Guerra Cibernética nas atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos

8

Capitão de Corveta (AFN) **Vanderlan** Silva da Costa

É graduado pelo Curso de Formação de Oficiais do Centro de Instrução Almirante Wandenkolk. Ao longo de sua carreira, realizou diversos cursos, com destaque para o Curso de Aperfeiçoamento de Oficiais do Corpo de Fuzileiros Navais (CAOCFN), o Curso de Guerra Cibernética para Oficiais e o Curso Superior (C-Sup). Entre as principais comissões, foi Comandante de Pelotão no 1º Batalhão de Infantaria de Fuzileiros Navais (Batalhão Riachuelo) e Encarregado da Seção de Ações Cibernéticas da extinta Subchefia de Inteligência no Comando de Operações Navais.

Introdução

Ao longo da história, tem-se observado que os contendores nos conflitos bélicos que prontamente se adaptam e integram novas tecnologias aos seus arsenais e estratégias obtêm vantagens decisivas sobre seus adversários. Esse fenômeno foi evidenciado pela introdução de elementos como a cavalaria e pelo uso de bigas, arcos, balestras e armas de fogo, entre outros inventos. Atualmente, as inovações tecnológicas continuam a remodelar os campos de batalha, fornecendo meios inovadores para alcançar a vitória (BRASIL, 2022a).

Figura 1: As inovações no campo de batalha.

Fonte: O autor.

Outro aspecto crucial é a aquisição de informações detalhadas sobre as forças oponentes, o que se mostra fundamental para o planejamento e a execução de operações militares exitosas. Nesse panorama, é comum a utilização de tropas especializadas em Operações Especiais e Inteligência, que desempenham atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA). No entanto, o emprego desses operadores implica desafios significativos em termos de Comando e Controle (C2), logística e manutenção do sigilo operacional.

Para mitigar esses desafios, buscando antecipar a coleta de informações e minimizar a exposição dos operadores em territórios hostis, várias nações têm desenvolvido e implementado ferramentas, técnicas e métodos de sensoriamento remoto. Entre eles, destaca-se o uso de plataformas satelitais, drones e sistemas de Guerra Eletrônica. Uma abordagem crescentemente relevante na aquisição de conhecimento é a Guerra Cibernética (GCiber), sobretudo através das ações de Exploração Cibernética (ExplCiber) e Ataque Cibernético (AtqCiber). Essas estratégias são empregadas para exfiltração de dados, estabelecimento e manutenção de vigilância e localização de tropas.

Embora a Guerra Cibernética exija recursos humanos e equipamentos altamente especializados, seus desafios em termos de Comando e Controle, Logística e manutenção do sigilo são consideravelmente menos complexos que aqueles associados ao emprego de operadores especiais, Inteligência ou plataformas de sensoriamento remoto.

Portanto, este artigo busca demonstrar como as ações de Guerra Cibernética podem ser decisivas nas atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos em Operações Navais.

1. Guerra Cibernética

Conforme apontam Singer e Friedman (2017), a Guerra Cibernética se estabelece como uma realidade

crescente nas esferas das operações militares e da segurança nacional, diferenciando-se dos conflitos tradicionais por ocorrer no ciberespaço – um domínio virtual que transcende fronteiras geográficas, propicia ações anônimas e tem rastreamento complexo.

Paralelamente, a Doutrina Militar de Defesa Cibernética do Brasil (BRASIL, 2014) conceitua a Guerra Cibernética como um tipo de conflito operado no ciberespaço, caracterizado por operações ofensivas e defensivas que envolvem sistemas computacionais, redes e ativos de informação. Essa dimensão do campo de batalha moderno foca no uso de tecnologias digitais para obter vantagem estratégica e infligir danos ao oponente. Nesse cenário, o emprego da Guerra Cibernética abrange ataques cibernéticos, espionagem digital e sabotagem de infraestruturas vitais.

Figura 2: Representação dos guerreiros cibernéticos.

Fonte: O autor.

Em consonância, a Doutrina Militar Naval (BRASIL, 2017) descreve a Guerra Cibernética como uma ação de guerra naval aplicável nos níveis operacional e tático visando objetivos ofensivos e defensivos e operando em contextos diversos, como operações de Inteligência e de Informação. As ações cibernéticas são classificadas em três categorias principais: Ataque Cibernético, Exploração Cibernética e Proteção Cibernética.

Dias (2022) enfatiza que as Operações Cibernéticas, sejam ofensivas ou defensivas, podem visar alvos que estejam no espaço cibernético ou que sejam acessíveis por ele. Assim, é importante reconhecer que, em operações militares ofensivas, as ações cibernéticas não se limitam a estratégias ofensivas, e vice-versa. A exploração, o ataque e a proteção cibernética desempenham papéis fundamentais em ambos os contextos, pois, mesmo em operações militares ofensivas, a proteção das próprias forças é essencial, assim como a capacidade de realizar contraofensivas em operações defensivas, alterando o curso do conflito e estabelecendo a iniciativa das ações, inclusive no espaço cibernético.

Um exemplo histórico significativo do uso da Guerra Cibernética é o ataque ao programa nuclear do Irã através do *malware* Stuxnet, descrito por Singer e Friedman (2017) como uma ferramenta avançada projetada para sabotar as centrífugas nucleares iranianas e comprometer a capacidade de enriquecimento de urânio do país. Esse ataque exemplifica o potencial das operações cibernéticas para causar danos significativos às infraestruturas críticas de uma nação.

Figura 3: Ataque cibernético Stuxnet EUA-Israel ao Irã.

Fonte: Yahoo! News, 2019.

Um caso contemporâneo envolve o conflito entre a Federação Russa e a Ucrânia, iniciado na crise da Crimeia em 2014. Nesse contexto, o ciberespaço tem sido um campo de batalha para os dois lados e também para coletivos de *hackers*. A Rússia, em particular, tem realizado ataques cibernéticos para apoiar suas ações militares cinéticas, causar impacto no campo informacional e obter dados estratégicos (CAMPANY, 2022; KILIAN, 2022).

No contexto das Operações de Inteligência, a Guerra Cibernética possibilita a obtenção de informações estratégicas, conforme delineado no Manual de Inteligência de Fuzileiros Navais (BRASIL, 2021a). Isso inclui a determinação e o dimensionamento da presença inimiga, viabilizados por ações de exploração e ataque cibernético que monitoram comunicações de dados e rastreiam dispositivos computacionais.

Por fim, duas características da Guerra Cibernética de especial relevância para as Operações Anfíbias são seu alcance global e a vulnerabilidade das fronteiras geográficas. Essas características simplificam significativamente as demandas logísticas e de comando e controle em comparação com as exigências para a atuação de Operadores Especiais ou de Inteligência infiltrados em território inimigo, permitindo operações efetivas no território adversário sem presença física.

2. Ações de Exploração e Ataque Cibernético

Embora a Doutrina Militar Naval (BRASIL, 2017) estabeleça a distinção entre Exploração e Ataque Cibernético como categorias diferentes, na prática esses dois aspectos se entrelaçam e dependem mutuamente um do outro

a tal ponto que, para os propósitos deste estudo, serão considerados como uma única entidade integrada.

A Doutrina Militar Naval (BRASIL, 2017) atribui à Exploração Cibernética o papel de fornecer consciência situacional do ambiente cibernético e apoiar as ações de Ataque Cibernético. Essa relação evidencia que um ataque eficaz requer uma ação prévia de esclarecimento ou reconhecimento fornecida pela Exploração Cibernética. Além disso, a contribuição da Exploração Cibernética para a geração de conhecimento de Inteligência está intrinsecamente ligada à manipulação de informações em ativos de interesse, uma função que a Doutrina Militar Naval (DMN) associa ao Ataque Cibernético (BRASIL, 2017). A DMN categoriza tanto a exploração quanto o ataque como geradores de efeitos ofensivos desejados, sublinhando ainda mais sua conexão inerente.

Conforme o Manual de Guerra Cibernética dos Grupamentos Operativos de Fuzileiros Navais (BRASIL, 2022a), a Exploração Cibernética é vista como uma fase preparatória essencial para a realização do Ataque Cibernético, podendo ser abrangida por ele.

Portanto, este artigo, ao abordar as Ações de Exploração e Ataque Cibernético (ExpAtqCiber), salienta as ações ofensivas de Guerra Cibernética visando aos seguintes objetivos:

- reconhecimento de espaços cibernéticos de interesse;
- obtenção de acesso a dados, redes, serviços ou sistemas dentro de um espaço cibernético de interesse;
- exfiltração de dados de dispositivos, serviços ou sistemas em um espaço cibernético de interesse;
- neutralização, degradação, corrupção ou destruição de um serviço ou sistema em um espaço cibernético de interesse.

Conforme será discutido mais adiante, ao tratar das atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos, os três primeiros objetivos listados estão diretamente relacionados a essas atividades. Quanto aos dados mencionados, eles podem incluir imagens, áudios e arquivos, enquanto os serviços e os sistemas abrangem as ferramentas de comando e controle, que podem fornecer informações cruciais para estabelecer a ordem de batalha do inimigo [1].

3. Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA)

As atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA) são fundamentais para a coleta coordenada de informações sobre o ambiente operacional, permitindo tanto a identificação e o monitoramento de alvos como o acompanhamento e a avaliação das ações conduzidas por tropas ou plataformas de armas. Essas atividades são cruciais na obtenção de conhecimentos precisos, relevantes e tempestivos que capacitem os comandantes a tomarem decisões com adequada consciência situacional e conduzirem operações eficazes (CANADA, 1999).

Segundo o *Congressional Research Service* (2022), as atividades de Inteligência, Vigilância e Reconhecimento (ISR) englobam a coleta, a análise e a disseminação de informações essenciais para o suporte à tomada de decisões. A Inteligência é adquirida através de múltiplas fontes, incluindo sensores eletrônicos, vigilância visual, interceptação de comunicações e fontes humanas. Esses dados são processados e avaliados para se transformarem em conhecimento de Inteligência, que é posteriormente distribuído aos comandantes e às unidades em campo.

Com o avanço tecnológico, as atividades de IRVA evoluem, incorporando inteligência artificial, análise de *big data* e sistemas de sensoriamento avançados, que aumentam a precisão da coleta de informações, agilizando a análise e aprimorando a eficiência na disseminação da Inteligência aos decisores. A força aérea americana considera o domínio cibernético como um dos campos para obtenção e integração de conhecimentos através das atividades de IRVA em apoio a operações letais e não letais (CONGRESSIONAL RESEARCH SERVICE, 2022).

A doutrina militar canadense aponta que a IRVA "interconecta vigilância, aquisição de alvos e reconhecimento para expandir a consciência situacional do comandante e orientar a manobra e os meios de ataque ofensivos" (CANADA, 1999). Os dados coletados por diversos sensores são tratados em centros de coleta e análise de inteligência, com agências e fontes atuando como sensores, incluindo equipes de reconhecimento especializadas e sistemas de informação.

[1] Ordem de batalha – "Informações sobre pessoal, unidades e equipamentos de uma força, amiga ou inimiga, incluindo, se possível, efetivo, identificação, localização, estrutura de comando, históricos e outros dados relativos a unidades e personalidades militares" (BRASIL, 2015).

O Manual de Inteligência de Fuzileiros Navais do Brasil (BRASIL, 2021a) não menciona diretamente a integração das atividades de IRVA, mas as considera parte da Inteligência Operacional com o objetivo de reduzir a incerteza e aumentar a capacidade decisória do comandante, permitindo o planejamento, a condução e a sustentação das operações militares. Os conceitos de IRVA, seu processamento e difusão pelo Centro de Análise de Inteligência são correlacionados às diversas Operações Navais.

Kilian (2022) descreve a névoa da guerra como um desafio superado pela Inteligência, que utiliza, entre outras ferramentas, a exploração cibernética. No Manual de Inteligência de Fuzileiros Navais (BRASIL, 2021a), a Inteligência é definida como Pesquisa de Inteligência, que se destina à obtenção de dados negados relevantes para o planejamento e a condução de operações militares empregando pessoal qualificado e meios especializados, inclusive tecnológicos.

O Reconhecimento foca na obtenção de dados sobre o inimigo, o terreno e as condições meteorológicas na Área de Operações (BRASIL, 2008), enquanto a Vigilância se concentra no acompanhamento de forças inimigas já identificadas, mantendo um fluxo contínuo de informações sobre sua localização, composição e movimentos (BRASIL, 2021a) e utilizando meios variados para observar o campo de batalha (BRASIL, 2008).

Por fim, as atividades de Aquisição de Alvos visam identificar, localizar e acompanhar alvos designados ou de oportunidade, aconselhando sobre o momento ideal para engajamento e avaliando os danos resultantes do emprego de fogos, sejam cinéticos ou não cinéticos (BRASIL, 2021a).

Assim, apesar de diferenças terminológicas na literatura, as atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos são identificadas como componentes vitais para o processo decisório do comandante, pois utilizam diversas fontes e agências para obtenção, processamento, integração e disseminação de informações cruciais e tempestivas, fundamentais para o planejamento, a execução, o controle e a sustentação das operações militares.

4. A Guerra Cibernética empregada em atividades de IRVA

Como observado anteriormente, as Operações Navais demandam um fluxo constante, coerente e tempestivo de dados em todas as suas fases. A integração das atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos com as ações de Guerra Cibernética amplia significativamente as possibilidades na construção de conhecimentos essenciais, atuando estas últimas como sensores fundamentais nesse processo.

Do ponto de vista organizacional, para a efetivação dessa tarefa podem ocorrer pelo menos duas configurações distintas: a estrutura de Guerra Cibernética (GCiber) pode integrar a Organização por Tarefas (OrgTar) de uma Força-Tarefa (FT), uma Força Componente (FCte) ou um Grupamento Operativo de Fuzileiros Navais (GptOpFuzNav); ou, alternativamente, a estrutura de GCiber pode estar subordinada a uma FT ou uma FCte de Guerra Cibernética, atuando em benefício dos demais (FT/FCte/GptOpFuzNav).

No primeiro cenário, é aconselhável que a estrutura de GCiber esteja diretamente subordinada ao Comandante da Força-Tarefa (CFT) ou do GptOpFuzNav, facilitando a continuidade e a eficiência no Comando e Controle (C2).

No segundo cenário – a formação de uma Força-Tarefa de Guerra Cibernética dentro da estrutura da Força Naval Componente (FNC) –, uma Força Conjunta de Guerra Cibernética (FCjGCiber) ou um Comando Conjunto de Guerra Cibernética (CCjGCiber) podem ser opções mais adequadas, pois são diretamente subordinadas ao Comandante do Teatro de Operações (ComTO) ou aos níveis político e estratégico (BRASIL, 2014). Essa configuração, embora implique uma coordenação adicional, alivia o CFT, ou o CmtGptOpFuzNav, das responsabilidades adicionais de C2. Contudo, é necessário avaliar as vantagens e as desvantagens de operar com tais Forças ou Comandos em detrimento de uma estrutura própria de GCiber, especialmente considerando a agilidade necessária nas Operações Navais em andamento.

4.1. Guerra Cibernética na fase do planejamento

Durante o planejamento das Operações Navais, uma dificuldade primária é a escassez de conhecimentos atuais sobre a Área de Operações (AOp) e os desafios associados ao estabelecimento de equipes de reconhecimento e vigilância no terreno, o que limita os dados aos já existentes em bases de dados ou bibliotecas (BRASIL, 2021b).

Após a definição da AOp, ações de Guerra Cibernética podem ser planejadas para adquirir conhecimentos tanto sobre a área e os objetivos potenciais como sobre a presença e os movimentos de tropas ou meios inimigos. Essas operações podem ser classificadas como Operações de Apoio a cargo de Força Amiga ou Operações Componentes.

Para realizar essas ações iniciais, a Força responsável deverá buscar obter e manter o acesso a sistemas de monitoramento, vigilância eletrônica e circuitos

fechados de TV nos objetivos e vias de transporte relevantes, bem como acessar sistemas de comando e controle dos objetivos e das forças inimigas presentes na AOp ou capazes de reforço.

Todos os conhecimentos adquiridos devem ser transmitidos prontamente ao Centro de Análise de Inteligência, que integrará essas informações com as obtidas por outras fontes.

Uma característica distintiva da Guerra Cibernética é a capacidade de gerar efeitos em locais específicos sem necessidade de proximidade física (BRASIL, 2022a). Portanto, a unidade responsável pelas ações ofensivas na AOp não precisa estar fisicamente presente, operando idealmente a partir da retaguarda. Isso permite manter operações contínuas e aproveitar melhores condições de conectividade para comunicação com o Comando da FT/GptOpFuzNav e para a execução de suas ações.

Se forem identificados objetivos que exigem proximidade física, como redes sem fio, Bluetooth ou dispositivos físicos segregados, uma parcela da Força ou Grupo-Tarefa poderá ser alocada especificamente para essas tarefas mais especializadas.

4.2. Guerra Cibernética durante a execução da Operação

Durante essa fase, a investigação de dados via espaço cibernético deve se concentrar nas variações das condições da Área de Operações. Em relação à Inteligência, o foco deve ser a obtenção de dados que revelem o grau de consciência situacional do inimigo acerca da presença e da localização da Força-Tarefa Anfíbia. Isso inclui informações sobre movimentações de tropas, meios navais e aéreos inimigos, comunicações e transmissão de dados sobre contraofensivas inimigas e os efeitos das ações da Força-Tarefa.

Nas atividades de Reconhecimento e Vigilância, a ênfase deve ser dada à observação de alterações no dispositivo inimigo na Área de Operações. Essa vigilância deve incluir também as tropas inimigas em condições de reforço, monitorando deslocamentos de tropas e meios navais inimigos na AOp com o objetivo de fornecer alertas antecipados e detectar movimentações por direções inesperadas.

Quanto à Aquisição de Alvos, é essencial buscar dados na Lista Integrada e Priorizada de Alvos, além de monitorar os efeitos dos fogos cinéticos e não cinéticos, mantendo atualizações sobre possíveis mudanças de posição.

As ações de Exploração e Ataque Cibernético devem estar em andamento nessa fase com o objetivo de exfiltrar informações de bases de dados e sistemas de Comando e Controle inimigos para atualizar a ordem de batalha do inimigo o mais próximo possível do tempo real.

O Comando e Controle nessa fase se torna mais complexo, visto que a comunicação com o Comando da Força-Tarefa ocorrerá exclusivamente através dos canais disponíveis nos meios navais onde esses Comandos estejam embarcados.

A Área de Operações da Força ou Grupo-Tarefa de Guerra Cibernética pode ser ampliada para incluir locais de onde possam ser mobilizadas tropas inimigas capazes de alterar o equilíbrio de forças na AOp.

Finalmente, a Força ou Grupo-Tarefa de Guerra Cibernética pode permanecer ativa após a conclusão da Operação para apoiar futuras ações de outras FTs na AOp.

Conclusão

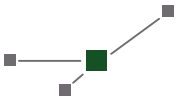
Ao longo deste artigo, foram exploradas as possibilidades de emprego da Guerra Cibernética em atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA) para aprimorar a coleta de informações que auxiliem no planejamento e na execução de Operações Navais.

Buscou-se apontar que as ações de Guerra Cibernética podem ser integradas eficazmente em todas as fases de uma Operação Naval, atuando como sensores cruciais para as atividades de IRVA. Essas ações demandam menos esforço logístico e de Comando e Controle, além de potencialmente envolverem um risco menor de comprometimento do sigilo em comparação com a infiltração e o emprego de Operadores Especiais ou de Inteligência.

Observou-se que tais ações podem ser iniciadas já na fase de planejamento, contribuindo para mitigar as incertezas e as complexidades inerentes ao planejamento, à execução e ao controle das operações militares. Essas ações se mantêm ativas nas fases subsequentes e, se necessário, podem continuar apoiando operações futuras.

Conclui-se, sem pretender esgotar o tema, que a integração dos dados coletados por meio das ações de Guerra Cibernética com aqueles obtidos por outros sensores — como equipes de reconhecimento, operadores de Inteligência em território inimigo e plataformas de sensoriamento remoto — enriquece o fluxo de dados para o Centro de Análise de Inteligência (CAI). Com uma quantidade maior de dados, o CAI pode disseminar informações mais detalhadas e tempestivas, aumentando a consciência situacional dos Comandantes de Forças-Tarefa ou de Grupamentos Operativos de Fuzileiros Navais.

Este artigo buscou destacar, ainda, a importância deste tema para a Marinha do Brasil. O avanço tecnológico, ao oferecer novas ferramentas para as Operações Navais, também aumenta a complexidade do campo de batalha, introduzindo o espaço cibernético como um novo domínio operacional. Assim como ocorreu no passado, quanto maior a consciência situacional do comandante, maiores as chances de tomar decisões acertadas e de superar a capacidade de resposta da força oponente. Dessa forma, ressalta-se a necessidade de obter informações operacionais com volume, qualidade e tempestividade adequados.



Referências Bibliográficas

BRASIL. Marinha do Brasil. Comando-Geral do Corpo de Fuzileiros Navais. **Manual de Ações de Guerra Cibernética dos Grupamentos Operativos de Fuzileiros Navais – CGCFN-60.2.** 1. ed. Rio de Janeiro, 2022a.

_____._____._____. **Manual de Inteligência de Fuzileiros Navais – CGCFN-20.** 1. rev. Rio de Janeiro, 2021a.

_____._____._____. **Manual de Operações de Esclarecimento de Fuzileiros Navais – CGCFN-1-4.** 1. rev. Rio de Janeiro, 2008.

_____._____._____. **Manual de Operações de Força de Desembarque – CGCFN-1-1.** 1. rev. Rio de Janeiro, 2021b.

_____._____._____. **Manual de Planejamento dos Grupamentos Operativos de Fuzileiros Navais – CGCFN-60.4.** 1. ed. Rio de Janeiro, 2022b.

_____._____. Estado-Maior da Armada. **Doutrina Militar Naval (DMN) – EMA-305.** 1. ed. Brasília, 2017.

_____._____._____. **Manual de Planejamento Operativo da Marinha – EMA-331, Vol I** – Processo de Planejamento Militar. 1. ed. Brasília, 2006a.

_____._____._____. **Manual de Planejamento Operativo da Marinha – EMA-331, Vol II** – Diretivas. 1. ed. Brasília, 2006b.

_____._____._____. **Manual de Planejamento Operativo da Marinha – EMA-331, Vol III** – O Trabalho das seções de Estado-Maior. 1. ed. Brasília, 2006c.

_____. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética.** 1. ed. Brasília, 2014.

_____._____. **Glossário das Forças Armadas.** 5. ed. Brasília, 2015.

_____. Presidência da República. **Decreto nº 95.480**, de 13 de dezembro de 1987. Dá nova redação para a Ordenança Geral para o Serviço da Armada. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/1980-1987/decreto-95480-13-dezembro-1987-446244-publicacaooriginal-1-pe.html>. Acesso em: 26 jul.2023.

CAMPANY, Luiggi. Ameaças Híbridas e Guerras Híbridas – uma breve análise aplicada aos conflitos russo-ucranianos de 2014 e 2022. **Revista Âncoras e Fuzis**, ano XXIV, nº 53. Rio de Janeiro: Comando do Desenvolvimento Doutrinário do Corpo de Fuzileiros Navais, 2022.

CANADA. Chief of the Defence Staff. **Information Operations – B-GL-300-005/FP-001**. Kingston, 1999.

CONGRESSIONAL RESEARCH SERVICE (CRS). **Intelligence, Surveillance and Reconnaissance Design for Great Power Competition**. CRS Reports Book 12. Coord. Hoehn, John R.; Smagh, Nishawn S. Kindle edition. Washington: Nimble Books LLC, 2022.

DIAS, Claudio Eduardo Silva. As Operações de Informação e os Grupamentos Operativos de Fuzileiros Navais (GptOpFuzNav). **Revista Âncoras e Fuzis**, ano XXIV, nº 53. Rio de Janeiro: Comando do Desenvolvimento Doutrinário do Corpo de Fuzileiros Navais, 2022.

KILIAN, Rudibert. Análise do Conflito entre Rússia e Ucrânia. **Revista Âncoras e Fuzis**, ano XXIV, nº 53. Rio de Janeiro: Comando do Desenvolvimento Doutrinário do Corpo de Fuzileiros Navais, 2022.

SINGER, P. W.; FRIEDMAN, A. **Segurança e Guerra Cibernéticas:** o que todos precisam saber. Traduzido por Geraldo Alves Portilho Junior. Rio de Janeiro: Biblioteca do Exército, 2017.

VALENTINI, Luis Felippe. Forças Anfíbias Combinadas: o Grupamento Operativo de Fuzileiros Navais em operações multinacionais. **Revista Âncoras e Fuzis**, ano XXIV, nº 53. Rio de Janeiro: Comando do Desenvolvimento Doutrinário do Corpo de Fuzileiros Navais, 2022.

YAHOO! NEWS. **Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran**. By Kim Zetter and Huib Modderkolk. September 02, 2019. Disponível em: <https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html?guccounter=1>. Acesso em: 29 fev. 2024.