita a melhorar a resiliência das redes utilizadas para a PCSD, tendo sido ainda identificadas as seguintes ações a desenvolver:

- Fortalecimento da capacidade de segurança das TI com base na capacidade técnica e procedimentos existente;
- Cooperação com as capacidades de segurança cibernética existente na UE;
- Desenvolver políticas e orientações de segurança de TI coerentes, tendo em consideração os requisitos deciberdefesa em contexto PCSD;
- Reforçar as capacidades de intelligence e de avaliação das ameaças cibernéticas, de forma a identificar novos riscos e elaborar avaliações de risco regulares e em tempo quase-real;
- Desenvolver e integrar a ciberdefesa para as operações civis e militares de CSDP no planeamento estratégico;
- Melhorar a coordenação de defesa cibernética;
- Revisão periódica dos requisitos de recursos de acordo com as ameaças e em coordenação com as demais instituições europeias.
- A cooperação civil-militar (instituições europeias, agências e setor privado) no domínio cibernético beneficiará de capacidades cibernéticas *dual-use*, I&D, intercâmbio de melhores práticas, partilha de informação e mecanismos de alerta precoce, avaliações de risco de resposta a incidentes, ações de sensibilização. As atividades conjuntas no domínio do treino e exercícios além de reforçarem a cooperação permitirão reduzir os custos.

7 A Situação em Portugal

Apesar do ciberterrorismo não ser o foco deste artigo, sendo este assunto referido apenas em algumas das referências utilizadas, a Estratégia Nacional de Combate ao Terrorismo mintegra um conjunto de elementos extremamente importantes para o enquadramento da temática da cibersegurança em Portugal.

A Estratégia Nacional de Combate ao Terrorismo tem como pressuposto o "[…] compromisso de combate ao terrorismo emtodas as suas manifestações", e

tem como objetivos estratégicos: detetar, prevenir, proteger, perseguir e responder. De entre as linhas de ação associadas a cada objetivo estratégico, destacam-se as consideradas mais relevantes e relacionadas com o domínio da cibersegurança, ciberdefesa e áreas conexas (PORTUGAL, 2015a).

Quadro 1 - Domínio da cibersegurança, ciberdefesa e áreas conexas

Detetar
- Reforçar a eficiência na partilha da informação entre as forças e serviços de segurança ou outras entidades, no âmbito das respetivas competências, ao nível nacional, europeu e internacional.

Prevenir
- Consciencializar os operadores públicos e privados da natureza crítica da segurança informática;
- Intensificar a cooperação entre todos os setores da sociedade civil, por forma a responder aos desafios que a utilização da Internet coloca no domínio da radicalização e do recrutamento para o terrorismo;
- Defender a sociedade de conteúdos de apologia da violência e do terrorismo publicamente acessíveis pela Internet, promovendo a sua remoção ou bloqueio.

Proteger
- Desenvolver um registo central de identificação de infraestruturas críticas, em todos os setores de atividade econômica e social, e prover à sua atualização;
- Desenvolver o 'Plano de Ação para a Proteção e Aumento da Resiliência das Infraestruturas Críticas';
- Implementar o 'Plano de Ação Nacional para a Proteção contra as Ciberameaças', integrado numa estratégia nacional de cibersegurança;
- Avaliar periodicamente as vulnerabilidades resultantes de infraestruturas essenciais, nacionais e europeias, para transportes e energia;
- Avaliar as vulnerabilidades dos sistemas de informação críticos e manter e acompanhar a adoção das medidas de correção face a ciberataques;

Perseguir
- Reforçar a colaboração e articulação ente os vários intervenientes e responsáveis nas áreas da cibersegurança, ciberespionagem, ciberdefesa e ciberterrorismo, nos termos da Constituição e da Lei;
- Robustecer uma abordagem integrada na resposta, operacionalizando um efetivo sistema nacional de gestão de crises;

Responder
- Executar ações que permitam exercitar os procedimentos e a articulação entre os diversos atores e desenvolver os mecanismos de interoperabilidade que permitam uma resposta pronta e eficaz a ocorrências terroristas, incluindo sistemas de informação críticos face a ciberataques.

Fonte: O AUTOR, 2016.

8 A Estratégia Nacional de Segurança do Ciberespaço

O Plano Global Estratégico de Racionalização e Redução de Custos com as Tecnologias de Informação e Comunicação (TIC) na Administração Pública, apresentado pelo Grupo de Projeto para as Tecnologias de Informação e Comunicação (GPTIC) foi aprovado pelo Governo em 2012 (PORTUGAL, 2012a). Esse plano foi estruturado em torno de cinco eixos de atuação[18], integrando 25 medidas de racionalização das TIC com caráter transversal e impacto potencial em toda a Administração Pública.

No âmbito da medida número 4 (Definição e Implementação de umaEstratégia Nacional de Segurança da Informação) estava previsto consolidar a Estratégia Nacional de Segurança da Informação (ENSI[19]), definindo os objetivos nacionais (aquilo que cada membro da Sociedade da Informação pode esperar e contar a nível nacional), responsabilidade (quem é responsável pela implementação da segurança da informação no país), organização (qual a estrutura definida para a segurança da informação), gestão (quem é responsável por estabelecer, controlar e medir e gerir o risco e auditar a segurança da informação) e serviços (que serviços são fornecidos a nível nacional e por quem) da segurança da informação.

O referido documento previa ainda que a ENSI integrasse o estabelecimento do Centro Nacional de Cibersegurança, a criação e certificação de uma solução de criptografia forte de origem nacional, e a revisão do quadro legal para a segurança das matérias classificadas.

O desenvolvimento desta medida foi atribuída ao Gabinete Nacional de Segurança (GNS), com a colaboração de todas as entidades relevantes em razão da matéria, no âmbito do grupo de trabalho existente na Rede Interministerial das TIC.

Na sequência da constituição da Comissão Instaladora do Centro Nacional de Cibersegurança[20] e dos trabalhos por ela desenvolvidos, foi aprovada pelo Governo a criação do Centro Nacional de Cibersegurança (CNCSeg) temporariamente inserido na estrutura do GNS, tendo por missão:"contribuir para que Portugal use o ciberespaço de uma forma livre, confiável e segura,

18 "(1) melhoria dos mecanismos de governabilidade; (2) redução de custos; (3) utilização das TIC para potenciar a mudança e a modernização administrativa; (4) implementação de soluções TIC comuns; e (5) estímulo ao crescimento económico."

19 A título informativo, refira-se que em 2005 foi elaborada a 'Política Nacional de Segurança da Informação no âmbito da Estratégia Nacional de Segurança da Informação' (UNISYS, 2005).

20 Resolução do Conselho de Ministros nº 42/2012 (PORTUGAL, 2012b).

através da melhoria contínua da Cibersegurança nacional e da cooperação internacional." (PORTUGAL, 2014).

Quadro 2 - Competências do Centro Nacional de Cibersegurança

Competências do Centro Nacional de Cibersegurança:

- Desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques;
- Promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança;
- Exercer os poderes de autoridade nacional competente em matéria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais;
- Contribuir para assegurar a segurança dos sistemas de informação e comunicação do Estado e das infraestruturas críticas nacionais;
- Promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança;
- Assegurar a produção de referenciais normativos em matéria de cibersegurança;
- Apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da cibersegurança;
- Assegurar o planeamento da utilização do ciberespaço em situação de crise e de guerra no âmbito do planeamento civil de emergência, no quadro definido pelo Decreto-Lei n.º 73/2013, de 31 de maio;
- Coordenar a cooperação internacional em matérias da cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros;
- Exercer as demais competências que lhe sejam atribuídas por Lei.

Fonte: O AUTOR, 2016.

Na sequência de um anteprojeto daEstratégia Nacional de Cibersegurança, proposto pela Comissão Instaladora do CNCSeg, foi aprovada a 'Estratégia Nacional de Segurança do Ciberespaço'(PORTUGAL, 2015c). O seu preâmbulo está alinhado com as visões e tendências enunciadas nos documentos de referência da União Europeia para a cibersegurança e áreas afins e nos relatórios *Global Risks* do Fórum Econômico Mundial, fazendo referência a um conjunto de elementos enquadradores que importa realçar:

- ✓ O desenvolvimento sociedade da informação e a dependência do país das tecnologias de informação e comunicação para realização de "funções vitais";
- ✓ Uma 'Agenda Digital' potenciadora de a atividade económica e social;
- ✓ O reconhecimento das vulnerabilidades das TIC de que decorrem riscos para a sociedade;
- ✓ A criminalidade sexual e a sua dimensão transnacional, potenciadas pela internet;
- ✓ O 'cibercrime' nas suas múltiplas facetas nomeadamente: fraude bancária e usurpação de identidade;
- ✓ O hacktivismo político através do 'desvio e revelação de informação', 'sabotagem informática' e a 'espionagem de Estado e industrial';
- ✓ O impacto na infraestruturas vitais de informação do ativismo religioso, criminal ou terrorismo;
- ✓ A segurança ciberespaço como espaço de soberania e prioridade nacional;
- ✓ A necessidade de uma eficaz gestão de crises e coordenação da resposta operacional
- ✓ A cooperação nacional, europeia e internacional;
- ✓ A necessidade de reduzir as fragilidades da segurança das redes e da informação e de aumentar a resiliência das infraestruturas críticas.

A Estratégia tem como finalidade "aprofundar a segurança das redes e da informação", enquanto condição indispensável à segurança e defesa das 'infraestruturas críticas' e 'serviços vitais de informação'[21].

A referência às Infraestruturas Críticas (IC) e não apenas às Infraestruturas de Informação Críticas (IIC) aparenta incorporar a visão da União Europeia de interdependência setorial das IC.

Ao visar potenciar uma utilização livre, segura e eficiente dociberespaçoa Estratégia reconhece a importância da liberdade no acesso às TIC e em particular à internet para a sociedade em geral e à segurança e eficiência na comunicação e transações eletrónicas, caraterísticas essenciais para a atividade económica. O seu âmbito é abrangente e procura dar resposta às necessidades dos cidadãos, empresas, setor público e privado.

A Estratégia está fundamentada num conjunto de princípios[22] [gerais] e

21 O conceito de serviços vitais de informação não é caraterizado no documento.

22 " […] nos princípios gerais da soberania do Estado, das linhas gerais da Estratégia da União

pilares[23] e desenvolve-se em quatro objetivos estratégicos, com uma orientação geral e específica, refletidos em seis eixos de intervenção, integrando medidas concretas e linhas de ação (PORTUGAL, 2015b).

Quadro 3: Objetivos Estratégicos e Eixos de Intervenção

Objetivos Estratégicos

- Promover uma utilização consciente, livre, segura e eficiente do ciberespaço;
- Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos;
- Fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais;
- Afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação.

Eixos de Intervenção

- Eixo 1 – Estrutura de segurança do ciberespaço;
- Eixo 2 – Combate ao cibercrime;
- Eixo 3 – Proteção do ciberespaço e das infraestruturas;
- Eixo 4 – Educação, sensibilização e prevenção;
- Eixo 5 – Investigação e desenvolvimento;
- Eixo 6 – Cooperação.

Fonte: O AUTOR, 2016.

Entre as múltiplas iniciativas enunciadas pela Estratégia realçam-se as seguintes, pela sua ligação às atividades desenvolvidas pelo Instituto da Defesa Nacional:

- ✓ Eixo 1 (Estrutura de Segurança do Ciberespaço): realização de exercícios de gestão de crises visando avaliar a preparação e maturidade das instituições;

Europeia para a Cibersegurança e na estrita observância da Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa, da Carta dos Direitos Fundamentais da União Europeia, da proteção dos direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade." (PORTUGAL, 2015c).

23 Subsidiariedade, complementaridade, cooperação, proporcionalidade e sensibilização.

- ✓ Eixo 4 (Educação, Sensibilização e Prevenção): promoção de uma cultura de segurança, assim como a informação e sensibilização da sociedade civil, entidades públicas e privadas, em especial as detentoras das infraestruturas críticas e a formação especializada de decisores públicos e privados;
- ✓ Eixo 6 (Cooperação): participação em exercícios de segurança e defesa do ciberespaço, nacionais e internacionais no contexto da União Europeia e da NATO.

9 Orientação Política para a Ciberdefesa

A ciberdefesa encara o ciberespaço como uma potencial ameaça à Defesa Nacional, pela sua vulnerabilidade a ataques cibernéticos às infraestruturas críticas e aos recursos de informação nacionais. O ciberespaço é considerado um novo domínio operacional em que podem ser conduzidas operações militares, indispensáveis às Forças Armadas para o seu Comando e Controlo.

É neste contexto que foi promulgada a orientação política para a ciberdefesa (PORTUGAL, 2013a), em articulação com um conjunto de documentos enquadradores, nomeadamente:

- ✓ O Conceito Estratégico de Defesa Nacional (PORTUGAL, 2013b), quando se refere aos potenciais efeitos dos ataques cibernéticos e identifica o ciberterrorismo e a cibercriminalidade como "ameaças e riscos prioritários", podendo afetar infraestruturas críticas e estruturas tecnológicas que suportam a organização social e econômica nacional; a criação de um Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN); e o levantamento da capacidade de ciberdefesa nacional;
- ✓ A Reforma Defesa 2020 (PORTUGAL, 2013c), que preconiza a centralização num serviço único coordenador das Comunicações e os Sistemas de Informação, em articulação com os Ramos, o estabelecimento de uma capacidade de apoio à decisão e a criação do Centro de Ciberdefesa na estrutura do Estado-Maior General das Forças Armadas (EMGFA).
- ✓ A Orientação para a Política de Ciberdefesa assemelha-se a uma Estratégia Nacional para a Ciberdefesa e visa definir os objetivos, estabelecer as linhas orientadoras e promover o levantamento da capacidade nacional de ciberdefesa.

Os princípios subjacentes a este documento de Política para a Ciberdefesa realçam:

- ✓ A prevenção, deteção, contenção e alerta dos ataques cibernéticos e danos associados;
- ✓ A proporcionalidade da resposta a cada tipo de ataque em função da avaliação da ameaça cibernética;
- ✓ O reforço da segurança dos Sistemas de Informação e Comunicação (SIC)24críticos de forma a potenciar a capacidade de recuperação;
- ✓ A defesa cooperativa das IIC em articulação e com o apoio da NATO e UE;
- ✓ A subordinação das ações e operações militares de ciberdefesa ao quadro legal em vigor;
- ✓ O recurso a capacidades técnicas associadas à cibersegurança;
- ✓ A complementaridade da ciberdefesa na gestão do risco operacional (SEWALL, 2009) das IIC através da criptografia, segurança da informação, segurança física e do pessoal;
- ✓ A existência de uma capacidade de recolha e análise de informação no ciberespaço;
- ✓ A necessidade de apoio jurídico à condução das operações;
- ✓ A adoção do quadro de segurança em vigor25 na classificação, manuseamento e acesso a informação sobre ciberdefesa;
- ✓ A necessidade de as Forças Armadas recrutarem e reterem recursos humanos qualificados de forma adequada ao ambiente operacional do ciberespaço;
- ✓ A exigência de uma abordagem conjunta[26] e cooperativa[27].*(PORTUGAL, 2013a).*

24 Entendemos que a designação "SIC críticos" utilizada no texto da 'Orientação Política para a Ciberdefesa' deve ser entendida como Infraestruturas de Informação Críticas (IIC), designação normalmente utilizada na bibliografia de referência sobre o ciberespaço.

25 Apesar de não ser referido explicitamente, tal poderá implicar adoção de normas estritamente nacionais ou NATO.

26 Envolvendo mais de um Ramo das Forças Armadas.

27 Apesar de não ser explícito, entendemos tratar-se de uma abordagem cooperativa nos planos bilateral e multilateral (UE, NATO, ONU).

Quadro 4: Objetivos Estratégicos e Linhas Orientadoras

Objetivos Estratégicos

- Garantir a proteção, a resiliência e a segurança das redes e dos SIC da defesa nacional contra ciberataques;
- Assegurar a liberdade de ação do País no ciberespaço e, quando necessário e determinado, a exploração proactiva do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse Nacional;
- Contribuir de forma cooperativa para a cibersegurança nacional.

Linhas Orientadoras

- Estrutura de Ciberdefesa Nacional
  - ✓ Órgão com caráter de orientação estratégica - militar das atividades de ciberdefesa;
  - ✓ Capacidade militar de resposta operacional a ciberataques e a incidentes informáticos.
- Planeamento de Defesa Militar
  - ✓ Integração da criação da Capacidade de ciberdefesa nos processos de Planeamento Nacional (Processo de Planeamento de Defesa Militar), da NATO (*NATO DefencePlanningProcess*- NDPP) e da União Europeia (*CapabilityDefencePlan* - CDP).
- Capacidade para conduzir Operações Militares em Redes de Computadores
  - ✓ Implementação de capacidades para conduzir todo o espectro de operações no ciberespaço (defensivas, de exploração e ofensivas).
- Reforço da Capacidade de Informações no Ciberespaço
  - ✓ Produção de conhecimento situacional e recolha de informação.
- Partilha da Informação de Ciberdefesa
  - ✓ Implementação de sistemas de partilha de informação e de alerta imediato[1].
  - ✓ Estratégia de ciência e tecnologia para a ciberdefesa.
- Sensibilização, Formação e Exercícios
  - ✓ Sensibilização de utilizadores dos SIC;
  - ✓ Formação e qualificação de peritos em ameaças cibernéticas e operações em redes de computadores;
  - ✓ Treino em ambientes degradados;
  - ✓ Participação em exercícios nacionais e internacionais de ciberdefesa;
  - ✓ Centralização da formação e treino em ciberdefesa
  - ✓ Constituição de um polo de excelência em ciberdefesa;
- Aquisições e Cadeia de Reabastecimento – Gestão de Risco
  - ✓ Adoção de requisitos de gestão de risco visando reduzir risco com *software* ou do *hardware.*

Fonte: O AUTOR, 2016

10 O Programa do XXI Governo Constitucional

O Programa do Governo (PORTUGAL, 2015a) enuncia um conjunto de linhas de orientação ou medidas no âmbito cibernético que importa realçar:

- ✓ No âmbito da defesa, o reforço do combate ao ciberterrorismo, através do Centro de Ciberdefesame pela cooperação e articulação internacional no combate ao cibercrime;
- ✓ No âmbito da segurança interna e política criminal:

• O estabelecimento de orientações estratégicas de segurança interna em resposta aos principais riscos e ameaças internas e externas, nomeadamente o cibercrime;

• A ampliação das responsabilidades e meios do Centro Nacional de Cibersegurança, preservando a segurança das infraestruturas e os direitos fundamentais, designadamente a privacidade, em articulação com as estruturas homólogas do setor da defesa nacional;

• A melhoria das capacidades da Polícia Judiciária, nomeadamente no combate à cibercriminalidade.

- ✓ A referência ao papel das Forças Armadas na luta contra as ameaças à segurança coletiva, em especial à cibercriminalidade.

11 O Curso de Cibersegurança e Gestão de Crises no Ciberespaço

No âmbito da sua missão, ao longo dos últimos anos, o Instituto da Defesa Nacional (IDN) tem promovido o estudo e debate sobre diversos temas no âmbito do Ciberespaço nomeadamente no âmbito, dos trabalhos para a produção de contributos para a revisão do Conceito Estratégico de Defesa Nacional (CEDN) (PORTUGAL, 2013b) e do Grupo de Estudos Contributos para uma Estratégia Nacional de Informação.

Essas iniciativas permitiram não só coligir contributos para o 'Conceito Estratégico de Defesa Nacional', mas também produzir uma edição da revista *Nação e Defesa* dedicada à cibersegurança e artigos especializados para duas edições (n.º 28, 30) de livros da coleção Atena (n.º 28 e 30)[28].

No domínio da investigação, na sequência de um projeto de cooperação sobre ciberseguraçaque, durante os anos de 2012 e 2013, foi desenvolvido entre

28 Disponíveis respetivamente em http://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf; emhttp://www.idn.gov.pt/index.php?mod=1331&cod=28#sthash.DhLLKdwZ.dpbs e em http://www.idn.gov.pt/index.php?mod=1331&cod=30#sthash.AQE0mc6B.dpbs. Mais recentemente o IDN publicou o nº34 da coleção Atena, disponível em http://www.idn.gov.pt/index.php?mod=1331&cod=34#sthash.guYjIP4q.dpbs.

o Instituto da Defesa Nacional (IDN) e a *Escuela de Altos Estudios de la Defensa* (EALEDE) do *Centro Superior de Estudios de la Defensa Nacional* (CESEDEN) foi produzido uma edição (n.º 12) do IDN Cadernos subordinada ao tema "Estratégia da Informação e Segurança do Ciberespaço.[29].

Como consequência da reflexão com especialistas nacionais e internacionais (UE, NATO e CESEDEN) concluiu-se haver necessidade de criar um Curso/ Seminário sobre Gestão de Crises e Politica de Desenvolvimento Estratégico para a Cibersegurança e Ciberdefesa de nível político-estratégico.

A criação deste curso estava ainda alinhado com os vetores de ação estratégica e respetivas linhas de ação enunciados pelo CEDN, nomeadamente contribuindo para uma abordagem integrada da segurança interna e para o sistema nacional de gestão de crises.

A organização do "Curso de Cibersegurança e Gestão de Crises no Ciberespaço" foi iniciada no final de 2013, através de uma parceria entre o IDN e a Academia Militar e visou contribuir para a preparação de quadros médios e superiores para lidar com os processos associados à gestão de crises no ciberespaço. A sua primeira edição decorreu entre 5 de março e 4 de abril de 2014 e os seus objetivos enfatizaram a sensibilização, partilha de conhecimento, desenvolvimento de capacidades analíticas, cultura estratégica e o estudo e a investigação científica nos domínios da segurança e defesa do ciberespaço (INSTITUTO DA DEFESA NACIONAL, 2016).

Quadro 5 - Objetivos Estratégicos do Curso de Cibersegurança e Gestão de Crises no Ciberespaço

- Sensibilizar os auditores para os riscos e ameaças que o ciberespaço coloca à segurança e defesa nacional;
- Promover a partilha de conhecimento relativo à gestão de crises no ciberespaço, de forma a habilitar à participação de forma qualificada no apoio aos processos de decisão;
- Desenvolver capacidades analíticas que potenciem, através da sensibilização para novos conceitos e metodologias, a adoção e desenvolvimento de estratégias organizacionais mais eficazes no combate às ameaças cibernéticas;
- Promover a formação para uma cultura estratégica de cibersegurança e de ciberdefesa, de forma a potenciar o desenvolvimento de competências científicas e/ ou profissionais;
- Promover o estudo e a investigação científica nos domínios da segurança e defesa do ciberespaço, bem como em domínios conexos.

Fonte: O AUTOR, 2016.

29 Disponível em http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf.

Em virtude de se tratar de um tema emergente na sociedade e em evolução permanente e atendendo à sua orientação para o "desenvolvimento de políticas e estratégias organizacionais" o curso foi concebido sob uma matriz multidisciplinar, eestruturadoatravés de um conjunto diversificado de temas que permitiam compreender as áreas associadas à gestão de crises no ciberespaço, agrupando os diferentes temas em cinco módulos fundamentais.

Figura 1- Curso de Cibersegurança e Gestão de Crises no Ciberespaço

Curso de Cibersegurança e Gestão de Crises no Ciberespaço

- **Módulo 1** - Perspetiva Global do Ciberespaço onde se procura caracterizar a relação Sociedade – Informação, num espaço virtual, livre e aberto como é o ciberespaço;
- **Módulo 2** - Economia, Tecnologia e Segurança, no qual se analisam os aspetos estruturais e funcionais do ciberespaço, contribuindo para a compreensão da natureza das ciberameaças e para a necessidade da sua regulação;
- **Módulo 3** - Cibersegurança, onde se discutem os aspetos ligados à segurança da informação e a necessidade de desenvolver uma Estratégia Nacional, capaz de combater o cibercrime, salvaguardar os interesses nacionais e proteger as infraestruturas críticas;
- **Módulo 4** - Ciberdefesa, no qual serão caracterizados os diferentes aspetos ligados à Segurança e Defesa do Ciberespaço, de forma a explorar sinergias nacionais e potenciar o desenvolvimento de esforços cooperativos no plano multinacional;
- **Módulo 5** - Exercício de Decisão Estratégica, que se configura como corolário do curso, procurando fomentar a discussão e levantar questões pertinentes relacionadas com situações de gestão de crises no ciberespaço, de forma a melhorar processos e facultar metodologias a utilizar na tomada de decisão.

Fonte: INSTITUTO DA DEFESA NACIONAL, 2016.

Durante o curso, é disponibilizada ampla informação e espaço de reflexão e debate sobre a problemática da gestão de situações de crise no ciberespaço, tal como está enquadrada e perspetivada nos âmbitos da segurança e da defesa nacionais, e proporcionado contacto atualizado com as realidades nacional e internacional.

Este programa inclui um exercício de decisão estratégica, uma vez que os responsáveis pela decisão estratégica têm que contribuir ativamente para o processo de tomada de decisão, sendo chamados a assumir também o papel de facilitadores na interação entre quem os apoia e outras entidades externas à sua organização. Este exercício, integrado no último módulo é eminentemente prático, visando à aplicação de conceitos e metodologias utilizadas para gerir crises de cibersegurança e promover o exercício das competências adquiridas pelos auditores durante o curso, procurando fomentar a discussão e levantar questões pertinentes relacionadas com situações de gestão de crises no ciberespaço, de forma a melhorar processos e facultar metodologias a utilizar na tomada de decisão.

Para concretizar as três edições deste curso já realizadas, foram convidados prestigiados conferencistas e instituições nacionais e internacionais, num verdadeiro espírito de abordagem abrangente e integrativa (*comprehensive approach*). Nas três edições do curso, participaram 256 auditores (2014, p. 77; 2015, p. 93; e 2016, p. 86) de acordo com a seguinte caraterização:

- ✓ Civis: 63%; Militares oumembros das Forças e Serviços de Segurança: 37%;
- ✓ Candidatos individuais: 46%; Candidatos institucionais: 54 %;
- ✓ Sexo masculino: 83%; Sexo feminino:17%;
- ✓ Quanto à sua formação académica e área científica da sua formação:
- ✓ Licenciatura: 65%
- ✓ Mestrado: 22 %
- ✓ Doutoramento: 7%
- ✓ Engenharia e ciências exatas: 37%
- ✓ Humanidades: 25 %
- ✓ Ciências Militares: 12%
- ✓ Direito: 10%
- ✓ Ciências Policiais, Forenses e Criminais ou Ciências Económicas e Empresariais: 8%.

As motivações manifestadas pelos auditores à frequência do curso durante os processos de candidatura encontram-se em torno dos seguintes domínios:

- ✓ Envolvimento em projetos de investigação no âmbito de formação pós-graduada (mestrado e doutoramento);
- ✓ Aquisição conhecimentos e desenvolvimento pessoal em áreas conexas ao curso;
- ✓ Empregabilidade, i.e., a cibersegurança perspetivada como fator diferenciador e potenciador do currículo pessoal;
- ✓ Desempenho funções, i.e., o candidato já desempenha ou prevê vir a desempenhar funções nos domínios da cibersegurança, ciberdefesaou áreas afins;
- ✓ Formação complementar.

12 *Strategic Decision Making Course & Exercise on Cyber Crisis Management*

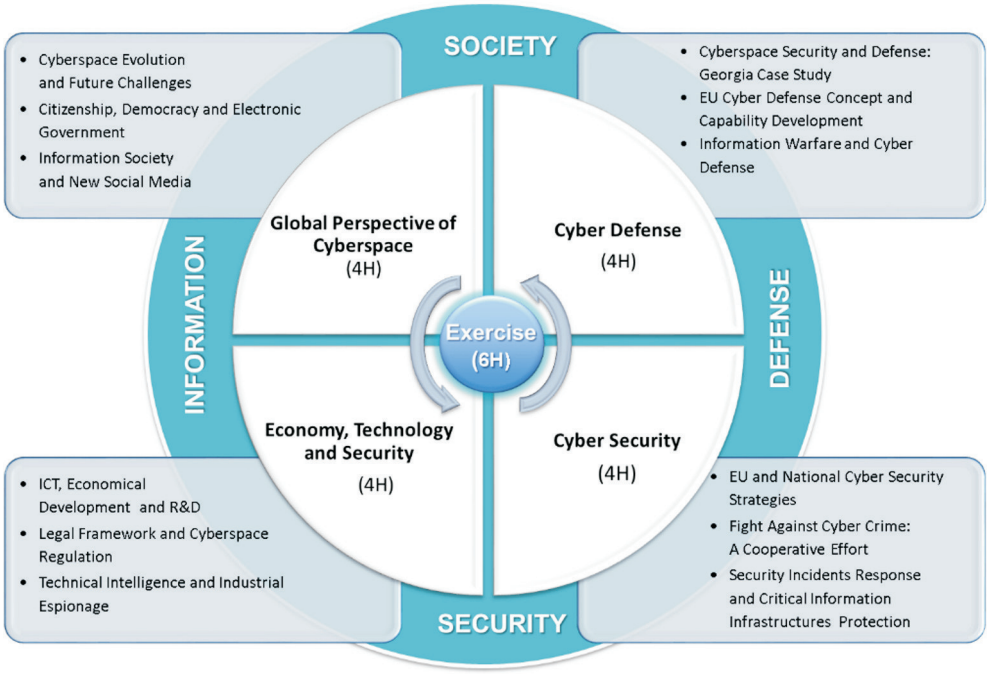
Na sequência de preparação do Conselho Europeu de 19/20 de dezembro de 2013, anteriormente referido, cujas conclusões referiam ao compromisso de apoio da UE a projetos dos Estados-membros da UE no domínio do exercício e treino cibernético, apoiados pela Agência Europeia de Defesa (AED), e da intenção de Portugal criar um Curso de Cibersegurança e Gestão de Crises no Ciberespaço, os representantes da AED e da Estónia presentes na 7ª reunião da Equipa de Projeto para a Ciberdefesa[30] da AED que decorreu em Bruxelas entre 29 e 30 de dezembro de 2013, manifestaram o seu interesse ao delegado português presente em estudar a viabilidade de um curso-piloto com carácter internacional financiado pela AED, tendo por base a estrutura e lições aprendidas no curso nacional, segundo uma lógica de *pooling&sharing* (EUROPEAN DEFENCE AGENCY, 2015).

A realização do *Strategic Decision Making Course & Exercise on Cyber Crisis Management* foi aprovada superiormente sob os auspícios da iniciativa conjunta do Ministério da Defesa Nacional e do Ministério da Defesa da Estónia e organizada pelo Instituto da Defesa Nacional, a Academia Militar de Portugal e a *MTÜ European Cyber Security Initiative* da Estónia, com o apoio da AED.

O currículo do curso-piloto internacional foi ajustado ligeiramente relativamente ao do curso nacional por forma a adequar-se a um perfil mais internacional dos participantes, bem como à parceria com a Estónia.

30 Project Team Cyber Defence.

Figura 2 - Pilot Strategic Decision Making Course & Exercise



Fonte: INSTITUTO DA DEFESA NACIONAL, 2016.

Para concretizar este curso piloto foram igualmente convidados prestigiados conferencistas e instituições nacionais e internacionais, nomeadamente do Exército Português, da Força Aérea Portuguesa, do Gabinete Nacional de Segurança, da Polícia Judiciária, do Instituto Superior Técnico, do CERT.PT, da Agência Europeia de Defesa, do *International Centre for Defence Studies* (ICDS) da Estónia e a *Estonian Information System's Authority*.

O curso-piloto teve 57 participantes dos quais 15 eram internacionais e oriundos da Alemanha, Itália, Estónia, Grécia e República Checa, assim como da NATO (NCIRC[31], NCIA[32], JALLC[33] e ACT/SEE[34]) e União Europeia (*EU Satellite Centre*); 58% eram civis e 42% militares ou das forças e serviços de segurança.

31 NATO Computer Incident Response Capability.
32 NATO Communications and Information Agency.
33 Joint Analysis and Lessons Learned Centre.
34 Allied Command Transformation Staff Element Europe.

13 Exercício de Decisão Estratégica

A ênfase deste exercício residiu nos processos de tomada de decisão e no enquadramento regulatório. O exercício procurou motivar os participantes a discutir e a compreender as questões divergentes e muitas vezes conflituantes associadas à tomada de decisões num quadro de emergência cibernética, bem como as consequências das escolhas feitas ou prescritas por regulamentos existentes, avaliar e comparar os procedimentos entre os vários países.

A sua finalidade principal foi a de elucidar os participantes sobre a natureza das ameaças cibernéticas, através da identificação de potenciais desafios e dificuldades, e inspirar discussões e avançar na busca de novas soluções. O exercício proporcionou ainda uma oportunidade para testar a implementação da gestão de risco e de mecanismos de escalonamento de uma crise cibernética.

O objetivo do exercício foi o de contribuir para a identificação de um conjunto de ferramentas conceptuais coerentes que poderiam ser usadas na avaliação e elaboração de futuros quadros de tomada de decisão.

O resultado desejado para exercício foi o de formar uma base sólida para avaliar os processos de tomada de decisão durante uma emergência cibernética ao nível estratégico.

14 Notas Conclusivas

Da análise das iniciativas da União Europeia, do quadro regulamentar nacional e dos relatórios internacionais de referência consultados, decorrem de forma consistente um conjunto de elementos que importa realçar perspetivar quando se aborda os múltiplos temas associados ao ciberespaço.

Desde logo o conceito cibersegurança ou segurança cibernética. Apesar da tendência para encarar tema como um assunto tecnológico, na realidade, ele congrega um conjunto holístico de atividades e recursos visando à proteção dos recursos físicos e virtuais das organizações e dos seus utilizadores, dos riscos do ambiente cibernético envolvente, não se circunscrevendo e requerendo uma abordagem multidisciplinar de gestão de risco, pois não será possível assegurar a segurança de todos os "ativos".

O relatório '*Global Risks'* apresenta-nos os principais riscos globais tecnológicos para 2016 e que envolvem o eventual colapso das infraestruturas de informação críticas e redes, ciberataques em larga escala, fraude ou roubo de dados e a extrema dependência de tecnologias emergentes.

Este relatório conclui ainda que as oportunidades proporcionadas pelas TIC têm como reverso da medalha o aumento das desigualdades na distribuição de riqueza e a ciber-dependência o que irá requerer o aprofundamento da resiliência tecnológica. Todavia, os riscos associados às tecnologias não têm sido compreendidos pelas instituições, nem concretizados os investimentos que permitem reduzir o risco operacional. A integração da gestão das infraestruturas físicas e cibernéticas, e o reforço da sua resiliência, dos processos de negócio e das TIC são consideradas fundamentais.

O relatório sobre as violações cibernéticas no Reino Unido, apesar de traduzir uma realidade muito específica, enuncia um conjunto de tendências que importa não descurar, nomeadamente: aumento do número e custo dos incidentes de segurança cibernética; violações cibernéticas provocados pelo pessoal das organizações, por erro humano, vírus ou utilização de tecnologias colaborativas ou BYOD[35]; deficiente compreensão das políticas de segurança associada a uma maior frequência de incidentes; faltas nas avaliações dos riscos e na eficiência dos gastos em segurança; e adoção de normas promovidas pelo governo e indústria britânica e congêneres internacionais, para a segurança da informação.

A União Europeia possui um quadro normativo extenso e complexo, com conceitos, iniciativas e orientações para as estruturas europeias e para os Estados-membros. Se por um lado os elementos constantes nesses documentos podem resultar do mínimo denominador comum que foi possível alcançar entre todos os parceiros, não é menos verdade que refletem a imagem da Europa neste domínio e sobre a qual cada país se deve perspetivar.

Nesse sentido, os diversos documentos consultados transmitem a necessidade de uma maior cooperação e coordenação entre instituições públicas e privadas, nomeadamente no domínio da segurança das redes e da informação, assim como entre as capacidades civis e militares. Em simultâneo, é reconhecida a existência de limitadas capacidades, recursos e processos para a prevenção, deteção e resolução de incidentes cibernéticos na Europa.

Quanto à proteção das infraestruturas críticas a UE alerta para a necessidade de tomar em consideração as interdependências entre as infraestruturas críticas, indústria e estado e a importância sistémica das tecnologias de informação e comunicação, relembrando que a responsabilidade primária pela sua segurança compete aos Estados-membros e seus proprietários ou operadores.

35 Bringyourowndevice: utilização de equipamentos pessoais (smartphones, tablets, computadores portáteis) na intranet das organizações.

Relativamente à proteção das infraestruturas de informação críticas constata-se que as estratégias nacionais são heterogéneas e descoordenadas, possuem limitadas capacidades de alerta rápido e de resposta a incidentes, sendo imperativo conceber planos de contingência para incidentes cibernéticos e o seu teste através de exercícios nacionais e à escala europeia, assim como a promoção de uma cultura de gestão de risco, associada a programas de educação, formação e investigação no domínio da segurança das redes e informaçãoe o desenvolvimento de requisitos mínimos e normas de segurança no desenho de produtos e serviços.

A Estratégia Nacional de Combate ao Terrorismo enuncia entre outras medidas, a necessidade de fazer o levantamento e atualização das infraestruturas críticas em todos os setores de atividade e a avaliação periódicadas suas vulnerabilidades bem como dos sistemas de informação críticos e acompanhar a implementação das medidas corretivas face a ciberataques; a elaboração do Plano de Ação para a Proteção e Resiliência das Infraestruturas de Comunicação e do Plano de Ação contra as Ciberameaças; e o desenvolvimento de mecanismos de partilha de informação.

A Estratégia Nacional de Segurança do Ciberespaço tem como foco as IC e os serviços vitais de informação. Estes últimos não estão caraterizados no diploma legal mas podemos depreender que se referem às IIC. Ao referir-se à influência da segurança das redes e da informação nas IC, a Estratégia aparenta refletir a visão europeia anteriormente evidenciada. A realização de exercícios de gestão de crise e a promoção de uma cultura de segurança e a sensibilização da sociedade civil e entidades públicas e privadas são atividades que merecem especial realce.

A Orientação Política para a Ciberdefesa objetiva o ciberespaço como um novo domínio operacional essencial para a o comando e controlo das Forças Armadas e decorre do conceito Estratégico de defesa Nacional e está articulado com a Reforma Defesa 2020, prevendo diversas medidas de que se destacam a criação de um órgão de orientação politico-estratégica e a capacidade militar de resposta operacional a ciberataques e a incidentes informáticos.

O programa do XXI Governo Constitucional realça as medidas que durante a presente legislatura são pretendidas das três estruturas nacionais existentes no âmbito do ciberespaço: Centro Nacional de Cibersegurança, Centro de Ciberdefesa e Polícia Judiciária.

Os cursos organizados em parceria pelo IDN e a AM são reconhecidamente um espaço de sensibilização para os temas associados ao ciberespaço, onde de forma didática e prática se procura contribuir para o desenvolvimento de uma verdadeira cultura de cibersegurança nos cidadãos, decisores e instituições, públicas e privadas.

Referências

ALLIED COMMAND TRANSFORMATION (ACT). *Role and structure*. [S.l.], 2010. Disponível em: <http://www.act.nato.int/role-and-structure>. Acesso em: 05 jan. 2016.

BOOZ ALLEN HAMILTON. *Cyber Power Index*: findings and methodology. [S.l.], 2013.

COUNCIL OF THE EUROPEAN UNION. *Achievements and next steps*: towards global cyber-security. Brussels, 2011a. (Critical Information Infrastructure Protection).

_____. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union*, Brussels, 23 Dec. 2008.

_____. *Transport, telecommunications and energy*: telecommunications items only. Bruxelas, 2011b. (Council meeting, 3093).

_____. *EU cyber defence policy framework*. Bruxelas, 2014a.

_____. *Foreign affairs*. Brussels, 2014b. (Council meeting, 3346).

EU SATELLITE CENTRE. [*Página inicial*]. [S.l.], 2015. Disponível em: <https://www.satcen.europa.eu/>. Acesso em: 20 abr. 2016.

EUROPEAN UNION'S JUDICIAL COOPERATION UNIT. *Home*. [S.l., 2016?a]. Disponível em: <http://www.eurojust.europa.eu/Pages/home.aspx>. Acesso em: 25 abr. 2016.

_____. *Sobre a EU*. [S.l., 2016?b]. Disponível em: <http://europa.eu/about-eu/agencies/regulatory_agencies_bodies/pol_agencies/eurojust/index_pt.htm>. Acesso em: 25 de abr. 2016.

EUROPEAN COMMISSION. *Communication from the commission*: European Programme for Critical Infrastructure Protection. Brussels, 2006a. (COM(2006) 786 final).

EUROPEAN COMMISSION. *Cybersecurity strategy of the European Union*: an open, safe and secure cyberspace. Brussels, 2013a.

_____. *Green paper on a European Programme for Critical Infrastructure protection*. Brussels, 2005. (COM(2005) 576 final).

_____. Parecer do Comité Económico e Social Europeu sobre a Proposta de diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. *Jornal Oficial da União Europeia*, Bruxelas, 2013/0027 (COD), 19 set. 2013b.

_____. *Protecting Europe from large scale cyber-attacks and disruptions*: enhancing preparedness, security and resilience. Brussels, 2009. (Critical Information Infrastructure Protection; COM(2009) 149 final).

_____. *A strategy for a Secure Information Society*: dialogue, partnership and empowerment. Brussels, 2006b. (COM(2006) 251 final). p. 6.

EUROPEAN COUNCIL. *Conclusions of the 19/20 December 2013*. Brussels, 2013. p. 26.

_____. *Conclusions of the 26/27 June 2014*. Brussels, 2014.

EUROPEAN DEFENCE AGENCY. *Polling & sharing*. [S.l., 2015]. Disponível em: <http://www.eda.europa.eu/what-we-do/eda-priorities/pooling-and-sharing>. Acesso em: 01 maio 2016.

_____; COUNCIL OF THE EUROPEAN UNION. Directive 95/46/ec of the european parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, Brussels, 23 Nov. 1995.

_____; _____. Directive 2002/21/ec of the european parliament and of the council of 7 March 2002 on a common regulatory framework for electronic communications networks and services. *Official Journal of the European Communities*, Brussels, 24 Feb. 2002.

EUROPEAN UNION'S LAW ENFORCEMENT AGENCY. *About us*. [S.l.], 2016. Disponível em: <https://www.europol.europa.eu/content/page/about-us>. Acesso em: 26 abr. 2016.

PORTUGAL. Decreto-Lei nº 69, de 9 de maio de 2014. Procede à segunda alteração ao Decreto-Lei n.º 3/2012, de 16 de janeiro, que aprova a orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança. *Diário da República*, Lisboa, 1. sér., n. 89, maio. 2014.

_____. Ministério da Defesa Nacional. Despacho n.º 13692, de 11 de outubro de 2013. Orientação política para a Ciberdefesa. *Diário da República*, Lisboa, out. 2013a.

_____. *Programa do XXI Governo Constitucional 2015-2019*. [S.l.], 2015a.

_____. Resolução do Conselho de Ministros n.º 7-A, de 20 de fevereiro de 2015. Aprova a Estratégia Nacional de Combate ao Terrorismo. *Diário da República*, Lisboa, 1. sér., n. 36, fev. 2015b.

_____. Resolução do Conselho de Ministros n.º 12, 07 de fev. de 2012. Recomenda ao Governo a alteração de normas do Decreto-Lei nº 61/2011, de 6 de maio, que regula o acesso e exercício da atividade das agências de viagens e turismo. *Diário da República*, Lisboa, 1. sér., n. 27, fev. 2012a.

_____. Resolução do Conselho de Ministros n.º 19, de 21 de março de 2013. Define as prioridades do Estado em matéria de defesa, de acordo com o interesse nacional, e é parte integrante da política de defesa nacional. *Diário da República*, Lisboa, 1. sér., n. 67, abr. 2013b.

_____. Resolução do Conselho de Ministros n.º 26, de 19 de abril de 2013. Reforma "Defesa 2020". *Diário da República*, Lisboa, 1. sér., nº 77, abr. 2013c.

_____. Resolução do Conselho de Ministros nº 36, de 12 de junho de 2015. Aprova a Estratégia Nacional de Segurança do Ciberespaço. *Diário da República,* Lisboa, 1. sér., n. 113, jun. 2015c.

_____. Resolução do Conselho de Ministros nº 42, de 13 de abril de 2012. Cria a Comissão Instaladora do Centro Nacional de Cibersegurança. *Diário da República*, Lisboa, 1. sér., n. 74, abr. 2012b.

INSTITUTO DA DEFESA NACIONAL (Portugal). *Curso de Cibersegurança e Gestão de Crises no Ciberespaço*. [S.l.], 2016. Disponível em: <http://www.idn.gov.pt/index.php?mod=1004&area=1600>. Acesso em: 01 de maio 2016.

INTERNATIONAL TECHNOLOGY UNION. *Definition of cybersecurity*. [S.l.], 2016. Disponível em: <http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>. Acesso em: 26 abr. 2016.

NORTH ATLANTIC TREATY ORGANIZATION. Joint Analysis and Lessons Learned Centre. *Home*. [S.l.], 2015. Disponível em: <http://www.jallc.nato.int/>. Acesso em: 01 maio 2016.

_____. Communications and Information Agency. *Home*. [S.l], 2014. Disponível em: <https://www.ncia.nato.int>. Acesso em: 01 maio 2016.

NEVES, Artur Castro. *A indústria de conteúdos*: uma visão estratégica. Lisboa: Ministério da Economia, Gabinete de Estudos Económicos, 2003. (Documentos de Trabalho, n. 49).

SCHWAB, Klaus. The fourth Industrial Revolution: what it means, how to respond. *World Economic Forum*, [S.l.], 14 Jan. 2016. Disponível em: <https://www.

weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond>. Acesso em: 19 abr. 2016.

SEWALL, Bill. Confidentiality, integrity & availability. *Information Security Handbook*, [S.l.], 2009. Disponível em: <http://ishandbook.bsewall.com/risk/Methodology/CIA.html>. Acesso em: 30 abr. 2016.

UNITED KINGDOM. HM Government. *Cyber Essentials*. London, 2014. Disponível em: <https://www.cyberstreetwise.com/cyberessentials>. Acesso em: 20 abr. 2016.

_____. Information Security Breaches Survey 2015: technical report. London, 2015.

UNISYS. *Política Nacional de Segurança da Informação*. [S.l], 2005. (Estrutura Nacional de Segurança da Informação).

WORLD ECONOMIC FORUM. *Partnering for cyber resilience*: towards the quantification of cyber threats. Geneva, 2015.

_____. *The global risks report 2016*. 11. ed. Geneva, 2016.

CIBERDEFENSA Y CIBERSEGURIDAD: NUEVAS AMENAZAS A LA SEGURIDAD NACIONAL, ESTRUCTURAS NACIONALES DE CIBERDEFENSA, ESTRATEGIAS DE CIBERSEGURIDAD Y COOPERACIÓN INTERAGENCIAS EN ESTE ÁMBITO

Pablo Edgardo Camps Lasserre*

1 Introducción

Para referirnos a la ciberseguridad y la ciberdefensa debemos comenzar por definir ambos términos para evitar ambigüedades. De acuerdo con el Consejo Argentino de Relaciones Internacionales (2013) la ciberdefensa es un "conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición." (CONSEJO..., 2013). Por su parte la ciberseguridad es definida como el "conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propias y negarlo a terceros". Si bien las definiciones tienen parte común, podemos diferenciar un término del otro considerando que la ciberseguridad se refiere más a lo preventivo para evitar que se tenga lugar un ataque, mientras que la ciberdefensa se identifica más con lo reactivo frente a un ataque.

Otro elemento que puede llegar a crear interrogantes es que tipo de estructuras deben articularse por parte de los estados para tener una adecuada seguridad en el ciberespacio. Sobre este punto, considerando que una cadena es tan frágil como su eslabón más débil, las soluciones más efectivas serán las que se establezcan estructuras robustas partiendo desde individuos que operan equipos en el ciberespacio formados y concientizados sobre la importancia de la seguridad, pasando por equipos con adecuados niveles de seguridad, software seguro y correctamente configurado y equipos de monitoreo y respuesta capaces de detectar amenazas y prevenir ataques antes de que ocurran o de que causen mayores daños en caso de concretarse.

El ciberespacio llegó para quedarse, y cada vez se extiende más en el actual mundo globalizado. Este nuevo ámbito de interacción humana está abierto a los diferentes actores que pueden ser tanto atacantes como víctimas. En este medio, los ataques 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

* Teniente Coronel perteneciente al Arma de Artillería del Ejército de la República Oriental del Uruguay. Licenciado en Ciencias Militares, diplomado como Oficial de Estado Mayor, Ingeniero Militar; habiéndose recibido como Ingeniero en Informática en la Universidad Católica del Uruguay, en el año 2006. Contacto: <pcamps@ucu.edu.uy

y atacar blancos gubernamentales, empresariales o particulares con objetivos dispares según el caso. Lo blanco y lo negro no son la norma en este espacio 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.

2 Nuevas Amenazas

Desde la llegada de las nuevas tecnologías de la información, se ha buscado a través de ellas facilitar tareas a sus usuarios, brindarles nuevos servicios y posibilidades muy variadas. Así fue posible progresivamente el procesamiento automático de la información, y posteriormente la comunicación entre computadores utilizando redes que se extendieron más y más hasta cubrir todo nuestro planeta. La creación de Internet, marca sin lugar a dudas un hito trascendente en la evolución de las nuevas tecnologías, pero el crecimiento exponencial en lo que a procesamiento y comunicaciones digitales se refiere ha alcanzado niveles no imaginados hace tan solo un par de décadas. En nuestros días es cada vez más común hablar de dispositivos inteligentes, utilizando un concepto tradicionalmente asociado exclusivamente con el ser humano.

De esta forma además de los teléfonos inteligentes que son de accesibilidad casi universal en el mundo desarrollado, agregamos los televisores inteligentes, las señales de tránsito inteligentes, vehículos inteligentes, y muchos dispositivos o aparatos que incluyen ese adjetivo en su descripción, y que basan las prestaciones que brindan en las tecnologías de la información y de las comunicaciones.

El amplio y vertiginoso crecimiento en torno a las tecnologías de la información paulatinamente abrió un nuevo espacio para el desarrollo de las actividades humanas: el ciberespacio. Este se constituyó de acuerdo con la revista The Economist (CIBERWAR, 2010) en el quinto dominio de interacción humana luego del terrestre, marítimo, aéreo y espacial. Pero es conveniente especificar a qué nos referimos cuando hablamos de ciberespacio. Existen al respecto múltiples definiciones pero en general coinciden en que abarcan los medios que basados en las tecnologías de la información y las comunicaciones son utilizados para brindar algún servicio. Acorde a lo anterior, y en función de lo que se planteará más adelante es conveniente puntualizar que Internet no es el ciberespacio, aunque constituye una parte muy importante de él.

Este nuevo ámbito virtual de interacción humana, que inicialmente fue abierto y buscó hacer disponible información y nuevas posibilidades, resultó campo fértil para que actividades mal intencionadas o ilícitas comenzaran a desarrollarse al igual que anteriormente lo hacían en el mundo real. En tal sentido las tradicionales amenazas mutaron su forma y ámbito de actuación, pasando ahora a accionar en el ciberespacio. Términos como ciberdelito, cibercrimen, ciberactivismo, ciberterrorismo,

ciberespionaje, ciberataque, ciberseguridad entre otros surgen como analogía a los anteriores y pasan a constituirse en nuevas amenazas en el ámbito cibernético.

Como consecuencia de la aparición de estas nuevas amenazas, los estados han debido encarar primeramente una transformación de sus estructuras y crear nuevas organizaciones para enfrentarlas. De igual forma, los marcos normativos han debido ser actualizados para perseguir y dar captura a quienes utilizan este nuevo ámbito para cometer actividades ilícitas. La República Oriental del Uruguay, al igual que las demás naciones, se encuentra en este proceso, y ha realizado importantes avances en la materia.

3 Normativa Nacional

La Ley 18.650 (URUGUAY, 2010) fue aprobada en el año 2010 y constituye luego de la Constitución de la República el Marco para la Defensa Nacional del País. La misma define en su artículo 1º la Defensa Nacional como sigue:

> 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.

Destaca en la definición realizada por la norma el carácter civil y militar de la defensa, lo que involucra y compete a todos los ciudadanos de la República. Además especifica finalmente su objetivo que es contribuir a generar las condiciones para el bienestar de la población. Se entiende naturalmente que cualquier actividad o acto que atente contra ese bienestar será objeto de la Defensa Nacional.

La norma (URUGUAY, 2010) a continuación establece en su artículo 2º las características de esa Defensa Nacional:

> La Defensa Nacional constituye un derecho y un deber del conjunto de la ciudadanía, en la forma y en los términos que se establecen en la Constitución de la República y en las leyes. Es un bien público, una función esencial, permanente, indelegable e integral del Estado. En su instrumentación confluyen coordinadamente las energías y los recursos del conjunto de la sociedad.

En este caso, se establece que la Defensa constituye un derecho y deber para toda la ciudadanía, y determina que el estado es el único que puede cumplir esa función. Con estas definiciones realizadas en su primer capítulo, la ley encuadra los conceptos fundamentales sobre su asunto.

El País aprobó además por decreto presidencial en el año 2014 su Política de Defensa Nacional (URUGUAY, 2014). Este documento comienza definiendo el escenario estratégico actual y el escenario futuro, pasando luego a establecer los intereses nacionales que inspiran al País como preámbulo de la determinación de los objetivos permanentes y estratégicos de la Defensa Nacional.

Una vez establecidos los objetivos mencionados, se identifican los posibles obstáculos a enfrentar, dentro de los cuales se menciona el Crimen Organizado. Dentro de este se incluye (URUGUAY, 2014): "[…] delitos como el narcotráfico, tráfico ilegal de armas, el lavado de activos, la trata de personas, la corrupción y el crimen cibernético, entre otros".

De igual forma se establece más adelante en el citado documento que otro posible obstáculo para lograr los objetivos de la Defensa Nacional es la Materialización del espionaje y los ataques cibernéticos (URUGUAY, 2014). A este respecto se establece que:

> En la actualidad se da en forma reiterada el espionaje por parte de Empresas, Organismos o Estados extrarregionales a los gobiernos de la región, las empresas públicas, así como a empresas privadas u organismos de la sociedad civil con el fin de captar ilícitamente información para obtener ventajas económicas y el control político, militar o social, en el plano estratégico de los países.

La Política de Defensa Nacional (CONSEJO, 2014), finalmente establece sus lineamientos estratégicos, diferenciando los aspectos nacionales de los internacionales. Entre los primeros incluye: "Proteger al Uruguay de ataques cibernéticos y preservar la reserva de datos producto de la gestión estatal y privada, tanto a nivel nacional como regional, en cuanto esta última corresponda.". El lineamiento especificado encauza las actividades de ciberdefensa o ciberseguridad que pueda realizar el País.

Como corolario de las normas presentadas, el Uruguay es encuentra próximo a aprobar su Política Militar de Defensa. La misma se encuentra en etapa de borrador actualmente, pero incluirá sin lugar a dudas lineamientos para el empleo de los recursos militares en el ámbito cibernético, alineados con el marco legal ya aprobado.

4 Estructuras Nacionales y Cooperación: Situación General del País

De acuerdo con los datos publicados por el Banco Mundial (THE WORLD BANK, 2016), 61,5 de cada 100 habitantes del país son usuarios de Internet. Este guarismo, que resulta bastante alto en la región, se debe a la promoción por parte del estado de diferentes políticas que favorecen el acceso a través de medios tanto alámbricos

como inalámbricos. En este sentido, además se han aprobado diferentes normas que han procurado desarrollar el gobierno electrónico, a la vez que garantizar un adecuado nivel de seguridad.

En lo relativo a garantizar el mencionado nivel de seguridad, algunas de las medidas adoptadas incluyen el desarrollo de una legislación que acompañe el desarrollo de las nuevas tecnologías, la capacitación de quienes las utilizan, la creación de políticas de seguridad cibernética (URUGUAY, 2009b) en todos los organismos estatales, y la capacidad de detección y respuesta a incidentes cuando ocurran.

A continuación se detallarán las principales agencias del país actualmente responsables de la ciberseguridad y ciberdefensa, encargadas de prevenir un ataque y eventualmente llevar adelante una defensa si se materializa el mismo. Si bien como se detallará más adelante, no existe a la fecha una estrategia nacional definida para la materia, la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC) dependiente de la Presidencia de la República, a través del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) constituye el primer escalón encargado de la seguridad y defensa cibernética del país.

A nivel de los ministerios de Defensa Nacional y del Interior, existen también organizaciones encargadas de brindar la seguridad y defensa cibernética. En el caso del primer ministerio mencionado, se explican sus características más adelante. En el caso del Ministerio del Interior, la Unidad de Delitos Cibernéticos de la Policía Nacional es el organismo que tiene a su cargo la investigación de los delitos cibernéticos.

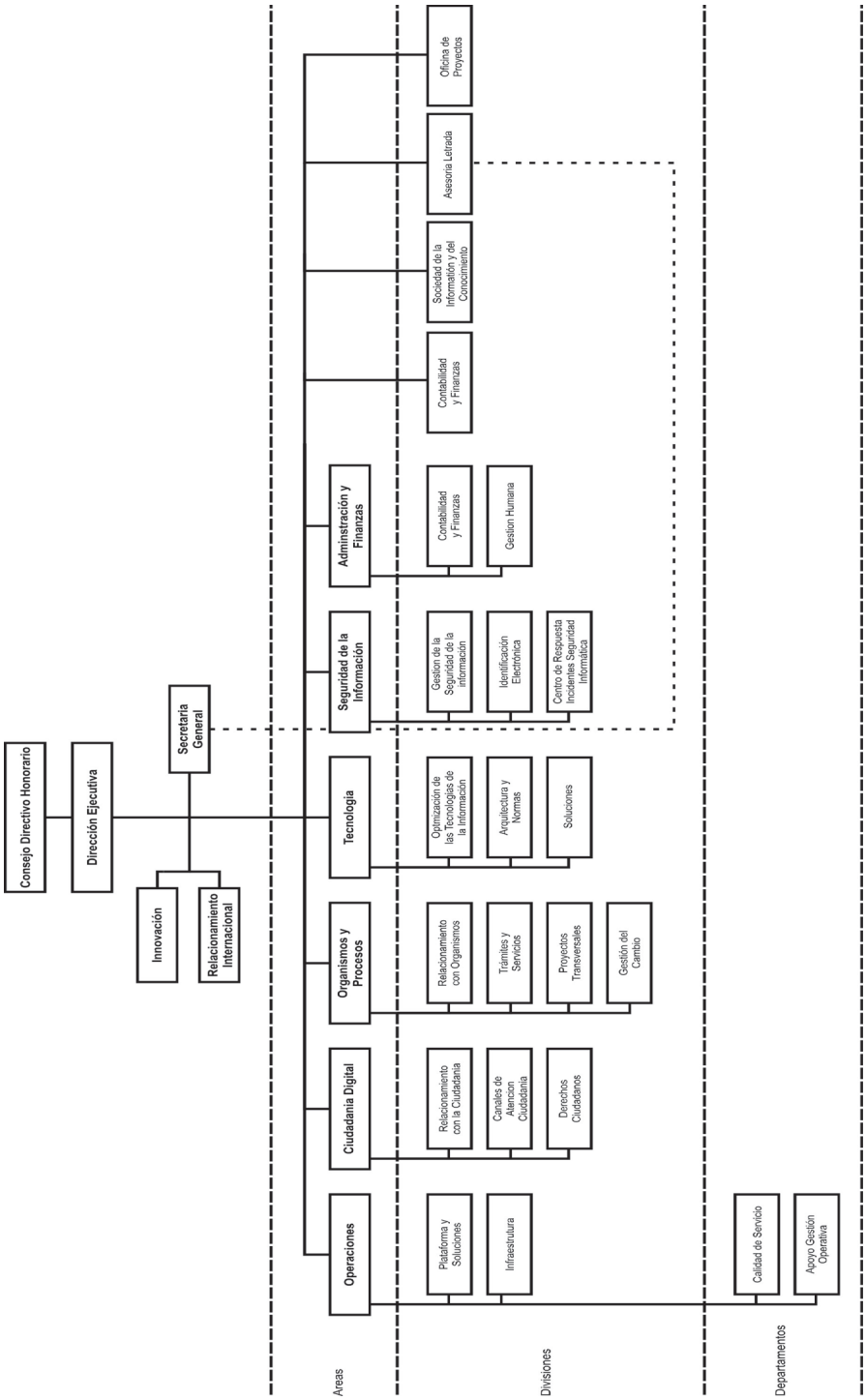
5 La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)

De acuerdo a lo establecido en su propia web, AGESIC (2016) "fue creada en diciembre de 2005 con la denominación 'Agencia para el Desarrollo de Gobierno Electrónico' (Artículo 72 - Ley Nº17.930) y su funcionamiento fue reglamentado en junio de 2006 (Decreto 205/006)." (AGENCIA..., 2016). Su misión es:

Liderar la estrategia de implementación del Gobierno Electrónico del país, como base de un Estado eficiente y centrado en el ciudadano, e impulsar la Sociedad de la Información y del Conocimiento como una nueva forma de ciudadanía, promoviendo la inclusión y la apropiación a través del buen uso de las tecnologías de la información y de las comunicaciones. (AGENCIA..., 2016).

La agencia está organizada en base a seis áreas dependientes de una Dirección Ejecutiva, y veintiuna divisiones que dependen de una de las áreas, o directamente de la dirección. Una de las áreas es la de Seguridad de la Información como puede observarse en la Figura 1.

Figura 1 - Organigrama de AGESIC



Fuente: agencia ara el desarrollo del gobierno de gestión electrónica y la sociedad de la información y del conocimiento, 2016.

Del área de Seguridad de la Información dependen las divisiones de Gestión de Seguridad de la Información, Identificación Electrónica y el Centro de Respuesta a Incidentes de Seguridad Informática. Cada una de estas divisiones tiene cometidos específicos que en su conjunto coadyuvan a obtener un nivel de seguridad adecuado, y es AGESIC quien establece las directivas asociadas y promueve su cumplimiento por parte de todas las dependencias gubernamentales.

Poco después de su creación, en el año 2007 AGESIC recibió la función de "impulsar el avance de la Sociedad de la Información y del Conocimiento, promoviendo que las personas, las empresas y el Gobierno realicen el mejor uso de las tecnologías de la información y las comunicaciones (AGESIC, 2016)." Este cometido lo ha cumplido a través del desarrollo de una Agenda Digital que periódicamente, en general asociada a los períodos de gobierno, se desarrolla basada en un consenso entre diferentes actores, y que constituye en los hechos la política digital del país para el período considerado.

6 El Centro Nacional de Respuesta a Incidentes de Seguridad Informática (Certuy)

Como se expuso anteriormente, este centro depende de AGESIC. El mismo fue creado en el año 2008 por la Ley 18.362 (URUGUAY, 2008), la cual establece que su cometido será "difundir las mejores prácticas en el tema, centralizar, coordinar la respuesta a incidentes informáticos y realizar las tareas preventivas que correspondan." (URUGUAY, 2008).

Más adelante, en el año 2009 al procederse a la reglamentación de la mencionada norma, a través del Decreto No. 451 (URUGUAY, 2009a)[1] se establece que el CERTuy "protegerá los sistemas informáticos que soporten activos de información críticos del Estado, así como los sistemas circundantes a estos."

El decreto mencionado profundiza además los cometidos derivados del definido originalmente en la ley. Los mismos son[2]:

> a) Asistir en la respuesta a incidentes de seguridad informática a los organismos estatales afectados. b) Coordinar con los responsables de la seguridad de la información de los organismos estatales para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad informática. c) Colaborar y proponer normas destinadas a incrementar los esfuerzos con la finalidad de aumentar los niveles de seguridad en los recursos y sistemas relacionados con las Tecnologías de la Información y la Comunicación (TIC) en el Estado. d) Asesorar y difundir información para incrementar los niveles de seguridad de las TIC, desarrollar herramientas, técnicas

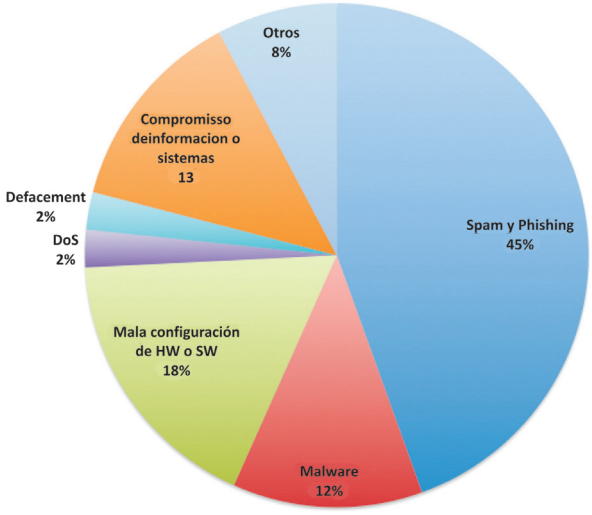
1 Capítulo I - Disposiciones Generales Artículo 1º.- Ámbito Objetivo. (URUGUAY, 2009a)

2 Ibíd. Capítulo I - Disposiciones Generales Artículo 4º.- Cometidos.

de protección y defensa de los organismos. e) Alertar ante amenazas y vulnerabilidades de seguridad en sistemas informáticos de los organismos. f) Realizar las tareas preventivas que correspondan. g) Coordinar planes de recuperación de desastres y realizar un análisis forense del incidente de seguridad informática reportado. h) Centralizar los reportes y llevar un registro de toda la información sobre incidentes de seguridad informática ocurridos en sistemas informáticos del Estado y reportados al CERTuy. i) Fomentar el desarrollo de capacidades y buenas prácticas así como la creación de equipos de respuesta ante incidentes de seguridad informática (CSIRT) para mejorar el trabajo colaborativo. j) Interactuar como único interlocutor nacional en las comunicaciones con organismos nacionales e internacionales de similar naturaleza. (URUGUAY, 2009a).

Basado en sus cometidos, el CERTuy en caso de incidentes de seguridad informática en el país coordina con el CSIRT-ANTEL [3], con otros CSIRT regionales y organizaciones internacionales. El Centro es quien lleva la estadística sobre ataques cibernéticos y es el encargado de emitir alertas sobre riesgos emergentes. La Figura 2 presenta la gráfica correspondiente a los ataques cibernéticos registrados en el País en 2015.

Figura 2 – Estadística de Incidentes 2015



Fuente: CERTUY, 2016.

3 Administración Nacional de Telecomunicaciones. Empresa estatal, es la principal empresa de telecomunicaciones nacional que brinda servicios de telefonía fija, móvil, de banda ancha y de datos. La misma cuenta con la mayor porción del mercado en las áreas mencionadas.

La gráfica presentada se elaboró en base a los 577 ataques registrados (CENTRO, 2016) durante el año. Ese número corresponde a un 20 % más de los ataques registrados por el Centro durante el año anterior.

7 Centro de Respuesta a Incidentes de Seguridad Cibernéticos de Defensa (DCSIRT)

En abril del año 2015 se creó en el ámbito del Ministerio de Defensa Nacional el Centro de Respuesta a Incidentes de Seguridad Cibernéticos de Defensa (DCSIRT). Su creación representa la primera organización en el ámbito específico de la Defensa Nacional encargada de atender los asuntos de ciberdefensa. La comunidad objetivo a la que dirige su acción son las organizaciones dependientes del propio 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.

Además de las eventuales acciones correctivas una vez que se materialice un ataque, el Centro se fija como objetivo medidas preventivas para minimizar su impacto. Entre ellas se puede mencionar la concientización en Gestión de Seguridad de la Información y la implementación de la Política de Gestión en Seguridad de la Información en el propio Ministerio entre otras. En este sentido, desde el año 2014 en el ámbito del Centro de Estudios Nacionales (C.AL.E.N.) , se realizan cursos sobre ciberseguridad dirigidos a profesionales provenientes del propio Ministerio, de otros organismos del estado e incluso del ámbito privado vinculados o simplemente interesados en la materia.

El DCSIRT a partir de su creación pasa a formar parte de la estructura nacional de respuesta a incidentes, y trabaja a nivel nacional en estrecha coordinación con el ya mencionado CERTuy. El Ministerio integra además el Consejo Asesor Honorario de Seguridad de la Información (CAHSI) junto a otras instituciones nacionales .

Fuera de fronteras el DCSIRT para cumplir con su cometido integra igualmente con múltiples redes y equipos de respuesta como el Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA) y los Ministerios de Defensa en el marco de la Unión de Naciones Suramericanas (UNASUR)." (MINISTERIO…, 2016).

8 Estrategia de Ciberseguridad

Como se ha expresado anteriormente, el País se encuentra en fase de desarrollo de su estrategia nacional de ciberseguridad, no contando actualmente con la misma. Sin embargo, los marcos legales aprobados, junto con las estructuras

de alerta y de respuesta ya creadas han demostrado que se avanza en la dirección correcta para ese desarrollo.

El pasado mes de marzo, fue publicado un informe sobre ciberseguridad en América Latina y el Caribe (ORGANIZATION..., 2016) realizado por la Organización de Estados Americanos y el Banco Interamericano de Desarrollo. El extenso estudio realizado por múltiples expertos desarrolló un Modelo de Madurez de Capacidad de Seguridad Cibernética para evaluar cada uno de los países. Este modelo mide cuarenta y nueve indicadores agrupados en las siguientes cinco áreas: 1) Política y estrategia nacional de seguridad cibernética; 2) Cultura cibernética y sociedad; 3) Educación, formación y competencias en seguridad cibernética; 4) Marco jurídico y reglamentario; y 5) Normas, organizaciones y tecnologías.

Cada uno de los indicadores, fue evaluado individualmente para todos los países de América Latina y el Caribe, estableciéndose cinco niveles de madurez. Los mismos se definieron como: Inicial, Formativo, Establecido, Estratégico y Dinámico, correspondiendo a cada uno un valor de uno a cinco respectivamente.

Como es posible observar en la Figura 3, el País recibe en cuatro de los seis indicadores del área de Política y estrategia una evaluación de estado Establecido o Estratégico, siendo los dos indicadores restantes evaluados como en estado Formativo.

Figura 3 - Valoración para Uruguay de Indicadores correspondientes al Área Política y Estrategia

Fuente: (ORGANIZATION..., 2016).

9 El Informe Basa su Evaluación en las siguientes Consideraciones:

La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) incluyó el tema de seguridad cibernética en su Agenda Digital quinquenal para 2011-2015, y enfatizará aún más la seguridad cibernética en el próximo plan a 5 años. Por otra parte, la Política de Defensa Nacional de Uruguay incorpora medidas de defensa cibernética. El mecanismo nacional de respuesta a incidentes de seguridad informática del país, el CERTuy establecido en 2008, coordina regularmente con otros CSIRT regionales y organizaciones internacionales. Además de respuesta a incidentes, el CERTuy suministra registros estadísticos sobre ataques cibernéticos y emite alertas sobre riesgos emergentes. Uruguay también se basa en el análisis y la respuesta de incidentes del CSIRT-ANTEL de la Administración Nacional de Telecomunicaciones, que fue fundada en 2005 para abordar cuestiones relacionadas con los datos y servicios de telefonía celular. Por otra parte, la Política de Defensa Nacional de Uruguay incorpora medidas de defensa cibernética. ORGANIZATION…, 2016.

Sin lugar a dudas queda un largo camino por recorrer para llegar a tener una completa estrategia de ciberdefensa y ciberseguridad, así como las estructuras conjuntas e integradas para enfrentar un eventual ataque. Sin embargo es posible delinear algunas características que muy probablemente tendrán las mismas.

En cuanto a la creación de una estrategia de empleo de medios en el ciberespacio, sin dudas la misma se ajustará a los preceptos que establece nuestra legislación en lo referido al ejercicio del derecho de legítima defensa consagrado en la Carta de las Naciones Unidas y se reserva el uso de la fuerza para los casos de agresión militar (URUGUAY, 2010). En este sentido, un ataque cibernético por parte del estado se daría únicamente ante una agresión externa en ese ámbito.

La creación de estructuras de ciberdefensa militares, seguramente estará encuadrada en el ámbito del Estado Mayor de la Defensa que depende del Ministerio de Defensa Nacional y le compete tanto la elaboración doctrinaria, como la planificación y el mando de las operaciones conjuntas de las fuerzas armadas.

10 Conclusiones

La disponibilidad creciente de las nuevas tecnologías de la información y de las comunicaciones ha dado lugar a la creación de un nuevo ámbito de interacción entre los seres humanos. En este lugar virtual se ofrecen y se brindan múltiples servicios de gran utilidad, pero han dado lugar a la realización de actividades ilícitas de diferentes características.

La realización de actividades que afecten la seguridad de los diferentes países por parte de otras naciones, organizaciones o individuos es posible, y puede causar efectos devastadores. Por esto, los estados deben adaptar su legislación y crear nuevas estructuras para combatir las nuevas amenazas que surgen. El Uruguay, al igual que los restantes países del orbe ha modernizado su marco legal y ha incluido a las amenazas provenientes del ciberespacio entre las que pueden afectar el bienestar de su población, pasando estas a ser objeto de la Defensa Nacional.

En virtud de lo anterior, se han estructurado políticas y se han creado al más alto nivel organizaciones para enfrentar las nuevas amenazas. El País ha identificado como primordial fomentar el gobierno electrónico y a la vez estructurar a nivel nacional redes que permitan brindar seguridad cibernética y garantizar el libre uso de los recursos reales y virtuales. Estas redes tienen como base la concientización de la población en lo referente a seguridad de la información y su capacitación para utilizar de la mejor forma los servicios.

A pesar de que el País carece de una estrategia de ciberseguridad, ha sido evaluado positivamente en un reciente informe conjunto del Banco Interamericano de Desarrollo y la Organización de Estados Americanos.

De igual forma se carece actualmente de una organización conjunta a nivel Fuerzas Armadas que tenga como cometido específico repeler ataques cibernéticos que afecten la seguridad nacional o eventualmente realizarlos como respuesta a un ataque anterior.

Referencias

AGENCIA PARA EL DESARROLLO DEL GOBIERNO DE GESTIÓN ELECTRÓNICA Y LA SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO. *Página Web.* 2016. Disponible en: <http://agesic.gub.uy>. Fecha de acceso: 20 marzo 2016.

CIBERWAR. *The Economist,* [S.l.], v. 396, n. 8689, 3-9 jul. 2010.

CENTRO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA DEL URUGUAY. *Estadística de incidentes CERTuy 2015.* Montevideo, 2016. Disponible en: <https://www.cert.uy/inicio/novedades/amenazas_y_alertas/estadistica_de_incidentes_certuy_2015>. Fecha de acceso: 20 marzo 2016.

CONSEJO ARGENTINO DE RELACIONES INTERNACIONALES. *Ciberdefensa-Ciberseguridad:* riesgos y amenazas. Buenos Aires, 2013. Disponible en: <http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf>. Fecha de acceso: 15 marzo 2016.

CONSEJO DE DEFENSA NACIONAL. Política de defensa nacional: un uruguay integrado a la región y abierto al mundo. Montevideo, 2014. Disponible en: <https://parlamento.gub.uy/documentosyleyes/leyes/ley/18172?width=800&height=600&hl=en_US1&iframe=true&rel=nofollow>. Fecha de acceso: 10 enero 2016.

MINISTERIO DE DEFENSA NACIONAL (Uruguay). *Centro de Respuesta a Incidentes* Informáticos del MDN. Montevideo, 2016. Disponible en: <http://www.mdn.gub.uy/?q=node/3994>. Fecha de acceso: 25 marzo 2016.

ORGANIZATION OF AMERICAN STATES; INTER-AMERICAN DEVELOPMENT BANK. Ciberseguridad *¿Estamos preparados en América Latina y el Caribe?* Washington, DC, 2016. Disponible en: <https://publications.iadb.org/handle/11319/7449?locale-attribute=en&locale-attribute=pt&locale-attribute=es&>. Fecha de acceso: 25 marzo 2016.

URUGUAY. Decreto nº 105/014, de 29 de abril de 2014. Aprobacion de la propuesta en materia de Politica de Defensa Nacional. *[Diario Oficial de la República Oriental del Uruguay],* Poder Ejecutivo, Montevideo, mayo 2014. Disponible en: <http://www.impo.com.uy/bases/decretos/105-2014>. Fecha de acceso: 10 enero 2016.

_____. Decreto nº 451/009, de 6 de octubre de 2008. Crea el 'Centro Nacional de Respuesta a Incidentes de Seguridad Informática' (CERTuy) en la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). *[Diario Oficial de la República Oriental del Uruguay],* Poder Ejecutivo, Montevideo, oct. 2009a. Disponible en: <https://www.cert.uy/wps/wcm/connect/certuy/8f327272-c58e-4a63-8bb7-b6d37db4ec22/Decreto+451-009.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=8f327272-c58e-4a63-8bb7-b6d37db4ec22>. Fecha de acceso: 20 enero 2016.

_____. Decreto nº 452/009, de 28 de septiembre de 2009. Administración Pública. Política de Seguridad de la Información. *[Diario Oficial de la República Oriental del Uruguay],* Poder Ejecutivo, Montevideo, oct. 2009b. Disponible en: <http://www.impo.com.uy/bases/decretos/452-2009>. Fecha de acceso: 20 enero 2016.

_____. Ley nº 18.362, de 6 de octubre de 2008. Rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2007. *[Diario Oficial de la República Oriental del Uruguay],* Poder Legislativo, Montevideo, oct. 2008. Disponible en: <https://

parlamento.gub.uy/documentosyleyes/leyes/ley/18362?width=800&height=600&hl=en_US1&iframe=true&rel=nofollow>. Fecha de acceso: 10 enero 2016.

_____. Ley nº 18.650, de 19 de febrero de 2010. Ley Marco de Defensa Nacional. *[Diario Oficial de la República Oriental del Uruguay],* Poder Legislativo, Montevideo, marzo 2010. Disponible en: <https://parlamento.gub.uy/documentosyleyes/leyes/ley/18650?width=800&height=600&hl=en_US1&iframe=true&rel=nofollow>. Fecha de acceso: 10 enero 2016.

THE WORLD BANK. *Internet users (per 100 people)*. [S.l.], 2016. Disponible en: <http://data.worldbank.org/indicator/IT.NET.USER.P2>. Fecha de acceso: 15 marzo 2016.

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