ESCOLA DE GUERRA NAVAL

CC LEANDRO ALVES GOUVEIA

RESILIÊNCIA CIBERNÉTICA:
mais um requisito para os Meios de Superfície

Rio de Janeiro

2023

CC LEANDRO ALVES GOUVEIA

RESILIÊNCIA CIBERNÉTICA:
mais um requisito para os Meios de Superfície

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CF Luiz Felipe Lima Santos

Rio de Janeiro
Escola de Guerra Naval
2023

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

Declaro que este trabalho acadêmico: a) corresponde ao resultado de investigação por mim desenvolvida, enquanto discente da Escola de Guerra Naval (EGN); b) é um trabalho original, ou seja, que não foi por mim anteriormente utilizado para fins acadêmicos ou quaisquer outros; c) é inédito, isto é, não foi ainda objeto de publicação; e d) é de minha integral e exclusiva autoria.

Declaro também que tenho ciência de que a utilização de ideias ou palavras de autoria de outrem, sem a devida identificação da fonte, e o uso de recursos de inteligência artificial no processo de escrita constituem grave falta ética, moral, legal e disciplinar. Ademais, assumo o compromisso de que este trabalho possa, a qualquer tempo, ser analisado para verificação de sua originalidade e ineditismo, por meio de ferramentas de detecção de similaridades ou por profissionais qualificados.

gov.br
Documento assinado digitalmente
LEANDRO ALVES GOUVEIA
Data: 28/11/2023 11:50:56-0300
Verifique em https://validar.iti.gov.br

AGRADECIMENTOS

Inicialmente, agradeço à minha amada esposa Priscila, pelo apoio nos momentos mais difíceis e pela inabalável compreensão nos afastamentos. Te amo!

Ao meu filho Henrique, que apesar de sua tenra idade ainda não lhe permitir expressar verbalmente, suas constantes demonstrações de amor e carinho eram o apoio que eu precisava para não esmorecer perante as dificuldades.

Aos meus pais Gersinaldo e Sandra, pelo amor incondicional, apoio irrestrito e ensinamentos basilares e fundamentais que levaram a realizar os meus sonhos.

Aos meus afilhados Carolina, Arthur e Ana Beatriz e minha sobrinha Ana Luíza, pela compreensão pelas minhas constantes ausências em datas significativas e por sua inspiradora admiração pela minha profissão.

Ao meu orientador, Capitão de Fragata Luiz Felipe Lima Santos pela disponibilidade, apoio, conselhos e suporte para conclusão deste trabalho.

Ao corpo docente da Escola de Guerra Naval, que em muito contribuíram para a minha formação profissional e pessoal.

A todos aqueles que torceram por mim e me ajudaram na forma de conselhos, ensinamentos e apoio.

Por fim, agradeço aos Oficiais-Alunos do Curso de Estado-Maior para Oficiais Superiores, pelo apoio, troca de experiências e momentos de amizade. “Turma Sylvio de Noronha, unida para lutar”.

Invenire Hostem et Delere.
(Autor desconhecido)

RESUMO

O presente trabalho propõe-se a avaliar o nível de proteção cibernética em meios de superfície de uma Marinha atual posto que é perceptível a grande quantidade de Sistemas de Tecnologia da Informação e Comando e Controle ($STIC^2$) presentes nos Navios de Guerra atuais. Desta forma, um ataque cibernético poderia obter o controle do meio de superfície como uma ação em prol das *Effects-Based Operations*. Esta estratégia visa obter o controle do inimigo indisponibilizando seus recursos até que não tenha mais capacidade ou motivação para continuar o combate. Para se contrapor a esse tipo de ataque, os sistemas do Navio devem possuir elevada Resiliência Cibernética. Este trabalho estudou a metodologia empregada pelo Departamento de Defesa dos Estados Unidos da América para afiançar a Resiliência Cibernética não somente nos meios de superfície como nos produtos de defesa das Forças Armadas daquele país. Em linhas gerais, as principais características dessa metodologia é que a resiliência deve ser contemplada desde a concepção dos meios, as redes e sistemas devem ser confiáveis e testes de desempenho devem ser conduzidos periodicamente. Após essa análise, foram avaliados quais sistemas presentes em meios de superfície poderiam ser suscetíveis a ataques cibernéticos e é notório que todos os sistemas são passíveis de sofrer ataque e um sistema pode ser permitir a disseminação para os demais sistemas. Isso posto, é possível concluir que os atuais meios de superfície dependem de $STIC^2$ para que sejam eficientes, o que os deixam passíveis de sofrer ataque cibernético. E a medida de proteção contra esse tipo de ataque é a resiliência cibernética, que deve ser elevada.

Palavras-chave: Guerra Cibernética. Resiliência cibernética. Navio. Meio de Superfície. *Effects-Bases Operations*.

LISTA DE ABREVIATURAS E SIGLAS

AIS – *Automatic Identification System*

C^2 – Comando e Controle

CMG – Capitão de Mar e Guerra

COTS – *Costumer-off-the-Shelf*

EUA – Estados Unidos da América

EMA – Estado-Maior da Armada

GPS – *Global Positioning System*

MD – Ministério da Defesa

MN – Milhas Náuticas

ONU – Organização das Nações Unidas

OTAN – Organização do Tratado do Atlântico Norte

SI – Sistema de Informação

$STIC^2$ – Sistema de Tecnologia da Informação e Comando e Controle

USB – *Universal Serial Bus*

VHF – *Very High Frequency*

SUMÁRIO

1 INTRODUÇÃO

Ganhar guerras sem destruir o inimigo não é uma estratégia nova. Há cerca de 2.500 anos, Sun Tzu (2000, p. 9, tradução nossa) pregava que "o líder habilidoso subjuga as tropas inimigas sem qualquer combate; captura suas cidades sem sitiá-las; derruba seu reino sem longas operações no campo."[1].

No início dos anos 1990, os Estados Unidos da América aplicaram esse princípio de Sun Tzu na Guerra do Golfo e os resultados foram expressivos. Naquela guerra, a Força Aérea estadunidense fora empregada em diversas missões de ataque a instalações de interesse militar, empregando bombas de precisão e mísseis lançados por aviões e navios. Diversas refinarias, depósitos de combustíveis, fábrica de produção de armamento e estações de comando e controle foram destruídas com efeitos colaterais praticamente nulos (DEPTULA, 2001). Desta forma, os Estados Unidos conseguiram minar as capacidades de reação do inimigo sem atingir diretamente seus meios e suas tropas. Essa era a aplicação do princípio de Sun Tzu que era possível com a tecnologia disponível à época.

Porém, o aumento das capacidades dos sistemas de informática aliado ao seu barateamento têm como consequência sua vasta penetrabilidade em todas as atividades humanas (CASTELLS, 1999). Sabendo que a utilização de sistemas de informática é inevitável, como avaliar se esse recurso é suficientemente seguro para emprego em um conflito? E em tempo de paz?

Este trabalho visa responder a estas perguntas, isto é, avaliar a importância e a abrangência da proteção cibernética para os atuais meios de superfície de uma Marinha, mas sem aprofundamento em características técnicas dos sistemas.

No intuito de construir gradualmente os argumentos, no segundo capítulo serão introduzidos os conceitos que permitem àqueles que não tenham conhecimento sobre Guerra Cibernética, o entendimento da relevância do tema.

No capítulo três será aprofundado o estudo sobre características e requisitos a serem considerados a fim de verificar a segurança dos sistemas de informática de qualquer sistema militar. Tal estudo valer-se-á da metodologia empregada pelo Departamento de Defesa dos Estados Unidos.

---

[1] No original em inglês: *"The skillful leader subdues the enemy's troops without any fighting; he captures their cities without laying siege to them; he overthrows their kingdom without lengthy operations in the field."*

No capítulo quatro serão avaliados os possíveis efeitos de ataques cibernéticos em caso de inobservância do nível de segurança adequada para um Navio de Guerra da Marinha e após serão investigadas a teoria e a realidade sobre este assunto.

Por fim, no quinto e último capítulo serão apresentadas as principais considerações, as linhas de pesquisa para trabalhos futuros e a importância do tema para a Marinha do Brasil.

Isso posto, no próximo capítulo será pormenorizada a proteção cibernética e sua crucialidade para sistemas de emprego militar. Adicionalmente será introduzida a estratégia estadunidense supracitada sob a ótica de dois Oficiais das Forças Armadas daquele país.

2 DESENVOLVIMENTO TEÓRICO

Neste capítulo, serão apresentados alguns conceitos de guerra cibernética que serão utilizados ao longo do trabalho, bem como a teoria sobre *Effects-Based Operations*[2], que sustentará a importância da proteção cibernética aos meios de superfície.

2.1 Guerra Cibernética

A Guerra Cinética ocorre no Domínio Físico do Ambiente Operacional e os meios empregados para essa guerra são os navios, carros de combate, aeronaves, soldados e outros do meio físico (BRASIL, 2021). O desenvolvimento tecnológico, especificamente dos sistemas digitais e da tecnologia de informação, ampliou as possibilidades nos mais diferentes tipos de atividades. Isso motivou a incorporação desse tipo de inovação nos meios cinéticos a fim de aumentar a eficiência dos meios.

Sistemas digitais podem realizar os complexos cálculos balísticos de canhões em milissegundos, manter continuamente aeronaves na derrota prevista e monitorar ininterruptamente o estado de funcionamento de equipamentos mecânicos e elétricos, entre outras aplicações. As vantagens da incorporação de sistemas digitais nos meios cinéticos são claras e, para algumas atividades ou tarefas, seu emprego é inevitável.

Contudo, os sistemas digitais trazem uma limitação que é a exposição dos meios a vulnerabilidades cibernéticas que, conforme a Doutrina Cibernética da Marinha (BRASIL, 2021), podem ser exploradas tanto intencional quanto acidentalmente por agentes externos para diversos fins.

Com isso, cabe destacar a definição do Ministério da Defesa de Guerra Cibernética:

> Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de Comando e Controle (C^2) do adversário, [...]. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comando e Controle ($STIC^2$) do oponente e defender os próprios $STIC^2$ (BRASIL, 2014, p. 19).

[2] A tradução livre do termo seria “Operações Baseadas em Efeitos”. Porém esse termo será mantido na língua inglesa durante todo o trabalho pois essa doutrina não foi formalmente adotada pelo Ministério da Defesa nem pela Marinha do Brasil.

O Ambiente Operacional em que qualquer força militar estiver inserida é composta de três dimensões, a saber, a dimensão humana, a dimensão física e a dimensão informacional. A cibernética atua nessas três dimensões (BRASIL, 2021). Conforme pode-se constatar, a Guerra Cibernética se desenvolve visando a exploração e o comprometimento dos STIC[2] e, desta maneira, pode afetar as três dimensões do Ambiente Operacional.

A junção desses recursos das dimensões ocorre na Espaço Cibernético, cuja relevância é destacada no documento doutrinário do Ministério da Defesa:

> Espaço Cibernético é um dos cinco domínios operacionais e permeia todos os demais. São eles: o terrestre, o marítimo, o aéreo e o espacial, que são interdependentes. As atividades no Espaço Cibernético[3] podem criar liberdade de ação para atividades em outros domínios, assim como atividades em outros domínios também criam efeitos dentro e através do Espaço Cibernético. O objetivo central da integração dos domínios é a habilidade de se alavancar capacidades de vários domínios para que sejam criados efeitos únicos e, frequentemente, decisivos (BRASIL, 2014, p. 18).

Por isso, para que seja mantida a liberdade de ação[4] no Espaço Cibernético e que os STIC[2] se protejam de exploração cibernética[5] e não sejam afetados por ataques cibernéticos[6], cabe às Forças investir recursos na Defesa Cibernética (BRASIL, 2021) de forma a manter a integridade das três dimensões.

Para os sistemas militares, uma das características fundamentais a ser desenvolvida é a resiliência cibernética, que a Doutrina de Defesa Cibernética do Ministério da Defesa define como: “a capacidade de manter as infraestruturas críticas de tecnologia da informação e comunicações operando sob condições de ataque cibernético ou de restabelecê-las após uma ação adversa” (BRASIL, 2014, p. 19).

Embora as publicações de referência das Forças Armadas do Brasil não sejam enfáticas quanto à importância da resiliência cibernética, sua definição já é uma indicação do quão crucial essa característica é. Da mesma forma, em âmbito nacional, é almejado um alto nível

---

3 O Espaço Cibernético é o espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas (BRASIL, 2014, p. 18).

4 Liberdade de ação no Espaço Cibernético é manter a capacidade de uso do Espaço Cibernético e o livre fluxo de dados protegidos de qualquer ameaça, garantindo os requisitos básicos da Segurança da Informação (SI) (BRASIL, 2021, p. 4-2).

5 É o ato de aproveitar-se furtivamente de vulnerabilidades cibernéticas de um sistema e conquistar acesso, a fim de estudá-lo e/ou preparar um ataque contra o mesmo. Visa, ainda, obter acesso antecipadamente ao sistema alvo, testar e preparar as técnicas e ferramentas de ataque que poderão ser utilizadas futuramente (BRASIL, 2021).

6 Conjunto de atividades com características ofensivas que compreendem interromper, negar, degradar, corromper ou destruir informações no espaço cibernético de interesse (BRASIL, 2021).

de proteção para o Espaço cibernético brasileiro. A Estratégia Nacional de Segurança Cibernética é a diretriz do governo federal que norteia as ações na área de segurança cibernética. Este documento estipula que um dos objetivos estratégicos do país é "Aumentar a resiliência brasileira às ameaças cibernéticas" (BRASIL, 2020, p. 8) e uma das ações estratégicas para atingir esse objetivo é "Proporcionar às infraestruturas críticas, maior resiliência que possibilite a contínua prestação de serviços essenciais" (BRASIL, 2020, p. 10).

Outros Estados têm visões parecidas quanto à necessidade de garantir a capacidade de pleno emprego do Espaço cibernético ainda que em condições adversas. Por exemplo, a Estratégia Nacional de Cibernética do Reino Unido, também valoriza a resiliência cibernética, considerando-a um dos cinco pilares para implementação de sua estratégia, e afirma que defesas cibernéticas fortes para proteção de redes e ativos nos níveis individuais, locais e nacionais. Além disso, o documento afirma que:

> A cibersegurança e a resiliência são fundamentais para os nossos objetivos estratégicos mais amplos enquanto ciberpotência: sem elas, não podemos esperar tirar o máximo partido do potencial transformacional das tecnologias digitais para reconstruir melhor, mais justo e mais forte, e para proteger a vantagem estratégica do Reino Unido no ciberespaço[7] (REINO UNIDO, 2022, p. 65, tradução nossa).

Do mesmo modo, mas especificamente no âmbito militar, as doutrinas de outras entidades expressam explicitamente a importância da resiliência cibernética. Por exemplo, a Organização do Tratado do Atlântico Norte (OTAN) considera essa característica fundamental por entender que esta permite a liberdade de ação no ciberespaço, contribuindo para emprego as Forças Armadas. O extrato abaixo resume o entendimento da OTAN sobre resiliência cibernética:

> Para garantir a confidencialidade, integridade e disponibilidade das informações, bem como a autenticidade[8] e não repúdio[9] de usuário/entidade, os sistemas de comunicação e informação, incluindo redes e repositórios de dados, devem ser altamente resilientes a ameaças do ciberespaço [...][10] (OTAN, 2020, p. 1, tradução nossa).

---

7 No original em inglês: *"Cyber security and resilience are foundational to our wider strategic aims as a cyber power: without them we cannot hope to take full advantage of the transformational potential of digital technologies to build back better, fairer and stronger, and to protect the UK's strategic advantage in and through cyberspace."*

8 Autenticidade garante que a informação seja produzida, expedida, modificada ou destruída por uma determinada pessoa física, órgão, entidade ou determinado sistema (BRASIL, 2019 pp. 7-2).

9 Não repúdio garante que o autor de uma informação não negue falsamente sua autoria (BRASIL, 2019).

10 No original em inglês: *"In order to assure confidentiality, integrity and availability (CIA) of information, as well as user/entity authentication and non-repudiation, communication and information systems (CIS), including networks and data repositories, must be highly resilient to threats from cyberspace […]."*

A publicação da OTAN destaca ainda que a resiliência cibernética é necessária na esfera das Forças Armadas tanto em tempos de paz quanto durante conflitos armados pois as operações militares dependem de diversas redes de informática, que incluem a infraestrutura dos países, sistemas de armas, sistemas de comando e controle (C^2) e sistemas logísticos. Entre outras medidas, a OTAN tem uma rede exclusiva para emprego dos membros de sua aliança e explicita que a resiliência da rede como um todo é equivalente à proteção garantida pelo ponto mais fraco da rede (OTAN, 2020).

A doutrina estadunidense também entende que a resiliência cibernética é uma das principais características para o país e, principalmente, no âmbito de suas Forças Armadas (EUA, 2019a). Essa doutrina será aprofundada no próximo capítulo deste trabalho.

Diante dessas considerações, entidades civis e militares entendem que a resiliência cibernética é uma capacidade essencial para manutenção da liberdade de ação no espaço cibernético.

Especificamente na expressão militar do Poder Nacional, quais poderiam ser os efeitos de proteção cibernética deficiente em seus meios? Quais consequências poderiam advir um ataque cibernético a um meio de superfície da Marinha? Uma das possibilidades é permitir que o inimigo conduza as *Effects-Based Operations*, estratégia essa que será desenvolvida a seguir.

2.2 Effects-Based Operations

Para presumir os efeitos da proteção cibernética insatisfatória e confirmar a importância da resiliência cibernética tanto em tempos de paz quanto em conflito armado, principalmente no que tange à ameaça sofrida pelos meios de superfície da Esquadra, será empregada a teoria das *Effects-Based Operations*, termo originalmente cunhado pelo Tenente General[11] da Força Aérea dos Estados Unidos David Deptula[12] (1952 -).

Para o General Deptula, a forma tradicional de condução das batalhas numa guerra, ou seja, eliminando sucessivamente meios e instalações, está ultrapassada. Em virtude da

[11] Tenente General é Oficial General de três estrelas naquele país.

[12] Ainda como Tenente-Coronel, participou do projeto original da campanha aérea da Coalizão contra o Iraque. Durante a Operação Escudo do Deserto/Tempestade do Deserto, foi o principal planejador da campanha aérea ofensiva do Comandante do Componente Aéreo da Força Conjunta (DEPTULA, 2001).

tecnologia hoje existente, a forma mais eficiente de atingir os objetivos numa campanha militar seria realizando ataques simultâneos a alvos cuidadosamente selecionados e de importância no nível Estratégico, Operacional e Tático (DEPTULA, 2001).

A diferença sobre a forma tradicional e sua proposta está na intensidade e no objetivo de aplicação da força militar. O autor sugere que se deve mudar o ponto de vista quanto à escolha dos alvos, pois ações diretas[13] e desgaste[14] dependem da destruição sequencial e individual de alvos. E o progresso e a avaliação do sucesso da campanha é feito por meio da contagem dos alvos abatidos. Contudo isso não garante o sucesso na guerra. Com o emprego das *Effects-Based Operations*, o progresso da campanha não é medido em termos de meios destruídos e sim, no exercício de influência e o controle efetivo sobre os sistemas que o inimigo tem dependência (DEPTULA, 2001).

Logo, percebe-se que a quantidade de alvos ainda não destruídos não deve ser o condutor do planejamento da campanha militar, pois isso levaria somente à necessidade de destruição de mais meios. Por outro lado, com emprego dessa estratégia, o foco se volta para o controle dos sistemas que o inimigo depende. A dependência desses sistemas propicia a redução gradativa da capacidade de reação do inimigo e a consequente perda de controle sobre eles causa efeitos ainda mais severos que a perda de meios (DEPTULA, 2001).

Essa teoria foi nomeada *Effects-Based Operations*, cujo objetivo é obter o controle sobre os recursos disponíveis pelo inimigo pois, desta forma, pode-se restringir suas possibilidades ao longo da campanha, abreviando a duração e efeitos adversos do conflito.

> Um conceito alternativo de guerra é baseado no controle – a ideia de que a capacidade de uma organização inimiga de operar como esperado é, em última análise, mais importante do que a destruição das forças das quais ela depende para a defesa. Para garantir o fim favorável do conflito, tornar a força inimiga inútil é tão eficaz quanto eliminar essa força inimiga. Além disso, controlar um adversário pode ser realizado mais rapidamente e com muito menos baixas[15] (DEPTULA, 2001, p. 11, tradução nossa).

---

[13] É a ação em que, no desenvolvimento das ações, predomina o emprego da massa e se busca o aniquilamento do inimigo pela batalha imediata (BRASIL, 2015, p. 18).

[14] Forma de conduzir operações que se pauta em uma maciça aplicação do poder combatente, a fim de reduzir a eficiência de lutar do inimigo, por meio da perda de pessoal e material (BRASIL, 2015, p. 134).

[15] No original em inglês: *"An alternative concept of warfare is based on control — the idea that an enemy organization's ability to operate as desired is ultimately more important than destruction of the forces it relies on for defense. In terms of securing favorable conflict termination, rendering the enemy force useless is just as effective as eliminating that enemy force. Furthermore, controlling an adversary can be accomplished quicker, and with far fewer casualties."*

O autor acrescenta que a obtenção do controle visa os sistemas que o adversário confia e depende para exercer influência e poder, como sua liderança, população, indústrias essenciais e de base, transporte, energia e forças militares. Por isso, segundo o General Deptula, a obtenção do controle deve ser o foco de uma campanha militar, uma vez que este pode influenciar até mesmo na vontade do inimigo em manter a campanha (DEPTULA, 2001).

E esta estratégia não ignora a destruição, apenas muda o enfoque para que o emprego dos meios seja feito de uma forma mais eficiente, como meio de obter efeitos em cada um dos sistemas que o inimigo emprega para conduzir as operações, sua logística e exercer influência sobre a tropa e população. Ou seja, não destruir os sistemas em si, mas impedir que o inimigo o utilize com liberdade de ação ou manobra. O controle sobre os sistemas inimigos facilita atingir os objetivos políticos que justificam o uso da força, segundo o General (DEPTULA, 2001).

O General David Deptula não foi o único a salientar sobre a importância das operações militares pautadas no cumprimento eficiente dos objetivos. Um deles foi o Capitão de Mar e Guerra da Marinha dos Estados Unidos Edward Smith[16] (1946 - 2020), que define as *Effects-Based Operations* como "conjuntos de ações coordenadas com intuito de moldar o comportamento de amigos, inimigos e neutros em paz, na crise e em guerra"[17] (SMITH, 2003, p. xiv, tradução nossa). Ele ainda acrescenta que apesar da curta definição, essa estratégia é complexa:

> Não se trata simplesmente de uma ação que cria um efeito em uma relação direta, se-isso-então-faça-aquilo, causa-e-efeito, mas de *conjuntos coordenados de ações*, isto é, o uso de múltiplas ações interdependentes. E não olha para um único efeito como resultado, mas sim para as ações que *moldam* um estado final de *comportamento*. Isso quer dizer que ela vê tanto um processo quanto um estado final que não são nem precisos nem apenas produtos das ações que nós mesmos executamos[18] (SMITH, 2006, p. 95, grifos do original, tradução nossa).

Isso posto, é possível notar que a abrangência proposta pelo CMG Smith é maior que

---

[16] Capitão de Mar e Guerra reformado da Marinha dos EUA com 30 anos de serviço. Era bacharel em Relações Internacionais pelo Estado de Ohio e mestre e doutor em Relações Internacionais pela *American University* (SMITH, 2003).

[17] No original em inglês: *"Effects-based operations are coordinated sets of actions directed at shaping the behavior of friends, foes, and neutrals in peace, crisis, and war."*

[18] No original em inglês: *"It does not speak simply of an action creating an effect in a straightforward, if-this-then-that, cause-and-effect relationship, but of coordinated sets of actions, that is, the use of multiple interdependent actions. And, it does not look to a single effect as the outcome but rather to the actions shaping a behavior end-state. This is to say that it sees both a process and an end-state that are neither precise nor solely the products of the actions we ourselves take."*

a do Gen Deptula, uma vez que a estratégia tem por objetivo alterar o comportamento do inimigo, tanto na paz quanto em crise e na guerra.

O CMG Smith concorda com o General Deptula que as *Effects-Based Operations* não ignoram completamente a destruição de meios e recursos do inimigo. Mas reforça que o objetivo dessa estratégia e, portanto, das operações militares conduzidas por ela, não é somente destruir as capacidades físicas do inimigo, mas induzi-lo para que siga uma linha de ação que seja do nosso interesse. O desgaste não será empregado para pura e simples destruição de meios, mas para reduzir as capacidades essenciais do inimigo (SMITH, 2003).

Em outras palavras, ambos Oficiais não descartam a necessidade do desgaste, ou seja, de destruir alvos. Contudo o objetivo não deve ser a mera redução da quantidade de meios do inimigo e sim, a redução de suas capacidades essenciais por meio de severamente avaria em um sistema vital para o inimigo.

Pela perspectiva do CMG Smith, as *Effects-Based Operations* têm grande efeito sobre a moral do adversário e, nesse aspecto, o CMG Smith é mais enfático que o Gen Deptula. Segundo o Oficial da Marinha estadunidense, um dos objetivos dessa modalidade de operação é afetar a vontade de lutar ou moldar o comportamento do inimigo ao ponto que ele não tenha vontade de continuar a guerra ou desorientá-lo de forma que não possa mais combater efetiva ou coerentemente (SMITH, 2003).

De acordo com o CMG Edward Smith, o que possibilita o sucesso do emprego das *Effects-Based Operations* é o avanço tecnológico, que permite que sejam empregados sensores mais precisos, mais rápidos e com maior abrangência. O rápido processamento dos dados obtidos por esses sensores permite o apoio à decisão de maneira mais rápida e precisa. Desta forma, os comandantes militares podem empregar seu moderno sistema de armas, composto por armamento inteligente e de alta precisão com extrema eficiência. Essa elevada capacidade de combate abalaria a moral dos combatentes pois, ao afetar sistemas vitais do inimigo, este perceberia por conta própria que não poderia vencer a guerra por falta de recursos para se contrapor (SMITH, 2003).

2.3 Aplicação da Guerra Cibernética nas *Effects-Based Operations*

O General Deptula, por ser Oficial da Força Aérea, criou as *Effects-Based Operations* pensando na sua aplicação na guerra cinética, especialmente no emprego da Força Aérea.

Contudo, ele pondera três implicações sobre sua teoria que merecem destaque. Segue abaixo o trecho de sua obra que as menciona:

> As implicações das *Effects-Based Operations* incluem: Primeiramente, as *Effects-Based Operations* oferecem uma alternativa viável ao desgaste e à aniquilação[19] como meios para forçar o comportamento de um adversário. Em segundo lugar, as *Effects-Based Operations* exploram os sistemas de armas atuais enquanto fazem a transição para a tecnologia emergente. Em terceiro lugar, para melhor explorar o potencial das *Effects-Based Operations*, os militares devem instituir mudanças organizacionais[20] (DEPTULA, 2001, p. 17, tradução nossa).

Estas três implicações cabem aprofundamento quanto a aplicação da Guerra Cibernética nas *Effects-Based Operations*.

Sobre a primeira implicação, por meio de ataque cibernético bem-sucedido, é possível afetar os alvos de interesse sem a necessidade de ações cinéticas contra o inimigo. Um exemplo foi vírus Stuxnet[21], que atingiu o objetivo de impedir a produção de armamento nuclear pelo Irã sem destruir as instalações nucleares do país.

Quanto à segunda implicação, a própria consideração do Espaço cibernético como um dos Domínios Operacionais já confirma a relevância da Guerra Cibernética no Ambiente Operacional. A importância aumenta ao constatar que este permeia os demais domínios (BRASIL, 2014). Na época que a doutrina *Effects-Based Operations* foi empregada pela primeira vez, durante a primeira Guerra do Golfo no início dos anos 1990, a exploração do quinto domínio não era considerada. Atualmente, ignorá-la é impensável.

Já em relação à terceira implicação, o potencial de exploração do Espaço Cibernético levou o Brasil a criar algumas estruturas permanentes e outras ativadas quando necessário, do nível político ao tático (BRASIL, 2012). E não somente o Brasil, mas diversos países criaram uma estrutura própria para lidar com o domínio informacional. Até mesmo organismos internacionais como a ONU e a OTAN têm sua estrutura própria para tal. Ou seja, o Espaço Cibernético levou a mudanças profundas não somente organizacionais como estruturais em diversos níveis nos Estados.

Quando se trata dos trabalhos apresentados pelo CMG Edward Smith, apesar dos

---

[19] O equivalente nas Forças Armadas do Brasil seria a Ação Direta (BRASIL, 2015).

[20] No original em inglês: *"The implications of effects-based operations include: First, effects-based operations offer a viable alternative to attrition and annihilation as the means to compel an adversary's behavior. Second, effects-based operations exploit current weapon systems while transitioning to emerging technology. Third, to best exploit the potential of effects-based operations, the military must institute organizational changes."*

[21] Foi um vírus produzido com um único propósito: avariar fisicamente as centrífugas de enriquecimento de Urânio-235 do Irã a fim impedir que chegasse ao nível de enriquecimento do metal que permitisse emprego em armamento nuclear (CLARKE; KNAKE, 2015).

exemplos e as possibilidades de aplicação também se voltarem para a guerra cinética, é feito um breve relato sobre emprego de guerra cibernética nas *Effects-Based Operations*, conforme o extrato abaixo:

> Na guerra da Era da Informação, um efeito físico inicial semelhante pode ser a entrada de um vírus de computador em uma rede de sistema ou a descoberta de um esforço para invadir uma rede. [...] No exemplo da guerra cibernética, da mesma forma, aceitamos quase instintivamente que o efeito físico inicial e direto não será o impacto final. Esperamos que esse efeito inicial ou direto crie algum tipo de efeito indireto adicional. E esperamos que alguma combinação desses efeitos eventualmente traga mudanças no comportamento, [...], esperamos que os efeitos criados por nossa ação não permaneçam isolados, mas se espalhem para outros Domínios Operacionais[22] (SMITH, 2003, p. 302, tradução nossa).

Com base na perspectiva de ambos os autores conforme as obras apresentadas como nas capacidades e possibilidades advindas da exploração Espaço Cibernético, fica patente que a Guerra Cibernética pode ser empregada em conjunto às guerras cinéticas em operações voltadas para controle do inimigo, como nas *Effects-Based Operations*.

De forma análoga, se a Guerra Cibernética pode ser empregada em proveito das *Effects-Based Operations*, toda força deve estar preparada para se contrapor a ameaças empregando essa estratégia, ainda mais quando uma das possibilidades do inimigo seria obter o controle de seus meios. Devido à quantidade de sistemas embarcados necessários para seu emprego, um meio de superfície da Marinha é um meio passível de sofrer ataque cibernético. A paralisia ou a desordem parcial ou total dos sistemas podem inviabilizar o seu emprego num conflito ou mesmo fora dele.

Por isso, deve-se garantir a resiliência cibernética desses meios de forma que os ataques eventualmente sofridos não causem danos aos sistemas essenciais. E esse assunto será abordado no próximo capítulo, ou seja, como assegurar o nível de resiliência cibernética em produtos de defesa.

---

[22] No original em inglês: *"In Information Age warfare, a similar initial physical effect might be the entry of a computer virus into a system network or the discovery of an effort to hack into a network. [...] In the cyberwar example, similarly, we almost instinctively accept that the initial, direct physical effect will not be the end of the impact. We expect that this initial or direct effect will create additional indirect effects of some sort. And we expect that some combination of these effects will eventually bring changes in behavior, [...], we expect that the effects created by our action will not remain isolated but will spread to other dimensions."*

3 RESILIÊNCIA CIBERNÉTICA EM PRODUTOS DE DEFESA[23]

No capítulo anterior, foi apresentada a definição de resiliência cibernética e sua importância para obtenção da proteção cibernética. Todavia, a definição não contém todos os elementos para que seus efeitos sejam percebidos, uma vez que carece de metodologia de implantação, requisitos e critérios para estabelecer o nível de resiliência requerida para o STIC^2 que se pretende defender.

Neste trabalho, será estudada a metodologia empregada pelo Departamento de Defesa dos Estados Unidos da América, que já apresentam um grau elevado de maturidade, tem estrutura voltada para segurança cibernética de seus sistemas, requisitos bem definidos e, principalmente, as publicações são ostensivas.

Outro fator igualmente relevante é a abrangência e escopo das medidas de segurança adotadas, uma vez que engloba todos os órgãos subordinados ao Departamento de Defesa, abarcando Marinha, Exército, Força Aérea, Corpo de Fuzileiros Navais e Força Espacial. Apesar de não fazer parte da estrutura do Departamento, a Guarda Costeira também emprega a mesma metodologia.

A atenção quanto à proteção cibernética dos STIC^2 do Departamento de Defesa dos Estados Unidos da América baseia-se no pressuposto que "vulnerabilidades cibernéticas fornecem oportunidades para que adversários possam explorar, roubar, alterar, interromper ou destruir funcionalidades, informações ou tecnologias dos sistemas"[24] (EUA, 2020b, p. 10, tradução nossa).

No intuito de evitar que as vulnerabilidades cibernéticas sejam exploradas, as publicações estadunidenses são mais enfáticas que as do Brasil quanto à importância da resiliência cibernética, ainda que tenham definições bastante semelhantes dos termos.

A doutrina estadunidense destaca que são necessárias três condições para obtenção da resiliência cibernética no nível operacional: recursos de informação (STIC^2) devem ser confiáveis; as operações militares devem continuar mesmo após degradação ou perda de recursos de informação; e a operação das redes devem ter os meios para manter-se em

---

[23] Equipamentos materiais, serviços e informações que tenham aplicação na área de Defesa. Inclui veículos e sistemas completos de qualquer natureza, bem como materiais para os mesmos (BRASIL, 2015).

[24] No original em inglês: *"Cyber vulnerabilities provide opportunities for adversaries to exploit, steal, alter, interrupt, or destroy system functionality, information, or technology."*

funcionamento diante de eventos adversos (EUA, 2019a).

Segundo aquele Departamento, essas condições seriam atendidas por meio de sete requisitos, dos quais se destacam: redes e sistemas reconhecidamente confiáveis, proteção aos programas de aquisição de produtos de defesa e execução de testes e avaliações de segurança cibernética durante o desenvolvimento dos projetos. Os demais requisitos envolvem, em suma, treinamento de pessoal e monitoramento contínuo (EUA, 2019a).

Os três requisitos destacados acima sobressaem perante os demais pois não são somente citados. Há publicações próprias que contêm instruções específicas para obtenção, manutenção e validação da segurança cibernética para cada um deles. Para expandir o entendimento sobre cada requisito e como garanti-lo dentro do Espaço cibernético do Departamento de Defesa, estes serão aprofundados ao longo deste capítulo.

3.1 Redes e Sistemas Confiáveis

O Departamento de Defesa estadunidense estipulou uma coleção de requisitos a serem atendidos pelas redes e sistemas sensíveis, principalmente àqueles afetos aos sistemas de combate. A esses STIC^2, foi atribuído o nome de "Sistema e Rede Confiável"[25] e sua confiabilidade advém, segundo a publicação, da integração de engenharia de sistemas, cadeia de suprimentos, inteligência, *hardware*, *software* e outros recursos que compõem cada STIC^2 (EUA, 2018a).

Além disso, o documento também deixa claro que o objetivo desse tipo de abordagem é garantir que os sistemas tenham a maior proteção cibernética possível. O extrato abaixo explicita essa preocupação:

> Esta instrução [...] estabelece políticas e imputa responsabilidades para minimizar o risco de que a capacidade de combate no âmbito do Departamento de Defesa seja prejudicada devido a vulnerabilidades no projeto do sistema, sabotagem ou subversão das funções críticas ao cumprimento de missão ou componentes críticos de um sistema, [...], por inteligência estrangeira, terroristas ou outros elementos hostis[26] (EUA, 2018a, p. 1, grifos e tradução nossos).

---

[25] A publicação refere-se como *Truted Systems and Networks* e este trabalho citará este termo conforme tradução apresentada.

[26] No original em inglês: *"This Instruction […] establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, […], by foreign intelligence, terrorists, or other hostile elements."*

Os requisitos para obtenção dessa certificação envolvem desde assegurar que os componentes críticos para cumprimento das missões tenham o nível de segurança adequado de acordo com o sistema e sua função até análise de inteligência dos fornecedores dos itens. E quanto maior a importância do sistema no contexto das missões militares, maior deverá ser a atenção quanto à segurança cibernética aplicada àquele item (EUA, 2014).

Segundo a publicação, a preocupação quanto à procedência dos componentes que compõem os sistemas deve ser constante, e a sistemática prevê que os componentes mais críticos sejam adquiridos de fornecedores com comprovada idoneidade perante o Departamento de Defesa. E caso sejam utilizados circuitos eletrônicos desenvolvidos especificamente para sistemas críticos, estes cuidados devem ser ainda maiores, uma vez que o fabricante poderia deliberadamente deixar brechas de segurança com o fim explorá-las posteriormente por saber que seria empregado pelas Forças Armadas estadunidenses (EUA, 2018a).

A doutrina também prevê que os requisitos de segurança devem ser atendidos durante todo o ciclo de vida dos sistemas, desde a concepção até o desfazimento. Ademais, deve-se ter procedimentos e ferramentas para controlar as configurações, versões de *software*, *hardware* e *firmware* durante todo o período de operação e impedir que sejam utilizados produtos falsificados ou de procedência duvidosa (EUA, 2018a).

A certificação de "Redes e Sistemas Confiáveis" é uma metodologia que auxilia os usuários dos STIC[2] a garantir que os equipamentos e sistemas sob sua égide têm a segurança cibernética adequada. Mas a certificação por si só não é o suficiente e os demais requisitos são igualmente importantes para impedir que produtos de defesa não tenham vulnerabilidades cibernéticas ao entrar em operação.

3.2 A sistemática de aquisição de produtos de defesa

As diversas publicações que versam sobre segurança cibernética enfatizam que as medidas de proteção cibernética devem ser tomadas desde a concepção até o desfazimento dos STIC[2]. Para garantir que um produto de defesa a ser introduzido no inventário do Departamento de Defesa tem a proteção cibernética adequada, a sistemática de aquisição de desses itens contém processos que estabelecem as autoridades envolvidas em aquisição e os gerentes dos projetos devem contemplar essa característica de segurança e orienta como

fazê-lo. Isso favorece para que, desde a sua concepção, esses programas tenham o nível esperado de proteção de acordo com a aplicação e relevância.

Com o fito de evitar que exploração de vulnerabilidades cibernéticas sejam empregadas pelos seus adversários, o Departamento de Defesa busca robustecer a segurança cibernética de seus STIC[2] em todas as etapas da sistemática de aquisição de produtos de defesa e na sua operação. Além disso, a atenção quanto à proteção cibernética deve abarcar também as plataformas, as armas e a base industrial de defesa. Essa preocupação deve ser contínua e tem que abranger toda a estrutura de aquisição (EUA, 2020b).

Apesar do foco na gênese dos STIC[2], a doutrina é enfática em afirmar que a proteção cibernética não pode ser garantida apenas na concepção, mas por todo o período de vida do projeto. Por isso, os projetos devem prever que os sistemas tenham a possibilidade de incorporar novas tecnologias para se contrapor às evoluções das ameaças cibernéticas, o que possivelmente será necessário durante o ciclo de vida do sistema. Inclusive, é previsto que os gerentes dos projetos submetam os sistemas à testes constantemente, a fim de avaliar se o nível vigente de segurança é aceitável ou se há necessidade de atualização (EUA, 2020b).

Contudo, o Departamento de Defesa entende que o ponto mais frágil dos projetos seja a cadeia de suprimentos dos produtos de defesa. Isso porque, os componentes são construídos por agentes externos às Forças Armadas, geralmente empresas civis, e boa parcela podem ser estrangeiras, o que é corroborado pela sistemática para certificação de "Sistema e Rede Confiável", que define que o risco da cadeia de suprimentos como:

> O risco de que um adversário possa sabotar, introduzir maliciosamente funções indesejadas ou subverter o projeto, a integridade, a fabricação, a produção, a distribuição, a instalação, a operação ou a manutenção de um sistema de modo a vigiar, negar, interromper ou degradar de outra forma a função, o uso ou a operação de tal sistema[27] (EUA, 2018a, p. 13).

O principal receio quanto à cadeia de suprimentos é que o fabricante ou o fornecedor do produto de defesa inclua um *backdoor*[28] em um dos componentes, permitindo que a

---

[27] No original em inglês: *"The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."*

[28] Backdoor é um método não documentado de entrada em sistemas (*software*, plataformas, dispositivos e outros) que pode ser usado de forma legítima por fabricantes para restaurar acessos. Porém, é possível explorar o mesmo método para dar acesso remoto a um centro de comando e controle externo ao sistema invadido, criando uma via permanente para futuras contaminações. Assim, um atacante poderia ter acesso ao sistema e até o controle completo do seu ambiente (SANT'ANNA, 2023).

brecha seja explorada posteriormente, e sem o conhecimento do Departamento de Defesa (EUA, 2020b).

Por isso, existem processos para escolher os fornecedores dos produtos e componentes, que levam em consideração as certificações que atende, histórico e reputação quanto à segurança cibernética. Além disso, deve-se ter uma lista alternativa de fornecedores para cada item, principalmente os estrangeiros, em caso de impossibilidade de fornecimento por questões de ordem técnica, mercadológica ou legal (EUA, 2020b).

E a preocupação quanto à cadeia de suprimentos é pertinente. Segundo Drª Sadie Creese[29] e Dr Duncan Hodges[30] (GREEN, 2015), um *backdoor* implantado durante a produção de um componente ou sistema é uma técnica muito sofisticada e pode ser muito difícil de ser descoberta. Esse recurso pode tanto facilitar o acesso externo ao sistema quanto enviar pacotes de informações a alguém de interesse do fabricante, e sem o consentimento do usuário. Os professores sugerem que a forma de mitigar esse risco é manter o acompanhamento constante dos fornecedores a fim de obter uma lista dos que são confiáveis. E essa abordagem é a seguida pelo Departamento de Defesa.

Uma ferramenta obrigatória no processo de aquisição dos produtos de defesa é o Gerenciamento de Risco. No Departamento de Defesa, existe um processo para avaliação e gerenciamento de risco que foi elaborado especificamente para segurança cibernética e para aquisição de qualquer novo STIC[2], e é obrigatório que o sistema seja submetido a esse procedimento, independentemente do método de aquisição (EUA, 2022a).

O processo de avaliação do risco ocorre em sete etapas: preparação, classificação, seleção, implementação, avaliação, autorização e monitoramento (EUA, 2022a). No intuito de tornar a análise mais concisa, o presente trabalho analisará apenas as etapas consideradas mais relevantes, que são a classificação, a seleção e a autorização. A supressão das demais etapas não prejudica o entendimento ferramenta.

Na etapa da classificação é avaliado o nível de segurança cibernética que o sistema a ser adquirido deve possuir para seja incorporado ao Departamento de Defesa (EUA, 2022a). Para tal, é feita uma correlação entre o tipo de missão que o sistema está envolvido, ameaça

---

[29] Doutora em Ciência da Computação e professora de Segurança Cibernética na Universidade de Oxford, no Reino Unido.

[30] Doutor em Ciência da Computação e Professor de Segurança Cibernética e Sistemas de Informação na Universidade Cranfield, no Reino Unido.

adversária esperada, nível de dependência de acesso ao espaço cibernético, impacto em caso de perda ou comprometimento do sistema. Fruto dessa correlação, são realizadas análises qualitativas e quantitativas com objetivo de atribuir ao sistema um dos dez níveis de classificação possível pela publicação (EUA, 2022b)[31].

A etapa da seleção consiste na escolha do sistema ou componente que será incorporado. Os critérios de escolha envolvem classificação quanto à segurança cibernética, custo-benefício e outros, sendo preferidos os que oferecem menores riscos à segurança cibernética (EUA, 2022a).

Na etapa da autorização ocorre a aprovação formal da autoridade competente para prosseguimento do projeto. Para isso, é necessário que seja confirmado o atendimento dos requisitos de segurança cibernética e que sejam aceitáveis eventuais riscos residuais após todo o processo de mitigação conduzidos nas etapas anteriores (EUA, 2022a).

Cabe ressaltar que, de acordo com a sistemática do Departamento de Defesa americano, somente com aval quanto à adequada segurança cibernética, por meio do gerenciamento do risco, é que qualquer projeto de produto de defesa pode ser executado e o STIC^2 pode entrar em operação (EUA, 2022a). Ou seja, a proteção cibernética já é um requisito fundamental para aquisição e implementação de produtos de defesa americanos.

Após toda a sistemática de incorporação de sistema, seleção de fornecedor e gerenciamento de risco, o sistema é aprovado para aquisição. Entretanto, só poderá de entrar em operação após a sua resiliência cibernética ser comprovada nos testes e avaliações, também previstos na sistemática de aquisição.

3.3 Avaliação[32] e teste de segurança cibernética

Outro importante requisito para todos os sistemas que irão entrar em operação no âmbito do Departamento de Defesa americano é sua aprovação na avaliação e nos testes dos sistemas e das redes quanto à segurança cibernética.

---

[31] Os requisitos para classificação de um sistema constam de uma publicação específica para tal.

[32] A avaliação a que se refere a partir deste momento não está relacionada à etapa de avaliação conduzida durante o processo de gerenciamento de risco e relatada no item 3.2 deste trabalho. A avaliação do item 3.3 refere-se à avaliação de desempenho e segurança cibernético dos STIC^2.

Esses testes devem ser conduzidos periodicamente por todo o ciclo de vida dos sistemas bem como em caso de mudanças significativas no sistema, na ameaça ou no ambiente operacional em que será empregado (EUA, 2020a). Além disso, a publicação que trata especificamente sobre a condução dos testes reforça que:

> O objetivo dos testes e avaliações de segurança cibernética é identificar e mitigar vulnerabilidades exploráveis do sistema que afetam a resiliência operacional dos produtos de defesa antes da implantação do sistema para incluir segurança e capacidade de sobrevivência. A descoberta precoce de vulnerabilidades do sistema pode facilitar sua correção e reduzir o impacto no custo, no cronograma e no desempenho[33] (EUA, 2020a, p. 9, tradução nossa).

Em suma, os testes visam confirmar que os sistemas têm a resiliência cibernética adequada esperada pelo Departamento de Defesa, de acordo com seus requisitos. Para tal, os sistemas são intensamente analisados quanto a capacidade de prevenir (proteger as funções operacionais do sistema das formas mais corriqueiras de ataques cibernéticos), mitigar (detectar e responder à ataques cibernéticos, mantendo em operação até o término da missão) e recuperar-se (de ataques cibernéticos e estarem pronto para a próxima missão). A classificação atribuída ao sistema durante o gerenciamento de risco também é considerada nos testes para que seja definido o escopo e âmbito dos testes. Em caso de classificações elevadas, alguns testes são conduzidos com apoio da *National Security Agency* (NSA)[34] (EUA, 2020a).

Os sistemas são submetidos a seis fases[35] em diferentes estágios do projeto a fim de certificar que o sistema tem a condição de segurança cibernética desejada pelo Departamento de Defesa americano (EUA, 2020a).

Cada fase é incremental, ou seja, antes de conduzir os testes de uma nova fase, são realizados os testes de todas as fases anteriores e cada fase analisa um aspecto diferente do sistema. Essas fases são bem definidas, com os testes, resultados esperados e critérios de aprovação estipulados. Outro detalhe que chama a atenção é que o fornecedor do sistema também é envolvido nos testes para, em conjunto com o Departamento de Defesa, afiançar

---

[33] No original em inglês: *"The goal of cybersecurity T&E is to identify and mitigate exploitable system vulnerabilities impacting operational resilience of military capabilities before system deployment to include safety, survivability, and security. Early discovery of system vulnerabilities can facilitate remediation and reduce impact on cost, schedule, and performance."*

[34] A Agência de Segurança Nacional dos Estados Unidos é uma agência de inteligência dos Estados Unidos que também faz parte do Departamento de Defesa. A NSA é a principal agência do país para coleta de informações por meio eletrônico (CLARKE; KNAKE, 2015).

[35] O detalhamento sobre essas fases foge do escopo deste trabalho e, por isso, não serão descritas.

o correto funcionamento do sistema e prestar esclarecimentos em caso de eventuais falhas, especialmente as mais graves (EUA, 2020a).

De maneira simplificada, a metodologia empregada propõe-se a identificar duas possibilidades de exploração das brechas nos sistemas: o que as ameaças cibernéticas podem provocar de falha na missão das Forças e como esse sistema pode ser explorado caso sofra um ataque cibernético bem-sucedido. Isso é feito identificando todas as superfícies de ataque, que é como são chamados os pontos do sistema ou componente em que é possível acessá-lo por meio de um ataque cibernético.

A publicação lista os principais componentes que recebem dados externos e, por isso, são suscetíveis à invasão. Dentre eles, são listados o receptor de GPS; equipamentos de criptografia, processamento ou armazenamento; unidades de marcação de geolocalização; switches de rede; transmissores/receptores de rádio e a cadeia de suprimentos (EUA, 2020a). Cabe destacar que unidades de superfície costumam conter a grande maioria desses equipamentos.

Além dos testes conduzidos pelo sistema como um todo, a mesma publicação prevê testes específicos para os *softwares* embarcados nos sistemas. Seu intuito é ajudar a descobrir vulnerabilidades e confirmar que os requisitos estipulados foram satisfeitos, bem como avaliar a funcionalidade e a segurança do sistema. Isso porque, erros de programação na produção desses *softwares* podem levar a vulnerabilidades a todos os sistemas (EUA, 2020a).

Por isso são necessários testes tão específicos, uma vez que o Departamento de Defesa tem que certificar o correto funcionamento e a inexistência de brechas em múltiplas circunstâncias e condições em que o *software* está envolvido. Igualmente, ao ser identificada uma suscetibilidade à ataque cibernético, a determinação precisa da linha de código com falha e sua correção é uma tarefa deveras demorada (EUA, 2020a).

Os testes de *software* não são executados apenas nos programas manipulados pelo usuário, mas por todos os outros *softwares* que suportam tecnologicamente a ele como sistema operacional, máquinas virtuais[36], *drivers* de componentes e quaisquer outros necessários pelo *software* principal (EUA, 2020a).

Tendo em vista a autoridade que o *software* tem sobre o sistema, a publicação considera três métodos de desenvolvimento: próprio, reutilização de outro sistema e soluções

[36] Máquinas virtuais são computadores de *software*, com a mesma funcionalidade que os computadores físicos (BRASIL, 2023).

prontas (chamado de *Commercial-Off-The-Shelf*[37], também conhecido pela sigla COTS) e testes específicos são conduzidos independentemente do método de desenvolvimento.

3.4 Considerações Finais

Diante do que foi apresentado ao longo deste capítulo, pode-se perceber que a metodologia para confirmação da resiliência cibernética dos STIC[2] no âmbito do Departamento de Defesa americano é abrangente, tem claras instruções e é devidamente delimitada com parâmetros bem estabelecidos.

A preocupação com a segurança cibernética é patente desde a concepção dos produtos de defesa, passando pela sua implantação e efetivo emprego operativo. Também merece especial atenção a cadeia de suprimentos dos componentes, uma vez que estes podem ser construídos já com recursos que facilitem o ataque cibernético externo, e isso é muito difícil de ser detectado. E o nível de proteção cibernética deve ser periodicamente testada, para que o sistema seja considerado confiável.

Sendo o país com maior investimento em defesa do mundo, e com atuação em todo o globo terrestre, o foco na proteção cibernética é notório pela robustez da sistemática, que entende que a obtenção e manutenção da resiliência cibernética é uma tarefa que exige a atuação de diversas entidades.

A metodologia apresentada nesse capítulo é aplicável a todos e quaisquer meios e sistemas adquiridos pelos Estados Unidos da América e por isso, não foi especificado quais requisitos são necessários para um meio de superfície.

No próximo capítulo, serão apresentados os sistemas embarcados nos meios de superfície, e porque a resiliência cibernética é importante para cada um deles.

---

[37] Produto de prateleira, em tradução coloquial. Trata-se de *software* e/ou *hardware* comercialmente pronto e disponível para venda, distribuição ou licenciamento para o público em geral (EUA, 2015).

4 RESILIÊNCIA EM STIC^2 DE MEIOS DE SUPERFÍCIE

Os capítulos anteriores desse trabalho demonstraram características da Guerra Cibernética e como aumentar a proteção cibernética dos sistemas vitais a fim de evitar que sejam explorados ou atacados ciberneticamente. E a obrigação de possuir sistemas com robusta proteção cibernética se justificam pelas características intrínsecas de empregos desses meios. Meios de superfície possuem centenas de militares habitando-os diariamente, permanecem constantemente afastados de suas bases ou pontos de apoio, dependendo de si próprios para resolução dos problemas inopinados. E, de acordo com a classe do Navio, possuem grande poder de fogo, o que é um risco para o Navio em si e para outros.

Para confirmar a premência da resiliência cibernética nos meios de superfície, neste capítulo serão apresentadas algumas vulnerabilidades presentes em meios de superfície que podem ser exploradas por ataque cibernético e alguns exemplos.

4.1 Sistemas embarcados em meios de superfície

A depender do projeto de construção, do fabricante e do emprego do Navio, existem diversos arranjos possíveis de sistemas para otimizar o emprego dos sensores, equipamentos, componentes e maquinário. Por isso, com o propósito de facilitar a análise dos possíveis efeitos de ataques cibernéticos aos sistemas comuns em meios de superfície, neste trabalho todos os recursos informacionais disponíveis em um meio serão divididos em cinco conjuntos de sistemas diferentes. Cada sistema seria composto por todo o *software* e *hardware* necessário para seu funcionamento. Isso posto, os componentes para funcionamento dos navios foram divididos nos seguintes sistemas:

- Sistema de controle das máquinas: que controla o sistema de propulsão, geração de energia, governo e demais máquinas auxiliares além dos sistemas de alerta e controle de avarias;

- Sistema de Navegação: que integra os sistemas do passadiço, camarim de navegação, configuração de derrotas, comunicações por rádio, carta náutica eletrônica entre outros recursos;

- Sistema de Armas: para gerenciar informações dos sensores, o emprego do armamento e equipamentos de Guerra Eletrônica;

- Sistema de Gerenciamento de Plataforma: para controlar os sistemas afetos a atividades específicas do Navio. Possivelmente não estaria presente em todos os navios, mas seria importante para Navios Aeródromos, Navios-Tanque, Navios-Rebocador e outros; e

- Sistema de Serviços Administrativos: empregado para tráfego de documentos e conforto da tripulação como o acesso à Internet.

Convém esclarecer que neste trabalho será considerado que estes sistemas funcionam de forma segregada aos demais sistemas dos Navio. De acordo com o projeto do Navio, esses sistemas podem ter interligação física ou lógica de um sistema com outro. Porém, nestes casos, a possibilidade de danos mais severos em caso de ataques cibernéticos é grande, dado que uma rede pode ser a porta de entrada para outro sistema que o atacante tem mais interesse. Além disso, essa interligação entre os sistemas permitiria que um ataque cibernético tenha amplitude e extensão ainda maiores.

A seguir, serão aprofundadas as ameaças que cada um desses sistemas pode sofrer.

4.1.1 Sistema de controle das máquinas

Foi-se o tempo que o monitoramento dos equipamentos da máquina se dava em um compartimento quente guarnecido por um militar com olhar fixo em diversos indicadores com marcações à caneta a fim de observar se os parâmetros estavam dentro dos limites ou se apresentam alguma flutuação que indicassem a iminência de uma falha.

Os navios atuais, em especial, os meios de superfície modernos, contêm plantas de propulsão com elevado grau de complexidade. E os sistemas informatizados desempenham papel fundamental para controlar a propulsão principal, máquinas auxiliares, geradores para produção de energia elétrica, além do nível de combustível, água e lubrificantes para funcionamento do navio como um todo. Isso porque eles podem monitorar continuamente os componentes vitais de cada um desses sistemas e, na ocorrência de comportamento anormal ou qualquer falha, um alerta pode ser apresentado a um operador (HART, 2004).

Dependendo do seu nível de autoridade, o sistema tem a capacidade de atuar em válvulas, bombas ou motores, evitando o agravamento das condições adversas observadas. Esse grau de controle o sobre sistema de propulsão e de geração de energia do Navio aumenta a segurança na operação do meio, evita avarias severas e permite a redução da tripulação a

bordo ou nos quartos de serviço, sem contar a redução do erro humano nesta equação (ZIVI, 2005).

A desvantagem advinda desse arranjo é a exposição desse sistema a ataques cibernéticos, os quais poderiam provocar a avaria de componentes importantes, a falta de controle pelos operadores sobre o comportamento das máquinas e, em casos mais severos, a inutilização prolongada do meio.

Por exemplo, um ataque ao sistema de controle da máquina do leme poderia resultar em guinadas inesperadas do Navio. Ou ao sistema de controle da propulsão principal poderia fazê-lo operar além dos limites estabelecidos, resultando em desgaste prematuro ou sérios danos à máquina. Caso fosse afetado o sistema de dessalinização da água do mar, comprometeria a permanência e o afastamento do Navio de um porto para abastecimento. As possibilidades são inúmeras.

Cumpre destacar que comportamentos anormais das máquinas poderiam ser difíceis de identificar, uma vez que é possível perturbar seu comportamento sem alterar as indicações para monitoramento. E, caso fosse diagnosticada pela tripulação a avaria de um componente, sua substituição não faria o sistema funcionar conforme esperado pois o ataque cibernético não ocorre sobre uma determinada bomba ou motor e sim sobre um módulo de controle. Neste caso, a substituição do componente possivelmente acarretaria em avaria em demais componentes pois o módulo de controle atuaria sobre o componente substituído até avariá-lo também.

4.1.2 Sistemas de Navegação

Para condução segura da navegação, um meio de superfície necessita de uma série de equipamentos e auxílios externos para determinar, com precisão, onde está e para onde está indo. Dentre eles, pode-se citar o receptor de posição por *Global Positioning System* (GPS), o *Automatic Identification System* (AIS)[38], o radar de navegação, a carta náutica, equipamentos de comunicação por rádio ou por satélite, entre outros. Por necessitarem de recepção de

[38] Sistema de identificação automática - Sistema composto basicamente por um equipamento que integra um *transponder* de VHF com um equipamento GPS, proporcionando o conhecimento de forma prática e rápida de importantes informações das embarcações nas proximidades do navio que o possui (BRASIL, 2015, p. 255).

dados externos ao Navio, essas informações podem sofrer um ataque cibernético e provocar perda de consciência situacional pelos militares no passadiço (DE SÁ et al., 2019).

A título de exemplo, o sinal de posição recebido pelo GPS pode ser modificado com intuito de enganar o receptor do sinal (BHATTI; HUMPHREYS, 2017). Valendo-se dos dados errôneos de posição do Navio, a equipe de navegação sugeriria rumos que resultariam desvio de sua derrota planejada. E o problema se faz ainda mais grave quando o Navio estiver conduzindo navegação em área de manobra restrita ou em baixa visibilidade, como à noite ou sob nevoeiro. Esse problema seria difundido para todos os demais equipamentos que fazem uso dos dados do sistema GPS, e o AIS é um desses equipamentos.

O AIS é um importante recurso de segurança para a navegação. Isso porque o sistema funciona por meio de transmissão constante de informações como nome, posição, rumo e velocidade (entre outros dados) de navios e auxílios à navegação. Com isso, aqueles que recebem os sinais têm uma clara visão da posição e intenção de manobra dos demais navios nas suas proximidades, formando assim, uma rede para tráfego das informações entre as embarcações e estações que possuem o sistema. Estações costeiras recebem essas informações e as replicam na internet, permitindo toda sorte de empregos como acompanhamento de frota por companhias de navegação, planejamento para entrada e saída de portos, reconhecimento de intensidade de tráfego marítimo e outros (BALDUZZI, 2014).

Um ataque cibernético que afete os sistemas embarcados nos navios ou banco de dados na internet pode ocasionar a transmissão de informações sobre navios inexistentes ou a supressão das informações de navios autênticos, induzindo os navios na região a crer que o tráfego na região está maior ou menor que de fato está. O aumento na carga de trabalho do pessoal no passadiço pode levar à perda de consciência situacional da tripulação. (BALDUZZI, 2014).

Para um meio de superfície, além das implicações nas questões de segurança marítima, isso também pode resultar em questões políticas. Por exemplo, pode-se alterar a posição no sistema de forma que um Navio militar esteja transitando pelas águas territoriais de outro Estado quando, na verdade, não está (BALDUZZI, 2014). Neste caso específico, o Estado de bandeira do Navio pode ser forçado a optar entre expor a fragilidade de seus sistemas ou a infração de acordos internacionais.

Similarmente, um ataque cibernético nos demais equipamentos do passadiço resultará em falhas na segurança de navegação, expondo não só o meio afetado como os demais navios transitando nas suas proximidades.

4.1.3 Sistemas de Armas

Diferentemente dos demais sistemas, que também são aplicáveis a navios civis, esse é exclusivo para navios militares e, por ser o cerne dos meios de superfície, talvez seja o que demande mais esforços técnicos para robustecer sua proteção cibernética. E esse é o sistema que demanda maior atenção em termos de meios navais.

Para os navios se contraporem aos mísseis ar-superfície, mísseis superfície-superfície ou aviões é necessário um elevado nível de integração entre os sistemas de detecção (sensores), comando e controle, e sistema de armas do navio. Isso porque a velocidade desenvolvida por essas ameaças é muito elevada e, por vezes, com trajetórias aleatórias, reduzindo o tempo de resposta do navio. Em função desse curto tempo de resposta disponível, que corresponde à diferença entre ser alvejado ou não, a automação entre a identificação da ameaça e a resposta do armamento se faz essencial. E essa premência de rapidez na resposta resulta no aumento da automação e, por isso, a resiliência nesse sistema tem que ser elevada.

E da mesma forma que é o sistema que mais necessita de proteção, é o sistema mais difícil de garantir sua segurança sem elevar exorbitantemente custos de desenvolvimento e manutenção. Isso porque a complexidade para desenvolvimento de um sistema de armas é muito elevada pois é composto por diversos subsistemas, que devem trabalhar em perfeita harmonia. Ou seja, a complexidade e a relevância do sistema demandam muito tempo e elevados custos para implementação. No intuito de reduzir o tempo de produção ou os custos, existem duas abordagens quanto à escolha dos componentes que comporão esse sistema, cada qual com suas vantagens e desvantagens inerentes: o desenvolvimento de componentes customizados ou aquisição de componentes comerciais (COTS) (KOCH; GOLLING, 2016).

A customização, tem a vantagem de permitir um nível maior de segurança, se for escolhido cuidadosamente o fornecedor e acompanhado o processo de fabricação do componente. Porém, o custo é maior e é possível que a disponibilidade de sobressalentes seja encerrada em um prazo mais curto do que o sistema operará (KOCH; GOLLING, 2016).

Já a aquisição de componentes COTS tem a vantagem de redução dos custos tanto para aquisição quanto para manutenção, pois é possível que o suporte seja garantido por mais tempo, uma vez que o aumento da escala de produção e uma gama maior de clientes justificaria o prolongamento do suporte pelo fabricante. Entretanto, como já relatado no capítulo anterior, componentes COTS podem conter vulnerabilidades de difícil identificação e de consequências severas, como o trecho abaixo evidencia.

> De acordo com um empresário do ramo de defesa dos EUA que falou sob condição de anonimato, um "fabricante europeu de chips" recentemente incorporou em seus microprocessadores um mecanismo de destruição que poderia ser acionado remotamente [...] Se no futuro o equipamento caísse na mão de adversários, "os franceses queriam uma maneira de desativar esse circuito", disse ele[39] (KOCH; GOLLING, 2016, p. 197).

Ou seja, a própria escolha dos componentes do sistema de armas já pode permitir o ataque cibernético, visto que esse tipo de sistema é um ativo de altíssimo valor, principalmente quando envolver Navios-Escolta, que tem grande variedade de armamentos e com grande poder de destruição. Também é possível desabilitar o funcionamento do sistema de detecção ou alarme, retardar ou impedir o lançamento de armamento ou contramedidas. Em casos extremos, é possível que um ataque cibernético externo tome o controle do sistema de armas do Navio, podendo resultar em fratricídio ou atingir alvos civis ou inocentes (KOCH; GOLLING, 2016).

Em suma, nesse essencial sistema, a vulnerabilidade cibernética advém de componentes falsificados, de dificuldades em manter o suprimento prolongado de sobressalentes, da possibilidade de manipulação para redução de seu desempenho ou da implantação de *backdoor* nos componentes.

4.1.4 Sistema de gerenciamento de Plataforma

Navios de apoio logístico, de desembarque, aeródromos e outros têm como características o grande tamanho e a maior tripulação quando comparados aos navios-escolta

[39] No original em inglês: *"according to a US defence contractor who spoke on condition of anonymity, a "European chip maker" recently built into its microprocessors a kill switch that could be accessed remotely [...] If in the future the equipment fell into hostile hands, "the French wanted a way to disable that circuit," he said"*

e patrulha. Outra diferença são os recursos específicos para condução de suas atividades características.

Os navios-tanque tem sistemas para controlar o acondicionamento e a transferência do combustível em seus tanques. Navios-aeródromo tem elevadores de aeronaves, equipamentos para lançamento e recolhimento de aeronaves, sistemas para controle das demandas de voo e manutenção das aeronaves, torre de controle e diversos outros bastante complexos. Navios de transporte de carros de combate têm a característica de permitir o lançamento dos veículos de combate enquanto ainda está no mar a fim de permitir uma Operação Anfíbia.

Um ataque cibernético nos sistemas que controlam essas especificidades do Navio pode inviabilizar o seu emprego na Força ao qual o meio estiver adjudicado. Dependendo da missão, pode até afetar a operação como um todo. A título de exemplo, um ataque cibernético que desabilite o funcionamento das bombas necessárias para transferência de óleo no mar por um navio tanque, pode-se reduzir temporariamente o alcance ou a permanência de uma Força de Superfície.

Da mesma forma, se um ataque similar for realizado ao sistema de controle das catapultas de lançamento ou sistema de recolhimentos das aeronaves de um navio aeródromo, não seria possível conduzir operações aéreas com aeronaves de asa fixa, reduzindo a capacidade de defesa aérea da Força ou impedindo o ataque pretendido.

O lançamento de veículos anfíbios por Navios de Desembarque depende de envelope de velocidade e posicionamento do Navio. Um ataque nesse sistema de controle de movimento do Navio pode obrigá-lo a permanecer fora deste envelope, impedindo o lançamento dos veículos anfíbios ou tornando o lançamento inseguro.

A similaridade entre os casos supracitados é que o ataque cibernético não permitiria que o meio de superfície realizasse a tarefa para o qual foi desenvolvido. E, em muitos casos, a anomalia no sistema manifestar-se-ia no momento derradeiro, e dificilmente seria associado a ações de Guerra Cibernética. Ou seja, os meios teriam sido inutilizados.

4.1.5 Sistemas administrativos

Pela sua natureza e aplicação, esses sistemas são os que apresentam menores efeitos sobre a segurança do Navio, pois um ataque cibernético afetaria sistemas e redes de baixa

relevância operativa. Porém, esses sistemas e suas redes são possivelmente as que têm a maior quantidade de usuários e, presumivelmente, a única rede que tem acesso à internet, sendo essa a maior fonte de infecção por vírus (ICS et al., 2021). Por isso mesmo, os usuários dessa rede são elementos que pode ser considerados o elo mais fraco desse sistema[40].

Não é razoável considerar que esta rede esteja diretamente integrada às demais redes de operação do navio. Porém, de forma indireta, um usuário descuidado pode infectar as demais redes do navio por meio de um dispositivo de armazenamento, um celular ou outro meio que possa conectar à porta USB[41]. E a "porta de entrada" desse vírus pode ser a rede administrativa. E essa maneira é apenas uma das formas de entrada.

Uma vez infectado, o sistema fica suscetível uma variedade de ataques cibernéticos já relatados anteriormente. Desta forma, apesar da pequena influência sobre a condição de segurança de navegação e operação do navio, a sua segurança quanto a riscos cibernéticos não pode ser negligenciada e nem subestimada.

Outra possibilidade igualmente crítica, cuja análise foge do escopo desse trabalho, é o acesso a documentos sigilosos. Isso porque por essa rede também trafegariam documentos e publicações reservadas e um ataque cibernético permitiria o acesso a planos, documentos ou manuais de conteúdo controlado.

4.1.6 Considerações

Nos sistemas acima elencados é possível perceber que estes contêm boa parte dos equipamentos listados pelo Departamento de Defesa dos Estados Unidos como passíveis a ataques cibernéticos, conforme apresentando no item 3.3 (página 26) deste trabalho. Isso corrobora que esses sistemas têm grande suscetibilidade a ataques e, por esse motivo, deve ser considerado um elevado nível de resiliência a fim de garantir a proteção cibernética dos meios de superfície.

---

[40] A Doutrina Cibernética do Brasil considera que o usuário é o "calcanhar de Aquiles" ou "o ela mais fraco" de todo sistema, sendo este considerado sua vulnerabilidade primária (BRASIL, 2021).

[41] *Universal Serial Bus* (Barramento Serial Universal) é uma porta disponível em diversos tipos de aparelhos eletrônicos para conexão de dispositivos e é capaz de transferir energia e dados.

4.2 Exemplos de ataques cibernéticos em navios

No intuito de exemplificar não somente a possibilidade como também os efeitos de ataques cibernéticos a meios de superfície, serão citados alguns casos ocorridos na Marinha do Reino Unido e na Marinha dos Estados Unidos que apresentam características típicas desse tipo de ataque.

4.2.1 Marinha do Reino Unido

Casos de manipulação de dados de AIS já foram reportados por navios britânicos, incluindo seu Navio Aeródromo, o *HMS Queen Elizabeth*, que tivera seus dados alterados de modo que esse navio, e outros seis Navios-escolta da Marinha do Reino Unido, estivessem navegando em direção à Irlanda do Norte quando, na verdade, estavam todos atracados (HARRIS, 2021).

Outro caso, que desta vez houve repercussões no campo político, foi do *Destroyer HMS Defender*. O Navio fora acusado pelo governo da Rússia de demandar o porto de Sevastopol, na Crimeia, sem autorização para tal, tendo chegado a duas milhas náuticas de entrar no porto. Contudo, há imagens que comprovam que o Navio estava atracado no porto de Odessa, na Ucrânia, durante todo o deslocamento apresentado pelo AIS.

O Reino Unido não explicou publicamente o que provocara ambas as discrepâncias entre as informações do sistema e demais evidências que os fatos não ocorreram. E entre os especialistas não há consenso sobre qual tipo de ataque pode ter sofrido o Navio. As possibilidades estão entre manipulação dos dados dos Navios no AIS (SUTTON, 2021), ou modificação de suas posições em seus equipamentos GPS, simulando que estivessem em movimento (HAMBLING, 2021).

4.2.2 Navios dos Estados Unidos da América

Os casos a serem relatados envolvem quatro Navios-Escolta, dois da Classe *Ticonderoga*, comissionados no final dos anos 1980, e dois da Classe *Arleigh Burke*, comissionados em meados dos anos 1990. Esses Navios estiveram envolvidos em um

incidente e três acidentes num espaço de tempo de seis meses, e serão relatados a seguir, na ordem de cronológica em que ocorreram.

O *USS Antietam* (Classe *Ticonderoga*) encalhou durante uma manobra de fundeio pouco depois de suspender de Tóquio, no Japão. O navio suspendeu com atraso devido a problemas em seus sistemas de armas e de controle das máquinas pouco antes do suspender. Após seu retorno à normalidade, o Navio suspendeu e demandou o fundeio. Durante a navegação para o ponto de fundeio, a tripulação recebia informações conflitantes quanto à posição do Navio e, após o fundeio em si, houve divergências entre a posição informada pelo sistema de navegação do Navio e a posição em que o *Destroyer* de fato fundeou (HLAVAC, 2017). Essa diferença nas informações recebidas resultou em um fundeio numa posição que não era adequada para o Navio, provocando seu encalhe. Neste caso, pode-se depreender que as falhas nos sistemas de armas e de controle de máquinas já poderiam ser reflexo do ataque cibernético, que se manifestou com a alteração da posição do Navio e seu encalhe.

O *USS Lake Champlain* (Classe *Ticonderoga*) colidiu com um barco pesqueiro de bandeira da Coreia do Sul durante exercícios com o Navio Aeródromo *USS Carl Vinson*. O relatório do acidente descreve que, apesar de o acidente ter ocorrido no período da manhã, a visibilidade estava entre três e nove milhas náuticas e o Navio estadunidense tinha o barco pesqueiro, de pouco mais de 18 metros de cumprimento, no seu radar até cerca de duas milhas náuticas (MN) de distância, quando este sumira da tela de seu sensor, só aparecendo novamente após a colisão. Paralelamente, a embarcação sul-coreana perdera sua posição GPS e sua comunicação por rádio (EUA, 2017). Neste tipo de ocorrência, a suspeita seria por manipulação da imagem do radar por meio de ataque cibernético. Também pode-se considerar que a embarcação sul-coreana também pode ter sido vítima de um ataque, uma vez que perdera GPS e o rádio, dois importantes auxílios que poderiam tê-lo ajudado a desviar do *Destroyer*.

O *USS Fitzgerald* (Classe *Arleigh Burke*) colidiu com um navio mercante de transporte de contêineres na costa do Japão. O relatório da investigação do acidente descreve que este ocorrera no período da madrugada e quando o navio mercante estava a cerca de 12 MN do *Destroyer*, a Oficial de Serviço no passadiço percebeu que tinha dificuldades em travar o alvo no radar do Navio. Posteriormente, conseguiu receber os dados, mas ainda com informações imprecisas e conflitantes com as luzes exibidas pelo contato. Enquanto isso, no COC, o Oficial de Superfície reportou que não tinha contatos em seu radar até que subitamente apareceu

um contato a cerca de 5MN de distância do navio, poucos segundos antes de sentirem o impacto da colisão. Esse contato que apareceu no radar estava próximo ao navio contêiner que colidiu com o *Destroyer*. Nenhum desses dois apareceram no radar até poucos segundos do impacto. Além da questão do desaparecimento do contato no radar, seis minutos antes do impacto, o *Destroyer* realizou uma guinada de dez graus para boreste que não foi ordenada pela Oficial de Serviço. Se essa guinada não tivesse ocorrido, o ponto de maior aproximação entre os navios teria sido de 0,5 MN e a colisão não teria ocorrido (EUA, 2020c). Neste caso, é possível que o ataque cibernético tenha mudado o rumo do Navio-Escolta estadunidense por interferência na máquina do leme ou por interferência na posição do Navio, induzindo o sistema de navegação a alterar o rumo para manter na derrota programada. Nota-se mais um caso em que contatos somem do *display* do radar, resultando em colisão, mesmo que tenha sido em um navio de 220 metros.

O *USS McCain* (Classe *Arleigh Burke*) colidiu com um navio tanque no estreito de Cingapura. O relatório detalhou que as seguidas alterações da estação de governo do Navio, ora a estação primária, ora a estação a secundária, ambas no passadiço, e por vezes, a estação reserva na praça de máquinas, resultou na alteração do regime de máquinas e leme do Navio sem que o quarto de serviço conseguisse identificar corretamente qual estação estava controlando e como atuar corretamente para reverter o quadro. Além disso, o Oficial de Serviço determinou o acendimento dos sinais de “navio sem governo”, o que foi executado pela sinalaria, contudo o navio mercante atingido afirmou que o Navio estadunidense não exibiu este sinal (EUA, 2019b). Ambas as ocorrências são características de ataques cibernéticos, denotando que o ataque pode ter atingido o sistema de controle da propulsão principal ou da máquina do leme.

Resumidamente, esses episódios envolveram falhas súbitas, e em momentos críticos, em sistemas confiáveis. Mas os fatos relatados têm outra semelhança entre si: os quatro navios compunham a Sétima Esquadra no momento em seus acidentes ocorreram. A Sétima Esquadra patrulha o Oceano Pacífico e parte do Oceano Índico, mar que banha países como China, Rússia e Coreia do Norte e que historicamente realizam ataques cibernéticos a seus oponentes. E apesar da Marinha dos Estados Unidos reforçar que nenhum dos casos envolveu ataques cibernéticos, uma consequência desses fatos fortuitos é que toda investigação de incidentes envolvendo seus navios terá uma equipe para avaliar intervenção externa em seus sistemas por meio de ataques cibernéticos (LAGRONE, 2017).

4.3 Considerações Finais

Diante do que foi apresentado neste capítulo, é possível perceber que o avanço das tecnologias de informações aplicadas nos meios de superfície modernos resultara em redução das tripulações devido a redução das cargas de trabalho, aumento da velocidade de resposta a ameaças e a aumento da eficiência dos navios em si. Contudo, esses mesmos avanços permitem mais uma forma de exploração pelo inimigo.

E uma dessas formas de exploração seria exatamente as *Effects-Based Operations*, cujo mote é aumentar a eficiência do emprego da força por meio do controle dos recursos do inimigo de forma a impedi-lo de combater, ou reduzir severamente essa capacidade. Como nos exemplos acima, embora haja casos não confirmados de ataque cibernético, é possível perceber que, caso os ataques fossem comprovados, a aplicação dessa estratégia seria clara, uma vez que o inimigo teria controlado os navios, gerado paralisia estratégica sem que tivesse tentado destruir os meios do inimigo.

Por isso, a forma mais eficiente de se contrapor a esse tipo de ameaça é garantindo uma forte resiliência cibernética em todos os sistemas embarcados nos meios de superfície. Como apresentado, a resiliência cibernética é um conceito de entendimento acessível, mas sua concretização é desafiadora. Portanto, é pertinente afirmar que deve ser implementada desde a concepção do sistema e ser constantemente testada e avaliada nas condições mais próximas possíveis do ambiente cibernético em que o meio será empregado a fim de confirmar a eficácia no nível esperado.

Diante dessas considerações, conclui-se que os meios de superfície devem estar preparados para enfrentar também a guerra no quinto domínio, tendo em vista que, à luz das *Effects-Based Operations*, é possível obter o controle da Força Naval inimiga por meio de Guerra Cibernética.

5 CONCLUSÃO

Conforme apresentado nos capítulos anteriores, pode-se observar que a exploração do Espaço Cibernético afeta a todos os níveis de um conflito contemporâneo e permeia os demais quatro domínios operacionais. Por conseguinte, o domínio marítimo também é afetado e a gama de ameaças possíveis por Guerra Cibernética é grande. Os meios de superfície não ficaram imunes a essa ameaça uma vez que a quantidade de sistemas informatizados nos navios mais modernos, e a dependência da tripulação em utilizá-los, os expõe em demasia a estes riscos, com consequências que podem ir desde o nível tático até o nível político.

As *Effects-Based Operations* são uma modalidade de emprego das Forças Armadas que não visa a destruição pura e simples dos recursos do inimigo e de seus meios militares ao longo do conflito. Esta considera mais eficiente incapacitá-los para que o inimigo não tenha a capacidade de impor seu ritmo de batalha. Sabotar o fornecimento de energia de uma base inimiga pode ser tão ou mais eficiente que destruí-la, e isso pode ser feito com reduzido número de baixas para ambos os lados.

E os efeitos da Guerra Cibernética podem ser aplicados com esse fim. Criar desordem ou anormalidades em sistemas que os usuários confiam pode mobilizar boa parte do pessoal a fim de identificar ou resolver um problema que não aparenta ser de origem externa. Acessar planos e arquivos secretos inimigos também garantem uma grande vantagem, pois é possível contrapor-se a um movimento esperado.

No capítulo três, analisou-se a metodologia estadunidense para fortalecer a resiliência cibernética de seus meios. E aquelas Forças Armadas já entenderam que a proteção do Espaço Cibernético de seus meios não pode ser relegada a um requisito meramente desejável, sendo atualmente considerada uma condição *sine qua non* para desenvolvimento ou aquisição de qualquer produto de defesa que, de qualquer forma que seja, possa estar sujeito à Exploração ou Ataque Cibernéticos.

A profundidade dessa sistemática de aquisição de meios fundamenta-se na premissa que qualquer meio deve estar em condições de combater em ambiente sob ataque cibernético. E, para isso, é considerado fundamental para o Departamento de Defesa dos Estados Unidos que as redes e sistemas sejam confiáveis, que os projetos de aquisição de meios devem garantir a proteção cibernética desde sua concepção e que esses sistemas

devem ser continuamente testados com o objetivo de confirmar que o nível de segurança esperado.

Para cada um dos requisitos supracitados, aquele Departamento tem uma gama de publicações que estabelecem requisitos, ações e responsabilização de cada ente para garantir que os componentes, sistemas ou meios sejam empregados em combate real sob a égide das Forças Armadas dos Estados Unidos e nas melhores condições possíveis quanto à Proteção Cibernética.

Essas publicações são enfáticas na necessidade da confirmação da procedência do equipamento, uma vez que este pode ser fornecido pelo fabricante já com brechas deliberadas para que sejam exploradas posteriormente. E além da origem do equipamento, é necessário ponderar sobre qual a origem do *software* que será embarcado nesses equipamentos. Aquisição de *software* já pronto, ou COTS, demanda menos tempo para produzir, mas o código pode incluir brechas propositais ou não. Já o desenvolvimento próprio demanda mais tempo, mas tem-se um controle maior sobre o comportamento do sistema, podendo ser auditado por outros entes governamentais.

As publicações em questão são bastante abrangentes, sendo aplicáveis a toda a Força e em meios e sistemas de quaisquer portes ou empregos. Por isso, não existe uma seção específica para meios de superfície. Contudo, a relevância dessa sistemática aplicada a meios de superfície da Marinha aparece na forma de equipamentos que requerem judicioso emprego pois são suscetíveis à ataques cibernéticos. Dos itens relacionados, quase todos são usuais em meios de superfície, ou seja, os Navios são passíveis a Guerra Cibernética.

No capítulo quatro foi analisado como a Guerra Cibernética pode interferir em um meio de superfície. Para tal, foram considerados cinco conjuntos de sistemas com funções específicas a bordo e a conclusão é que todos podem sofrer ataque cibernético e as consequências podem resultar em incapacitação do Navio para emprego em combate.

O final do capítulo quatro reforçou a hipótese levantada ao final do capítulo dois, qual seja, que meios de superfície necessitam de elevada resiliência cibernética para emprego em conflitos atuais. Isso porque, como pode ser evidenciado pelos exemplos, a necessidade de possuir $STIC^2$ para se contrapor às ameaças cinéticas cada vez mais avançadas resultou na exposição do Navio às ameaças cibernéticas.

E isso pode ser explorado com emprego da estratégia de controle dos recursos do inimigo, levando-o a impossibilidade de lutar. Essa estratégia foi cunhada pelo General Dave

Deptula no início dos anos 2000 e foi empregada na Operação Tempestade no Deserto na Guerra do Golfo, no início dos anos 1990. As contribuições do CMG Edward Smith também são relevantes, pois sua abordagem é mais abrangente e fica claro que as *Effects-Based Operations* são uma alternativa para empregar eficientemente meios militares de custos cada vez mais elevados e com orçamentos cada dia mais reduzido.

E, com isso, percebe-se que a pergunta do trabalho foi respondida e, no que tange a pesquisas futuras, sugere-se aprofundar quanto às ações que as três Forças Armadas do Brasil tomam para garantir a resiliência cibernética em seus meios. E os exemplos vividos pelo Reino Unido e pelos Estados Unidos da América relatados no capítulo quatro são evidências que a Guerra Cibernética não pode ser subestimada ou ignorada.

REFERÊNCIAS

BALDUZZI, Marco; PASTA, Alessandro; WILHOIT, Kyle. **A security evaluation of AIS automated identification system**. Proceedings of the 30th Annual Computer Security Applications Conference, 2014.

BHATTI, Jahshan; HUMPHREYS, Todd E. **Hostile Control of Ships via False GPS Signals: Demonstration and Detection**. Navigation, v. 64, n. 1, p. 51-66, 2017.

BRASIL. Gabinete de Segurança Institucional. **Estratégia Nacional de Segurança Cibernética - E-Ciber**. Brasília:[s.n.], 2020

_____. _____. **Glossário de Segurança de Informação**. Disponível em: <https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/glossario-de-seguranca-da-informacao-1>. Acesso em: 19 jun. 2023.

_____. Marinha do Brasil. Diretoria Geral de Material da Marinha. **DGMM-0540: Normas de Tecnologia de Informação da Marinha**. Rio de Janeiro: [s.n.], 2019.

_____. _____. Estado-Maior da Armada. **EMA-419: Doutrina Cibernética na Marinha**. [S.l.: s.n.], 2021.

_____. Ministério da Defesa. **MD15-G-01:Glossário das Forças Armadas**. Brasília:[s.n.], 2015.

_____. _____. **MD31-M-08: Doutrina Militar de Defesa Cibernética**. Brasília: [s.n.], 2014.

_____. _____. **MD31-P-02: Política Cibernética**. Brasília: [s.n.], 2012.

CASTELLS, Manuel. **A sociedade em rede**. 6. ed. São Paulo: Paz e Terra, 2005.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito**. Rio de Janeiro: Brasport, 2015.

DE SÁ, Alan et. al. **O Encontro da Guerra Cibernética com as Guerras Eletrônica e Cinética no Âmbito do Poder Marítimo**. Revista da Escola de Guerra Naval, v. 25, n. 01, p. 89–128, 2019.

DEPTULA, David A. **Effects-based Operations**. [s.l.]: Aerospace Education Foundation, 2001.

ESTADOS UNIDOS DA AMÉRICA (EUA). Committee on National Security Systems (CNSS). **CNSSI No. 4009: CNSS Glossary**. Fort Meade: [s.n.], 2015

_____. Department of Defense. **Cybersecurity Test and Evaluation Guidebook**, v. 2.0 change 1. [S.l.: s.n.], 2020a.

_____. _____. **DoDI 5000.90: Cybersecurity for Aquisition Decision Authorities and Program Managers**. [S.l.: s.n.], 2020b.

_____. _____. **DoDI 5200.44: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks**. [S.l.: s.n.], 2018a.

_____. _____. **DoDI 8500.01: Cybersecurity**. [S.l.: s.n.], 2019a.

_____. _____. **DoDI 8510.01: Risk Management Framework for DoD Systems**. [S.l.: s.n.], 2022a.

_____. _____. **Trusted Systems and Networks (TSN) Analysis**. Washington, DC: DASD(SE) and DoD CIO, 2014.

_____. _____. Department of the Navy. **Report on the Collision between USS LAKE CHAMPLAIN (CG 57) and Fishing Vessel NAM YANG 502**. Washington: [s.n.], 2017.

_____. _____. Joint Chiefs of Staff. **Cyber Survivability Endorsement Implementation Guide**, v. 3.0. [S.l.: s.n.], 2022b.

_____. National Transportation Safety Board. **Collision between US Navy Destroyer John S McCain and Tanker Alnic MC Singapore Strait**. Washington: [s.n.], 2019b.

_____. _____. **Collision between US Navy Destroyer Fitzgerald and Philippine-Flag Container Ship ACX Cristal**. Washington: [s.n.], 2020c.

GREEN, James A. **Cyber Warfare**. [s.l.]: Routledge, 2015.

HAMBLING, David. **GPS cyberattack falsely placed UK warship near Russian naval base**. New Scientist. Disponível em: <https://www.newscientist.com/article/2282149-gps-cyberattack-falsely-placed-uk-warship-near-russian-naval-base/>. Acesso em: 7 maio 2023.

HARRIS, Mark. **Phantom Warships Are Courting Chaos in Conflict Zones**. Wired. Disponível em: <https://www.wired.com/story/fake-warships-ais-signals-russia-crimea/>. Acesso em: 19 maio 2023.

HART, Dennis. **An approach to vulnerability assessment for Navy Supervisory Control and Data Acquisition (SCADA) system**. Disponível em: <http://hdl.handle.net/10945/1413>. Acesso em: 27 jun. 2023.

HLAVAC, Tyler. **Navy probe blames captain's judgment in USS Antietam grounding**. Stars and Stripes. Disponível em: <https://www.stripes.com/theaters/asia_pacific/navy-probe-blames-captain-s-judgment-in-uss-antietam-grounding-1.480879>. Acesso em: 1 jun. 2023.

ICS et. al. **The guidelines on cybersecurity onboard ships**. Disponível em: <https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf>. Acesso em: 15 jun. 2023.

KOCH, Robert; GOLLING, Mario. **Weapons Systems and Cyber Security – A Challenging Union**. 2016 8th International Conference on Cyber Conflict (CyCon), v. 8th edition, p. 191–203, 2016.

LAGRONE, Sam. **Cyber Probes to be Part of All Future Navy Mishap Investigations After USS John S. McCain Collision**. USNI News. Disponível em: <https://news.usni.org/2017/09/14/cyber-probes-part-future-navy-mishap-investigations-uss-john-s-mccain-collision>. Acesso em: 07 jun. 2023.

LOUREIRO, Marcus Vinícius de Castro. **Ataques Cibernéticos: Ameaças reais ao Poder Naval**. Revista Marítima Brasileira, v. 137, n. 01/03, p. 80–86, 2017.

ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE (OTAN). **AJP-3.20: Allied Joint Doctrine for Cyberspace Operations**. [S.l.: s.n.], 2020.

REINO UNIDO. Ministry of the Cabinet Office. **National Cyber Strategy 2022**. [S.l.: s.n.], 2022.

SANT'ANNA, Hellen. **Você sabe o que são e como evitar backdoors?** Blockbit. Disponível em: <https://www.blockbit.com/pt/blog/como-evitar-backdoors/>. Acesso em: 9 jun. 2023.

SMITH, Edward A. **Complexity, networking, and effects-based approaches to operations**. Washington: CCRP Publications, 2006.

_____. **Effects-Based Operations**. Washington: CCRP Publications, 2002.

SUTTON, H. I. **Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base**. USNI News. Disponível em: <https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-base.>. Acesso em: 12 jun. 2023.

ZIVI, Edwin. **Design of robust shipboard power automation systems**. Annual Reviews in Control, v. 29, n. 2, p. 261–272, 2005.

TZU, Sun. **The art of war**. Leicester: Allandale Online Publishing, 2000.