ADERLAN RICARDO LIMA RODRIGUES

EFEITO DAS AÇÕES DE GUERRA CIBERNÉTICA NOS SISTEMAS DE COMANDO E CONTROLE DOS GRUPAMENTOS OPERATIVOS DE FUZILEIROS NAVAIS

Trabalho Acadêmico – Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do certificado do Curso Superior de Segurança e Defesa Cibernética.

Orientador: Cel R1 João de Azevedo

Rio de Janeiro

2023

CSSDC2023 ESG

_____

ADERLAN RICARDO LIMA RODRIGUES

À minha amada esposa Christiane, minha companheira de vida, e à minha adorável filha Vittoria, fonte constante de inspiração todos os dias da minha vida.

RESUMO

Os avanços tecnológicos do século XXI promoveram uma transformação significativa nas operações militares, estimulando a adoção de inovações que reconfiguraram a estratégia de guerra. A utilização de sistemas integrados de Tecnologia da Informação e Comunicações (TIC) facilitou a eficiência na cadeia de comando, criando um ambiente cibernético altamente conectado, cujos dados e informações são compartilhados quase em tempo real. A introdução da Internet das Coisas (IoT) nas atividades militares resultou na Internet das Coisas Militar (IoMT) ou Internet das Coisas em Campo de Batalha (IoBT), empregando dispositivos de detecção, biometria e expressões faciais no contexto da Inteligência Artificial (IA). A conectividade e a interoperabilidade dos sistemas de Comando e Controle (C2) são fundamentais para as operações dos Fuzileiros Navais, permitindo comunicação eficaz e coordenação em tempo real. No entanto, a digitalização e a conectividade também trouxeram diversas vulnerabilidades para ataques cibernéticos, incluindo acesso não autorizado, exploração de falhas de segurança e ameaças de engenharia social, comprometendo a integridade dos sistemas de C2 e a confidencialidade das informações. Este estudo aborda a forma de emprego dos Fuzileiros Navais com a estrutura dos Grupamentos Operativos de Fuzileiros Navais (GptOpFuzNav) e destaca as implicações da Guerra Cibernética (GCiber) nas operações militares, enfatizando os efeitos das ações de ataque, exploração e proteção cibernéticas, especialmente nos sistemas de C2, com o potencial de impactar tanto no mundo físico quanto no ciberespaço. O trabalho também ressalta a importância do treinamento e da simulação em ambientes cibernéticos para capacitar os militares a lidar com ameaças cibernéticas complexas, ilustrando com exemplos de ataques cibernéticos em contextos militares, como o incidente Stuxnet nas instalações nucleares iranianas de Natanz e as ações cibernéticas durante os conflitos Russo-Geórgia e Russo-Ucrânia.

Palavras-chaves: transformação digital; guerra cibernética; comando e controle e Fuzileiros Navais.

ABSTRACT

The technological advancements of the 21st century have brought about a significant transformation in military operations, driving the adoption of innovations that have reconfigured the strategy of warfare. The use of Integrated Information Technology and Communications (ITC) systems has facilitated efficiency in the chain of command, creating a highly interconnected cyber environment where data and information are shared nearly in real-time. The introduction of the Internet of Things (IoT) into military activities has led to the Military Internet of Things (MIoT) or Internet of Battlefield Things (IoBT), employing detection devices, biometrics, and facial expressions within the context of Artificial Intelligence (AI). Connectivity and interoperability of Command and Control (C2) systems are fundamental to Brazilian Marine Corps operations, enabling effective communication and real-time coordination. However, digitization and connectivity have also introduced various vulnerabilities to cyberattacks, including unauthorized access, security vulnerabilities exploitation, and social engineering threats, compromising the integrity of C2 systems and the confidentiality of information. This study addresses the employment of Brazilian Marine Corps troops within the structure of Marine Corps Operational Groups (GptOpFuzNav) and highlights the implications of Cyber Warfare (CW) in military operations, emphasizing the importance of cyber attack, exploitation, and protection actions, especially within C2 systems, with the potential to impact both the physical world and cyberspace. The work also underscores the importance of training and simulation in cyber environments to empower military personnel to deal with complex cyber threats, illustrating with examples of cyberattacks in military contexts, such as the Stuxnet incident in Iranian Natanz nuclear facilities and cyber actions during the Russo-Georgian and Russo-Ukrainian conflicts.
Keywords*: digital transformation; cyberwarfare; command and control and Marines.*

SUMÁRIO

1 INTRODUÇÃO

O século XXI trouxe à superfície novos desafios e inovações tecnológicas que nas últimas décadas implicaram em mudanças significativas na arte da guerra, pois proporcionaram aos chefes militares e demais estudiosos do assunto novas ferramentas para conquistar vitórias sobre seus oponentes.

Essas inovações tecnológicas, muitas vezes complexas, aplicadas em um ambiente de incertezas, que é característico dos conflitos, permitirá que os Grupamentos Operativos de Fuzileiros Navais (GtpOpFuzNav), ao desempenharem suas atividades estabeleçam cadeias de comando para a disseminação de ordens e otimização dos processos decisórios, que proporcionam dados e informações praticamente em tempo real, empregando sistemas de voz, dados ou imagens existentes.

1.1 Apresentação do tema

Para o estabelecimento desta cadeia de comando os GptOpFuzNav contam com uma estrutura de Tecnologia da Informação e Comunicações (TIC) composta de computadores, rádios e sistemas funcionando de forma integrada. Essa integração fez surgir um ambiente virtual, onde as informações digitais transitam, são processadas e/ou armazenadas, denominado Espaço Cibernético (ECiber) que segundo definido por Brasil (2022) é um ambiente formado por ativos de TIC, onde dados e informações digitais são criados, armazenados, modificados, trafegados e processados. Adicionalmente, conforme apresentado por Brasil (2020), o ECiber constitui um dos domínios operacionais com atuação transversal aos demais domínios clássicos.

O desenvolvimento da indústria 4.0 proporcionou grande conectividade aos variados sistemas militares e a aproximação da Internet das Coisas (IoT) ao campo de batalha, criando assim a *Internet of Military Things* (IoMT) ou *Internet of Battlefield Things* (IoBT), permitindo que sejam implementados variados dispositivos de detecção não só do oponente como também das próprias forças amigas tais como biometria, gestos, expressões faciais e demais movimentos conforme apresentado por Cameron (2019). Adicionalmente, todas essas conexões poderão brevemente serem

potencializadas com o emprego de inteligência artificial (IA). Entretanto, o emprego da IA nas atividades militares não será objeto de estudo no presente trabalho.

A conectividade no campo de batalha e a grande utilização do ECiber apresentam vantagens, como a capacidade de coordenação eficiente entre unidades militares, compartilhamento de informações em tempo real e aprimoramento das estratégias de combate. No entanto, essa mesma conectividade também traz consigo desvantagens, incluindo a vulnerabilidade crescente a ataques cibernéticos, pois podem comprometer a integridade dos sistemas de Comando e Controle (C2), bem como a confidencialidade das informações militares.

1.2 Problema de Pesquisa

O problema da pesquisa está em estudar quais são os impactos das ações de Guerra Cibernética nos sistemas de C2 dos GptOpFuzNav que é decorrente da crescente incorporação de sistemas de TIC para emprego nas estruturas de C2 que permeiam todas as frações do GptOpFuzNav.

1.3 Objetivo

O objetivo deste trabalho consiste em identificar como as ações de Guerra Cibernética podem impactar o sistema de C2 dos GptOpFuzNav e apresentar suas implicações nas capacidades militares no combate contemporâneo.

1.4 Justificativa

Atualmente, as operações no ECiber (tanto ofensivas quanto defensivas) representam uma realidade às atividades militares em âmbito global, proporcionando vantagens substanciais na execução de suas tarefas. É amplamente reconhecido que o envolvimento nesse campo específico apresenta desafios consideráveis e implicações significativas para as Forças Armadas mais avançadas, podendo, em certas situações, resultar na impossibilidade de cumprir com êxito as missões atribuídas.

1.5 Metodologia resumida

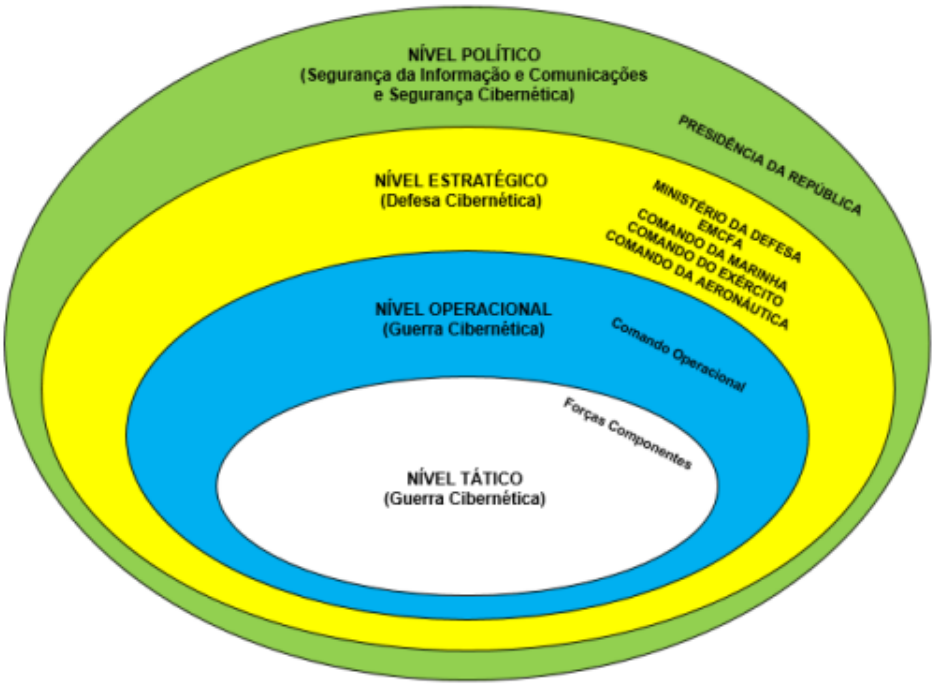
A metodologia de pesquisa adotada neste estudo baseou-se em uma abordagem qualitativa, utilizando a técnica de pesquisa bibliográfica extensiva. A coleta de dados foi realizada por meio de uma busca sistemática em bancos de dados eletrônicos, incluindo periódicos científicos, repositórios de teses e dissertações, bem como fontes de informação pública pertinentes ao tema. A seleção dos artigos, teses e dissertações permitiu a compilação de um conjunto diversificado de informações relevantes, contribuindo para a compreensão abrangente e aprofundada do contexto investigado. A utilização dessa abordagem possibilitou a análise crítica de estudos prévios e a síntese de conhecimento existente, fornecendo uma base para as discussões e conclusões apresentadas neste trabalho.

2 REFERENCIAL TEÓRICO

2.1 Segurança e Defesa Cibernéticas

A organização básica dos órgãos da Presidência da República e dos Ministério descrita em Brasil (2023) determina que, dentro da disciplina cibernética, a Segurança Cibernética esteja a cargo da Presidência da República, por meio as ações de planejamento, coordenação e supervisão exercidas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e a Defesa Cibernética seja de responsabilidade do Ministério da Defesa, por meio das Forças Armadas, conforme indicado na figura 1.

Figura 1 – Níveis de decisão do ECiber



Fonte: BRASIL, 2014.

No contexto do Ministério da Defesa as ações no ECiber possuem as seguintes denominações, de acordo com o nível de decisão, conforme apresentado na figura 1 acima identificada.

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

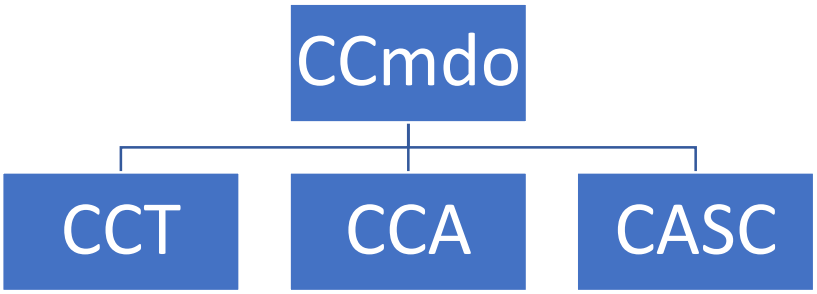
Níveis operacional e tático – **Guerra Cibernética** – denominação restrita ao âmbito interno das Forças Armadas.

2.2 Grupamentos Operativos de Fuzileiros Navais

De acordo com a doutrina do Corpo de Fuzileiros Navais da Marinha do Brasil, prevista em Brasil (2020), os Grupamentos Operativos de Fuzileiros Navais (GptOpFuzNav) são organizações por tarefas, nucleadas na forma de Componentes, agrupando elementos necessários para o atendimento de uma missão específica.

Os GptOpFuzNav poderão ser nucleados em unidades de valor Companhia de Fuzileiros Navais até uma Brigada de Fuzileiros Navais possuindo como componentes básicos, o Componente de Comando (CCmdo), o Componente de Combate Terrestre (CCT), o Componente de Combate Aéreo (CCA) e o Componente de Apoio de Serviços ao Combate (CASC) conforme apresentado na figura 2.

Figura 2 – Organização de um GptOpFuzNav



Fonte: BRASIL, 2020.

O CCmdo é o responsável por acolher o Comandante e seu Estado-Maior para o exercício do C2 da atividade. Dentro do CCT estarão agrupados os elementos destinados à realização de grande parte das atividades cinéticas, tais como a coordenação de fogos. O CCA é o responsável pela coordenação de todas as atividades relacionadas ao espaço aéreo dos GptOpFuzNav enquanto o CASC possui

a responsabilidade de atender as funções logísticas necessárias para o cumprimento da missão dos GptOpFuzNav.

Essa organização permite aliviar o Comandante da elevada sobrecarga de tarefas rotineiras de combate, de apoio ao combate e de apoio de serviços ao combate, proporcionando melhor eficiência das ações planejadas. Caso necessário poderão ser ativados “outros componentes” para o atendimento a uma missão específica como por exemplo um Hospital de Campanha (HCamp), um Grupo de Apoio ao Desembarque Administrativo (GRADA) e um Grupo de Operações Civis-Militares dentre outros.

2.3 Guerra Cibernética (GCiber)

Dentro do ECiber os GptOpFuzNav realizarão as ações de Guerra Cibernética (GCiber) com a finalidade potencializar os efeitos das ações geradas pelas funções de combate Comando e Controle, Manobra, Apoio de Fogo, Inteligência, Logística, Proteção e Mobilidade e Contramobilidade, conforme descrito por Brasil (2022) e também apresentado por Bombassaro Neto (2020).

Ainda de acordo com Brasil (2022), as ações de GCiber são classificadas em três tipos. O Ataque Cibernético (AtqCiber), que possui a finalidade de degradar, corromper, interromper, negar, ou destruir informações ou sistemas computacionais do oponente. Já a Exploração Cibernética (ExpCiber) reflete a capacidade de conduzir ações de busca ou coleta nos sistemas de TIC de interesse, a fim de obter dados e/ou aumentar consciência situacional do ECiber. Por último, temos as ações de Proteção Cibernética (PtçCiber), que são atividades de caráter permanente, que representa a capacidade de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito.

3 DESENVOLVIMENTO

3.1 Sistemas de C2 dos GptOpFuzNav e a interoperabilidade

A evolução tecnológica tem sido um fator determinante nas transformações das operações militares ao longo dos anos. Desde a Revolução Industrial no século XVIII, a tecnologia tem sido um fator determinante para o desenvolvimento econômico e social. Com o passar dos anos, a tecnologia evoluiu de forma exponencial, permitindo que as pessoas se conectem e compartilhem informações em tempo real.

Uma das mudanças mais significativas foi a inserção dos dispositivos de TIC nas operações militares, substituindo gradualmente métodos tradicionais, como o uso de papel, bússola e carta, permitindo maior eficiência, precisão e velocidade das ações militares. Esses dispositivos de TIC devidamente conectados e configurados permitem um elevado grau de interoperabilidade aos GptOpFuzNav e o estabelecimento de um sistema de C2 que permite ao Comandante o exercício do ciclo decisório em melhores condições do que seus oponentes.

Adicionalmente o conceito de operação do Sistema Militar de Comando e Controle do Ministério da Defesa prevê que as Forças Armadas do Brasil operem em elevado grau de interoperabilidade[1] por meio do estabelecimento de enlaces satelitais, redes operacionais de defesa e redes das Forças, além da existência de Centros de Comando e Controle nos níveis táticos, operacionais e político/estratégicos que permitirão o fluxo de ordens e relatórios a fim de imprimir uma velocidade do ciclo decisório maior do que aquela observada para o oponente (BRASIL, 2015a).

3.2 Importância dos sistemas de C2 nas operações dos GptOpFuzNav

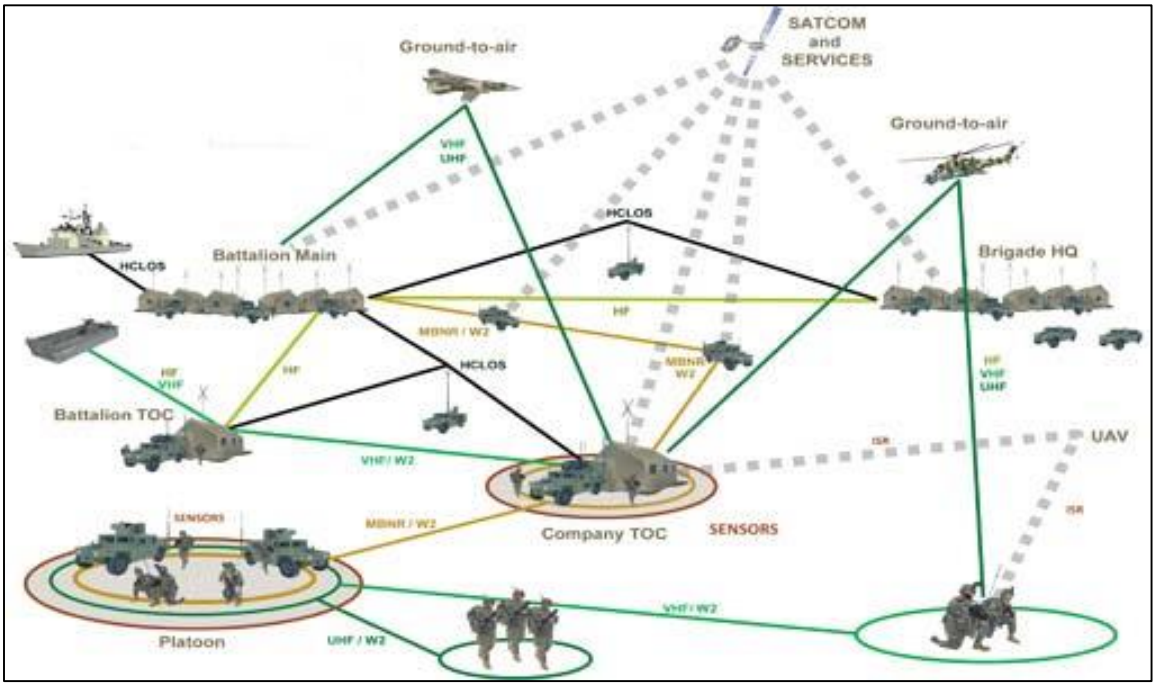
A introdução de dispositivos de TIC permitiu a criação de enlaces físicos e lógicos, fundamentais para o exercício do C2 praticamente em tempo real e o início do processo de operação em redes. Adicionalmente estamos observando alguns fenômenos da indústria 4.0 sendo aplicados com sucesso nas atividades militares,

[1] O Ministério da Defesa define como sendo a capacidade dos sistemas, unidades ou forças de intercambiarem serviços ou informações ou aceitá-los de outros sistemas, unidades ou forças e, também, de empregar esses serviços ou informações, sem o comprometimento de suas funcionalidades (BRASIL, 2015b)

particularmente o emprego de redes privativas de tecnologias 4G e 5G que proporcionam elevado grau de velocidade e conectividade entre os sensores militares dentro do conceito de IoMT/IoBT.

A forma de organização dos GptOpFuzNav demanda elevado grau de coordenação e o estabelecimento de enlaces que garantem o efetivo exercício do C2. Esses enlaces, muitas vezes apoiados por sistemas de comunicação via satélite, têm proporcionado aos GptOpFuzNav uma grande conectividade, mesmo em ambientes remotos ou adversos. Os enlaces satelitais, por exemplo, possibilitam a comunicação global e expedicionária, permitindo que as operações militares sejam planejadas e executadas com eficácia em qualquer parte do mundo, a exemplo do diagrama representado pela figura 3.

Figura 3 – Exemplo de diagrama de rede utilizado pelos GptOpFuzNav



Fonte: KURDZIEL, 2014.

Segundo Rodrigues e Silva (2018), atualmente os GptOpFuzNav empregam Rádios Definidos por Software (RDS), enlaces satelitais, aplicações para Gerenciamento de Área de Operações, aplicações para a coordenação de Apoio de Fogos e processamento de informações que proporcionam um aumento na velocidade do processo decisório do Comandante do GptOpFuzNav colocando-o em vantagem no desempenho de suas funções. A reunião dessas ferramentas descritas possibilita a formação de uma "rede operacional", conforme ilustrado na figura 3. Essa rede é

configurada e operada de modo similar a uma rede de informática encontrada nas empresas, escritórios e unidades administrativas, com seus servidores, protocolos, endereços, facilidades e vulnerabilidades.

Ao analisar as informações descritas, fica evidente a existência de um sistema de TIC que desempenha um papel crucial no suporte ao C2. Esse sistema não apenas aprimora a eficiência operacional, mas também contribui para o aumento da velocidade do processo decisório. No entanto, é imperativo reconhecer que esses sistemas, devido à sua conectividade e complexidade, estão suscetíveis a uma série de ameaças cibernéticas, tornando essencial a implementação de medidas robustas de proteção dos ativos.

3.3 Vulnerabilidades dos sistemas de C2 dos GptOpFuzNav frente a ameaças cibernéticas.

As possibilidades de acesso os sistemas de militares de TIC podem ser descritas de acordo com o apresentado por Gomes, Cordeiro e Pinheiro (2016) em que se destacam as ações de exploração cibernética aos sistemas utilizados. A empresa *Lockheed Martin* desenvolveu o modelo *Cyber Kill Chain*, composto por sete (7) fases, apresentadas na figura 4, que permite uma melhor visibilidade e entendimento das ações a serem realizadas por um atacante no espaço cibernético.

Figura 4. Modelo Cyber Kill Chain

Fonte: DONDA, 2021.

No processo *Cyber Kill Chain* o reconhecimento é caracterizado pelas atividades de observação, estudo, pesquisa e *o modus operandi* do alvo pretendido com a finalidade de identificar suas vulnerabilidades a serem exploradas. Já na fase do armamento o invasor desenvolve ou adquire uma arma cibernética, que pode ser

um malware, um vírus, ou outra semelhante, com a finalidade de explorar a vulnerabilidade encontrada, uma combinação de vulnerabilidades ou até mesmo uma nova não explorada (*zero day*). A fase da entrega constitui as ações para a transmissão e envio do vetor preparado ou adquirido para o ataque, que poderá ser realizado por um e-mail de *phishing* ou drives USB por exemplo. Na fase da exploração, o *malware* ou outra arma cibernética selecionada inicia o processo de exploração do alvo com movimentações laterais e elevação de privilégios. Durante a fase da instalação o *malware* realiza a instalação de um acesso (*backdoor*) que permite ao atacante a entrada na rede sempre que desejar. Seguindo para a fase de Comando e Controle o *malware* permitirá que o invasor tenha acesso à rede ou sistema, controlando os ativos de interesse de forma remota. A última fase, chamada de ações no objetivo, o invasor irá decidir o que será realizado para o cumprimento de sua ação, como criptografia, destruição ou exfiltração dos dados. Estas ações também podem ser encontradas de forma detalhada na matriz apresentada pela MITRE ATT&CK (MITRE *Adversarial Tactics, Techniques, and Common Knowledge*) que também procura identificar e imitar o comportamento de invasores em ambientes Windows, Mac, Linux, nuvem, dispositivos móveis (Android e IOS) e sistema de controle industrial (*Industrial Control System* - ICS).

Considerando que o elo mais sensível da cadeia de informação é o ser humano, conforme apresentado por Mitnick e Simon (2003), a baixa mentalidade de segurança, desde os níveis iniciais de formação acadêmica dos militares, seja em estabelecimentos civis ou militares, é uma vulnerabilidade que deve ser permanentemente atacada. Nesse processo, acredita-se que a ação de aumento desta mentalidade produzirá resultados positivos na rotina administrativa e pessoal dos envolvidos, evitando, assim, o sucesso da engenharia social.

A vulnerabilidade causada pelo baixo controle de dispositivos que permitem a extração e inserção de dados nos dispositivos de TIC que compõem o sistema de C2 dos GptOpFuzNav contribui de forma decisiva para a ação de vírus e *worms* de variadas categorias. O estabelecimento de procedimentos que visam limitar o acesso a métodos de inserção e extração de dados (por exemplo: portas USB, PenDrive, etc.) e o emprego de programas antivírus atualizados proporcionarão uma redução significativa desta forma de ação. Nesse ínterim, cabe ressaltar que os GptOpFuzNav, mesmo atuando de forma isolados, são vulneráveis às ações de GCiber, utilizando

técnicas específicas, a exemplo da ação adotada pelo vírus Stuxnet no sistema de controle das centrífugas da usina nuclear de Natanz, no Irã (ZETTER, 2014).

Adicionalmente os sistemas de TIC utilizados necessitam de atualizações de *softwares* e *firmwares* necessários para a correção de falhas durante o desenvolvimento dos produtos e ou correção de vulnerabilidades lógicas descobertas. O processo de atualização constitui uma vulnerabilidade a ser controlada para garantir a segurança e a utilização segura dos sistemas após a execução do procedimento, pois durante o processo de atualização o sistema de TIC poderá ser intencionalmente comprometido. Adicionalmente, a implementação de regras lógicas de acesso e proteção deve ser realizada e constantemente revisada para evitar que os servidores existentes possam ser alvo de ações de GCiber inimigas.

Outras vulnerabilidades que devem ser combatidas incluem a necessidade de proibição de utilização de dispositivos pessoais e o registro indevido de imagens, que podem facilmente ser explorados por meio de metadados, tornando-se fonte de dados importantes para o oponente e comprometendo as ações dos GptOpFuzNav (HENNE; SMITH, 2013).

Adicionalmente, os GptOpFuzNav possuem acesso à Rede Operacional de Defesa (ROD) para o exercício do C2. A ROD pode utilizada para proporcionar serviços de TIC em operações conjuntas e singulares e utiliza o Sistema Militar de Comunicações por Satélite (SISCOMIS) como canal principal e as redes da Forças como meio alternativo (BRASIL, 2015a). Esta conectividade apresenta as vulnerabilidades características de uma *Wide Area Network (WAN)* e que devem ser tratadas a fim de mitigar os riscos decorrentes. Além disso, em um rol não exaustivo, a aplicação da Inteligência Artificial (IA), possui a capacidade de potencializar a exploração dessas vulnerabilidades apresentadas.

3.4 Desafios para Defesa Cibernética nos sistemas de C2 dos GptOpFuzNav

Ao analisar as informações pertinentes, fica evidente a complexidade dos desafios enfrentados pelo sistema de C2 dos GptOpFuzNav em seu ECiber contra ameaças potenciais. Para que o efeito das ações de GCiber inimigas seja minimizado contra os sistemas de C2 dos GptOpFuzNav e, ao mesmo tempo, essas unidades sejam capazes de potencializarem as funções de combate nos demais domínios, são necessárias atuações permanentes do ECiber dos GptOpFuzNav.

Um desses desafios envolve a necessidade de elevar o nível de consciência e defesa cibernética entre os Fuzileiros Navais, a fim de reduzir a vulnerabilidade do sistema. De acordo com Machado (2016) uma das formas dos militares de elevar a maturidade e de adquirir a capacidade de atuar no ECiber, que demanda capacidades especificas, está o emprego de simuladores Cibernéticos Cibernéticos tais como o *CyberProtect*, desenvolvido pelo Departamento de Defesa Americano; o *Military Academy Attack/Defense Network* (MAADNET), que foi criado para auxiliar a formação dos cadetes da Academia Militar Norte Americana; o *CyberOps: NetWarrior*, desenvolvido pela Agência de Defesa de Sistemas da Informação, do Departamento de Defesa Norte Americano; o *The cyber Defense Technology Experimental Research laboratory (DETERlab)*, que foi desenvolvido pela Universidade de *Utah* e é utilizado como um laboratório nas aulas de segurança cibernética; o *CyberCIEGE*, do Centro de Estudos de Segurança de Sistemas de Informação e Pesquisas, da Universidade de Pós-graduação dos EUA e o *Real-Time Immersive Network Simulation Enviromment (RINSE)*, que é um simulador desenhado para realizar treinamento e exercício de segurança cibernética em tempo real. Ainda de acordo Machado (2016), no Exército Brasileiro (EB) temos o simulador de Operações de Guerra Cibernética (SIMOC) que é o ambiente utilizado pelo Centro de Instrução de Guerra Eletrônica para capacitar militares e civis nos cursos e estágios de Guerra Cibernética. Todos esses simuladores podem ser utilizados de acordo com a sugestão de competências e metodologia necessária de treinamento proposta por Almeida Jr. (2021).

Para o funcionamento do sistema de C2 utilizado pelos GptOpFuzNav, descrito por Rodrigues e Silva (2018), existe a necessidade de utilização de servidores e hardwares que requerem atualizações contínuas para evitar potenciais vulnerabilidades. A indústria de hardwares no Brasil ainda possui grande necessidade de desenvolvimento. Porém, segundo Malagutti e Gama Neto (2020), uma das soluções para a eliminação da dependência tecnológica de softwares, evitando ação de *backdoors*, é o emprego de software de código aberto, em particular distribuições Linux, por motivação de segurança e defesa. Países como Estados Unidos da América, China, Rússia, Coreia do Sul, Coreia do Norte, Índia e Turquia já adotam tal solução. Cabe ressaltar que os navios americanos da classe *Zumwalt*, já incorporaram o *Linux Red Hat* em seus sistemas de navegação, manutenção, armamentos e monitoração (GALLAGHER, 2013).

Além disso, considerando as vulnerabilidades inerentes a uma *Wide Area Network* (WAN), é crucial implementar estratégias eficazes para lidar com essas questões. Para mitigar tais riscos, os GptOpFuzNav empregam o sistema de PtçCiber conhecido como *Dreadnought*, desenvolvido pela Marinha do Brasil, que se baseia em um hardware robusto e escalável, combinado com software livre, modular e customizável (MOTA JUNIOR; MARTINS, 2022).

Por fim, é fundamental estar preparado para a eventual incorporação da IA nesse domínio, a fim de enfrentar os desafios em constante evolução neste domínio.

3.5 Guerra Cibernética nas Operações Militares

A Guerra Cibernética (GCiber) se diferencia da Guerra Cinética tradicional pelo fato de ser capaz de produzir impactos no mundo real e no ciberespaço devido à sua natureza transversal, ao passo que a Guerra Cinética afeta apenas o mundo físico. Tais ações cibernéticas podem ser executadas tanto por agentes estatais quanto não estatais e sua condução nos conflitos recentes demonstram que dificilmente teremos uma Guerra puramente cibernética (LEHTO, 2023).

Como emprego da atividade cibernética sem a participação direta do componente militar, de acordo com Rid e McBurney (2012), podemos citar as ações como a explosão do gasoduto transiberiano em 1982, creditado à Central de Inteligência Americana (CIA), os ataques às diversas redes na Estônia por semanas motivados após a retirada de estátua representativa do Exército Vermelho. Ainda segundo a empresa I-StarTI Tecnologia[2] podemos citar o ataque originário da China ocorrido em 2009 que invadiu quase 1.300 computadores em 103 países, atingindo embaixadas e escritórios governamentais ao redor do mundo. No ano seguinte, em 2010, foi creditado também à China um ataque direcionado ao Ministério da Defesa da Índia, no qual informações confidenciais sobre o sistema de segurança nacional da Índia foram subtraídas e em outro episódio, a chamada "Unidade 61398" do Exército de Libertação do Povo Chinês foi acusada de invadir as redes de computadores de empresas norte-americanas, incluindo a Westinghouse Electric e a US Steel Corp.,

[2] Empresa de segurança da informação nacional. Informação publicada pela empresa em seu sitio institucional por seu diretor de negócios Marcio Zilli. Disponível em: https://i-starti.com.br/2021/01/25/ciberguerrilha-retro/.

desencadeando preocupações significativas sobre a segurança cibernética e as relações internacionais.

Para apresentar o emprego da GCiber nas operações militares podemos citar a Operação Orchard, que de acordo com Clark e Knake (2010), foi conduzida pelo estado de Israel contra a Síria em 2007, na qual aeronaves militares bombardearam uma instalação nuclear em construção, por meio de uma Medida de Ataque Cibernético associada à uma Medida de Ataque Eletrônico ao sistema radar sírio, chamando a atenção o fato do sistema de defesa antiaérea sírio não apresentar alertas de invasão do espaço aéreo no momento do ataque.

De forma adicional, temos o emprego das ações de GCiber no conflito Russo-Geórgia ocorrido em 2008 que ocorreram precedendo as ações cinéticas do exército Russo, afetando o acesso as fontes de informação externa, sistema bancário, sistema de energia elétrica por exemplo, em complementos aos ataques cinéticos convencionais (SÁ; MACHADO; ALMEIDA, 2019).

Um dos exemplos mais estudados é o do artefato cibernético descrito como Stuxnet, cujo desenvolvimento e emprego inicial é creditado aos Estado Unidos da América e Israel e segundo os conceitos apresentados por Rid e McBurney (2012) pode ser considerado uma *Cyber Weapon*. O artefato foi o responsável por fornecer dados inconsistentes ao sistema *Supervisory Control and Data Acquisition* (SCADA) utilizado pelas centrífugas de enriquecimento de urânio na usina de Natanz enquanto efetuava a alteração de velocidade física das centrífugas, ocasionando falha no processo de enriquecimento de urânio, danificação das centrífugas e atraso no programa em geral. Dentre os aspectos importantes deste fato é que o artefato atingiu seu objetivo mesmo a usina de Natanz estando com suas redes de controle de forma “isolada”.

De acordo com Pagliusi (2022), com a potencialização das tecnologias disruptivas, tal como a internet das coisas, computação em nuvem, sistemas autônomos e inteligência artificial, as ações de GCiber aumentaram significativamente a superfície de potencial ataque, migrando do ambiente de TIC para o da Tecnologia Operacional (TO). Essa TO pode ser compreendida como qualquer conjunto de hardware e software que são empregados com a finalidade de obter informações, controlar ou garantir a segurança de funcionamento, seja em uma organização ou em âmbito nacional.

A evolução das ações no espaço cibernético ao longo do tempo tem sido marcada por uma crescente sofisticação e complexidade. Um exemplo dessa evolução pode ser observado nas ações cibernéticas empregadas durante o conflito entre Rússia e Ucrânia. Nesse contexto, tecnologias disruptivas, como a Inteligência Artificial, desempenharam um papel significativo na condução dessas operações. Conforme apresentado por Pagliusi (2022), russos e ucranianos utilizam táticas de atuação híbrida, que incluem ações cibernéticas, para alcançar diversos objetivos, como causar danos às infraestruturas, interrupção de serviços, obter informações estratégicas e conquistar a simpatia de parcela da população.

Essas ações cibernéticas operando de forma integrada, potencializou os demais domínios operacionais, fazendo com que o ciberespaço se torne um campo de batalha essencial, interconectado com os aspectos tradicionais do conflito. De acordo com o relatório publicado pela Microsoft (2023) podemos destacar as ações da Rússia para prover informações e apoiar sua guerra contra a Ucrânia, ações Iranianas com o objetivos de atacar seus alvos de interesse e fortalecer sua posição geopolítica, ações chinesas com o objetivos de facilitar a aceitação de seus produtos estratégicos em mercados de interesse e conseguir apoio ao seu projeto de nova rota da seda e os norte coreanos que utilizam as ações no ECiber com o objetivo de patrocinar o desenvolvimento de seus projetos de estado obtendo informações desejadas e recursos financeiros.

Essa interconexão demonstra a crescente importância da cibernética nas operações militares contemporâneas, atuando de forma híbrida, reforçando a ideia de que as ações no espaço cibernético têm o potencial de influenciar e moldar os desfechos em outros domínios.

3.6 Efeitos das ações de GCiber nos sistemas de C2 dos GptOpFuzNav

A digitalização dos sistemas de comando e controle de navios de guerra e a integração de outros recursos navais na mesma rede aumentam a vulnerabilidade a ataques cibernéticos. Mesmo com criptografia, a maioria das embarcações permanece conectada à internet, por meio satelital, apresentando riscos de segurança, mesmo com separação física entre as redes. Informações detalhadas sobre ataques cibernéticos em meios navais militares são difíceis de confirmação. Porém, de acordo com o *CHIPS Articles*, elaborado pelo Gabinete do Vice-Chefe de

Operações Navais para Guerra de Informação do Departamento da Marinha dos Estados Unidos da América, em junho de 2017, um navio comercial navegando perto da costa russa enfrentou uma situação perigosa quando seu sistema de navegação GPS indicou erroneamente que a embarcação estava a 32 quilômetros de distância, no interior de um aeroporto. Além desse incidente, pelo menos outros 20 navios na região relataram problemas semelhantes com seus sistemas de identificação automática, que eram também os mesmos utilizados pelos navios da Marinha dos Estados Unidos. Nesse contexto fica evidente a necessidade de proteção cibernética aos meios navais e a crescente preocupação de construção de navios que sejam digitais-nativos (PERUZZI, 2019).

De acordo com Rodrigues e Silva (2019) a partir do emprego de um sistema integrado de Comando e Controle torna-se imperativo que os GptOpFuzNav possuam um sistema de GCiber para se contraporem as vulnerabilidades e as ameaças em sistemas digitais operativos conforme apresentado por Magalhães (2019). As vulnerabilidades de sistemas operacionais desatualizados, aquisição de *hardware* e *software* de empresas fora da base de defesa nacional são vulnerabilidades que devem ser monitoradas no âmbito dos GptOpFuzNav, seja por ocasião da aquisição de materiais e sistemas, manutenções programadas ou falha de configuração de enlaces satelitais. Essa exploração por um adversário poderá causar grandes danos, como por exemplo a inserção de erros programados nas rotinas de apoio de fogo, classificação equivocada de alvos, alterações planejadas de limites, supressão de ordens e relatórios além das incorreções no georreferenciamento por meio do *Global Positioning System* (GPS).

Os ataques cibernéticos aos sistemas de C2 de unidades terrestres representam uma grave ameaça à segurança das atividades e ao pessoal envolvido. Eles podem prejudicar a confidencialidade, integridade e disponibilidade de informações, interferir no controle das forças e dos recursos militares e causar desorientação entre os envolvidos. Stokes (2018) relata um incidente cibernético que ocorreu nas redes de C2 de uma unidade dos Fuzileiros Navais dos Estados Unidos da América, situada em uma região do Nordeste da Ásia. Durante a ação no Posto de Comando, houve um ataque cibernético direcionados às redes de C2, interrompendo seu funcionamento. Estes ataques coincidiram com uma ofensiva cinética realizada pelo inimigo, que envolveu disparos de artilharia na mesma área. Como resultado, os Fuzileiros Navais americanos se viram obrigados a abandonar os sistemas de C2

modernos e retornar ao uso de ferramentas tradicionais, como lápis, papel, bússola, transferidor, acetatos e rádios analógicos.

O GptOpFuzNav por possuírem seu *modus operandi* semelhante aos Fuzileiros Navais americanos estão passiveis de sofrerem ataques semelhantes em suas estruturas de C2. Ataques cibernéticos aos sistemas de C2 dos GptOpFuzNav, resultantes da exploração das vulnerabilidades já apresentadas, poderão causar danos similares aos sofridos pelas unidades americanas, além de comprometer seus sistemas de armas, alterar seu ambiente informacional e impedir o cumprimento da missão.

4 CONSIDERAÇÕES FINAIS

O avanço tecnológico e a aplicação de TIC têm gerado uma transformação, também no campo militar, culminando no ECiber. Esse domínio cibernético, que é transversal aos domínios clássicos, se caracteriza pela criação de uma rede interconectada que contribui para a celeridade do processo decisório dentre outras atividades. Apesar das vantagens evidentes, é importante ressaltar que o ECiber não está imune a desafios, especialmente quando consideramos as ameaças inimigas que exploram as vulnerabilidades, conforme descrito em modelos como o *Cyber Kill Chain* ou o MITRE. Observa-se que as forças militares modernas têm cada vez mais utilizado esse domínio cibernético em suas operações. Nesse sentido, o presente trabalho destaca a relevância crucial de abordar as vulnerabilidades nas redes de C2 dos GptOpFuzNav, pois a exploração dessas vulnerabilidades pode resultar em consequências, como a inserção de erros programados nas rotinas de apoio de fogo, classificação incorreta de alvos, alterações deliberadas de limites em operações, supressão de ordens e relatórios, imprecisões do GPS, além da total paralisia dos sistemas de TIC, proporcionando uma volta às ferramentas analógicas de outrora, tais como papel, lápis, cartas e rádios em modo voz.

Por fim, a ocorrência do ataque cibernético aos Fuzileiros Navais dos Estados Unidos da América, operando na região da Ásia, destaca a necessidade urgente de ações mais enérgicas e vigilantes a serem implementadas, de forma permanente, nos GptOpFuzNav nesse domínio. A similaridade do *modus operandi* reforça a importância de garantir a segurança e a eficácia das operações militares e a necessidade de aperfeiçoar a capacidade de PtçCiber dos sistemas de C2. Tais ações requerem aprimoramentos nos processos de capacitação e domínio de tecnologias.

REFERÊNCIAS

ALMEIDA JR., José Augusto de. **Identificação de Competências dos Cyber Red Teams Militares e Proposta de Metodologia de Treinamento Contínuo para Projeção do Poder na Guerra Cibernética.** 2020. 64 p. Dissertação (Mestrado profissional em Engenharia Elétrica) - Universidade de Brasília, Brasília, DF, 2020. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/01/Dissertacao___Jose_Augusto_de_Almeida_Junior__2_-2.pdf. Acesso em: 16 out. 2023.

BOMBASSARO NETO, Samuel. A atuação da Guerra Cibernética como elemento multiplicador do poder de combate da Força Terrestre Componente em operações ofensivas. **A Defesa Nacional**, Rio de Janeiro, n. 841, p. 63-73, 2020. Disponível em: https://ebrevistas.eb.mil.br/ADN/article/view/5612. Acesso em: 16 out. 2023.

BRASIL. Comando da Marinha. Comando-Geral do Corpo de Fuzileiros Navais. **Manual Básico dos Grupamentos Operativos de Fuzileiros Navais -** Manual CGCFN 0-1. Rio de Janeiro: CGCFN, 2020. 54 p.

BRASIL. Comando da Marinha. Comando-Geral do Corpo de Fuzileiros Navais. **Manual de Ações de Guerra Cibernética dos Grupamentos Operativos de Fuzileiros Navais -** Manual CGCFN 60.2. Rio de Janeiro: CGCFN, 2022. 46 p.

BRASIL. Lei nº 14.600, de 19 de junho de 2023. Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios. **Diário Oficial da União**: seção 1, Brasília, DF, ano 161, n. 116, p. 1-127, 20 jun. 2023.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética -** Manual MD31-M-07. Brasília, DF MD, 2014. 36 p.

BRASIL. Ministério da Defesa. **Conceito de Operações do Sistema Militar de Comando e Controle -** Manual MD31-S-02. Brasília, DF: MD, 2015a. 64 p.

BRASIL. Ministério da Defesa. **Glossário das Forças Armadas -** Manual MD35-G-01. Brasília, DF: MD, 2015b. 288 p.

CAMERON, Lori. Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT. **IEEE Computer Society**, 2019. Disponível em: https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt. Acesso em: 16 out. 2023.

CLARK, Richard A.; KNAKE, Robert K. **Cyber War**: the next threat to national security and what to do about it. New York: Ecco, 2010.

THE CYBER Threat is Real. Deputy Chief of Naval Operations for Information Warfare (N2N6). **The Department of the Navy´s Information Technology Magazine**. Washington, DC: Department of the Navy, [202-]. Disponível em:

https://www.doncio.navy.mil/Chips/ArticleDetails.aspx?ID=9537. Acesso em: 16 out. 2023.

DONDA, Daniel. Cyber kill chain. **Daniel Donda**, 04 out. 2021. Disponível em: https://danieldonda.com/cyber-kill-chain/. Acesso em: 16 out. 2023.

GALLAGHER, S. The Navy's newest warship is powered by Linux. **Ars Technica**, 18 Oct. 2023. Disponível em: https://arstechnica.com/information-technology/2013/10/the-navys-newest-warship-is-powered-by-linux/. Acesso em: 10 out. 2023.

GOMES, Mauro Guedes Ferreira Mosqueira; CORDEIRO, Sandro Silva; PINHEIRO, Wallace Anacleto. A Guerra Cibernética: exploração, ataque e proteção cibernética no contexto dos sistemas de Comando e Controle (C2). **Revista Militar de Ciência e Tecnologia**, Rio de Janeiro, v. 33, n. 2, p. 11-18, 2016. Disponível em: https://rmct.ime.eb.br/arquivos/revistas/RMCT_web_3_tri_2016.pdf. Acesso em: 16 out. 2023.

HENNE, B.; SMITH, M. Awareness about photos on the Web and how privacy-privacy-tradeoffs could help. *In*: FINANCIAL Cryptography and Data Security. Berlin: Springer Berlin Heidelberg, 2013. p. 131-148. Disponível em: https://link.springer.com/chapter/10.1007/978-3-642-41320-9_9. Acesso em: 16 out. 2023.

KURDZIEL, Michael. **Harris integrated battlefield communications architecture**. [*S. l.: s. n.*], 2014. Disponível em: https://www.researchgate.net/figure/Harris-Integrated-Battlefield-Communications-Network-Architecture_fig3_269321977. Acesso em: 16 out. 2023.

LEHTO, M. Cyber Warfare and War in Ukraine. **Journal of Information Warfare**, v. 22, n. 1, 2023. Disponível em: https://natolibguides.info/cyberdefence/articles. Acesso em: 16 out. 2023.

MACHADO, A. F. A. **Simulador de operações de guerra cibernética: ferramenta de treinamento e preparo de recursos humanos para atuarem no ciberespaço**. 2016. 67 p. Trabalho de Conclusão de Curso (Pós-graduação Lato Sensu em Redes de Computadores com Ênfase em Segurança) - Instituto CEUB de Pesquisa e Desenvolvimento, Centro Universitário de Brasília, Brasília, DF, 2016. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/235/12394/1/51400171.pdf. Acesso em 16 out. 2023.

MAGALHÃES, K. M. C. Contramedidas cibernéticas em sistemas operativos. **Revista Marítima Brasileira**, Rio de Janeiro, v. 139, n.10/12, p. 92-111, 2019. Disponível em: https://portaldeperiodicos.marinha.mil.br/index.php/revistamaritima/issue/view/559. Acesso em: 16 out. 2023.

MALAGUTTI, M. A. O.; GAMA NETO, R. B. Por que o Brasil deveria adotar uma distro Linux própria? **Revista Brasileira de Estudos de Defesa**, v. 7, n. 2, 2020.

Disponível em: https://rbed.abedef.org/rbed/article/view/75248. Acesso em: 16 out. 2023.

MICROSOFT. **Microsoft Digital Defense Report 2023**: Global Cyberattacks. [*S. l.*]: MICROSOFT, 2023. Disponível em: https://www.microsoft.com/en/security/security-insider/microsoft-digital-defense-report-2023/. Acesso em: 16 out. 2023.

MITNICK, Kevin D.; SIMON, William L. **A Arte de Enganar**. São Paulo: Pearson Education do Brasil, 2003.

MOTA JUNIOR, Salvador; MARTINS, Norival Lourenço. Sistema Dreadnought. **Revista Passadiço**, Rio de Janeiro, v. 34, n. 42, p. 50-50, 2022. Disponível em: https://www.portaldeperiodicos.marinha.mil.br/index.php/passadico/article/view/3731. Acesso em: 16 out. 2023.

PAGLIUSI, Paulo Sergio. Guerra Cibernética russo-ucraniana: lições para o Brasil e para o mundo**. Revista do Clube Naval**, Rio de Janeiro, v. 2, n. 402, p. 74-79, 2022. Disponível em: https://portaldeperiodicos.marinha.mil.br/index.php/clubenaval/article/view/3189. Acesso em: 16 out. 2023.

PASTOR, Vicente; DÍAZ, Gabriel; CASTRO, Manuel. State-of-the-art simulation systems for information security education, training and awareness. *In*: IEEE EDUCON Conference, 2010, Madrid. **Proceedings** [...]. New York: IEEE, 2010. p. 1907-1916. Disponível em: https://ieeexplore.ieee.org/abstract/document/5492435. Acesso em: 16 out. 2023.

RID, Thomas; McBURNEY, Peter. Cyber-Weapons, **The RUSI Journal**, v. 157, n. 1, p. 6-13, 2012. Disponível em: https://indianstrategicknowledgeonline.com/web/rusi%20cyber%20weapons.pdf. Acesso em: 16 out. 2023.

PERUZZI, Luca. The New Generation Digital Native FDI Belh@rra Frigate. **European Defence Review Magazine**, Paris, 03 Nov. 2019. Disponível em: https://www.edrmagazine.eu/the-new-generation-digital-native-fdi-belhrra-frigate. Acesso em: 16 out. 2023.

RODRIGUES, Aderlan R. L.; SILVA, Maurício S. da. O Sistema Integrado de Comando e Controle do Corpo de Fuzileiros Navais (SIC2CFN) e a Tecnologia da Informação e Comunicações (TIC) nos Grupamentos Operativos de Fuzileiros Navais (GptOpFuzNav). **Revista Âncoras e Fuzis**, Rio de Janeiro, n. 50, p. 26-31, 2019. Disponível em: https://portaldeperiodicos.marinha.mil.br/index.php/ancorasefuzis/article/view/2284. Acesso em: 16 out. 2023.

SÁ, Alan Oliveira de; MACHADO, Raphael Carlos Santos; ALMEIDA, Nival Nunes. O encontro da guerra cibernética com as guerras eletrônica e cinética no âmbito do Poder Marítimo. **Revista da Escola de Guerra Naval,** Rio de Janeiro, v. 25, n. 1, p. 89-128, 2019. Disponível em:

https://portaldeperiodicos.marinha.mil.br/index.php/revistadaegn/article/view/4347. Acesso em: 16 out. 2023.

STOKES, Maj Paul L. Closing the MAGTF C2/Cyber Gap. The requirement of a C2/Cyber center of excellence. **Marine Corps Gazette**, v. 102, n. 4, 2018. Disponível em: https://www.mca-marines.org/wp-content/uploads/0418-Closing-the-MAGTF-C2Cyber-Gap.pdf. Acesso em: 16 out. 2023.

ZETTER, Kim. **Countdown to zero day**: stuxnet and the launch of the world's first digital weapon. New York: Crown Publishing Group, 2014.