ESCOLA DE GUERRA NAVAL

CC(T) Anderson de Araujo Medeiros

ATAQUE CIBERNÉTICO À CADEIA DE SUPRIMENTOS: O CASO STUXNET E AS LIÇÕES APRENDIDAS PARA A DEFESA CIBERNÉTICA NA MB

Rio de Janeiro

2021

CC(T) Anderson de Araujo Medeiros

ATAQUE CIBERNÉTICO À CADEIA DE SUPRIMENTOS: O CASO STUXNET E AS LIÇÕES APRENDIDAS PARA A DEFESA CIBERNÉTICA NA MB

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso Superior.

Orientador: CC MIGUEL HENRIQUE ALEXANDRE DIAS ALVES

Rio de Janeiro

Escola de Guerra Naval

2021

AGRADECIMENTOS

Primeiramente a Deus por ter me sustentado durante todos os momentos. A Ele toda honra e glória, pois é fiel e cumpre tudo o que promete.

A minha esposa Shirley e filha Isabella pelo apoio incondicional durante todo o período do curso. Mesmo em momentos de afastamento, sempre estiveram me incentivando. Vocês são meus alicerces, um grande presente que Deus me deu.

Ao meu orientador, Capitão de Corveta Miguel Henrique Alexandre Dias Alves, pela disponibilidade e camaradagem nas orientações precisas, de forma objetiva e profissional, que contribuíram para o aperfeiçoamento desse trabalho.

A equipe de coordenação e instrutores, da Escola de Guerra Naval, pelo apoio, dedicação e profissionalismo ao transmitir os ensinamentos que contribuíram para o brilhantismo do curso.

Aos meus amigos da turma QT-2005 pelo apoio e incentivo que dedicaram durante todo o curso. Foi um ano de muitas lutas, mas Deus permitiu que chegássemos juntos nesta etapa final.

A toda equipe da Divisão Técnica de Comando e Controle do Comando de Operações Navais, pelo apoio durante o transcorrer do C-Sup-2021.

RESUMO

O horizonte cibernético para os próximos anos tende a ampliar a conexão mundial, trazendo mais usuários para esse ambiente; e a oferecer novas tecnologias. Em contrapartida às facilidades encontradas nesse espaço, existe a possibilidade de ele ser comprometido por ameaças que exploram as suas vulnerabilidades, com o objetivo de realizar ataques cibernéticos e, assim, roubar dados, invadir sistemas e controlar o funcionamento de infraestruturas críticas de Defesa Nacional. Uma dessas ações maliciosas, assunto abordado nesse trabalho, é o Ataque à Cadeia de Suprimentos, cuja quantidade de ataques vem aumentando nos últimos anos, com o desenvolvimento de novas técnicas que possibilitam a sua concretização em alvos como empresas e instituições civis e militares. O tema ambiente cibernético e sua defesa tem sido objeto de prioridade por parte do Governo brasileiro, em especial pelas Forças Armadas, que têm desenvolvido documentos normativos e ações voltados para esse tema. Entre esses documentos, podem ser destacados a Estratégia Nacional de Segurança Cibernética, que possui um escopo voltado para a proteção de infraestruturas críticas e da cadeia de suprimentos; o Plano Estratégico da Marinha; a Política e a Estratégia Nacional de Defesa. A partir desses e de outros documentos normativos, ações devem ser desenvolvidas para a defesa do Espaço Cibernético pela Marinha do Brasil, a fim de que haja proteção do seu Poder Naval e, assim, possa proporcionar um adequado preparo para um possível conflito cibernético. O embasamento teórico desse trabalho de pesquisa se consolidou em bibliografia e em estudo de caso sobre o entendimento de ataques voltados à cadeia de suprimentos, bem como de ações a serem empreendidas sobre o tema. Mediante a análise das atividades em andamento e das possibilidades de concretização desse tipo de ataque, foi observado a existência de oportunidades para a sua concretização, bem como de necessidades de melhorias nos procedimentos existentes na Marinha do Brasil para a sua mitigação. Nesse sentido, são abordadas ações normativas, de qualificação de pessoal e de segurança de sistemas, com o potencial de contribuir para a segurança do Poder Naval, e, assim, proporcionar o fortalecimento da Segurança e da Defesa Cibernética da Marinha do Brasil.

Palavras-chave: Ataque à Cadeia de Suprimentos. Espaço Cibernético. Defesa Cibernética. Segurança Cibernética. Ataque Cibernético.

LISTA DE ABREVIATURAS E SIGLAS

AEN	Ações Estratégicas Navais
APF	Administração Pública Federal
DCTIM	Diretoria de Comunicações e Tecnologia da Informação da Marinha
ENaDCiber	Escola Nacional de Defesa Cibernética
END	Estratégia Nacional de Defesa
ENSC	Estratégia Nacional de Segurança Cibernética
ET	Estação de Trabalho
EUA	Estados Unidos da América
FA	Forças Armadas
MB	Marinha do Brasil
MD	Ministério da Defesa
NAVSEA	*Naval Sea Systems Command*
PLC	*Programmable Logic Controllers*
PCT	Programa de Obtenção das Fragatas Classe Tamandaré
PEM	Plano Estratégico da Marinha
PLACAPE-TIC	Plano de Capacitação de Pessoal de Tecnologia da Informação e Comunicações da Marinha
PND	Política Nacional de Defesa
SHCDCiber	Sistema de Homologação e Certificação de Produtos de Defesa Cibernética
SIC	Segurança da Informação e Comunicações
SO	Sistema Operacional
TIC	Tecnologia da Informação e Comunicações

SUMÁRIO

1 INTRODUÇÃO

O atual momento, em que as capacidades para a atuação em um ambiente de conflito cibernético têm evoluído de forma rápida, suscita a sociedade e os órgãos governamentais, incluindo as Forças Armadas (FA), a estarem continuamente preparados para uma adequada participação nesse tipo de conflito.

Dessa forma, ações de preparo e defesa cibernética devem ser adotadas para que haja uma real capacidade de enfrentamento dos cenários adversos que possam surgir, garantindo, assim, a Defesa Nacional e a proteção do Espaço Cibernético[1] do País.

A defesa do Espaço Cibernético tem sido objeto prioritário de estudo e de atuação no âmbito das FA, o que demonstra a relevância do tema. A pertinência do assunto possibilitou a sua inclusão na Política Nacional de Defesa (PND) e na Estratégia Nacional de Defesa (END), em que é ressaltada a necessidade de se dar atenção às áreas de segurança e de defesa do espaço cibernético brasileiro, a fim de garantir o adequado funcionamento dos sistemas de informação, de gerenciamento e de comunicações de interesse nacional (BRASIL, 2020f).

Nesse cenário, de crescentes ataques cibernéticos, há preocupação sobre como seria possível preparar os Navios da Marinha do Brasil (MB), em tempo de paz, para um futuro conflito envolvendo a área cibernética. Nesse contexto, o problema a ser analisado será baseado na prevenção de Ataque à Cadeia de Suprimentos dos sistemas e equipamentos ofertados à MB, em especial aos meios navais, bem como nas ações que possibilitem o incremento da mentalidade de segurança dos seus usuários.

Essa abordagem se justifica pela necessidade de se dotar, os meios navais, de sistemas e equipamentos que sejam confiáveis e livres de códigos maliciosos, que, muitas vezes, podem ser embutidos no processo de fabricação ou na cadeia logística e, posteriormente, ser acionados, possibilitando, como consequência, um funcionamento inadequado em uma época de conflitos.

A quantidade de ocorrências de Ataques à Cadeia de Suprimentos tem evoluído nos últimos anos e desafiado instituições a manterem sua área de Defesa Cibernética devidamente preparada para enfrentar esse tipo de ameaça. Conforme citado por Rigues (2020), como exemplo recente, ocorrido no final do ano de 2020, e que também será

1 É um conceito amplo, que engloba um conjunto de sistemas e equipamentos ligados em uma rede de comunicação em um ambiente de Internet. Nesse ambiente, estão incluídos os sistemas de uso corporativo, financeiros, militares, entre outros. Nele são controladas e conectadas várias redes de computadores mundiais. Um local em que há comunicação, armazenamento e compartilhamento de informações (SINGER; FRIEDMAN, 2014).

comentado nas seções seguintes, tem-se o caso da empresa estadunidense SolarWinds, que foi alvo de um ataque que atingiu mais de 18.000 clientes e expôs vários dados sigilosos. Além desse exemplo, tem-se o caso do *Stuxnet*, que será descrito em uma seção à parte nesse trabalho; por meio deste código malicioso, foi realizado um ataque a uma usina nuclear iraniana e que provocou um efeito cinético.

Dessa forma, nesse trabalho de pesquisa, pretende-se responder à seguinte pergunta: Quais ações devem ser consideradas, a fim de se evitar a presença de códigos maliciosos nos sistemas e equipamentos utilizados pelos navios da MB; e quais procedimentos podem ser adotados para aumentar a mentalidade de segurança de seus usuários, para possibilitar um adequado preparo para um possível conflito cibernético?

Sendo assim, o objetivo geral desse estudo é contribuir para a identificação de possíveis áreas que podem ser exploradas em um ataque, assim como aspectos normativos relacionados à defesa e a capacitação que atendam ao tema relacionado ao Ataque à Cadeia de Suprimentos na MB, proporcionando um adequado preparo para uma época de conflito.

Para alcançar esse objetivo geral, foram delimitados os seguintes objetivos específicos: a) analisar os aspectos normativos sobre as possibilidades de prevenção de ataques cibernéticos nos sistemas e equipamentos militares; b) analisar as ações que possam ser empregadas para utilização segura dos sistemas e equipamentos dos navios, a fim de minimizar ataques em possíveis conflitos cibernéticos; e c) analisar as ações que possam ser adotadas para o incremento da mentalidade de segurança dos usuários dos sistemas e equipamentos, com o objetivo de melhorar o preparo em possíveis conflitos cibernéticos.

Esse trabalho foi elaborado por meio de um estudo de caso e uma pesquisa bibliográfica sobre o problema, a partir das teorias existentes em legislações, livros, doutrinas, artigos acadêmicos, normas e sites da Internet.

Assim, para facilitar a leitura e o entendimento da pesquisa, dividiu-se o documento em cinco seções, iniciando pela Introdução, que apresenta os aspectos abordados no desenvolvimento desse trabalho.

Na segunda seção, são apresentados os conceitos relacionados ao Espaço Cibernético e o Ataque à Cadeia de Suprimentos, sua normatização na Administração Pública Federal (APF) e FA.

Na terceira seção, será apresentado um caso efetivo de Ataque à Cadeia de Suprimentos, ocorrido no ano de 2010, envolvendo o código malicioso *Stuxnet*, na usina iraniana de Natanz. Será detalhado como este ataque foi realizado e as vulnerabilidades encontradas, que possibilitaram concretizar o objetivo da operação.

Na quarta seção, utilizando-se o conhecimento do caso *Stuxnet*, serão apresentados os aspectos normativos voltados para a defesa do Espaço Cibernético, com foco na cadeia de suprimentos de produtos ofertados à MB. Como exemplo, foi utilizada a possibilidade do fornecimento de itens, por diversos países, para os sistemas do Programa de Obtenção das Fragatas Classe Tamandaré (PCT). Além disso, foram apresentadas formas de se aumentar a mentalidade de segurança do pessoal da MB, a fim de prepará-los para um possível conflito cibernético.

Por fim, na última seção, são tecidas as considerações finais a respeito da pesquisa realizada, concluindo a exposição.

2 O ESPAÇO CIBERNÉTICO, SUAS AMEAÇAS E A NORMATIZAÇÃO NACIONAL

Dentro da sociedade global, há um avanço significativo dos serviços disponibilizados à população na área digital. Isso permitiu que, nas últimas décadas, muito em função da facilidade de acesso à Internet, mais pessoas se beneficiassem desses serviços, criando uma espécie de revolução digital. Esse rápido avanço resultou em um intenso uso do Espaço Cibernético, para as mais variadas atividades e para a oferta de serviços, por parte de empresas privadas e da APF.

No entanto, com esse avanço, existe a possibilidade de ocorrerem ameaças que podem pôr em risco os serviços disponibilizados no Espaço Cibernético, colocando em perigo a APF e a própria sociedade. A proteção do Espaço Cibernético requer vigilância contínua e mudanças políticas, tecnológicas e educacionais, a fim de que seja proporcionado um adequado preparo para o enfrentamento dessas ameaças à Segurança Nacional (BRASIL, 2020a).

Atualmente, os acessos a vários sistemas podem ser realizados por meio de computadores ligados em rede, inclusive pela Internet. Um possível ataque ao Espaço Cibernético pode permitir que países tenham o seu fornecimento de energia ou suas comunicações cortados, pela execução de códigos maliciosos em seus sistemas de controle, originados de ataques cibernéticos.

Além de incluir a Internet, o Espaço Cibernético também engloba redes distintas, que, muitas vezes, não deveriam estar disponíveis para um acesso mais amplo a qualquer pessoa, ou seja, deveriam estar segregadas. Como exemplo, têm-se as transações que envolvem recursos financeiros e sistemas de controle de infraestruturas críticas, que podem

ser invadidos, controlados e destruídos. Assim, o sucesso de um ataque ao Espaço Cibernético poderia colapsar um sistema financeiro, retirar um satélite de sua órbita ou mesmo comprometer uma cadeia de suprimentos (CLARKE; KNAKE, 2015, p. 60).

Como pode ser observado, o conceito de Espaço Cibernético é amplo e requer especial atenção. Trata-se de um ambiente em que redes distintas utilizam o mesmo espaço, o que possibilita a ocorrência de ações criminosas, ameaças e tentativas de invasão nos serviços e sistemas disponibilizados à população, empresas e instituições públicas. Com isso, percebe-se a importância de se criar políticas adequadas de segurança, a fim de se evitar o sucesso dessas ações. Sendo assim, dentro do conceito do Espaço Cibernético, percebe-se que Mar, Terra e Ar não são mais os únicos ambientes para a atuação das FA. Há uma outra dimensão em que as instituições militares precisam atuar e dedicar especial atenção (BRASIL, 2020f).

No Espaço Cibernético, existem ameaças que devem ser identificadas, pela possibilidade de concretizarem um ataque cibernético. Para um melhor dimensionamento da quantidade desses ataques, estima-se que, no ano de 2020, o Brasil tenha sofrido mais de 8,4 bilhões de tentativas de ataques cibernéticos, de um total de 41 bilhões em toda a América Latina (COMPUTERWORLD, 2020).

Outra constatação sobre essas ações, é que, em 2019, o Brasil ficou em 3º lugar entre os países que mais sofreram esse tipo de ataque, ficando atrás apenas dos Estados Unidos da América (EUA) e da República Popular da China. Essa avaliação considerou mais de 157 países em seu levantamento. Um dos fatos que possivelmente mais contribuíram para esse cenário foi o aumento de dispositivos móveis da população, proporcionando mais espaço e oportunidade para a ocorrência desses crimes (IMASTERS, 2019).

A identificação de vulnerabilidades e de ameaças é de fundamental importância para o estabelecimento de requisitos de segurança de um sistema ou uma rede. Nesse contexto, a análise dessas vulnerabilidades possibilita a identificação de falhas de segurança no ambiente computacional das organizações, implementando, assim, controles eficientes sobre os seus equipamentos e sistemas (BRASIL, 2020a).

Nesse contexto de ameaças cibernéticas, será abordado, nesse trabalho de pesquisa, o Ataque à Cadeia de Suprimentos. Esse tipo de ação maliciosa explora as vulnerabilidades de um sistema, podendo ocorrer por falhas de projeto ou ser intencionalmente introduzida por agentes maliciosos durante a sua fabricação, distribuição, operação e manutenção (SÁ; MACHADO; ALMEIDA, 2019).

2.1 Ataque à Cadeia de Suprimentos

Uma das ameaças cibernéticas existentes é identificada como Ataque à Cadeia de Suprimentos, ou *Supply Chain Attack.* Esse tipo de ameaça é definido como uma técnica na qual se insere um código malicioso, ou um componente malicioso, em um *software* ou *hardware*, que teoricamente seria confiável. Ao comprometer o fornecedor desse *software* ou *hardware*, espiões podem danificar os sistemas de distribuição e transformar qualquer aplicativo, atualização de software ou, até mesmo, o equipamento físico, que são enviados aos clientes, em um Cavalo de Troia[2]. Com a intrusão, os criminosos conseguem criar uma ponte para as redes dos clientes do fornecedor, chegando a centenas ou milhares de vítimas (GREENBERG, 2021).

Clark e Knake (2015) descrevem que uma das situações em que o Espaço Cibernético permite uma exploração em um possível conflito cibernético — e talvez uma das mais importantes — é o fato de existirem falhas em *softwares* e *hardwares*. Esses dispositivos são feitos por muitas empresas distintas e não há como garantir a não ocorrência destas falhas durante o processo de fabricação. Em alguns casos, uma mesma empresa fabrica o hardware e o software que será instalado e utilizado em seus equipamentos, gerando uma dupla possibilidade de exploração por parte de um oponente.

Dessa forma, os autores descrevem, como exemplo, a fabricação de um equipamento no mercado estadunidense. A maioria dos notebooks é produzida por grandes empresas, tais como Dell, HP e a chinesa Lenovo. Apesar de as primeiras empresas serem norte-americanas, os seus componentes, e, em alguns casos, os códigos executados, podem ser elaborados em outros países, o que também ocorre com os *softwares.*

Como exemplo concreto dessas falhas, os autores apresentam o processo de produção e rastreio de um notebook Dell descrito pelo seu dono, Thomas Friedman, no livro "O Mundo é Plano", em que o escritor relata que a cadeia de fornecimento do notebook envolveu, aproximadamente, 400 empresas, localizadas nos EUA, Europa e na Ásia.

O início do seu pedido foi feito pelo telefone, e a atendente se encontrava na Índia. O notebook teve o seu projeto executado pela equipe de engenheiros da Dell, em Austin, no Texas, e foi montado na fábrica de Penang, na Malásia. Os componentes foram fabricados em diversos países, tais como: Taiwan, Filipinas, Costa Rica, República Popular da China, Coreia do Sul, Alemanha, Japão, Singapura e Tailândia.

---

2 Código malicioso que, frequentemente, está disfarçado de um programa legítimo. Ele pode ser empregado por criminosos virtuais para obter acesso aos sistemas dos usuários. Executa tarefas além das que foi projetado, sem o conhecimento do usuário (BRASIL, 2019b).

Após a montagem desses componentes, foi gravado o Sistema Operacional (SO) *Windows* no disco rígido. Este *software* é apontado por Clark e Knake (2015) como tendo, aproximadamente, 40 milhões de linhas de código, sendo escrito em vários locais pelo mundo.

Diante desse detalhamento, em função de uma falha intencional ou não, dentro de toda a cadeia logística de montagem e da instalação dos programas, poderia ocorrer um Ataque à Cadeia de Suprimentos. Os países que viessem a adquirir esses equipamentos poderiam se tornar alvo desse ataque.

Citando um exemplo recente de Ataque à Cadeia de Suprimentos, tem-se o caso da SolarWinds. Esta empresa estadunidense desenvolve programas para gerenciamento e monitoramento de infraestrutura de redes. Considerada uma grande empresa de Tecnologia da Informação dos EUA, ela foi alvo, no final de 2020, de um ataque cibernético que se espalhou para os seus clientes (PETRY, 2021).

O objetivo dos atacantes era entrar na rede de clientes da empresa e, com isso, atingir os clientes desses clientes, criando uma grande cadeia de espionagem. Dentro da rede das vítimas, o programa malicioso começou a se comunicar com o servidor de comando e controle, dando início ao segundo estágio do ataque: a implantação de outros códigos maliciosos, como um ataque por negação de serviço, em que se tenta tornar um recurso do computador indisponível, inundando sua rede com solicitações e dados (PETRY, 2021).

Nesse ataque, foi possível observar o quão sofisticado foram as técnicas utilizadas para a sua efetivação, as quais envolveram, como alvo, várias empresas e órgãos do governo, incluindo clientes militares.

Muitas das empresas ou órgãos do Brasil, inclusive a MB, utilizam *softwares* e *hardwares* adquiridos de outros países, pois dificilmente se constrói toda a tecnologia a partir do zero, sendo necessário, então, buscá-las em outros Estados parceiros. Como há a necessidade dessas aquisições, há também um risco considerável associado a essa prática, pois, como citado, códigos maliciosos podem estar incorporados.

Assim sendo, cada equipamento e dispositivo adquirido e cada aplicativo utilizado precisam ser verificados e monitorados quanto a possíveis riscos de segurança. É com esse objetivo que se vislumbra a necessidade de normatização, preparo e maior conscientização sobre um possível Ataque à Cadeia de Suprimentos proveniente desses produtos ofertados e as suas consequências para a MB.

2.2 O contexto cibernético da Cadeia de Suprimentos na APF

A preocupação com aspectos relacionados à soberania nacional tem crescido no Brasil, como uma nação que tem se destacado em níveis de influência mundial. Nesse contexto, o avanço da tecnologia brasileira, em suas mais diversificadas áreas, inclui a crescente preocupação com a segurança cibernética, hoje, um assunto discutido em nível global (BRASIL, 2020f).

A possibilidade de ser alvo de um ataque cibernético de origens das mais diversas e que pode causar danos consideráveis a estruturas estratégicas ou mesmo a setores importantes e vitais para a nação brasileira, faz com que a Defesa Cibernética passe a ter papel fundamental para a Defesa Nacional (BRASIL, 2020g).

Observa-se um aumento do risco da efetivação de ataques pelos Estados, com os mais diversos motivos, sejam eles de ordem econômica, tecnológica ou miliar. Nesse contexto, a Defesa Cibernética vem se firmando como de valiosa importância para o resultado satisfatório das operações militares em todos os escalões de comando, protegendo suas infraestruturas contra um ataque externo (BRASIL, 2014a).

Em uma conjuntura mundial de incertezas e ameaças, assim como pela existência de novos participantes nos cenários de conflito, a sociedade brasileira deverá estar preparada para esse possível enfrentamento. Para isso, medidas deverão ser adotadas para capacitá-la a responder de forma oportuna e adequada, antecipando-se aos possíveis cenários adversos à Defesa Nacional.

O Ministério da Defesa (MD) e as FA têm atuado de forma ativa nas áreas de Segurança da Informação e Comunicações (SIC), Segurança Cibernética e Defesa Cibernética. Nesse cenário, normas e doutrinas têm sido elaboradas, a fim de garantir um adequado tratamento a possíveis conflitos no Espaço Cibernético.

No ano de 2014, foi aprovada a Doutrina Militar de Defesa Cibernética, que tem como objetivo proporcionar uma normatização sobre esse assunto no âmbito do MD, para uma adequada atuação conjunta das FA no ambiente cibernético. Essa doutrina define, ainda, que, a partir do estabelecimento do Setor Cibernético, decorrente da aprovação da END, dois campos distintos passaram a ser reconhecidos: a Segurança Cibernética, a cargo da Presidência da República; e a Defesa Cibernética, a cargo do MD, por meio das FA.

Considerando que a Defesa Cibernética envolve aspectos da soberania nacional, especial atenção deve ser dada ao tema, nos mais altos níveis político-estratégicos. Assim, o próprio poder público terá condições mínimas e recursos para conduzir ações necessárias à proteção cibernética nacional e garantir que toda a sociedade possa usufruir dos benefícios que a Internet e os sistemas computacionais podem oferecer.

Ressalta-se que é responsabilidade de cada FA a adoção de medidas de proteção e de Defesa Cibernética dos seus respectivos ativos de informação. Assim, cada uma deve dispor de mecanismos próprios de defesa para as suas respectivas infraestruturas críticas; além de ter um preparo adequado e condições de evitar um possível ataque cibernético, sabotagem ou atos de espionagem, a fim de manter a soberania nacional (BRASIL, 2014a).

A PND, outro documento que destaca a importância da Defesa do Espaço Cibernético, descreve a necessidade do Brasil de reunir capacidades a nível nacional, com o objetivo de desenvolver condições que garantam a soberania do País, sua integridade e a consecução dos objetivos nacionais (BRASIL, 2020h).

No documento, são definidos fundamentos, de âmbito nacional e internacional, sobre a necessidade de se priorizar ações estratégicas que envolvam conflitos cibernéticos. Assim, deve-se dar atenção para a defesa do Espaço Cibernético brasileiro, garantindo, de forma adequada, o funcionamento de sistemas de informações, o gerenciamento e as comunicações voltados para o interesse nacional. Dessa forma, tenta-se evitar acessos indesejados e bloqueios ao tráfego de informações, que, em caso de ataque, poderiam expor ou paralisar atividades ou operações de grande importância para instituições brasileiras, inclusive militares.

A fim de orientar os segmentos do Estado brasileiro quanto ao cumprimento dos Objetivos Nacionais de Defesa relacionados na PND, foi elaborada a Estratégia Nacional de Defesa. Com fundamentos na PND, a END define as estratégias que servirão de guia para que a sociedade brasileira execute ações de defesa da Pátria.

Na END, no âmbito cibernético, são relacionadas as Ações Estratégicas de Defesa[3] para desenvolver os setores estratégicos de defesa cibernética, as capacidades de monitorar o espaço cibernético, as capacidades de defender e de explorar o Espaço Cibernético e o desenvolvimento da tecnologia cibernética (BRASIL, 2020f).

Em função da necessidade de se criar um documento normativo sobre segurança cibernética, foi aprovada, no ano de 2020, a Estratégia Nacional de Segurança Cibernética (ENSC), sendo elaborada com o objetivo de abordar aspectos relacionados à segurança cibernética, defesa cibernética, segurança das infraestruturas críticas, segurança da informação sigilosa e à proteção contra vazamento de dados.

Destaca-se, aqui, que a ENSC foi o primeiro módulo da Estratégia Nacional de Segurança da Informação a ser elaborado, conforme previsto no Decreto nº 9.637, de 26 de

3 Têm por objetivo orientar ações a serem executadas na consecução dos Objetivos Nacionais de Defesa. Podem contribuir para mais de uma Estratégia de Defesa, podendo ser de mesma natureza ou de naturezas ou distintas (BRASIL, 2020f).

dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação e que dispõe sobre princípios, objetivos, instrumentos, atribuições e competências de segurança da informação para os órgãos e entidades da APF.

Ao se analisar a ENSC, no que tange à segurança cibernética, observa-se que foram definidos três objetivos estratégicos: tornar o Brasil mais próspero e confiável no ambiente digital; aumentar a resiliência brasileira às ameaças cibernéticas; e fortalecer a atuação brasileira em segurança cibernética no cenário internacional (BRASIL, 2020a).

Em relação aos objetivos estratégicos apresentados na ENSC, foram estabelecidas dez ações estratégicas. Dentre essas dez ações, no contexto de uma proteção contra o Ataque à Cadeia de Suprimentos, é possível identificar aquelas que envolvam ações relacionadas a esse tema. Como a inclusão, nas políticas de segurança cibernética, de requisitos relacionados à gestão da cadeia de suprimentos e de monitoramento da inclusão de requisitos de segurança cibernética pelos fornecedores que participam da cadeia de suprimentos (BRASIL, 2020a).

Um outro aspecto a ser considerado se refere à proteção cibernética das empresas que representam as infraestruturas críticas. Para melhor entendimento, pode-se conceituá-las como instalações, serviços e bens que, caso haja alguma interrupção ou destruição, provocarão impactos sociais, econômicos, políticos ou de segurança nacional. Assim, existe a necessidade de que essas empresas mantenham ações voltadas para a segurança cibernética, a fim de mitigar as ameaças (BRASIL, 2020a).

Analisando os documentos normativos citados, conclui-se que requisitos voltados para a segurança cibernética têm sido contemplados e especificados, de forma a serem implementadas ações que preservem a soberania nacional em um provável conflito cibernético. Em especial, o Ataque à Cadeia de Suprimentos vem sendo objeto de preocupação nesse cenário. Aspectos voltados para mitigar esse tipo de ataque começaram a ser descritos, a fim de que sejam cumpridos procedimentos para a proteção de infraestruturas críticas.

Em função da importância e para uma melhor exemplificação de um Ataque à Cadeia de Suprimentos, suas causas e efeitos, será apresentado, na próxima seção, um caso desse tipo de ataque, que ocorreu nas usinas nucleares iranianas localizadas em Natanz, por meio de um código malicioso denominado *Stuxnet*, no ano de 2010.

3 ATAQUE À CADEIA DE SUPRIMENTOS, O CASO ENVOLVENDO O *STUXNET*

Essa seção tem o propósito de apresentar o exemplo de um ataque cibernético, que utilizou uma arma digital, para explorar as vulnerabilidades da cadeia de suprimentos e atingir o seu objetivo.

Serão descritas as etapas que foram seguidas, suas consequências, as vulnerabilidades encontradas e o resultado obtido por meio dessas fragilidades. Além disso, serão identificadas lições aprendidas e aspectos importantes, que devem ser observados para que se evite, ou, pelo menos, minimize, as consequências desse tipo de ataque.

O exemplo escolhido para demonstrar um caso real envolvendo um Ataque à Cadeia de Suprimentos aconteceu no ano de 2010, quando um código malicioso conseguiu se infiltrar no sistema de centrífugas de enriquecimento de urânio de um programa nuclear iraniano, desenvolvido na instalação de Natanz, cidade do Irã.

Esse caso ficou mundialmente conhecido e ainda é objeto de estudo de vários trabalhos que envolvem temas relacionados à Segurança da Informação, Ataques e Segurança Cibernética. Este caso, que aqui será analisado, foi o ataque realizado pelo *worm*[4] denominado *Stuxnet*.

Destaca-se, como uma característica diferenciada dessa ação, que esse ataque utilizou técnicas e conceito voltados para uma arma cibernética cinética[5], o que significa que possibilitou que ocorresse um efeito cinético, ou seja, atingiu algo, pessoas ou material, no mundo real.

Esse conceito, de efeito cinético, é descrito nos princípios que foram propostos por Parks e Duggan (2011, p. 31), os quais definem que, para uma guerra cibernética ter um verdadeiro sentido, ela deve afetar direta ou indiretamente algo no mundo real.

O *Stuxnet* foi considerado um caso prático em que uma arma digital possibilitou atingir, de forma direta, o mundo físico, realizando os mesmos objetivos de ataques realizados com armas cinéticas, tal qual um míssil (SÁ; MACHADO; ALMEIDA, 2019, p. 97).

Além disso, também foi considerado a primeira arma digital mundial que possibilitou anunciar uma nova era da guerra digital, em função de suas funcionalidades e

---

4 *Worm* é um programa malicioso auto-replicante que possui a capacidade de se propagar automaticamente para vários computadores., independente de ação humana. Pode atingir uma grande quantidade de alvos de forma rápida.

5 O conceito de arma cibernética cinética é aquele em que programas ou equipamentos são projetados ou possuem capacidade de causar danos físicos, direta ou indiretamente, tanto em pessoas como em equipamentos, por meio de uma exploração de vulnerabilidades dos sistemas e processos de informação (BRASIL, 2019b).

sofisticada capacidade de ataque, o que o distinguiu como tendo características únicas (ZETTER, 2017, p. 3).

3.1 O objetivo do ataque

O contexto para o desencadeamento desse ataque ocorreu quando o Irã iniciava o enriquecimento de urânio na instalação piloto de Natanz, no início do ano de 2007. Essa instalação começou a ser construída, de forma secreta, no ano de 2002. Sua construção constituía violações aos acordos de salvaguarda com a Agência Internacional de Energia Atômica (AIEA), que obrigavam o Irã a declarar suas atividades relacionadas ao seu programa nuclear[6]. A revelação da existência de Natanz causou grande temor e desentendimentos no cenário internacional, pois o fato de este centro nuclear desenvolver suas atividades em segredo, tornou-se elemento essencial para o entendimento de que o Irã elaborava seu programa nuclear com finalidades militares (ZETTER, 2017).

O ambiente de dúvidas, sobre o que realmente era desenvolvido na usina de Natanz, foi foco de grande investigação internacional, e não era nenhum segredo que muitos países poderiam fazer qualquer coisa para eliminar o seu programa nuclear. Na realidade, os iranianos estavam tentando fazer isso há quase uma década, já que o seu programa nuclear vinha sendo objeto de investigação por vários anos (ZETTER, 2017, p. 33).

Considerando cenário em que o programa nuclear era desenvolvido, ainda com dúvidas sobre o que efetivamente ocorria, foi vislumbrada a possibilidade de utilização de uma arma cibernética que neutralizasse o avanço dos projetos nucleares iranianos. Sendo assim, esse artefato cibernético foi desenvolvido para causar danos físicos em outro Estado; sendo considerado um ataque cibernético cinético.

3.2 O cenário para o início do desenvolvimento do *Stuxnet*

O período em que se iniciou o desenvolvimento do *Stuxnet* ainda é desconhecido. Acredita-se que tenha sido no ano de 2006, após o Irã suspender o seu acordo de enriquecimento de urânio e iniciar a instalação das primeiras centrífugas em salas subterrâneas na usina de Natanz. A partir daquele momento, as discussões sobre um possível ataque ficaram mais acentuadas (ZETTER, 2017, p. 189).

Foi nesse momento que militares estadunidenses supostamente levaram ao conhecimento do presidente dos EUA, George Walker Bush, a proposta de uma

6 O Irã participava do tratado de não proliferação de armas nucleares e estava obrigado a divulgar informações sobre a existência de qualquer nova instalação nuclear antes da introdução de material nuclear no local, possibilitando que os inspetores pudessem começar seu monitoramento (ZETTER, 2017, p. 36).

ciberoperação, que foi posteriormente denominada “Jogos Olímpicos”. As possibilidades para um ataque já vinham sendo objeto de estudo do presidente americano, mas, em função das duas operações em execução, no Iraque e no Afeganistão, havia a decisão para que não se iniciasse uma outra batalha no Oriente Médio. Então, seus assessores fizeram a proposta de desenvolver um destruidor de *bunker* que pudesse proporcionar resultados satisfatórios, similares aos cinéticos, sem o desgaste e as consequências desses outros ataques (ZETTER, 2017, p. 190).

A proposta da ciberoperação foi considerada uma boa alternativa no cenário em questão. A operação consistia no planejamento de um ataque cibernético, o que seria mais seguro do que o bombardeamento para penetrar concreto reforçado, por Forças Aéreas, proposto por Israel (CLARK; KNAKE, 2015, p. 229).

Assim, a operação foi autorizada; no entanto, ela somente deveria ser empregada caso houvesse requisitos que possibilitassem a garantia de que a sua execução atrasaria o programa nuclear iraniano sem causar danos colaterais ou chamar atenção. Além disso, ela não poderia prejudicar o funcionamento de outros sistemas não relacionados ao programa nuclear (ZETTER, 2017, p. 191).

O estudo dos equipamentos iranianos, feito por informantes israelenses, os especialistas em computação e física nuclear dos EUA e de Israel tinha como objetivo a paralisação das centrífugas, de forma a aparentar um acidente qualquer, sem gerar nenhuma desconfiança de ataque cibernético nos engenheiros iranianos (CLARK; KNAKE, 2015, p. 231).

Assim, o programa de desenvolvimento do *Stuxnet* foi iniciado, sem se saber ao certo o que ele traria como consequência ao ser ativado, mas como uma solução viável para o objetivo de destruir ou retardar os projetos nucleares do Irã.

A ideia era muito interessante e seu conceito bem avançado, pois, por meio de um artefato digital, seria possível alcançar os mesmos efeitos de uma arma cinética, sem, no entanto, expor vidas em um conflito armado; além da possibilidade de desenvolvê-lo e efetuar sua execução de forma secreta.

3.3 Objetivo do ataque

De acordo com Karnouskos (2011), o objetivo do *worm Stuxnet* era realizar um ataque ao sistema de controle industrial da empresa Siemens[7], conhecido como

7 Empresa alemã proprietária dos sistemas de controle industrial, projetados para trabalhar com os Controladores Lógicos Programáveis — PLC (ZETTER, 2017).

SCADA[8]. Seu alvo seriam os SCADA que foram projetados para utilizar PLC[9]. Os programas alvos, Siemens WinCC[10] / Step 7[11], programas de controle do SCADA, executados em ambiente *Windows*, eram, então, infectados ao interceptar suas comunicações.

Esses programas estavam instalados em estruturas críticas em todo o mundo, inclusive no sistema de controle das centrífugas da usina nuclear de Natanz; mas o objetivo do ataque eram os fornecedores específicos desses sistemas PLC, ou seja, vindos da Vacon (vendedor finlandês) e da Fararo Paya (Irã). Com a interceptação e as informações obtidas, o ataque poderia ser feito (ZETTER, 2017, p. 217-229).

Assim como nas outras etapas, essa fase de execução deveria ser a mais precisa possível, pois não haveria margem para nenhum tipo de erro. O *Stuxnet,* ao iniciar o seu ataque, coletava as informações de funcionamento das centrífugas. Após essa análise, decidia o procedimento a ser seguido para alterar a forma de funcionamento desses equipamentos, com o objetivo de destruí-los. Ele fechava válvulas para aumentar a pressão no interior das centrífugas e, quando se atingia cinco vezes o nível normal, o gás de urânio, no interior das centrífugas, condensava e se solidificava. Conforme o sólido resultante ficava preso no rotor da centrífuga girando, ele o danificaria ou permitiria que ficasse desbalanceado e colidisse com a parede da centrífuga, causando, como consequência, a sua destruição. Além disso, o programa passava informações incorretas ao operador do sistema, a fim de evitar uma ação corretiva (ZETTER, 2017, p. 230).

Assim, interferindo no funcionamento das centrífugas, o *Stuxnet* agia para danificar os seus alvos, objetivo da operação e de seu ataque. Dessa forma, conclui-se que o objetivo foi atingido, pois houve a interferência planejada por seus idealizadores.

3.4 Forma de ataque e vulnerabilidades encontradas

O *Stuxnet* teve uma grande repercussão e difusão. Conforme citado, seu surgimento ocorreu pela preocupação que existia sobre a questão do avanço do desenvolvimento do programa nuclear iraniano, suas reais intenções e pela necessidade de se evitar ou retardar esse avanço. Acredita-se que o desenvolvimento desse *worm,* altamente

8 SCADA, Supervisory Control and Data Acquisition [controle de supervisão e aquisição de dados] — são sistemas de controle industrial geralmente utilizados quando os sistemas gerenciados estão geograficamente dispersos sobre grandes áreas — como em oleodutos, sistemas ferroviários e distribuição de água e energia elétrica (ZETTER, 2017).

9 Programmable Logic Controllers (PLCs) [Controladores Lógicos Programáveis] — são pequenos computadores que são utilizados em fábricas ao redor do mundo para controlar coisas como os braços de um robô ou esteiras de transporte em linhas de montagem. (ZETTER, 2017).

10 Ferramenta de visualização utilizada para monitorar os PLC e os processos que eles controlam (ZETTER, 2017).

11 Aplicação proprietária da Siemens para a programação de sua linha de PLC.

sofisticado, foi um esforço conjunto com especialistas de diferentes formações e um grande investimento em tempo e custo (ZETTER, 2017, p. 353).

Após sua descoberta, por volta do ano de 2010, foram feitas análises em seu código, a fim de descobrir o que realmente esse *worm* tinha como alvo e quais ações pretendia executar. Essa análise foi realizada por empresas especializadas em segurança da informação, tal como a Symantec. A partir da análise do seu código, foi possível identificar a sua forma de atuação, o que possibilitou um estudo mais aprofundado sobre essa arma digital (LOPES, OLIVEIRA, 2014, p. 60).

Ao analisar a forma como ele foi desenvolvido, identificou-se, inicialmente, que o *Stuxnet* tinha uma grande semelhança com o sistema de um míssil. A porção míssil era responsável por espalhar o *Stuxnet*, já a outra parte era focada na carga que continha parte do código que afetava o sistema da Siemens, que era utilizado no sistema das centrífugas. Carregava consigo ogivas para a efetivação do ataque, quando identificasse seu alvo, no caso, os PLC das usinas iranianas (ZETTER, 2017, p. 225).

Foi identificado, também, que a forma de propagação, para atingir seu alvo, não teria equipamentos conectados à Internet, impossibilitando sua infecção pelo meio tradicional, que seria pelo correio eletrônico ou execução direta de código malicioso pela Internet. A sua propagação deveria ser por meio de dispositivos de *pendrive,* sendo sua condução realizada por pessoas que faziam o seu transporte até o destino final. Assim atenderia aos requisitos impostos de sigilo da operação e o de não proliferação em cascata para outros sistemas (ZETTER, 2017, p. 92).

Após a infecção do equipamento, uma técnica bem projetada era utilizada para a sua autopropagação. Com o objetivo de não ser identificado, o *Stuxnet* utilizava um *software* bem elaborado, denominado *rootkit,* que permitia ficar oculto e não ser identificado por programas identificadores de códigos maliciosos, como, por exemplo, um antivírus. Ele identificava adequadamente todos os antivírus e adaptava-se a cada um deles, com o objetivo de não ser descoberto. Caso não fosse possível se adaptar e ficar oculto, o *Stuxnet* interrompia suas funcionalidades e desligava-se. Além disso, nesta autopropagação, ele utilizava um *exploit*[12] *zero day*[13], que atacava as funções essenciais do SO *Windows* (ZETTER, 2017, p. 60).

---

12 *Exploit [explorador]* — Programa de ataque utilizado para instalar códigos maliciosos em equipamentos, aproveitando-se de falhas identificadas em seus aplicativos (ZETTER, 2017).

13 *Exploit zero day [explorador dia zero]* — Tipo de *exploits* com uma propriedade mais avançada, pois atuam em falhas desconhecidas pelos fabricantes ou desenvolvedores do próprio *software.* Isso permite entender que, momentaneamente, não há correções para detectar tal *exploit* e tampouco atualizações disponíveis para reparar as vulnerabilidades que possibilitam o seu ataque. Sendo assim, os *exploits zero day* dificilmente são encontrados ou identificados (ZETTER, 2017).

Além do uso do *exploit zero day*, outras técnicas de propagação, em um total de 8 (oito), foram utilizadas pelo *Stuxnet.* Assim, percebe-se que esse *worm* pode ser propagado de forma abrangente e eficaz, identificando seu alvo conforme o andamento de sua propagação. Em uma dessas técnicas de propagação, utilizada pelo *Stuxnet*, foi feito uso de certificados digitais subtraídos de empresas. Esses certificados são recursos de segurança confiáveis utilizados por fabricantes de software para assiná-los, a fim de garanti-los como produtos legítimos. De posse desses certificados de autenticidade, o *Stuxnet* não era detectado como código malicioso ao ser instalado nos sistemas (FALLIERE; O'MURCHU; CHIEN, 2010).

Outra forma de propagação foi efetivada ao infectar os arquivos de projetos utilizados para programar as PCL, obtendo as credenciais de acesso, nome de usuário e senha, que a Siemens incluía neles. Era uma senha de fábrica, para que os sistemas funcionassem automaticamente, sem a necessidade de informá-las a cada operação. De posse dessas credenciais, o *Stuxnet* aproveitava esta vulnerabilidade para controlar o acesso a um banco de dados de projeto, acessado por programadores, e injetava o seu código, que era, dessa forma, compartilhado por estes especialistas, afetando, assim, a cadeia de suprimentos do projeto (ZETTER, 2017, p. 91).

O *Stuxnet* também utilizou a cadeia de suprimentos para efetivar o seu ataque, ao interceptar comandos passados de um arquivo de biblioteca dinâmica para os PLC. Ele descriptografava e analisava este aquivo de biblioteca e substituía o seu conteúdo por seus próprios comandos. Assim, possibilitava que a PLC tivesse o seu código alterado. As PLC então conectadas às estações de monitoramento ficavam em constante comunicação com as máquinas, transmitindo informações sobre a situação de funcionamento, nesse caso, com o código embutido pelo *Stuxnet*, o que permitia transmitir falsas informações (ZETTER, 2017, p. 174).

Com o avançar das descobertas, pode-se identificar, ainda, que o *Stuxnet* impressionava por seu poder de destruição e que era parte de uma grande operação de espionagem cibernética, que tinha dimensões maiores que uma única arma digital (ZETTER, 2017, p. 271).

Dentre essas descobertas, foi identificado um conjunto de ferramentas de espionagem, apelidado de "*Flame*". Ao analisar o *Flame,* descobriu-se uma outra forma de Ataque à Cadeia de Suprimentos, pois ele realizava um tipo sofisticado de ataque ao sistema de atualizações do SO *Windows*, o *Update* da *Microsoft,* para que pudesse, dessa forma, propagar-se entre as máquinas de uma rede local. Esse fato ocorre em razão de que todas as atualizações e correções de código e de segurança para o *Windows* são obtidas neste

repositório, e, caso ele venha a ser comprometido, ele pode infectar todos os equipamentos que lá buscaram suas atualizações (ZETTER, 2017, p. 281).

Dentre os fatos apresentados, pode-se observar que as características do *Stuxnet*, em relação à sua forma de propagação e ataque, foram muito bem elaboradas, o que permitiu considerá-lo uma arma cibernética inovadora. Utilizou-se de técnicas avançadas de programação para que o código malicioso do *worm* atingisse o seu objetivo. O objetivo de atingir infraestruturas críticas foi conseguido. As centrífugas da usina de Natanz foram afetadas e o que se viu foi um avanço em conceito de ataque cibernético, que, nesse caso, teve um efeito cinético.

3.5 Aspectos a serem observados

Entende-se que o *Stuxnet* deixou um legado no contexto em que se discute as possibilidades de utilização de armas digitas, em uma época de conflitos cibernéticos. Seu conceito inovador possibilitou que se demonstrasse que vulnerabilidades, até então desconhecidas, podem ser exploradas em um ataque cibernético, incluindo ambientes militares em uma época de conflitos.

Dentre essas vulnerabilidades, podem ser destacadas: a exploração de *exploits zero-day*, que exploram vulnerabilidades desconhecidas pelos fabricantes do equipamento ou *software*; a propagação de códigos maliciosos, mesmo sem o uso da Internet ou conexão em rede; possibilidade de provocar danos físicos a alvos de ataque; Ataque à Cadeia de Suprimentos, permitindo que clientes recebam artefatos contaminados em seus produtos.

Observa-se, ainda, a possibilidade de ataque a um SO, que é utilizado mundialmente, como um ponto de grande preocupação. Ao utilizar a cadeia de suprimentos, nesse caso, o sistema de atualizações do *Windows (Microsoft Update)*, como meio de ataque, pode-se expor vários equipamentos, que buscam suas atualizações, a códigos maliciosos. Sistemas críticos de vários setores essenciais da sociedade utilizam o SO *Windows*. Até em meios militares esta plataforma ainda é utilizada, inclusive com versões descontinuadas pelo fabricante. A Marinha dos EUA, por exemplo, já manifestou que as aplicações da *Microsoft* afetam ferramentas importantes de comando e controle em sistemas legados, tanto em navios quanto nas operações de terra, o que possibilita a existência de vulnerabilidades que podem ser exploradas em ataques cibernéticos.

Em matéria datada do ano de 2014, o chefe do Naval Sea Systems Command (NAVSEA), Vice Almirante William Hilarides, alertou sobre a ameaça ao sistema de comando e controle de seus submarinos, uma vez que um chip de computador que controlava

o mecanismo do motor do submarino funcionava com SO *Windows*; sendo que esse chip interligava outras partes do navio, recebendo e enviando informações por uma rede não segura. Dessa forma, pela vulnerabilidade identificada, um ataque poderia causar sérios danos ao submarino (MAMJADUR, 2014).

Durante o ataque do *Stuxnet* foram atingidos equipamentos em diversos países, conforme consta no relatório elaborado pela empresa Symantec, que foi a responsável por investigar e analisar em detalhes o código do *Stuxnet*. O Brasil aparece como um dos países que tiveram equipamentos infectados, tendo o Irã como o país mais afetado, com um total de, aproximadamente, 60.000 infecções (FALLIERI; O'MURCH; CHIEN, 2010).

Uma das consequências mais duradouras do *Stuxnet*, que deve ser considerada, em relação aos seus conceitos e características, foi a possibilidade de a utilização de códigos maliciosos, como armas digitais, terem gerado uma espécie de corrida armamentista digital entre países, o que poderá alterar o contexto e o panorama dos conflitos cibernéticos.

Sendo assim, será descrito, na próxima seção, o que vem sendo desenvolvido no âmbito da MB, no que se refere às ações voltadas para a defesa do Espaço Cibernético, com alguns aspectos que contemplam o Ataque à Cadeia de Suprimentos, tema desse trabalho. Aspectos normativos, de preparo, de capacitação e outros relevantes, a fim possibilitar um adequado preparo dos navios da MB para a época de incremento dos conflitos cibernéticos.

4 O ENFRENTAMENTO DOS CONFLITOS CIBERNÉTICOS NA MB

Conforme descrito nas seções anteriores, pode-se concluir que um Ataque à Cadeia de Suprimentos é uma ação, que ocorre no ambiente cibernético, que merece especial atenção dos agentes envolvidos na proteção do Espaço Cibernético, possibilitando que se garanta, dessa forma, a soberania nacional e a preservação das infraestruturas críticas das instituições públicas ou privadas.

Entende-se que, dentro do contexto de políticas, doutrinas e normas estabelecidas para que se desenvolvam ações de defesa do Espaço Cibernético, conforme mencionado na segunda seção, a ENSC tem um papel de destaque no que concerne às iniciativas, a serem desenvolvidas, voltadas à segurança cibernética da cadeia de suprimentos.

Conforme contido na ENSC, há a necessidade de se estabelecer políticas de SIC para os requisitos voltados à gestão da cadeia de suprimentos. Essas políticas devem ser monitoradas continuamente, tanto pelos órgãos contratantes quanto pelas empresas fornecedoras de produtos e serviços.

No exemplo que foi abordado na terceira seção, o ataque realizado pelo *Stuxnet,* demonstrou-se que não há lugar tão seguro que não possa ser atingido por algum código malicioso. Outrossim, nesse ataque, pode-se observar que, além de provocar danos no funcionamento de sistemas e equipamentos, há a possibilidade de se causar danos cinéticos, ou seja, atingir o mundo real, provocando destruição material.

Diante das vulnerabilidades encontradas, o *Stuxnet* avançou, e pôde deteriorar os sistemas em que foi instalado. Essas vulnerabilidades foram provocadas tanto por pessoas quanto por brechas, identificadas durante o seu ataque.

A partir do que foi visto, no exemplo do *Stuxnet*, depreende-se que o previsto na ENSC e nos outros documentos normativos e doutrinas, como a PND, END e a Doutrina Militar de Defesa Cibernética, devem ser abordados em cada FA de forma ampla e concreta.

A questão da existência de vulnerabilidades ou falhas em equipamentos ou sistemas de infraestruturas críticas, de comunicações, ou mesmo de armas gera uma certa preocupação, no meio militar, sobre o que efetivamente pode ser alvo de um suporto ataque cibernético.

Por esse motivo, é necessário o estabelecimento de um adequado programa de ações voltadas para a proteção da cadeia de suprimentos de itens fornecidos aos meios navais da MB, a fim de evitar que um ataque originado em uma falha de algum item impossibilite o seu correto uso em época de conflito.

A importância desse tema decorre da atual situação em que a MB se encontra, com o desenvolvimento de vários programas estratégicos que envolvem importantes projetos. O objetivo é proporcionar, ao País, uma Força Naval adaptada à nossa realidade e capaz de defender a Pátria, salvaguardando os interesses nacionais, atendendo às expectativas da sociedade (BRASIL, 2020d).

Dentre esses projetos, de grande relevância para a MB, pode-se citar o PCT, que tem como objetivo renovar a Esquadra com modernos navios de grande capacidade tecnológica. Nesse programa, serão construídos, inicialmente, 4 (quatro) navios de alto poder de combate (BRASIL, 2020e).

Em apresentação, realizada no ano de 2019, sobre a composição dos sistemas que possivelmente serão utilizados nos navios, pôde-se perceber a grandeza do PCT e seus benefícios para a MB. No entanto, pela diversidade e complexidade desses sistemas, a MB deve manter o contínuo controle e gerenciamento destas aquisições (BRASIL, 2019c).

Analisando-se as possibilidades de fornecimento de itens para o PCT, conclui-se que vários países participarão da cadeia de suprimentos, provendo equipamentos que

comporão os vários sistemas que serão utilizados, tais como os de armamento, de sensores e de comunicações, conforme apresentado na FIG. 1 do ANEXO. Como exemplo, há previsão de que seu sistema de sensores seja dotado de equipamentos cujos fornecedores estão sediados em países como:

- EUA - Radar Busca de superfície1 Raytheon[14] (Banda S) e Radares de Navegação[15] Raytheon (Banda X);
- França - Alças Optrônicas: Safran Paseo XLR e Radar de Direção de Tiro (DT)[16] : Thales STIR 1.2 EO MK2;
- Alemanha - Sonar[17] de Casco: ATLAS Elektronik ASO 713;
- Espanha - MAGE: Indra Rigel;
- Inglaterra - Radar 3D: BAE ARTISAN 3D.

Pela observação desse pequeno exemplo de países que farão parte da cadeia de suprimentos do PCT, conclui-se que existe a necessidade de se utilizar todos os meios necessários para preservar esse programa de tão grande relevância para a MB e para o interesse nacional.

Um código malicioso, que venha a ser instalado em um desses sistemas e equipamentos, pode proporcionar uma degradação ou falha em seu funcionamento ou mesmo na integração com outros sistemas, em uma época de conflito em que a MB possa vir a participar.

No estudo de caso apresentado, relacionado ao *Stuxnet*, pode-se concluir que existe a possibilidade de um efeito cinético causado por um ataque cibernético. Em uma análise sobre as possibilidades de aquisição, em diversos países, de equipamentos para os meios da MB, foi verificado que, diante do apresentado, esse tipo de ataque pode comprometer esses equipamentos, causando, assim, o seu mau funcionamento. A instalação de um *worm* durante a fabricação ou no momento de atualização de algum sistema, pode comprometer toda a cadeia de suprimentos, fato que ocorreu no caso apresentado.

4.1 Normatização

Dentro do contexto normativo, o Plano Estratégico da MB (PEM) é o documento em que são apresentados os elementos doutrinários de mais alto nível da MB, assim como as

14 Detecta alvos de superfície e determina suas distâncias e marcações. Além disso, pode fornecer informações para navegação (MIGUENS, 2019).
15 Possibilita determinar a posição do navio na execução da navegação (MIGUENS, 2019).
16 Utilizado para orientação das armas do navio (MIGUENS, 2019).
17 Utilizado para detectar e localizar objetos submersos na água por meio das ondas sonoras que os alvos refletem ou produzem (MIGUENS, 2019).

suas Ações Estratégicas Navais (AEN). Alinhado com a PND e a END, ele descreve AEN necessárias ao alcance dos Objetivos Navais previstos na Política Naval (RODRIGUES, 2021).

Ao se analisar o PEM, percebe-se a importância dada à necessidade de se desenvolver ações voltadas para a defesa do Espaço Cibernético. Considera-se de suma importância o enfrentamento de ameaças e vulnerabilidades encontradas no Espaço Cibernético, que estão em crescente desenvolvimento e que possibilitam a ocorrência de Ataques Cibernéticos às infraestruturas marítimas, podendo torná-las indisponíveis.

No caso específico da possibilidade de ocorrência de um Ataque à Cadeia de Suprimentos, o PEM prevê que as nossas infraestruturas críticas não estão imunes a ações cibernéticas criminosas que exploram e instalam programas maliciosos em sistemas ou implantam circuitos em equipamentos para um posterior acionamento, proporcionado a indisponibilidade desses sistemas e equipamentos (BRASIL, 2020d, p. 28).

Não foram encontradas Ações Estratégicas específicas, voltadas para o enfrentamento de um Ataque à Cadeia de Suprimentos; no entanto, o PEM prevê a Estratégia Naval "Defesa Cibernética" para o desenvolvimento da capacidade cibernética na MB, a fim de garantir que todas as OM, inclusive os meios navais, sejam protegidas contra quaisquer ações de agentes inimigos no campo cibernético, incluindo um Ataque à Cadeia de Suprimentos.

Em se tratando de desenvolvimento de Sistemas Digitais (SD)[18], pela própria MB ou por empresas contratadas, são previstos na DGMM-0540 (Normas de Tecnologia da Informação da Marinha) requisitos que deverão ser atendidos quando da sua aquisição ou desenvolvimento. Há procedimentos a serem seguidos por todo o ciclo de vida dos sistemas, passando pelas fases de planejamento, obtenção, produção, manutenção e desativação, o que permite um melhor gerenciamento durante todo o ciclo de vida desses sistemas (BRASIL, 2019a, p. 14-1).

No que se refere à fase de obtenção, há critérios a serem atendidos para que uma empresa ou fornecedor seja selecionado e contratado. Esta fase é de grande importância, pois é na seleção do fornecedor que deve ser realizada a verificação de sua capacidade técnica e definidos os requisitos de segurança a serem cumpridos.

18 São os sistemas que utilizam recursos de Tecnologia da Informação, efetuando o processamento de todo o ciclo da informação digital para apoiar o processo de tomada de decisão. São categorizados como Administrativos (projetados para apoio às atividades administrativas desenvolvidas na MB) ou Operativos (projetados para que sejam empregados nas operações navais ou em proveito delas) (BRASIL, 2019a).

Além disso, na contratação do serviço, é previsto, na DGMM-0540, o acompanhamento da implementação do produto, o que torna o processo mais transparente e permite que os códigos dos programas, a serem desenvolvidos pela contratante, possam ser inspecionados. Assim, caso haja, as ações maliciosas poderão ser identificadas antes de sua implantação na MB. Após essa fase de acompanhamento, sua homologação será avaliada por uma equipe designada pela Diretoria de Comunicações e Tecnologia da Informação da MB (DCTIM)[19], que avaliará os aspectos de segurança.

Em complemento ao previsto na DGMM-0540, há, ainda, documentos técnicos, elaborados pela DCTIM, em que são descritos os requisitos necessários a serem cumpridos, em relação à segurança dos SD. Nesse item, destaca-se a DCTIMBOTEC 31/002/2020 que define orientações sobre o processo de homologação de um SD, como também, aspectos de segurança necessários para o funcionamento desses sistemas (BRASIL, 2020b).

Ao serem cumpridos os procedimentos previstos na DGMM-0540 e em Boletins Técnicos da DCTIM, para a contratação ou desenvolvimento de SD, será possível a implantação dos requisitos de segurança, evitando que códigos maliciosos estejam presentes nesses sistemas.

Portanto, a proteção de SD contra ameaças cibernéticas requer uma ampla abordagem, focando no seu acompanhamento, na fase de desenvolvimento, priorizando a avaliação de riscos de ações cibernéticas adversas.

A importância de serem cumpridos os procedimentos previstos em normas e outros documentos condicionantes, elaborados pela MB, visa não somente a atender aos aspectos de segurança voltados para a proteção cibernética, mas também a cumprir o previsto na ENSC, no que tange à necessidade de serem estabelecidos requisitos mínimos de segurança cibernética nos contratos elaborados pelas entidades e órgãos da APF.

4.2 Capacitação de Pessoal

Um outro aspecto de grande relevância, voltado para o enfrentamento de conflitos cibernéticos, está relacionado à capacitação de pessoal. Nesse contexto, há a necessidade de se ter profissionais continuamente capacitados, a fim de que eles estejam preparados para um possível combate.

Em função da importância de uma adequada formação profissional, há a necessidade de serem desenvolvidos programas de capacitação destinados ao adequado

19 DCTIM — Órgão de Direção Especializada responsável pela condução da atividade de SIC e normatização dos procedimentos de gestão de SIC na MB.

aprimoramento dos recursos humanos, com o objetivo de fortalecimento da segurança cibernética na APF, em especial na MB.

Nesse contexto, as instituições devem se articular por meio de ações e parcerias com o setor privado, no País e no exterior, para o estímulo do desenvolvimento de massa crítica, vislumbrando, inclusive, a disponibilização de treinamentos relacionados à segurança cibernética, em plataformas virtuais (BRASIL, 2020a).

Assim, para o devido enfrentamento de ações cibernéticas adversas, a MB tem procurado manter seus militares e servidores capacitados, para, caso necessário, eles estejam em condições de realizar ações de defesa do Espaço Cibernético. A Política Naval estabeleceu o Objetivo Naval "Desenvolver a Capacidade Cibernética da MB", visando a que todas as OM da MB estejam protegidas contra quaisquer ações de agentes adversos no campo cibernético (BRASIL, 2019d).

Na MB, cursos voltados para a qualificação de pessoal na Área Cibernética têm sido disponibilizados por meio do Plano de Capacitação de Pessoal de Tecnologia da Informação e Comunicações da Marinha (PLACAPE-TIC). Por esse Plano, as ações de Planejamento, Controle e Execução são realizadas para os processos de elaboração dos Programas de Cursos da MB, necessários ao preparo do pessoal de Tecnologia da Informação e Comunicações (TIC), a fim de capacitá-los para o exercício de suas funções e adequado desempenho de suas atividades e projetos de interesse da MB (BRASIL, 2020c).

Em uma análise do PLACAPE-TIC, horizonte 2021-2027, foi verificado que há oferta de cursos, tanto em nível de Pós-Graduação quanto de Aperfeiçoamento, voltados para a área de Guerra e Defesa Cibernética. Essas vagas são disponibilizadas para militares, envolvendo Oficiais e Praças.

Além do PLACAPE-TIC, outra forma de disponibilidade de cursos, voltados para a capacitação técnica do pessoal da MB na área cibernética e da segurança da informação, tem sido ofertada pela Escola Nacional de Defesa Cibernética (ENaDCiber). Só no ano de 2021, foram ofertadas mais de 70 (setenta) vagas para formação nessas áreas, que foram preenchidas com pessoal que se encontra em setores responsáveis pela TI na MB, como a DCTIM, o Centro de Tecnologia da Informação da Marinha (CTIM) e os Centros Locais de Tecnologia da Informação (CLTI), cujos conhecimentos poderão ser empregados nas diversas OM, inclusive no apoio aos meios Operativos (BRASIL, 2021a).

Essa disponibilidade de cursos tem papel fundamental na área de Defesa Cibernética. Como citado, a MB tem que estar com o seu pessoal devidamente preparado para um período de conflito cibernético. Em relação ao tema desse trabalho — no caso, o Ataque à

Cadeia de Suprimentos —, provavelmente haja a necessidade de que sejam disponibilizadas vagas de formação em áreas que atendam esse tema específico, como, por exemplo, as que enfoquem Segurança de Sistemas Digitais Operativos ou Segurança Cibernética da Cadeia de Suprimentos.

4.3 Ações em andamento

Além da importância da capacitação de pessoal, abordada no item anterior, há outras ações que são desenvolvidas e que têm contribuído, de forma satisfatória, para que se eleve o nível de mentalidade de segurança do pessoal. Essa evolução tem permitido que os militares da MB estejam mais preparados para um possível enfrentamento, quando da ocorrência de um Ataque Cibernético.

Dentre as ações adotadas, destaca-se a participação dos militares em exercícios de Guerra Cibernética. A MB vem conduzindo, há alguns anos, esses exercícios, que objetivam encontrar vulnerabilidades que possam ser exploradas em um possível Ataque Cibernético, bem como elevar a mentalidade de segurança dos seus participantes.

Como exemplo, tem-se o exercício denominado “OCTOPUS”, que é realizado com a participação dos meios Operativos da MB. Esses exercícios nos meios Operativos objetivam a busca por vulnerabilidades que permitam a degradação do Sistema de Comando e Controle, assim como a realização de ações nos meios que compõem a Operação (BRASIL, 2021b).

A ENSC prevê que a realização de exercícios cibernéticos possibilite uma elevação do nível de proteção nas Infraestruturas Críticas Nacionais, sendo a sua execução de suma importância. Cita, ainda, que, em um cenário de ameaças cibernéticas, organizações podem sofrer o mesmo ataque, sendo necessário que as informações sobre o ocorrido, sobre o tratamento realizado e sobre as lições aprendidas sejam compartilhadas por todos (BRASIL 2020a).

A execução dos exercícios, além de possibilitar que os sistemas e pessoas, alvos desses exercícios, tenham as suas capacidades testadas, ela permite que as equipes envolvidas sejam devidamente treinadas em um ambiente controlado. Assim, elas terão suas habilidades colocadas em prática e serão preparadas para um real Ataque Cibernético.

Uma outra forma de se incrementar a mentalidade de segurança do pessoal da MB, são os adestramentos internos, com temas que enfoquem os conceitos de Guerra Cibernética e de Segurança da Informação. Todas as OM, incluindo os meios Operativos, devem manter e cumprir um plano de adestramento de SIC, mantendo um elevado nível de

conscientização sobre o assunto. Essa tarefa pode ser atingida por meio de notas em Plano do Dia, Palestras, Adestramentos e Exercícios Internos (BRASIL, 2019a, p. 9-19).

Além das possibilidades de se incrementar a mentalidade de segurança, há um outro aspecto importante a ser observado. Tal aspecto, citado no estudo de caso, relacionado ao *Stuxnet*, uma das ações envolve o Ataque à Cadeia de Suprimentos do sistema de atualização do SO Windows. Esse ataque comprometeu todos os equipamentos que efetuaram atualizações em seus sistemas.

Uma alternativa para se evitar esse tipo de ataque seria possível caso a própria instituição disponibilizasse as atualizações de seus Sistemas. Na MB, já está disponível um repositório para atualização dos Sistemas Operacionais Linux-Ubuntu. Todas as Estações de Trabalho (ET) da MB, que utilizam o SO Ubuntu, devem utilizar somente o repositório disponibilizado internamente. Esse procedimento evita um possível Ataque à Cadeia de Suprimentos nas ET da MB, em função de não haver a necessidade de se buscar essa atualização externamente — nesse caso, na Internet (BRASIL, 2018, p. 4).

4.4 Ações a serem empreendidas

Além dos aspectos de qualificação e capacitação de pessoal, citados anteriormente, há outros aspectos importantes a serem observados, como o de se definir critérios de segurança na aquisição de produtos de defesa, a fim de eliminar vulnerabilidades tecnológicas nos equipamentos e sistemas a serem adquiridos.

Conforme detalhado nesse estudo, os equipamentos e sistemas, muitas das vezes, podem ser desenvolvidos por vários países. Sendo assim, códigos maliciosos podem ser incorporados durante todo esse processo, o que pode proporcionar um Ataque à Cadeia de Suprimentos. Requisitos sobre a capacidade dos fornecedores em garantir a segurança da cadeia de suprimentos e de confidencialidade devem constar nos processos de aquisição.

A definição dos requisitos de segurança em equipamentos não é uma tarefa muito trivial, considerando a complexidade de produtos utilizados pelo Poder Naval. No entanto, o Brasil estabeleceu o Sistema de Homologação e Certificação de Produtos de Defesa Cibernética (SHCDCiber), que tem o objetivo de desenvolver um sistema avaliativo de segurança cibernética para esses produtos, baseado em normas internacionais (SÁ; MACHADO; ALMEIDA, 2019, p. 116).

O SHCDCiber foi estabelecido no ano de 2014, e atribuído ao Exército Brasileiro (EB), em articulação com as demais forças, visando à potencialização da defesa cibernética nacional (BRASIL, 2014b).

Assim, esse sistema de homologação vem sendo desenvolvido em parceria com renomadas Instituições, com o objetivo de especificar requisitos de segurança, para os dispositivos e sistemas, e definir metodologias de auditoria que permitam atestar a competência de laboratórios na área de segurança (INMETRO, 2018).

Dessa forma, o SHCDCiber será de alta relevância para o atendimento aos objetivos nacionais, voltados para a definição de requisitos a serem atendidos, visando à proteção de sistemas e equipamentos a serem adquiridos pela APF, em especial pelas FA.

5 CONCLUSÃO

Ao longo do desenvolvimento dessa pesquisa, foram identificados os conceitos relacionados ao Espaço Cibernético, sua normatização no âmbito da APF e da MB, em aspectos relacionados ao tema desse trabalho. Outro ponto, é a importância de um adequado preparo das FA, em especial o da MB, para atuação em conflitos cibernéticos, para que, assim, consigam proteger o País contra ameaças nesse ambiente, buscando garantir a soberania nacional.

Dentre as ameaças que podem afetar o Espaço Cibernético, foi abordado o Ataque à Cadeia de Suprimentos e suas possibilidades de exploração nos sistemas e equipamentos dos meios navais utilizados pela MB. Além disso, também foram citadas algumas formas de incrementar a mentalidade de segurança de seus usuários, a fim de dotá-los de um adequado preparo para uma possível conflito.

Ao longo do desenvolvimento desse trabalho de pesquisa, foi verificada a abordagem da MB ao assunto Ataque à Cadeia de Suprimentos, tema contido em documentos de alto nível, como o PEM e a ENSC. Diante do que foi elaborado, constatou-se que o assunto é amplo, de difícil identificação quando da efetivação de um ataque, e, por esse motivo, requer especial atenção quanto às ações necessárias, que devem ser desenvolvidas, para que as consequências desse ataque sejam evitadas ou minimizadas.

No contexto da MB, o tema Ataque à Cadeia de Suprimentos, por ser novo e uma ameaça em crescente desenvolvimento no âmbito dos conflitos cibernéticos, ainda requer um aprofundamento de estudos, para que sejam desencadeadas ações efetivas de enfrentamento.

Em análise aos aspectos relacionados aos sistemas e equipamentos, verificou-se que há a necessidade de se elaborar e aprimorar normas que contemplem requisitos de segurança quando da sua aquisição e utilização nos meios navais. Esses requisitos devem estabelecer ações a serem cumpridas e que possibilitem à MB um acompanhamento do

desenvolvimento desses sistemas e equipamentos, que, em muitas ocasiões, são originados de fornecedores de vários países, e pelo fato de que, nessa cadeia de suprimentos, códigos maliciosos podem ser incorporados para um posterior acionamento.

Ainda em relação ao processo de aquisição de produtos, sugere-se que nos certames de contratação sejam incluídas condições a serem cumpridas pelos fornecedores, tais como: cumprimento de legislações nacionais e internacionais relacionadas à segurança cibernética, plano de segurança da cadeia de suprimentos, atualização de sistemas e política de proteção de dados.

A possibilidade de se criar um modelo de homologação e avaliação de produtos cibernéticos e a fiscalização do processo de fornecimento da cadeia de suprimentos permite que sejam identificados riscos que podem, em um momento futuro, prejudicar ações de combate realizadas pelos meios navais da MB. Conforme citado, no exemplo do *Stuxnet*, vulnerabilidades foram encontradas durante o seu ataque, o que proporcionou o sucesso de sua operação. A busca e eliminação dessas vulnerabilidades, que podem ser exploradas em um Ataque à Cadeia de Suprimentos dos meios navais, possibilita que esses meios tenham um desempenho adequado quando da ocorrência de um conflito cibernético.

Na questão envolvendo o aprimoramento da mentalidade de segurança cibernética, foi observado que as ações empreendidas pela MB vêm sendo aprimoradas e desenvolvidas de forma satisfatória. Esse aprimoramento de ações é efetivado em atividades de capacitação, como cursos e adestramentos. Além disso, há a realização de exercícios de guerra cibernética envolvendo todas as OM da MB, incluindo os meios navais.

Um adequado preparo do pessoal da MB é de suma importância para que todos estejam qualificados e devidamente capacitados para um possível período de conflito, que requererá uma dedicação ainda maior do seu pessoal. O aprimoramento da mentalidade de segurança deve ser contínuo e frequente, a fim de possibilitar um alto grau de comprometimento pelos envolvidos.

A realização e participação dos meios navais nos exercícios cibernéticos permitem avaliações importantes quanto aos aspectos de segurança que podem ser explorados em um ataque. A contribuição, resultante desses exercícios, agrega conhecimento e experiência, possibilitando o incremento da SIC e da defesa no Espaço Cibernético.

Conforme identificado, há desafios a serem vencidos para que se obtenha um nível ideal de enfrentamento cibernético, em especial contra um Ataque à Cadeia de Suprimentos. No entanto, a MB vem, há alguns anos, realizando ações pioneiras para a sua defesa no Espaço Cibernético. Ainda assim, existe a necessidade do desenvolvimento de

políticas e de normas que definam ações para proteger a MB desse tipo de ataque, como também; bem como a do contínuo investimento em capacitação de seu pessoal.

É nesse contexto que a MB deve manter seu permanente aprimoramento, para que, dessa forma, possa enfrentar essas ameaças cibernéticas, a fim de corresponder ao que a sociedade brasileira espera de suas FA, mantendo a defesa da Pátria e a garantia da lei e da ordem, e, além disso, garantir a proteção das infraestruturas críticas, tão importantes para a defesa nacional.

Por fim, conclui-se que a proteção contra um possível ataque cibernético é uma tarefa que envolve várias ações, e que, mesmo não garantindo a eliminação total dos riscos identificados, há a necessidade de se identificar limitações, em áreas críticas, para, assim, permitir que se possa melhorar procedimentos internos e fortalecer a segurança de sistemas, equipamentos, pessoal e meios navais, contra as possíveis agressões externas. Mesmo que a segurança e a defesa não sejam totalmente perfeitas, deve-se ter condições de resposta e de rápida recuperação.

REFERÊNCIAS

BRASIL. Comando de Defesa Cibernética. Escola Nacional de Defesa Cibernética. **Ofício n. 108,** de 5 de julho de 2021. Dispõe sobre a Seleção de Militares para Capacitação em Defesa Cibernética. Brasília, DF, 2021a.

BRASIL. **Decreto nº 10.222,** de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. 2020a. Diário Oficial da União, seção 1, Brasília, DF, p. 1-38, 5 fev. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 5 abr. 2021.

BRASIL. Diretoria de Comunicações e Tecnologia da Informação da Marinha. **DCTIMBOTEC 30/003/2018:** Estação de Trabalho Padrão da MB. Rio de Janeiro, 2018.

BRASIL. Diretoria de Comunicações e Tecnologia da Informação da Marinha. **DCTIMBOTEC 31/002/2020:** Recomendações e Requisitos Mínimos de Segurança da Informação para Sistemas Digitais na MB. Rio de Janeiro, 2020b.

BRASIL. Diretoria de Comunicações e Tecnologia da Informação da Marinha. **Plano de Capacitação de Pessoal de Tecnologia da Informação e Comunicações da Marinha — PLACAPE-TIC** — Horizonte 2021 a 2027. Rio de Janeiro, 2020c.

BRASIL. Diretoria-Geral do Material da Marinha. **DGMM-0540** — Normas de Tecnologia da Informação da Marinha. 3. rev. Rio de Janeiro, 2019a.

BRASIL. Estado-Maior da Armada. **Plano Estratégico da Marinha (PEM).** Brasília: 2020d.

BRASIL. Gabinete de Segurança Institucional. **Glossário de Segurança da Informação**. 1.ed. Brasília, 2019b. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em: 2 ago. 2021.

BRASIL. Marinha do Brasil. Centro de Comunicação Social da Marinha. **Programa "Classe Tamandaré"**. 2020e. Disponível em: https://www.marinha.mil.br/programa-classe-tamandare. Acesso em: 30 jul. 2021.

BRASIL. Marinha do Brasil. Centro de Comunicação Social da Marinha. **Projeto "Classe Tamandaré" Marinha do Brasil seleciona a melhor oferta**. 2019c. Disponível em: https://www.marinha.mil.br/projeto-classe-tamandare-marinha-do-brasil-seleciona-melhor-oferta. Acesso em: 30 jul. 2021.

BRASIL. Marinha do Brasil. Comando em Chefe da Esquadra. **Navios da Esquadra realizam exercício de Guerra Cibernética durante a Operação "ADEREX-Anfíbia/Superfície 2021".** 2021b. Disponível em: https://www.marinha.mil.br/noticias/navios-da-esquadra-realizam-exercicio-de-guerra-cibernetica-durante-operacao-aderex. Acesso em: 2 ago. 2021.

BRASIL. Marinha do Brasil. **Política Naval.** Brasília. 2019d. Disponível em: https://www.marinha.mil.br/politicanaval. Acesso em: 2 jun. 2021.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa** (encaminhada para apreciação do Congresso Nacional), 2020f. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-defesa/pnd_end_congresso_.pdf. Acesso em: 5 abr. 2021.

BRASIL. Ministério da Defesa. **Glossário das Forças Armadas**. 2015. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md35-G-01-glossario-das-forcas-armadas-5-ed-2015-com-alteracoes.pdf/view. Acesso em: 5 abr. 2021.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional** (encaminhada para apreciação do Congresso Nacional). 2020g. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_branco_congresso_nacional.pdf. Acesso em: 3 abr. 2021.

BRASIL. Ministério da Defesa. **MD31-M-07:** Doutrina Militar de Defesa Cibernética. 1. ed. Brasília, 2014a. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_07a_defesaa_ciberneticaa_1a_2014.pdf. Acesso em: 13 abr. 2021.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa** (encaminhada para apreciação do Congresso Nacional), 2020h. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-edefesa/pnd_end_congresso_.pdf. Acesso em: 5 abr. 2021.

BRASIL. Ministério da Defesa. **Portaria Normativa n. 2.777/MD,** de 27 de outubro de 2014. Dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional e dá outras providências. Brasília, DF, 2014b.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética:** a Próxima Ameaça à Segurança e o que Fazer a Respeito. Rio de Janeiro: Brasport, 2015.

COMPUTERWORLD. **Mais de 8,4 bilhões de tentativas de ataques cibernéticos atingiram o Brasil em 2020**. 2020. Disponível em: https://computerworld.com.br/seguranca/mais-de-84-bilhoes-de-tentativas-de-ataques-ciberneticos-atingiram-o-brasil-em-2020/. Acesso em: 10 jun. 2021.

FALLIERE, Nicolas; O'MURCHU, Liam; CHIEN, Eric. **W32 Stuxnet Dossier**. Symantec Corporation. W32.Stuxnet Dossier. 2010. Disponível em: https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf. Acesso em: 13 jul. 2021.

GREENBERG, Andy. Hacker Lexicon: What Is a Supply Chain Attack? **WIRED**, 2021. Disponível em: https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/, Acesso em: 4 jun. 2021.

IMASTERS. **Brasil é terceiro país que mais recebe ataques cibernéticos.** 2019. Disponível em: https://imasters.com.br/noticia/brasil-ataques-ciberneticos. Acesso em: 11 jun. 2021.

INMETRO. **Inmetro vai desenvolver sistema de certificação de produtos de defesa cibernética**. 2018. Disponível em: https://www.gov.br/inmetro/pt-br/centrais-de-conteudo/noticias/inmetro-vai-desenvolver-sistema-de-certificacao-de-produtos-de-defesa-cibernetica. Acesso em: 3 ago. 2021.

KARNOUSKOS, Stamatis. **Stuxnet Worm Impact on Industrial Cyber-Physical System Security.** IECON Proceedings (Industrial Electronics Conference), Alemanha: 2011. Disponível em: https://papers.duckdns.org/files/2011_IECON_stuxnet.pdf. Acesso em: 15 jul. 2021

LOPES, Gills; OLIVEIRA, Carolina F. J. Stuxnet e defesa cibernética estadunidense à luz da análise de política externa. **Revista Brasileira de Estudos de Defesa**, v. 1, n. 1, 2014, pp. 55-69. Disponível em: https://rbed.abedef.org/rbed/article/view/39457/30874. Acesso em: 14 jul. 2021.

MAJUMDAR, Dave. NAVSEA: Submarines Control Systems are at Risk for Cyber Attack. **USNI News,** 2014. Disponível em: https://news.usni.org/2014/10/22/navsea-submarines-control-systems-risk-cyber-attack. Acesso em: 5 jul. 2021.

MIGUENS, Altineu Pires. **Navegação: A ciência e a Arte.** Diretoria de Hidrografia e Navegação. v. 1, 1. rev. atual., 2019. Disponível em: https://www.marinha.mil.br/dhn/?q=pt-br/npublicacoes. Acesso em: 10 ago. 2021.

PARKS, Raymond C.; DUGGAN, David P. Principles of Cyberwarfare. **IEEE Security & Privacy**, v. 9, n. 5, pp. 30-35, 2011.

PETRY, Guilherme. **Um dos ataque mais sofisticados da década. The Hack**, 2021. Disponível em: https://thehack.com.br/um-dos-ataque-mais-sofisticados-da-decada-revela-fireeye-sobre-ataque-a-solarwinds/. Acesso em: 5 de jun. 2021.

RIGUES, Rafael. **SolarWinds:** ataque foi o "maior e mais sofisticado" que o mundo já viu, 2021. Disponível em: https://olhardigital.com.br/2021/02/15/noticias/solarwinds-ataque-foi-o-maior-e-mais-sofisticado-que-o-mundo-ja-viu/. Acesso em: 6 ago. 2021.

RODRIGUES, Marcos Silva. Plano Estratégico da Marinha — PEM 2040. **Revista Escola de Guerra Naval,** Rio de Janeiro, v. 27, n. 1, pp. 1-18. Janeiro/Abril. 2021. Disponível em: https://revista.egn.mar.mil.br/index.php/revistadaegn/article/download/1087/804. Acesso em: 12 jul. 2021.

SÁ, A. O.; MACHADO, R. C. S.; NIVAL, N. A. O Encontro da Guerra Cibernética com as Guerras Eletrônica e Cinética no Âmbito do Poder Marítimo. **Revista Escola de Guerra Naval,** Rio de Janeiro, v. 25, n. 1, p. 89-128. Janeiro/Abril. 2019. Disponível em: https://revista.egn.mar.mil.br/index.php/revistadaegn/article/download/797/pdf. Acesso em: 5 jul. 2021.

SINGER, P.; FRIEDMAN, A. **Cybersecurity and Cyberwar:** What Everyone Needs to Know. Oxford University Press. 1. ed., 2014.

ZETTER, Kim. **Contagem Regressiva até Zero Day**. Rio de Janeiro: Brasport, 2017.

ANEXO - Sensores previstos para as Fragatas Classe Tamandaré

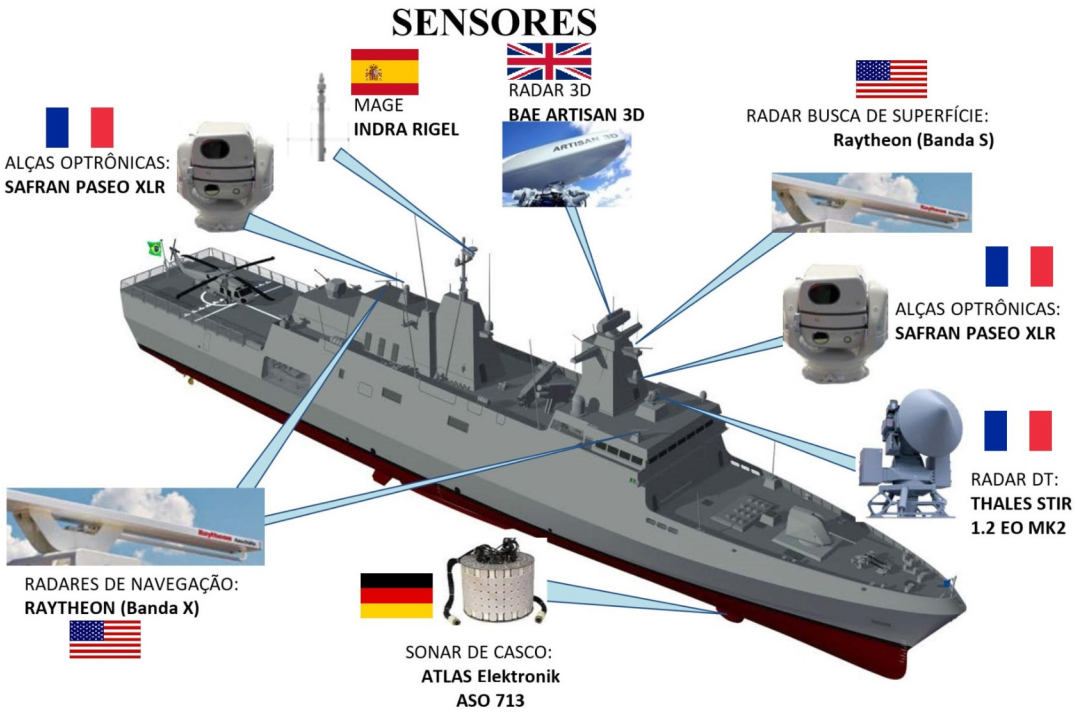

FIGURA 1 — Sensores e seus países fabricantes
Fonte: BRASIL, 2019c