Defesa Cibernética Brasileira: O Uso do SIMOC para a Formação de Combatentes

Mayane Bento Silva[1];
Adenilson Costa Corrêa[2],
Juliana Ferreira Cardoso[3],
Luís Felipe Pinto de Oliveira[4],
Luiz Gustavo Lavandoski da Silva[5],
Valéria Rosa Braga[6],

RESUMO

A segurança cibernética é de extrema importância, principalmente para os Estados, que veem como um alto risco o vazamento de dados, essencialmente os militares. Então visando à segurança de seus dados, os Estados começaram a investir em tecnologias, que anteriormente eram de uso comercial e de entretenimento, os jogos e simuladores, sendo utilizados para treinamento e estudo de táticas. Este artigo busca apresentar e explicar a utilização no contexto nacional do simulador SIMOC voltado a formação de combatentes. Este trabalho usou como quadro teórico, principalmente a literatura nacional, complementando com a internacional buscando referências na temática. Por fim, conclui-se explanando sobre o avanço do Brasil e suas perspectivas na região Sul-Americana.

Palavras-chave: Defesa cibernética. SIMOC. Simuladores. Jogos. Defesa nacional.

1. INTRODUÇÃO

O presente artigo visa apresentar e debater a questão do uso de simuladores no Brasil utilizando de artificio o desenvolvimento de formas para beneficiar e garantir a soberania e o poder do Brasil. Esta área relativamente nova, surgiu no século XX, mas ganha uma espécie de governabilidade, que modificou todos os agentes do sistema, sejam eles os Estados e empresas, assim como político, econômico e militar.

Considerando que o governo brasileiro passa a utilizar nas questões de defesa de território - onde se inclui o ciberespaço além do efetivo militar, crescendo a utilização de acadêmicos, pesquisadores e empresas responsáveis por desenvolvimento tecnológico - o ciberespaço brasileiro apresenta capacidades e fraquezas - as chamadas vulnerabilidades e sensibilidades - que se tornam fatos bons relacionados à América Latina, mas que ao comparar com países como EUA e Rússia, entende-se que o sistema brasileiro é novo e pode ser um bom moderador nessa área, por conta da guerra eletrônica, algo que o Brasil possui certo domínio.

Uma das possibilidades do Brasil para essa questão é o Simulador de Operações Cibernéticas (SIMOC), que foi desenvolvido em cooperação das forças armadas e a empresa privada TI Decatron, para possibilitar que o governo brasileiro, em necessidade, tenha condições de atuar em uma guerra eletrônica.

A partir disso, o presente artigo busca analisar o que há de vanguarda na questão de defesa tecnológica e responder a seguinte pergunta, **como o uso de simuladores, em especial o SIMOC, tem ajudado nas problemáticas relacionadas ao espaço cibernético do Brasil?**

[1] Professora responsável – Universidade da Amazônia – UNAMA;
[2] Aluno do 7º semestre do Curso de Relações Internacionais da Universidade da Amazônia - UNAMA;
[3] Aluna do 7º semestre do Curso de Relações Internacionais da Universidade da Amazônia - UNAMA;
[4] Aluno do 7º semestre do Curso de Relações Internacionais da Universidade da Amazônia - UNAMA;
[5] Aluno do 7º semestre do Curso de Relações Internacionais da Universidade da Amazônia - UNAMA;
[6] Aluna do 7º semestre do Curso de Relações Internacionais da Universidade da Amazônia - UNAMA;

Para responder essa pergunta, foram utilizadas pesquisas bibliográficas referente a dados do Ministério da Defesa (MD), assim como artigos científicos de estudiosos da área, tal qual notícias sobre o assunto, disponíveis tanto nos sites do CIGE como em outros, e os demais departamentos do Exército, tal qual sítios de notícias.

Este trabalho está apresentado em tópicos: o segundo tópico busca apresentar o contexto do Brasil diretamente com a história da defesa cibernética brasileira; O terceiro ponto será a breve descrição da atual doutrina de defesa cibernética do Brasil; O quarto ponto será o responsável por apresentar a metodologia de gamificação e sua utilização em âmbito nacional; No quinto ponto, apresentaremos o modelo SIMOC e sua utilização; E, como último ponto, a conclusão com os resultados e a tendência na região.

2. A DEFESA CIBERNÉTICA NO BRASIL

Começando pelo contexto internacional, com a evolução social sendo modificada mais rápido do que a evolução Estatal, e a rápida integração digital pelo advento da globalização, criou-se o novo espaço virtual e logo universal que juntou todas as pessoas em um 'pequeno' espaço, o Ciberespaço (LÉVY, 1999)

O mundo cibernético está cada vez mais presente nas relações entre Estados, empresas e até nas relações interpessoais, e juntamente desta questão cibernética vem a necessidade de uma segurança nesse setor, sendo priorizada pelos Estados, principalmente nas Forças Armadas.

Ao decorrer do século XX, a internet foi introduzida como força militar, contudo foi após a abertura desse recurso para a sociedade civil que o mundo cibernético foi expandido de forma acelerada. Os Estados sempre buscam a segurança de seus dados, principalmente da área militar, pois estes são capazes de mostrar suas forças e fraquezas. Com a vinda da internet, a facilidade de acesso e até mesmo roubo desses conteúdos chamou a atenção de todas as camadas da sociedade, incluindo dos Estados, que visando à segurança, começaram a investir na parte cibernética.

Além de tais riscos, a internet contribuiu para uma nova revolução mundial, com as informações de formas rápidas e fáceis, a tecnologia se adaptou e evoluiu de maneira acelerada, trazendo os jogos digitais e simuladores, que no início tinham apenas caráter comercial e de entretenimento, mas com o avanço tecnológico e as ameaças digitais, começaram a ser utilizados com foco de treinamento.

Logo, com a virada dos séculos e o rápido desenvolvimento mundial modificando os mecanismos dos Estados, o Brasil passou a atuar, na forma de segurança da informação no segmento governamental, por meio da medida provisória nº 2.216-37 de 31 de agosto de 2001, que criou o principal órgão de atividades desse setor, e que foi modificado em 2006 com o Departamento de Segurança de Informação e Comunicação (DSIC).

Em função de defesa cibernética propriamente para questões militares para a questão da defesa de soberania, desenvolveu em dezembro de 2008 a formulação da Estratégia Nacional de Defesa (END) e a aplicação do setor cibernético em 2009 no âmbito da força terrestre, como um dos três setores estratégicos do Brasil (ESTRATÉGIA NACIONAL DE DEFESA, 2009).

O CDCiber foi o centro, cuja a responsabilidade de coordenar e integrar esforços para garantir a defesa foi dada. Ainda sendo uma realidade muito atual, o setor cibernético é algo que vem sendo evoluído gradativamente, porém comparado aos países mais desenvolvidos – como EUA - ainda se encontra em um estágio inicial (SENADO FEDERAL, 2014).

A defesa cibernética é definida no Brasil em três níveis: político, estratégico e operacional e tático.

> Nível político - Segurança da Informação e Comunicações e Segurança Cibernética - coordenadas pela Presidência da República e abrangendo a Administração Pública Federal direta e indireta, bem como as infraestruturas críticas da Informação Nacionais; nível estratégico - Defesa Cibernética - a cargo do Ministério da Defesa, Estado Maior Conjunto das Forças Armadas e Comandos das Forças Armadas, interagindo com a Presidência da República e a Administração Pública Federal; e níveis operacional e tático - Guerra Cibernética - denominação restrita ao âmbito interno das Forças Armadas (MD31-M-07).

Por conta dessa divisão é reprimido o uso do termo "defesa cibernética" para quando o planejamento e execução das ações cibernéticas forem em nível estratégico de decisão e no de "guerra cibernética" para quando for no nível de decisão tático ou operacional (MD31-M-07).

Aderiu-se ao Projeto Estratégico de Defesa Cibernética, que foi substituído em 2016 pelo Programa Estratégico do Exército Defesa Cibernética. Com essa evolução o cenário de defesa nacional houve a capacitação de recursos humanos para o domínio nos chamados 'temas multidisciplinares'. Essa capacitação se deu tanto na proteção dos ativos, quanto na atuação em rede, e na coordenação de relações com instituições civis, acadêmicas e empresariais na questão de pesquisas.

Os resultados são as produções nacionais de softwares, hardwares, simuladores de guerra eletrônica – como o SIMOC – e a realização de seminários e programas de capacitação. Por conta desses fatos, o Exército Brasileiro conseguiu lugar no grupo restrito de organismos nacionais e internacionais que possuem competência no desenvolvimento de proteção e contenção de ataques em campo cibernético.

3. ATUAL DOUTRINA DE DEFESA NACIONAL NO CAMPO CIBERNÉTICO

Para apresentar os principais pontos da doutrina de defesa nacional na área cibernética são necessárias algumas abordagens pontuais que representam e apresentam essa importância na temática.

No contexto internacional a questão do uso do campo cibernético passa por muitas discussões, principalmente na relação à previsão de emprego das Forças Armadas (FFAA) e isso tem sido bastante citado no Direito Internacional de Conflitos Armados (DICA), por conta das novas tecnologias e módulos de combate empregados, como eventualmente ocorrem no oriente médio.

No Brasil, o planejamento para esse campo cibernético começa a ser pensado no governo de Fernando Henrique Cardoso (FHC), com a distinção de Defesa e Segurança Pública, na Política Nacional de Defesa (PND). A PND logo então em suas novas 'atualizações' contou não somente com a opinião de militares, mas também com a presença de representantes da sociedade civil, uma vez que a soberania nacional não é algo que seja de interesse unicamente militar.

Assim, com o desenvolvimento de alguns documentos que são de imensa importância para a soberania tais como o Livro Branco de Defesa Nacional, PND, surge a Estratégia Nacional de Desenvolvimento (END) introduzindo então a questão cibernética como fonte de domínio para garantia de soberania do Brasil.

Alguns documentos explicam diretamente como se fomenta essa doutrina, como o MD31-M07 (manual de doutrina cibernética de 2014), aprovada em abril de 2013 pelo ex-Ministro da Defesa Celso Amorim, com a finalidade de expandir o pensamento no assunto contribuindo para a atuação das forças armadas na defesa do Brasil no espaço cibernético. (Ministério da Defesa, 2014).

A doutrina Militar de Defesa Cibernética foi estabelecida como uma unidade de conhecimento para gestão das questões envolvidas ao espaço cibernético, agregando melhor

compreensão ao ministério da defesa junto aos sub-setores da defesa nacional de acordo com a decisão em três níveis do governo.

O espaço cibernético como um domínio de defesa, é considerado um novo âmbito da geoestratégia onde um país deve gerar segurança, por sua condição estratégica de permeia todos outros quatro (terrestre, marítimo, aéreo e espacial) é necessária uma atenção especial nessa contemporaneidade, devido à grande facilidade de acesso aos meios computacionais às incertezas quanto a atores desconhecidos e insegurança presente no âmbito internacional.

A defesa cibernética, compreendida como a tomada de decisão diante das ações necessárias a segurança no espaço cibernético, no âmbito nacional busca promover a proteção de sistemas vitais ao interesse estatal, deter ataques de possíveis inimigos, alcançar o desenvolvimento de inovações para melhorar o aparato tecnológico nacional e progredir na construção de um sistema integrado para mitigar erros e falhas.

Os princípios para o emprego da defesa cibernética levam em consideração algumas peculiaridades tais como: a produção de ações que gerem vantagens estratégicas, operacionais e táticas, a busca por adaptação às continuas e diversas modificações do espaço cibernético, a criação de procedimentos para ocultar estratégias de ataque e dificultar o rastreamento dessas ações pelos inimigos.

A gestão sobre defesa cibernética é dividida em três níveis: **o político**, coordenado pela presidência da república que abrange administração federal e os órgãos decisórios de caráter público, responsável pela ciber-segurança; **o estratégico**, coordenado pelo Ministério da Defesa, estado maior e conjunto de Comando das Forças Armadas, responsável pela defesa cibernética; **e o nível operacional e tático**, sobre a coordenação exclusiva das forças armadas, responsável em caso de guerra cibernética. (MD31-M07 pg. 17/36).

Por conta do Comando de Defesa Cibernética (CDCiber), em 2017 iniciou uma nova linha de ‘integração’ entre as forças armadas que era a participação de oficiais-generais de ambas forças para a questão da defesa cibernética. Chamado de “interoperatividade”, precisava agora mais do que nunca ter uma melhor capacidade na atuação das forças militares brasileira no campo do ciberespaço, assim agora Marinha e Força Aérea integram o quadro.

Muito se fala a respeito de poder cibernético, mas é fato de que, ao contrário do que ocorreu com as armas nucleares, ninguém teorizou doutrinas de dissuasão de poder cibernética. Tais doutrinas de dissuasão são essenciais para engajamento diplomático e estratégico com outros Estados. Dessa forma com a integração do processo decisório para uma melhor formulação das ações a serem tomadas, a doutrina militar de defesa cibernética busca preparar as forças armadas para o enfretamento de potenciais ameaças, com a adequação de um maior entendimento sobre a área, com capacidade de resposta e previsão de cenários de ações cibernéticas externas que venham a ameaçar os interesses e a defesas nacionais

4. A UTILIZAÇÃO DOS JOGOS DIGITAIS E SIMULADORES COMO FORMA DE APRENDIZADO

Os jogos e simuladores digitais estão em alta na atual sociedade que está imersa no mundo cibernético, por conta da facilidade de acesso a informações e possíveis atualizações dos sistemas utilizados para a aprendizagem. É visto que os jogos digitais e simuladores estão cada vez mais populares, tanto com o público em geral quanto com instituições específicas, como escolas, faculdades, cursos, etc. Vários estudos têm apontado a relevância dos jogos e simuladores para determinadas questões, como a utilização em simulações de voos, estudo de estratégias, trabalho em equipe de forma coordenada, além de ser bem mais barato do que fazer a ação em si, mesmo que pequena escala apenas para teste.

Uma sequência de jogos bem populares que podemos mencionar é o “Civilization”, criado por Sid Meier, este jogo individual de estratégia regida por jogadas em turnos, do qual

o jogador é instigado a fazer com que a sua nação possua domínio mundial, tendo que travar guerras, fazer acordos, desbravar terras para conseguir recursos, investir tanto na questão de segurança quanto na parte da felicidade do povo que vive nas cidades que este já criou. Também existem jogos do estilo *FPS* (*First Person Shooter*) do quais são bem populares pelo trabalho em equipe e da montagem de estratégias para conquistar o objetivo, podendo ser conquistar a "bandeira" inimiga, matar todos os integrantes do outro time, salvar os "reféns" (que geralmente são *NPCs – Non-player Character* -, que são personagens padrão não jogáveis gerados pelo sistema), entre outros.

Mas porque os jogos e simuladores digitais estão tão populares e são importantes na atual sociedade? Como já dito, além de serem bem mais baratos do que fazer um treinamento, os jogos e simuladores disponibilizam a opção de os participantes/alunos fazerem várias vezes a mesma "fase", melhorando suas capacidades e forçando a não memorização, e sim o aprendizado, além de poderem testar novos meios de resolução de problemas, sendo mais flexível. A utilização de simuladores e jogos digitais é vista desde o período da corrida espacial, quando os pesquisadores faziam simulações de voo para melhor desempenho das naves, e também é vista no treinamento dos pilotos, como o Simulador de Força G. Com o avanço da tecnologia, os simuladores ficaram cada vez mais sofisticados e realistas, sendo utilizados em várias áreas, desde as autoescolas brasileiras, com a direção a noite e em diferentes mudanças climáticas, até bases militares, como a norte americana da qual utiliza para treinamento de pilotos de caças.

5. SIMULADOR NACIONAL DE OPERAÇÕES CIBERNÉTICAS (SIMOC)

O espaço cibernético surge como um novo ambiente de interação humana, trazendo significativas transformações para a sociedade, esta que passa a solicitar maior espaço de discussão. As mudanças tecnológicas tiveram grande efeito nas várias camadas sociais, os aspectos transversais do ciber contribuíram para a sua grande difusão, gerando facilidade de comunicação e diluição na hierarquia de burocratização. Contudo, essas facilidades e avanços alcançados com o advento da sociedade em rede, trouxe consigo maior exposição para a vulnerabilidades e sensibilidades das infraestruturas críticas que compõe os Estados, o que por sua vez clama por princípios e instrumentos capazes de garantir a Defesa Nacional dos Estados.

Diante desse cenário, o Estado Brasileiro observou a necessidade de possuir meios de contrapor as ameaças cibernéticas. A volatilidade da conjuntura mundial mostrou que a defesa brasileira deveria estar permanentemente preparada, sempre garantindo a preservação dos interesses nacionais. Dessa forma, para garantir esse objetivo da melhor maneira, foi criado o Centro de Instrução de Guerra Eletrônica (CIGE), uma Organização Militar (OM) referência na América Latina por ser a maior em matéria de segurança cibernética e treinamento de oficiais e cadete do exército brasileiro. (MD 31 D-03).

Visando a segurança no ambiente cibernéticos alguns meios começaram a ser desenvolvidos, notando-se a necessidade de possuir recurso humano apto a combater qualquer ameaça oriundo do ciberespaço. Assim, para controlar possíveis ataques, os departamentos de defesa começaram a utilizar simuladores para ajudar no treinamento militar. Atualmente, vários simuladores têm sido usados, dentre eles podemos citar o Military Academy Attack/Defense Network (MAADNET), que basicamente cria uma estrutura de ataque que se baseia na vulnerabilidade de sistemas, o que possibilita uma variedade de ferramentas que podem ser táticas e agressivas.

Contudo, esses simuladores não correspondiam totalmente as necessidades brasileiras, por essa razão, a solução encontrada foi criar um simulador que suportasse as especificidades do CIGE.

> Esse processo durou aproximadamente um ano e várias soluções foram avaliadas. Embora existam soluções extremamente elaboradas e interessantes, nenhuma delas atende plenamente todas as necessidades do CIGE. As principais deficiências incluem: requisitos de controle de exportação das nações; totalmente dependente do fornecedor na evolução dos cenários de treinamento; falta de soluções de conformidade para as atividades de rotina do CIGE; o custo do produto; e a determinação da Estratégia Nacional de Defesa do Brasil para promover a indústria de defesa nacional (MACHADO, COSTA E REZENDE, 2015).

Buscando atingir as necessidades nacionais de um ambiente simulado seguro e adequado para o treinamento de militares brasileiros, passou-se a desenvolver um simulador brasileiro. O Simulador Nacional de Operações Cibernéticas (SIMOC) surgiu para auxiliar no treinamento dos militares brasileiros para uma possível guerra cibernética. Fazendo parte do programa de Estratégia da Defesa Nacional do Centro de Comunicações e Guerra Eletrônica do Exército (CComGEx), o SIMOC cria e planeja treinamentos em um ambiente de rede. A primeira versão do simulador foi testada em novembro de 2012, onde 24 oficiais do CComGEx participaram de um curso de seis meses onde operaram o SIMOC, o que os tornou aptos a atuar contra ameaças virtuais como hackers e a própria guerra cibernética. (MACHADO, COSTA E REZENDE, 2015)

Durante o treinamento, os oficiais foram divididos em dois grupos, os quais receberam o mesmo cenário, o simulador criou um treinamento para cada time, que tinham como objetivo acessar uma das infraestruturas críticas de um país fictício, acessando e explorando as vulnerabilidades, afim de comprometer o modelo. O treinamento considerado satisfatório para a primeira versão do SIMOC, durou três dias e contou com um design de rede corporativa com cerca de 45 ativos de rede preparado pelos instrutores. (MACHADO, COSTA E REZENDE, 2015).

Em 2013, um novo exercício utilizando o simulador brasileiro foi realizado. Nessa operação cada time recebeu um treinamento exclusivo baseado em práticas realizadas anteriormente no SIMOC. Dessa vez, o sistema foi configurado para adotar duas maquinas físicas para permitir o uso de um modelo representativo da uma usina termelétrica. A maquete da usina tinha um cooler que representava uma turbina que estava conectada a uma rede, o qual era controlada pelos oficiais em treinamento. (MACHADO, COSTA E REZENDE, 2015).

O outro exercício realizado foi em 2014, neste foi usado uma segunda versão do simulador. Com os pontos de melhoria aprendidos com a primeira versão, os instrutores desenvolveram um projeto de rede e também uma série de atividades que deveriam ser realizadas pelos alunos. Nesse treinamento o modelo usando também evoluiu, passando a ser uma cidade, onde os trainees poderiam interagir com vários aspectos da infraestrutura, como iluminação, linha de trem, portões de barragem e entre outras utilidades do modelo, com isso os alunos que participavam do exercício conseguiram observar os efeitos de um ataque cibernético em uma infraestrutura real. (MACHADO, COSTA E REZENDE, 2015).

O SIMOC surgiu com o objetivo de ser uma ferramenta capaz de gerar automaticamente redes virtualizadas com acesso à web, assim podendo fornecer uma simulação virtual, estocástica e dinâmica. Assim, a criação de redes virtuais dele não requer intervenção manual, tendo também um sistema que corresponde as necessidades do treinamento proposto (MACHADO, COSTA E REZENDE, 2015).

6. CONCLUSÃO

De certa forma, a utilização de jogos na capacitação e profissionalização dos responsáveis por garantir a segurança do território é o maior ponto de sensibilidade que o Estado Brasileiro pode ter. Os treinamentos usando o SIMOC, como podemos observar, tem se mostrado promissor. As limitações encontradas no simulador, não reduziram a grande capacidade que este tem de trazer benefícios para a capacitação no ambiente cibernético. Dessa forma, é possível perceber que as limitações consequentemente levantam novas ideias que deveram implementar o SIMOC.

O Brasil a pesar de ser um Estado que fomenta sua política externa de forma pacifica, precisa manter um condicionamento das forças de defesa capaz de mostrar que há capacidade e instrumentos internos para combater possíveis ameaças, assim fazendo com que o país tenha mais preponderância tecnológica e de envolvimento com parcerias tecnológicas na região Sul-Americana, utilizando da cooperação internacional para agregar conhecimento sobre o ciberespaço, mitigar as imperfeições existentes e acompanhar as mudanças que são intrínsecas a esse domínio de defesa.

É claro que por se tratar de um mecanismo de defesa do Estado, esses investimentos externos deveriam alcançar um pilar básico de conhecimento no planejamento e organização estatal, já que o Sistema Internacional é Anárquico e os Estados possuem interesses em manter sua segurança a cima de tudo, mesmo que para isso tenha que atacar um Estado que está ainda no caminho se considerado um risco futuro. E nessa questão deixamos uma dúvida para possíveis pesquisas, A guerra cibernética, junto dos simuladores vieram para aposentar a infantaria e o combate tradicional?

REFERÊNCIAS

CANALTECH; **Exército Brasileiro Começa a Utilizar Simulador de Guerra Cibernética, o Simoc**; 2013. Disponível em: <https://canaltech.com.br/seguranca/Exercito-brasileiro-apresenta-simulador-de-guerra-cibernetica-o-Simoc/>. Acesso em: 25/03/2018.

CIGE; **Laboratório de Sinais – CIGE**; 2017. Disponível em: <http://www.ccomgex.eb.mil.br/index.php/laboratorios/250-laboratorios-sinais-cige >. Acesso em: 20/03/2018.

CUPERSHMID, Ana Regina M.; AMORIM, Joni A.; MATOS, Carlos Eduardo A. B.; **Uso de Realidade Aumentada Para o Treinamento Militar**; 2015. Disponível em: <http://rmct.ime.eb.br/arquivos/RMCT_3_tri_2015/RMCT_187_E8A_13.pdf>. Acesso em: 26/04/2018.

DECEx, EXÉRCITO BRASILEIRO; **O Uso de Simuladores no Ensino**; 2016. Disponível em: <http://www.portaldeeducacao.eb.mil.br/index.php/im-educacao-e-tecnologia/159-editor2>. Acesso em: 24/04/2018.

DEFESA NET; **Projeto Simaf – Simulador de Apoio de Fogo;** 2016. Disponível em: <http://www.defesanet.com.br/doutrina/noticia/23451/Projeto-SIMAF---Simulador-de-Apoio-de-Fogo/>. Acesso em: 27/04/2018.

DEFESA NET; **Simulação de Combate: Exército Materializa Tendência Global**; 2017. Disponível em: <http://www.defesanet.com.br/doutrina/noticia/26156/Simulacao-de-combate--Exercito-materializa-tendencia-global-/>. Acesso em: 19/04/2018.

EPEx, EXÉRCITO BRASILEIRO; **Defesa Cibernética "coordena e integra a defesa cibernética**"; 2013. Disponível em: <http://www.epex.eb.mil.br/index.php/defesa-cibernetica/defesa-cibernetica>. Acesso em: 11/03/2018.

GOVERNO DO BRASIL; **Apresentado o Simulador Nacional de Guerra Eletrônica**; 2013. Disponível em: <http://www.brasil.gov.br/defesa-e-seguranca/2013/01/apresentado-simulador-nacional-de-guerra-eletronica>. Acesso em:27/04/2018.

KOJIIO, Radael; SCOZ, Murilo; **Jogos Digitai: Uma Alternativa para Treinamento e Transferência de Habilidades Cognitivas**; 2016. Disponível em: <http://www.revistas.udesc.br/index.php/hfd/article/view/8792/6197>. Acesso em: 24/04/2018.

LEVY, Pierre; **Cibercultura**. São Paulo: Ed. 34, 1999;
MNISTÉRIO DA DEFESA; **Doutrina Militar de Defesa Cibernética: MD31 -M-07**; 2014. Disponível em: <http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf>. Acesso em: 13/03/2018.

ROSSINI, Carolina; Segurança Cibernética na Latino América: Atuação da OEA; 2015. Disponível em: <https://antivigilancia.org/pt/2015/06/construa-sua-seguranca-a-atuacao-da-oea-na-seguranca-cibernetica/>. Acesso em: 25/03/2018.

R7 NOTÍCIAS; **Exército Usa Tecnologia de Games Para Treinar Soldados**; 2012. Disponível em: <https://noticias.r7.com/tecnologia-e-ciencia/noticias/exercito-usa-tecnologia-de-games-para-treinar-soldados-20121103.html>. Acesso em: 20/04/2018.

SALDAN, Eliane; **Guerra Não-Virtual, Doutrina Precisa Definir Guerra Cibernética**; 2011. Disponível em: <https://www.conjur.com.br/2011-ago-06/guerra-cibernetica-urgentemente-definicao-doutrina>. Acesso em: 27/03/2018.

SENADO FEDERAL. **Por Uma Política Nacional de Segurança Cibernética**. Disponível em: <https://www12.senado.leg.br/emdiscussao/edicoes/espionagem-cibernetica/realidade-brasileira-sem-cultura-de-inteligencia/por-uma-politica-nacional-de-seguranca-cibernetica>. Acesso em: 25/02/2018.

TECMUNDO. **Simuladores X Games: Muito Parecidos, Mas Muito Diferentes Ao Mesmo Tempo**; 2015. Disponível em: <https://www.tecmundo.com.br/simuladores/83691-simuladores-x-games-parecidos-muito-diferentes-mesmo-tempo.htm>. Acesso em: 20/04/2018.