ESCOLA DE GUERRA NAVAL

CC MARCOS FELIPE MARINHOS MOURA

NOTPETYA:

o Ataque Cibernético Mais Devastador Relacionado ao Conflito Russo-Ucraniano Realizado em Junho de 2017 e as Lições Aprendidas para o Aprimoramento da Defesa Cibernética Brasileira

Rio de Janeiro

2023

CC MARCOS FELIPE MARINHOS MOURA

NOTPETYA:

o Ataque Cibernético Mais Devastador Relacionado ao Conflito Russo-Ucraniano Realizado em Junho de 2017 e as Lições Aprendidas para o Aprimoramento da Defesa Cibernética Brasileira

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.

Documento assinado digitalmente
gov.br
MARCOS FELIPE MARINHOS MOURA
Data: 27/11/2023 22:03:03-0300
Verifique em https://validar.iti.gov.br

AGRADECIMENTOS

Agradeço a Deus pela infinita misericórdia que me concede o dom da vida.

Minha profunda gratidão à minha amada família, em especial aos meus pais por desempenharem um papel fundamental na minha educação e formação de caráter. A todos os meus familiares, incluindo avós, tios, primos, meu coração transborda de gratidão.

À minha namorada Emily que me apoiou e incentivou em um período de grande dedicação acadêmica, compreendendo as ausências que esta jornada exigia. Te amo muito.

Agradeço aos amigos, em especial aos integrantes da Turma Almirante Sylvio de Noronha, que desde o ano 2000, por ocasião do ingresso no Colégio Naval, compartilham desafios e lutas. A amizade e o apoio mútuo de vocês foram fundamentais para o nosso sucesso.

Ao Capitão de Fragata Luiz Felipe Lima Santos, meu orientador, agradeço pelos ensinamentos que foram fundamentais para o sucesso na elaboração desse trabalho e ao Major Frederico Chaves Salóes do Amor, instrutor da Escola de Comando e Estado-Maior do Exército, pelas orientações técnicas relacionadas a Defesa Cibernética.

Por fim, agradeço à Escola de Guerra Naval pelas experiências e lições aprendidas. A dedicação e conhecimentos transmitidos pelo corpo docente foram fundamentais para o crescimento profissional e pessoal dos oficiais-alunos. O tempo e esforço na formação dos futuros líderes navais deixarão um impacto duradouro na nossa trajetória acadêmica e militar.

“Em junho de 2017, as forças militares russas lançaram o ataque cibernético mais destrutivo e oneroso da história.

O ataque, apelidado de “NotPetya”, rapidamente se espalhou pelo mundo, causando prejuízos de bilhões de dólares na Europa, Ásia e Américas. Fazia parte do esforço contínuo do Kremlin para desestabilizar a Ucrânia e demonstra cada vez mais claramente o envolvimento da Rússia no conflito em curso. Esse também foi um ataque cibernético irresponsável e indiscriminado que terá consequências internacionais.”

Secretaria de Imprensa da Casa Branca
Em 15 de fevereiro de 2018

RESUMO

Investigou-se o ataque cibernético do malware NotPetya, ocorrido em 27 de junho de 2017, supostamente realizado pela Rússia contra a Ucrânia, buscando verificar a sua aderência à Doutrina Militar de Defesa Cibernética e à Doutrina Cibernética da Marinha. A pesquisa não teve acesso ao planejamento militar cibernético russo, mas baseou-se em fontes confiáveis, incluindo o trabalho investigativo de Greenberg para inferir como o ataque foi realizado. Esse ataque foi considerado o mais devastador da História, causando um prejuízo de 10 bilhões de dólares, impactando diversas entidades ucranianas e empresas globalmente. Adotando o confronto entre teoria e realidade como desenho da pesquisa, buscou-se realizar uma análise detalhada das doutrinas, das estratégias existentes, dos antecedentes históricos e da aderência do ataque às doutrinas abordadas. Na conclusão, foi enfatizada a crescente vulnerabilidade do Brasil diante do avanço das capacidades de Guerra Cibernética e ressaltou a necessidade da revisão constante das Hipóteses de Emprego para enfrentar as ameaças em constante evolução e a crescente importância da utilização das ferramentas cibernéticas na condução das operações navais. Em síntese, a dissertação atingiu os seus objetivos, verificando a aderência do ataque aos principais conceitos apresentados, apontando aprimoramentos pertinentes para a Defesa Cibernética Brasileira.

Palavras-chave: Guerra Cibernética; Doutrina Militar de Defesa Cibernética; Doutrina Cibernética da Marinha; NotPetya; Rússia; Ucrânia; SandWorm

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

C2 -	Comando e Controle
END -	Estratégia Nacional de Defesa
EUA -	Estados Unidos da América
FAB -	Força Aérea Brasileira
GRU -	Inteligência Militar Russa
GSI -	Gabinete de Segurança Institucional da Presidência da República
MB -	Marinha do Brasil
MD -	Ministério da Defesa
NSA -	Segurança Nacional dos Estados Unidos
OTAN -	Organização do Tratado do Atlântico Norte
PR -	Presidente da República
SegOrg -	Segurança Orgânica
SIC -	Segurança da Informação e das Comunicações
TI -	Tecnologia da Informação
TIC -	Tecnologias da Informação e Comunicação
UE -	União Europeia
URSS -	União das Repúblicas Socialistas Soviéticas
VPN -	Rede Privada Virtual

SUMÁRIO

1 INTRODUÇÃO

A partir do dia 24 de fevereiro de 2022, a Rússia iniciou diversas ações cinéticas[1] em território ucraniano, na tentativa, dentre outras, de frear o avanço da Organização do Tratado do Atlântico Norte (OTAN) sobre o leste europeu. Essas ações são consequências de uma escalada das hostilidades que intensificou após o evento conhecido como Euromaidan[2], em novembro de 2013.

Ao longo desse conflito, podemos observar que ambos os países vêm adquirindo novas capacidades cibernéticas cada vez mais destrutivas. Entre os diversos ataques cibernéticos realizados pela Rússia em território ucraniano, um foi considerado o mais devastador da História por ter causado um prejuízo de aproximadamente de 10 bilhões de dólares, impactando diversas entidades ucranianas e empresas em todo mundo. Estamos falando do ataque cibernético do NotPetya, realizado no dia 27 de junho de 2017.

O ataque do NotPetya criptografava irreversivelmente os dados contidos no sistema operacional Windows® da Microsoft Corporation. Segundo Greenberg (2021), o suposto desenvolvimento e a autoria foram de um grupo de hackers chamado SandWorm, que aparentemente teria vínculos com a Inteligência Militar Russa (GRU). Cabe ressaltar que, em virtude da grande relevância deste ataque cibernético para o conflito em curso, decidimos adotá-lo como objeto de nosso estudo.

Com efeito, o propósito deste trabalho é analisar se o planejamento das ações do ataque cibernético do NotPetya, realizado em 27 de junho de 2017, tem aderência com a atual Doutrina de Militar de Defesa Cibernética e a Doutrina Cibernética da Marinha.

Destacamos que não obtivemos acesso a documentos que descrevessem de forma detalhada o planejamento russo para o ataque, contudo, por meio do trabalho de Greenberg (2018, 2021) que realizou diversas entrevistas com os atores impactados pelo NotPetya, foi possível inferir como foi realizado tal planejamento e comparar com a nossa doutrina.

Neste trabalho constituído por cinco capítulos, com relação à metodologia científica, utilizaremos como desenho da pesquisa o confronto entre teoria e realidade, a abordagem

---

[1] Ações Cinéticas - São aquelas desencadeadas no interior da Área de Operações, que envolvem movimentos (fogos, voos, deslocamento de tropas e de blindados) e produzem resultados tangíveis (destruição, captura, conquista etc.) (BRASIL, 2015, p. 17).

[2] Euromaidan - Nome dado para as manifestações nacionalistas ucranianas e favoráveis à associação a União Europeia que culminaram na derrubada do governo pró-russo (KORYBKO, 2018, p. 87).

qualitativa e o procedimento de pesquisa documental e bibliográfica. Após esta introdução, serão examinados, no segundo capítulo, os principais conceitos doutrinários e estratégicos relacionados ao setor cibernético brasileiro, contidos na Doutrina de Militar de Defesa Cibernética e a Doutrina Cibernética da Marinha.

No terceiro capítulo, analisaremos as causas e os antecedentes históricos que levaram a deflagração do conflito; como uma das principais empresas de logística marítima, a Maersk, foi afetada e como foi realizado o ataque à Ucrânia.

No quarto capítulo, realizaremos o confronto entre os principais conceitos doutrinários e estratégicos e os fatos relacionados com o ataque do NotPetya. Por fim, no quinto capítulo, apresentaremos as conclusões e as principais contribuições para o desenvolvimento da Defesa Cibernética Brasileira.

2 PRINCIPAIS CONCEITOS DE DEFESA CIBERNÉTICA

Neste capítulo abordaremos os principais documentos e conceitos relacionados às doutrinas militares brasileiras do setor cibernético, bem como alguns teóricos do poder aéreo que poderão ser aplicados na Defesa Cibernética. Essa abordagem inicial servirá para compreender a importância do espaço cibernético [3] para uma nação, bem como sua transformação no quinto domínio da guerra[4]. Além disso, o entendimento da doutrina será fundamental para compreender a dinâmica do ataque cibernético do NotPetya.

Conforme definido no Glossário das Forças Armadas, as doutrinas militares estabelecem uma forma padrão de se pensar sobre determinada área da defesa e direcionam ações no preparo e no emprego das Forças Armadas, sendo essas duas ações mutáveis ao longo do tempo por meio da incorporação de novos conhecimentos e experiências conforme os objetivos nacionais (BRASIL, 2015). Adicionalmente, Ribeiro (2010) contribui com uma definição de doutrina:

> A doutrina indica soluções fundamentadas para problemas tácticos ou técnicos repetitivos, sobre os quais exista experiência acumulada. A consideração de procedimentos doutrinários de natureza táctica e técnica, dentro das situações reais enfrentadas, é parte essencial da operacionalização estratégica, concorrendo, em grande medida, para a avaliação da exequibilidade e da aceitabilidade das operações em estudo. Por outro lado, a doutrina condiciona o desenvolvimento dos instrumentos do poder e a preparação dos homens com responsabilidade de operar os meios (RIBEIRO, 2010, p. 45).

Assim, concluímos que as doutrinas militares passam por constantes processos de revisão e atualização para atender aos objetivos estratégicos e políticos de uma nação. Percebemos que elas são criadas por meio da combinação entre a teoria, a pesquisa e a análise de exercícios operacionais, de conflitos anteriores e das futuras ameaças.

Finalizada essa parte inicial que tratou sobre a importância das doutrinas militares, a seguir abordaremos os principais documentos políticos e estratégicos que têm abrangência sobre a Defesa Cibernética.

---

[3] Espaço Cibernético - 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] "O 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." (BRASIL, 2014, p. 18).

2.1 Principais Documentos Políticos e Estratégicos

Na Política Nacional de Defesa (PND), documento de alto nível que estabelece as diretrizes fundamentais para o planejamento de defesa, podemos verificar dois conceitos importantes e a diferença entre Segurança Nacional e Defesa Nacional. Enquanto a Defesa Nacional está focada na proteção contra ameaças externas por meio de ações militares, a Segurança Nacional abrange de forma mais ampla a proteção contra ameaças internas e externas, com o objetivo de assegurar a estabilidade e de promover o bem-estar da população, além de preservar a soberania e proteger os interesses do país (BRASIL, 2020d).

A Estratégia Nacional de Defesa (END), que define as orientações para assegurar que as Forças Armadas estejam devidamente preparadas e capacitadas visando salvaguardar a segurança nacional tanto durante períodos de paz como em momentos de crise[5], reconheceu a importância do setor cibernético e de suas duas áreas de atuação: a Segurança Cibernética, sob a responsabilidade do Presidente da República (PR), e a Defesa Cibernética, sob a responsabilidade do Ministério da Defesa (MD) por meio das Forças Armadas (BRASIL, 2014).

A Defesa Cibernética, incluída dentro do conceito de Segurança Cibernética, concentra as atividades de defesa, ataque e exploração[6] no espaço cibernético com o objetivo na Defesa Nacional. A Segurança Cibernética, por sua vez, engloba outras preocupações como a proteção das infraestruturas críticas[7] e dos ativos de informação[8] do país (BRASIL, 2014).

Durante esse trabalho de pesquisa será utilizada a nomenclatura Defesa Cibernética em detrimento à Guerra Cibernética[9], pois aquela é mais abrangente conforme definido na

---

[5] Crise - conflito desencadeado ou agravado imediatamente após a ruptura do equilíbrio existente entre duas ou mais partes envolvidas em um contencioso. Caracteriza-se por um estado de grandes tensões, com elevada probabilidade de agravamento (escalada) e risco de guerra, não permitindo que se anteveja com clareza o curso de sua evolução (BRASIL, 2015, p.80).

[6] A definição dessas atividades é ampliada na subseção 2.2.4.

[7] Infraestruturas Críticas - instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade (BRASIL, 2014, p. 19).

[8] Ativos de informação - meios de armazenamento, transmissão e processamento de dados e de informação, os equipamentos necessários a isso (computadores, equipamentos de comunicações e de interconexão), os sistemas utilizados para tal, os sistemas de informação de um modo geral, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso (BRASIL, 2014, p. 18).

[9] Guerra Cibernética – corresponde ao uso ofensivo e defensivo de informação e de sistemas de informação para negar, explorar, corromper, degradar ou destruir as capacidades de Comando e Controle (C^2) do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para

Doutrina Militar de Defesa Cibernética.

A Estratégia Nacional de Segurança Cibernética, aprovada em 2020, tem como objetivo passar orientações do Governo Federal à sociedade sobre ações que serão implementadas na área de Segurança Cibernética no quadriênio 2020-2023 (BRASIL, 2020a). Nessa estratégia, que contempla a Defesa Cibernética, destacam-se os seguintes objetivos estratégicos:

> 1. Tornar o Brasil mais próspero e confiável no ambiente digital;
> 2. Aumentar a resiliência brasileira às ameaças cibernéticas; e
> 3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional (BRASIL, 2020a).

Outro documento importante para a nossa análise é a Política Cibernética de Defesa, aprovada em 2012 pela portaria do MD n° 3.389, que tem o objetivo de guiar, em todos os níveis estratégicos, a Defesa Cibernética dentro desse ministério (BRASIL, 2012).

Dentre os objetivos dessa política destacam-se: os compromissos de atuação, de forma conjunta, das Forças Armadas no espaço cibernético, impedindo e dificultando a sua utilização contra os interesses da Defesa Nacional; e o desenvolvimento e a atualização da doutrina do setor cibernético. Além disso, tem como pressuposto básico que todas as ações ofensivas no ciberespaço deverão estar alinhadas com as Hipóteses de Emprego[10] (HE) (BRASIL, 2012).

Essas HE e as suas respectivas estratégias militares a serem empregadas são definidas pelo documento de mais alto nível conhecido como a Estratégia Militar de Defesa[11], condicionada pela END e decorrente da Política Militar de Defesa[12] (BRASIL, 2007).

Dessa forma, analisando a Política Cibernética de Defesa, podemos perceber que as ações ofensivas no ciberespaço deverão estar previstas nas HE pelo Nível Político, em virtude

---

desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC. (BRASIL, 2014, p. 19).

[10] Hipóteses de Emprego - antevisão de possível emprego das Forças Armadas em determinada situação ou área de interesse estratégico para a Defesa Nacional. É formulada considerando-se o alto grau de indeterminação e imprevisibilidade de ameaças ao País, sendo perfeitamente caracterizada e mensurável. Com base nas hipóteses de emprego, serão elaborados e mantidos atualizados os planos estratégicos e operacionais pertinentes, visando a possibilitar o contínuo aprestamento do Poder Nacional como um todo, e em particular do Poder Militar, para emprego na defesa dos interesses nacionais (BRASIL, 2015, p. 139).

[11] Estratégia Militar de Defesa - Documento elaborado no nível setorial, que orienta o planejamento estratégico das forças armadas e estabelece ações para a consecução dos objetivos estabelecidos na Política Militar de Defesa, ao mesmo tempo em que contém as hipóteses em que as forças poderão ser empregadas (BRASIL, 2015, p. 110).

[12] Política Militar de Defesa - Documento de nível setorial, decorrente da Política de Defesa Nacional, no qual são estabelecidos objetivos e diretrizes que orientem e condicionem o preparo e o emprego das Forças Armadas para a defesa do País (BRASIL, 2015, p. 213).

de possíveis efeitos e consequências cinéticas para a nação e sobre os outros países, que podem transformar uma situação de paz em um conflito. Com as HE, o setor cibernético pode desenvolver estratégias, treinamentos e aquisição de material para a prepararão do emprego militar.

Ao longo do tempo, com as mudanças no cenário internacional e o surgimento de novas ameaças, concluímos que as HE são adaptativas devendo passar por processos contínuos de atualização para se ter uma Defesa Cibernética efetiva.

2.2 Principais Documentos Doutrinários sobre a Defesa Cibernética

Em dezembro de 2008, a END definiu três setores estratégicos prioritários para a Defesa Nacional: o setor nuclear, o setor cibernético e o setor espacial (BRASIL, 2014). Esses setores, identificados como áreas cruciais, demandam uma atenção especial devido a sua importância para a segurança e a soberania do país.

O setor cibernético foi destacado como uma área prioritária devido à crescente dependência das infraestruturas críticas e das comunicações digitais, que tornou o país suscetível a ataques cibernéticos (BRASIL, 2020a).

Por meio da Diretriz Ministerial nº 0014, emitida em 9 de novembro de 2009 pelo MD, foram estabelecidas medidas para garantir a implementação da END nos setores estratégicos da defesa, atribuindo responsabilidades específicas a cada uma das Forças Armadas. Dentre essas responsabilidades, o Exército foi designado para a importante tarefa de coordenar o setor cibernético, integrando os esforços entre diferentes entidades e instituições visando enfrentar de maneira eficaz as ameaças cibernéticas.

Nesse contexto e alinhado com os objetivos da Política Cibernética de Defesa, a Doutrina Militar de Defesa Cibernética, aprovada em 18 de novembro de 2014, foi estabelecida para proporcionar unidade de pensamento e de atuação conjunta das Forças Armadas na defesa do Brasil no espaço cibernético (BRASIL, 2014). Em virtude da nossa nação necessitar ter capacidade para se contrapor às ameaças externas no campo cibernético, medidas precisam ser adotadas para responder oportuna e adequadamente aos possíveis cenários nefastos à Defesa Nacional.

Com o objetivo de definir a estrutura cibernética e os respectivos fundamentos doutrinários na Marinha do Brasil (MB), alinhada com as normas vigentes do Governo Federal

e do MD, foi aprovada em 2021 a Doutrina Cibernética da Marinha. Essa doutrina apresenta os conceitos fundamentais, os princípios doutrinários e as orientações em níveis estratégico, operacional e tático para a aplicação da Guerra Cibernética. Seu propósito é o desenvolvimento da Capacidade Cibernética e da resiliência cibernética[13] dos sistemas de informação no âmbito da MB. Além disso, a doutrina busca garantir a eficácia e a segurança das operações navais em um contexto cada vez mais influenciado pelas tecnologias digitais e as ameaças cibernéticas.

Dessa forma, a seguir trataremos dos principais conceitos contidos na Doutrina para analisar o ataque cibernético em questão.

2.2.1 A Estrutura do Setor Cibernético e os Níveis de Decisão

Conforme representado na FIG. 1, três são os níveis de decisão para as ações no espaço cibernético no contexto do MD: no nível político se encontra a Segurança da Informação e das Comunicações[14] (SIC) e a Segurança Cibernética, sob a coordenação da PR, tendo como abrangência a Administração Pública Federal direta e indireta, tal como as infraestruturas críticas das informações nacionais; no nível estratégico se encontra a Defesa Cibernética, sob a coordenação do MD, Estado-Maior Conjunto das Forças Armadas e Comandos das Forças Armadas, se comunicando com a Presidência da República e com a Administração Pública Federal; e por fim, nos níveis operacional e tático se encontra a Guerra Cibernética, cujo emprego é restrito ao âmbito das Forças Armadas.

2.2.2 Princípios de Emprego de Defesa Cibernética

Para analisar os principais aspectos relacionados ao ataque cibernético em baila é necessário relacionar, conceituar e expandir os princípios de emprego de Defesa Cibernética contidos na Doutrina Militar de Defesa Cibernética (2014):

a) Princípio do Efeito: as ações produzem necessariamente algo no mundo real por

---

[13] Resiliência Cibernética - 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).

[14] Segurança da Informação e das Comunicações - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações. (BRASIL, 2014, p. 19).

meio da interação no espaço cibernético (BRASIL, 2014). Por exemplo, um ataque cibernético direcionado a uma usina hidrelétrica pode ocasionar a interrupção do fornecimento de energia em determinada região, podendo afetar outros setores como serviços públicos, comunicações e transportes;

b) Princípio da Dissimulação: objetiva ocultar a autoria e a origem de ações no espaço cibernético (BRASIL, 2014). Clarke e Knake (2015) abordam sobre a importância das técnicas de ocultação na condução de operações maliciosas para aumentar a probabilidade de sucesso e a dificuldade de detectar e responder a esses ataques;
c) Princípio da Rastreabilidade: em contraposição ao princípio da dissimulação, este objetiva identificar a origem e o autor de ações cibernéticas ofensivas exploratórias. A rastreabilidade permite ao atacado obter provas legais para responsabilizar judicialmente o atacante (BRASIL, 2014). A capacidade de rastreabilidade pode prevenir ataques como afirmam Clarke e Knake (2015), pois tal princípio pode contribuir com a dissuasão cibernética, em comparação com a dissuasão nuclear que aconteceu com os Estados Unidos da América (EUA) e a União das Repúblicas Socialistas Soviéticas (URSS) no período da Guerra Fria (1947-1991). Dessa forma, ambos os lados evitariam ataques por temer efeitos assimétricos em retaliação; e
d) Princípio da Adaptabilidade: as rápidas mudanças no espaço cibernético impõem que a Defesa Cibernética seja flexível e com rápida capacidade de detecção e reposta. Por outro lado, o atacante terá que buscar a capacidade de adaptação maior que a do adversário, explorando as vulnerabilidades para a obtenção da vantagem tática (BRASIL, 2014).

2.2.3 Características da Defesa Cibernética

Nessa subseção, abordaremos as principais características da Defesa Cibernética contida na doutrina que nos ajudarão a entender os acontecimentos relacionados ao ataque do NotPetya. Entre elas, destacamos: Alcance Global, Vulnerabilidade das Fronteiras Geográficas, Insegurança Latente, Mutabilidade, Incerteza e o Paradoxo Tecnológico.

As batalhas no ciberespaço podem ser travadas a milhares de quilômetros. Dessa forma, podemos pontuar duas de suas características que são o Alcance Global, que permite ações em diferentes locais simultaneamente em virtude das redes interconectadas, e a

Vulnerabilidade das Fronteiras Geográficas, que permite aos agentes atuarem fora de seus limites geográficos (BRASIL, 2014).

A Mutabilidade afirma que o espaço cibernético está em constante mudanças em virtude das alterações tecnológicas e por causa da criatividade humana em buscar vulnerabilidades (BRASIL, 2014). Podemos afirmar que essa Mutabilidade gera a Insegurança Latente, que diz que todo sistema computacional possui vulnerabilidade, de ordem técnica ou humana, e que essas poderão ser exploradas por ações internacionais ou não (BRASIL, 2014).

A Incerteza diz que toda ação no espaço cibernético pode gerar resultados desejáveis e indesejáveis, em virtude das diversas variáveis relacionadas ao comportamento dos sistemas informatizados (BRASIL, 2014). Existe a possibilidade de um ataque cibernético realizado retornar ao país do atacante por meio da capilaridade das redes digitais.

As nações que mais possuem serviços e infraestruturas de alta tecnologia terão uma maior dependência nas tecnologias de informação e, consequentemente, ficarão mais suscetíveis a ataques cibernéticos. Esse problema é conhecido como o Paradoxo Tecnológico (BRASIL, 2014).

2.2.4 Os Tipos de Ações Cibernéticas

Nessa subseção nos aprofundaremos com relação aos três tipos de ações no espaço cibernético: exploração, proteção, e ataque cibernéticos (BRASIL, 2014). Será também apresentado um tipo específico de ataque cibernético que será de muita importância para entendermos o objeto desse estudo.

A exploração cibernética refere-se às atividades de busca e de coleta de informações na rede de dados ou no sistema do oponente, com o objetivo de serem usados para a inteligência ou para o planejamento de ataques (BRASIL, 2014).

Nessa fase, percebemos que o agressor empregará todas as suas ferramentas que identificam e exploram vulnerabilidades para coletar a maior quantidade possível de informações, podendo empregar técnicas de invasão. Contudo, se for ocasionado qualquer tipo de dano, a exploração se configurará como um ataque, e isso ainda será explicado logo adiante.

A proteção cibernética é uma atividade contínua que visa neutralizar ataques e a exploração cibernética pelos oponentes contra comunicações amigas, dispositivos

computacionais e rede de computadores (BRASIL, 2014).

Conforme definimos na subseção 2.2.3, ao nos depararmos com a Insegurança Latente dizendo que todo sistema computacional possui vulnerabilidades e que em algum momento poderão ser exploradas, chegamos à conclusão que o sistema mais avançado de segurança poderá estar em risco. Dessa forma, destacamos que além da importância de investir em proteção cibernética, é necessário também desenvolver a resiliência cibernética.

A proteção envolve evitar que informações que estão armazenadas e que circulam nessas redes sejam interrompidas, negadas, degradadas ou destruídas (GOMES; CORDEIRO; PINHEIRO, 2016). Já a resiliência, no nosso entendimento, é a restauração tempestiva das condições iniciais de um sistema em um momento anterior ao ataque cibernético.

Por fim, o ataque cibernético consiste em uma série de ações maliciosas que objetivam interromper, negar, reduzir a qualidade, corromper ou destruir informações e sistemas que estejam contidos em computadores, redes ou nas comunicações do oponente (BRASIL, 2014).

Dentre os diversos tipos de ataques, o nosso trabalho destacará um tipo de malware[15] conhecido como *ransomware*[16]*,* abreviatura do inglês *ransom software* (software resgate). A transmissão pode ser realizada por links maliciosos ou downloads automáticos (SEGUIN; LATTO, 2021).

O NotPetya foi considerado incialmente um *ransomware*, entretanto como o pagamento do resgate não restaurava o acesso aos dados dos computadores, foi reclassificado como um *wiper,* pois criptografava permanentemente os arquivos e sem a possibilidade de recuperação dos dados, concluindo-se que seu único objetivo era causar destruição (BELCIC, 2023).

2.3 O Ciberespaço ou Espaço Cibernético

O termo Ciberespaço, do inglês *cyberspace*, que é a união das palavras *cybernetics* e

---

[15] Malware - software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou de danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de malware estão os vírus, worms, trojans(ou cavalos de Troia), spyware, adware e rootkits (BRASIL, 2019).

[16] *Ransomware* - classe de software malicioso que pode criptografar os arquivos ou restringir o acesso dos usuários de algum sistema, extorquindo digitalmente as vítimas, exigindo na maioria das vezes o pagamento em criptomoeda para realizar a liberação (LISKA; GALLO, 2019, p. 16).

space, foi elaborado pelo autor William Gibson que popularizou o termo em 1984 com a publicação do livro Neuromancer. Gibson descreveu esse termo como uma alucinação consensual em que milhões de pessoas em todo o mundo recebiam em suas mentes representações gráficas de dados cuja origem seriam os computadores (MANDARINO, 2010).

No filme Matrix, uma referência da cultura pop lançado em 1999, podemos observar a representação hollywoodiana de um espaço cibernético, no qual este é uma realidade simulada e distópica, representada por diversas colunas de números e de símbolos verdes piscando e correndo de cima para baixo.

Saindo do mundo da ficção e voltando para a realidade, temos o conceito oficial de espaço cibernético estabelecido pelo Glossário de Segurança de Informação do Gabinete de Segurança Institucional da Presidência da República (GSI):

> Espaço virtual composto por um conjunto de canais de comunicação da Internet e outras redes de comunicação, que garantem a interconexão de dispositivos de tecnologia da informação. Engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo, além de todas as ações, humanas ou automatizadas, conduzidas por meio desse ambiente (BRASIL, 2019).

Esse espaço foi construído pelo ser humano e aflorou com a evolução da internet e da globalização nos anos 1990, caracterizado por uma intrincada e descentralizada rede de transmissão e compartilhamento de informações. Essa rede abrange não apenas a internet, que é uma rede global de computadores, mas também inclui redes privadas, como as intranets, e as telecomunicações em geral. Essa estrutura complexa proporciona um ambiente dinâmico e interativo para a troca de dados, comunicação e interações sociais, desempenhando um papel significativo na forma como as pessoas se relacionam e acessam informações na era digital (GAMA NETO, 2017).

De forma crítica, percebemos que as visões apresentadas sobre o espaço cibernético não são discordantes, havendo uma certa complementaridade. Cada vez mais nos tornamos dependentes da tecnologia que se integra nas nossas atividades diárias, tanto pessoais quanto profissionais. A sobrecarga de informações e a dependência excessiva da tecnologia está levando a sociedade a se isolar nas redes sociais, jogos on-line ou outras atividades virtuais, passando a viver em uma realidade distorcida e gerenciada por algoritmos e inteligências artificiais, como representado no filme Matrix.

Nesse mesmo ciberespaço, a ocorrência de conflitos tem se tornado evidente, como afirma Pagliusi:

> O terreno cibernético constitui promissor cenário para conflito bélico entre nações, caracterizado pela assimetria, dificuldade de atribuição de responsabilidades e paradoxo da maior vulnerabilidade do mais forte. Quanto mais desenvolvido tecnologicamente um país, maior a superfície digital exposta a ataques. Habituados a ver guerras como operações cinéticas, localizadas geograficamente, com objetivos e alvos identificáveis, é difícil dar importância real ao que ocorre no mundo sem fronteiras do espaço cibernético. Porém, cada vez mais, os combates são virtuais, o que não os faz menos letais, pois são preparação para ações no plano físico (PAGLIUSI, 2022, p. 75).

Podemos assim concluir que o ciberespaço é um ambiente virtual complexo, que se tornou extremamente importante para a manutenção da paz e o gerenciamento dos conflitos. A compreensão de suas características e os seus riscos são de vital importância para a soberania do país na era atual.

Para uma adequada aplicação do poder combatente, percebemos que a Doutrina Cibernética da Marinha ampliou diversas informações não contidas na Doutrina Militar de Defesa Cibernética, com relação ao planejamento operacional e às ações operativas, assim como às atividades administrativas de prevenção.

Isso posto, na próxima seção abordaremos as camadas do ciberespaço definidas pela Doutrina Cibernética da Marinha que podem ser alvos de um ataque cibernético.

2.3.1 As Camadas do Espaço Cibernético

O espaço cibernético pode ser descrito por meio de três camadas que se interrelacionam: estrato físico, estrato Lógico e estrato das identidades virtuais (BRASIL, 2021).

A primeira camada, o estrato físico, também conhecido como hardware, é formada pelos componentes tangíveis da infraestrutura de tecnologias da informação e comunicação (TIC), como por exemplo servidores, roteadores, *switches*, firewalls, modems, computadores, impressoras, unidades de armazenamento e cabos de rede (BRASIL, 2021). Os componentes desse estrato devem ser protegidos por meio da implementação dos planos de Segurança Orgânica (SegOrg) que visam a proteção desses componentes contra os danos físicos intencionais – sabotagem, vandalismo, terrorismo e espionagem – ou acidentais – falhas técnicas, erros humanos, desastres naturais e falhas de energia (BRASIL, 2021).

A segunda, o estrato lógico é a parte intangível da TIC que corresponde ao software, aos dados, às redes de comunicação, aos sistemas de informação, aos protocolos de

comunicação e aos algoritmos. Esses componentes são fundamentais na manipulação, armazenamento e transmissão segura das informações no espaço cibernético (BRASIL, 2021). Uma das formas de se atingir essa camada é com a inserção de malware em uma de suas vulnerabilidades (LATTO, 2020).

Desse modo, percebemos que a primeira camada fornece toda a infraestrutura necessária para processar demandas do próprio sistema ou dos usuários e a segunda permite que programas explorem o potencial dos equipamentos.

Já a última camada, o estrato das identidades virtuais é as representações digitais de cada usuário por meio de suas contas nas redes ou em TIC, podendo ser de uma pessoa ou entidade que opera de forma autônoma. Essas identidades são formadas por dados pessoais ou organizacionais, como nome, CPF/CNPJ, endereços, e-mail, números de telefone, logins e senhas de conta (BRASIL, 2021).

Cada indivíduo pode criar e gerenciar múltiplas identidades virtuais, utilizando inúmeros identificadores, como por exemplo ter diversas contas em diversas redes sociais. Esses identificadores são utilizados para estabelecer conexões com outras identidades digitais, permitindo que elas interajam com outros usuários, plataformas e sistemas dentro desse ambiente virtual (BRASIL, 2021).

Um dos principais objetivos do ataque nessa camada é o roubo de identidade para se obter vantagens indevidas, realizar fraudes, roubar informações sensíveis, se passar por outra pessoa ou entidade, espalhar desinformação ou causar danos às vítimas. Esse ataque pode comprometer as contas de usuário, roubar a identidade, permitir acesso não autorizado a sistema, vazamento de informações pessoais ou financeiras e danos à reputação (KASPERSKY, 2023).

Um exemplo emblemático com relação a vulnerabilidades dessa camada foi a invasão de hackers ao sistema do Exército e a divulgação de dados pessoais de mais de 7 mil militares entre 08 e 09 de novembro de 2015, cuja motivação foi uma represália à forma como o Exército estava conduzindo os jogos de Guerra Cibernética (CAPIROTO, 2015). Apesar do incidente não ter comprometido os sistemas estratégicos de defesa dos servidores, esse caso demonstrou o quanto de Defesa Cibernética Nacional precisa ser aprimorada e que as vulnerabilidades críticas devem ser corrigidas.

Em virtude do acima exposto, para o pleno funcionamento das atividades no ambiente cibernético, as três camadas precisam estar integralmente protegidas. Dessa forma, nos

alinhamos com o expresso por De Oliveira e Portela (2017), que os documentos produzidos pelo nível político e estratégico devem enfatizar ações que fortaleçam as três camadas, reconhecendo papéis distintos e complementares no ecossistema cibernético.

Após abordar as três camadas do espaço cibernético e a importância de cada uma delas, iremos nos aprofundar nos tipos de vulnerabilidades, em especial naquelas utilizadas no ataque relacionado ao NotPetya.

2.3.2 As Vulnerabilidades do Espaço Cibernético

As ameaças cibernéticas referem-se à possibilidade de uma vulnerabilidade ser aproveitada por uma agente malicioso de forma intencional ou acidentalmente devido a causas naturais a erros humanos ou a falhas de sistemas. O termo ameaça pode ser interpretado como os agentes (hackers, criminosos cibernéticos ou espiões cibernéticos) e os seus métodos de ataque, podendo ser não previstos e desconhecidos pelo defensor (BRASIL, 2021).

A existência dessas vulnerabilidades nos sistemas de informação está relacionada a diversos fatores técnicos e humanos. Elas surgem devido a falhas no processo de desenvolvimento de equipamentos, sistemas e softwares, possibilitando a exploração das brechas de segurança. Além disso, a inserção de linha de códigos por indivíduos mal-intencionados é uma vulnerabilidade, uma vez que eles podem realizar tarefas não autorizadas (BRASIL, 2021).

Outro aspecto, é a vulnerabilidade causada pela configuração inadequada de sistemas ou equipamentos. Quando a configuração não é realizada adequadamente, surgem pontos fracos que podem ser explorados por invasores. Além disso, a falta de atualização dos equipamentos e sistemas também levam ao seu surgimento, visto que as atualizações mais recentes trazem geralmente as correções de segurança para enfrentar as ameaças (BRASIL, 2021).

Face o exposto, podemos afirmar que todas as vulnerabilidades acima estão associadas à Insegurança Latente, uma das características da Defesa Cibernética, que afirma que todos os sistemas têm potenciais falhas de segurança.

E por último, as ações humanas inadequadas resultam em vulnerabilidades como por exemplo o hábito de compartilhar senhas, utilização de senhas fracas, abertura de anexos de

e-mails suspeitos, instalação de programas piratas ou a visita a sites não confiáveis (BRASIL, 2021).

2.3.3 A Classificação das Vulnerabilidades Técnicas

Conhecer as vulnerabilidades técnicas é de grande importância para a Defesa Cibernética, já que os pontos fracos podem ser explorados por agentes mal-intencionados. Essas vulnerabilidades podem ser classificadas em diferentes categorias, dependendo do seu status de divulgação e correção. Basicamente, essas vulnerabilidades são classificadas em conhecida e não-conhecidas (BRASIL, 2021).

A primeira categoria é dividida em outras três subcategorias: vulnerabilidades conhecidas, divulgadas e corrigidas; vulnerabilidades conhecidas, divulgadas e não-corrigidas; vulnerabilidades conhecidas e não divulgadas (BRASIL, 2021).

Para o nosso objeto de estudo, iremos nos aprofundar sobre as vulnerabilidades conhecidas e não divulgadas também chamada de vulnerabilidade de dia zero ou *zero-day*[17]. A definição dessa vulnerabilidade de acordo com o Glossário de Segurança da Informação é a seguinte:

> Falha na segurança de um software que ainda não é conhecida por seus desenvolvedores, pelos fabricantes de soluções de segurança e pelo público em geral. Também é considerada uma Vulnerabilidade de Dia Zero a falha de segurança que já é conhecida pelo fornecedor do produto, mas para a qual ainda não existe um pacote de segurança para corrigi-la. Por não ser conhecida ou por não haver ainda um patch de segurança para essa falha, ela pode ser explorada por hackers em Explorações de Dia Zero. A correção de uma vulnerabilidade de dia zero geralmente é tarefa do fabricante do software, que precisará lançar um pacote de segurança para consertar a falha (BRASIL, 2019).

O mesmo glossário afirma que a exploração de dia zero é um tipo de ataque cibernético que se aproveita dessa vulnerabilidade por meio das falhas de segurança desconhecidas pelos desenvolvedores para infectar um dispositivo com algum tipo de malware. Esse tipo de ataque é o mais perigoso, visto que é o mais difícil de ser detectado, uma vez que não há correção disponível para a vulnerabilidade. Contudo, outras medidas podem ser utilizadas para mitigar ou evitar esse ataque, como o uso de ferramentas de segurança que monitoram o comportamento do tráfego e o acesso aos dispositivos, que serão importantes na

---

[17] A expressão *zero-day* é a mais difundida no jargão hacker (GREENBERG, 2018).

identificação de atividades suspeitas ou maliciosas (BRASIL, 2019).

A expressão “dia zero” vem do fato de que os desenvolvedores tiveram “zero dias” para corrigir e disponibilizar uma atualização de segurança para garantir a proteção dos usuários (GREENBERG, 2018).

Nessa análise, iremos abordar uma vulnerabilidade de dia zero relacionada ao malware NotPetya, que é conhecida como EternalBlue. Essa vulnerabilidade foi a mais persistente e prejudicial, pois afetava o protocolo de compartilhamento de arquivos do Windows®. Sua notoriedade ganhou força quando um grupo conhecido como Shadow Brokers divulgou a informação de forma ostensiva, em 14 de abril de 2017, para hackers mal-intencionados que realizaram a disseminação de malwares de forma rápida e eficiente (BURDOVA, 2020).

O EternalBlue, originalmente desenvolvido pela Agência de Segurança Nacional dos Estados Unidos (NSA), se constitui de uma série de vulnerabilidades de softwares da Microsoft Corporation criadas como ferramentas de ataque cibernético. Ela foi usada em diversas missões de coleta de informações e contraterrorismo pela NSA. Infelizmente, a sua divulgação acidental causou graves consequências para a segurança cibernética em todo o mundo (BURDOVA, 2020).

2.4 Estratégias Aplicadas na Condução da Defesa Cibernética

Como abordado no início desse capítulo, uma doutrina militar precisa passar por testes práticos para a sua avaliação e sua implementação, devendo também estar alinhada com a estratégia. Entretanto, Coutau-Bégarie (2010) ao analisar a estratégia marítima teórica observou que sempre houve um retardo desta sobre a prática. A escola teórica do canhão não observou os riscos do submarino na Primeira Guerra Mundial e os partidários dos Porta-Aviões foram ignorados diante dos partidários dos encouraçados na véspera da Segunda (COUTAU-BÉGARIE, 2010).

Criada no século XX, a aeronave foi empregada inicialmente pelos Exércitos e Marinhas utilizando as mesmas táticas do domínio terrestre e marítimo. Com o tempo, novos teóricos surgiram e desenvolveram a nova estratégia aérea, o que tornou evidente a necessidade da criação de uma nova Força. Essa nova Força se consolidou entres os países, visto que o tempo de reação, os meios e as táticas são diferentes entres esses domínios (PAGLIUSI, 2022).

Nesse contexto, o Almirante Vidigal (1985) narra a conturbada criação da Força Aérea

Nacional em 1941, que mais tarde seria a Força Aérea Brasileira (FAB), que foi influenciada pelo sucesso Alemão da Luftwaffe no início da Segunda Guerra Mundial, extinguindo a Aviação Naval e a Aviação Militar. Todas as aeronaves, pilotos e instalações foram transferidos para a FAB, sob os protestos dos Estados-Maiores do Exército e da Marinha.

Anos depois, a Aviação Naval iria renascer na MB em virtude da importância tática da aviação embarcada na condução das operações navais, sendo consolidada com a aquisição do Navio Aeródromo Ligeiro Minas Gerais, em 1957, para a realização de guerra antissubmarino (VIDIGAL, 1985).

Face ao exposto, podemos inferir que há um retardo da criação de uma suposta estratégia cibernética com relação à prática. Como as armas cibernéticas são criações recentes, observamos a aplicação da tática aérea no ciberespaço devido à falta de tática cibernética própria.

Em 2017, na cidade de São Francisco, uma conferência anual de cibersegurança corporativa abordou a importância das instituições conquistarem a resiliência cibernética. Para isso, aconselhou o referido modelo de decisão estratégica, conhecido como ciclo OODA: observar, orientar-se, decidir e agir (CLARKE; KNAKE, 2021).

O criador desse ciclo foi o Coronel John Boyd, ex-aviador da Força Área Americana, que a partir da abordagem teórica da paralisia estratégica recomendou maximizar a fricção contra o inimigo, combinando diversas ações com a maior rapidez possível, para deixá-lo sem reação (COUTAU-BÉGARIE, 2010). Lind (1985) exemplifica as etapas do ciclo da seguinte forma:

> O conflito pode ser visto como ciclos competitivos, no tempo, de observação-orientação-decisão-ação. Cada parte no conflito começa observando. Observa a si próprio, seu entorno físico e seu inimigo. Baseado em sua observação, orienta-se, quer dizer, faz uma imagem mental ou “uma fotografia” da situação. Baseado nesta orientação, toma uma decisão. Coloca esta decisão em prática, ou seja, em ação. Então, devido a sua ação, a situação é alterada, observa novamente, e inicia-se o processo de novo. As ações empreendidas fazem o ciclo girar, algumas vezes denomina-se este como “Ciclo de Boyd” ou “Ciclo OODA” (LIND, 1985, p. 5, tradução nossa)[18].

Conforme representado na FIG. 2, essa ideia foi aplicada aos ciberdefensores, que para ter êxito precisavam “penetrar” no ciclo OODA dos agentes maliciosos para contra-atacar com

---

[18] Do original em inglês: *Conflict can be seen as time-competitive observation-orientation-decision-action cycles. Each party to a conflict begins by observing. He observes himself, his physical surroundings and his enemy. On the basis of his observation, he orients, that is to say, he makes a mental image or "snapshot" of his situation. On the basis of this orientation, he makes a decision. He puts the decision into effect, i.e., he acts. Then, because he assumes his action has changed the situation, he observes again, and starts the process anew. His actions follow this cycle, sometimes called the "Boyd Cycle" or "OODA Loop.*

mais velocidade e agilidade (CLARKE; KNAKE, 2021).

A grande dificuldade encontrada de se utilizar esse teórico no domínio cibernético é que atualmente um hacker leva um dia para penetrar em um sistema e aproximadamente duzentos para que os defensores o encontrem. Os atacantes têm uma dedicação exclusiva para gerar estragos, porém as organizações precisam conciliar as tarefas de defesa com o ciclo de negócios (CLARKE; KNAKE, 2021).

Concluímos que o ciclo OODA é mais fácil de ser aplicado em um ataque cibernético em comparação à proteção cibernética. Assim a proteção deve buscar a resiliência cibernética e adotar outras medidas como ferramentas de segurança que monitoram o comportamento do tráfego e o acesso aos dispositivos.

Outro teórico da paralisia estratégica que tem sido utilizado na criação de uma estratégia cibernética é o Coronel John Warden, ex-piloto da mesma Força do Coronel Boyd. Ele considerou que o inimigo é composto por diversos subsistemas que precisam ser atacados simultaneamente em seus pontos fracos para causar a paralisia estratégica.

Conforme destacado na FIG. 3, esses subsistemas são formados por cinco anéis concêntricos: Lideranças Nacionais, Funções Vitais (rede elétrica, instalações petrolíferas), Infraestrutura Nacional (sistema de transporte), População e Força Militar Desdobrada (COUTAU-BÉGARIE, 2010).

Para melhor exemplificar, Warden faz a seguinte analogia biológica para traçar paralelos com o corpo humano:

> O cérebro, recebendo informações dos olhos e do sistema nervoso central, representa a liderança do corpo. Alimentos e oxigênio são duas funções orgânicas essenciais, enquanto vasos sanguíneos, ossos e músculos fornecem a infraestrutura. As células constituem a população do corpo, enquanto linfócitos e leucócitos, juntamente com outros glóbulos brancos, fornecem proteção contra os ataques. Se qualquer parte do corpo parar de funcionar, isso terá um efeito mais ou menos importante no resto do corpo (FADOK, 1995, p. 30, tradução nossa)[19].

Estudos realizados por Gonçalves (2018), Carvalho (2020) e Coutinho (2020) verificaram a possibilidade de aderência dessa teoria em ataques cibernéticos. Considerando que um atacante cibernético é mais rápido que um ataque aéreo e que a penetração nos

---

[19] Do original em inglês: *The brain, receiving inputs from the eyes and central nervous system, represents the body's leadership. Food and oxygen are two organic essentials, while blood vessels, bones, and muscles provide the infrastructure. Cells constitute the body's population, while specific lymphocytes and leukocytes, along with other white blood cells, provide protection from attack. If any part of the body stops functioning, it will have a more or less important effect on the rest of the body.*

diversos subsistemas pode ser feita de forma simultânea e instantânea, consideramos, portanto, que a aplicação da teoria de Warden no ciberespaço é válida.

Seguindo as observações de Pagliusi (2022), verificamos que a História nos fornece indícios de que países criarão forças armadas específicas para cada domínio de guerra, como por exemplo a recente criação da Força Espacial dos EUA, em 20 de dezembro de 2019, que tem como atribuição as operações militares no quarto domínio da guerra, o espaço sideral (EUA, 2023). Assim há de se esperar que em um futuro não tão distante seja criada a Força Cibernética utilizando para isso as suas próprias teorias, meios e combatentes especializados no quinto domínio da guerra.

Concluímos, dessa forma, o nosso capítulo teórico e passamos para o capítulo de análise do nosso objeto de estudo.

3 NOTPETYA E O ATAQUE À INFRAESTRUTURA UCRANIANA

Neste capítulo, será relatado os principais fatos relacionados ao ataque cibernético do malware NotPetya, em 27 junho de 2017, que teve como alvo o governo e a infraestrutura da Ucrânia e, por conseguinte, se difundiu pelo resto do mundo, em especial pelas empresas globais que estavam conectadas em rede com aquele país. O conhecimento desses fatos serão grande importância no próximo capítulo onde faremos a aderência com a teoria do segundo capítulo.

Cabe ressaltar que apesar dos fortes indícios de que o ataque tenha se originado na Rússia, esse país até o momento não assumiu formalmente a responsabilidade. Para um melhor desenvolvimento da pesquisa, iremos adotar o conteúdo do trabalho investigativo realizado por Greenberg (2018, 2021) que atribui o desenvolvimento e a disseminação do malware NotPetya ao grupo de hackers conhecido como Sandworm, grupo supostamente ligado à GRU.

Assim, serão abordadas as causas e os antecedentes históricos do conflito Rússia-Ucrânia do fim da Guerra Fria até o momento em que foram realizados os ataques e como o conflito se tornou um campo de testes para a Guerra Cibernética. Em seguida, serão detalhados os métodos utilizados, capacidades, objetivos e consequências do ataque.

3.1 As Causas e Antecedentes Históricos

As animosidades entre Rússia e Ucrânia foram acentuadas com o fim da Guerra Fria pelos seguintes motivos: confronto entre o nacionalismo ucraniano e o nacionalismo russo; avanço da OTAN e da União Europeia (UE) sobre o Leste Europeu; e a perda da influência nas áreas da antiga URSS por meio da ascensão da democracia ocidental (APARECIDO; AGUILAR, 2022).

A Ucrânia possui 77,8% da etnia ucranianas e 17,3% da etnia russa (RABOCZKAY, 2022), sendo que a maioria dessa última está próxima com a fronteira da Rússia. As duas etnias guardam um nacionalismo que diverge entre si. Os nacionalistas ucranianos, com o fim da Guerra Fria, obtiveram do Ocidente o apoio necessário para a sua independência em 24 de agosto de 1991. Eles abraçaram o modelo de democracia ocidental e desde então buscam uma maior aproximação com o Ocidente, sendo favoráveis que o país faça parte da OTAN e

UE. Já os nacionalistas russos, ucranianos de etnia russa, opõem-se ao Ocidente e defendem que a Ucrânia deva fazer parte da área de influência da Rússia. Essas tensões são acentuadas ainda mais pelo apoio do governo russo aos separatistas pró-Rússia presentes no território ucraniano (APARECIDO; AGUILAR, 2022).

Outro ponto de destaque, é a obstinação dos EUA e de seus aliados de trazer a Ucrânia para área de influência do Ocidente, promovendo a democracia no país e buscando incorporá-la na OTAN e UE. Entretanto, o que mais tem incomodado a Rússia é a OTAN, pois a sua expansão põe em risco a segurança de seu país (APARECIDO; AGUILAR, 2022).

Essa expansão do Ocidente para as áreas de influência russa tem como objetivos: asfixiar a Rússia, criar instabilidade política, ocupar vácuos de poder e obter acesso ao gás natural e ao petróleo eurasianos (APARECIDO; AGUILAR, 2022).

Ao longo da História da Rússia, o país sofreu diversas invasões oriundas do leste e do oeste desde o século IX. Dentro do subconsciente coletivo, o avanço do Ocidente é visto com desconfiança, já que começa a afetar o entorno estratégico russo (APARECIDO; AGUILAR, 2022).

A Ucrânia, em especial os nacionalistas ucranianos, consideram a URSS, e indiretamente a Rússia, como a opressora e a agressora que os isolou do convívio da sociedade ocidental. A aproximação da Ucrânia com o Ocidente, deixa claro a rejeição à Rússia, mas essa não consegue aceitar (APARECIDO; AGUILAR, 2022).

A OTAN, uma aliança de defesa coletiva, é considerada pela Rússia como uma ferramenta de dominação ocidental. De acordo com Aparecido e Aguilar (2022), com o discurso de democracia e de direitos humanos, os EUA usam a aliança para atender aos interesses econômicos americanos, em especial quando se trata de reservas de petróleo e de gás natural (APARECIDO; AGUILAR, 2022).

Em face ao exposto, percebemos que a Rússia busca um estado final[20] para o conflito que é a manutenção da Ucrânia em sua esfera de influência, evitando a sua aproximação com Ocidente. Já a Ucrânia busca consolidar a sua soberania e a sua independência se afastando da influência russa e se aproximando com o Ocidente.

Para Brzezinski (1997), a Rússia foi prejudicada pela independência da Ucrânia, pois

---

[20] Estado final - Situação política ou militar a ser alcançada ao final das operações e que indica se o efeito desejado foi alcançado (BRASIL, 2015, p. 108).

perdeu sua posição de domínio no Mar Negro. A cidade de Odessa, a noroeste da Península da Crimeia, desempenha um papel estratégico como uma porta de entrada essencial para o comércio com o Mediterrâneo e outras regiões do mundo. Dessa forma, ele conclui que uma das condições para a Rússia voltar a ser uma grande potência é mantendo a Ucrânia em sua área de influência. Sem a Ucrânia, se tornaria apenas um império asiático, em conflito com o Cáucaso e na Ásia Central.

Segundo Huntington (1997), os conflitos no mundo pós Guerra Fria deixaram de ser econômicos ou ideológicos para ser culturais. Assim, a Ucrânia tornou-se a linha de cisão entre duas civilizações: o mundo ocidental, sendo os Estados-Núcleos os EUA e a Europa, e o mundo ortodoxo oriental, sendo a Rússia o Estado-Núcleo dessa civilização. Uma das preocupações dele seria o declínio da civilização ocidental e caso os EUA e a Europa não se unirem, há a possibilidade de ser eliminados separadamente pelas outras civilizações.

Logo, nesse cenário conflituoso, Korybko (2018) observou que o movimento Euromaidan, em novembro de 2013, foi uma bem-sucedida aplicação da Guerra Híbrida[21] pelos EUA, tendo a Guerra Cibernética como uma de suas ferramentas. Desde então, percebemos a intensificação deste tipo de guerra da Rússia contra a Ucrânia para causar instabilidade e enfraquecimento.

Aquele país tinha se tornado um campo de testes para o desenvolvimento das táticas russas de Guerra Cibernética, e um grupo em particular conhecido como Sandworm estava invadindo dezenas de organizações e empresas ucranianas (GREENBERG, 2018). A cada ano, a intensidade dos ataques cibernéticos se intensificava, a ponto de causar apagões em diversas partes da Ucrânia nos invernos de 2015 e 2016.

É relevante mencionar que Korybko (2018) buscou os teóricos da estratégia área, Boyd e Warden, para desenvolver a teoria aplicada à Guerra Híbrida. Para ele, os EUA estão utilizando uma nova tática em países não alinhados com sua visão político-ideológica e que as nações-alvos precisam compreender esses métodos utilizados para se defender de possíveis golpes de Estado.

Finalizada as considerações sobre as causas e os antecedentes históricos sobre o

---

[21] Guerra Híbrida - Caracteriza-se quando as ações de combate convencional são aglutinadas, no tempo e no espaço, com operações de guerra irregular, de guerra cibernética e de operações de informação, dentre outras, com atores estatais e não estatais, no ambiente real e informacional, incluindo as redes sociais (BRASIL, 2018, p. 183).

conflito russo-ucraniano, iremos abordar o ataque cibernético do malware NotPetya.

3.2 O Caso Maersk

No dia 27 de junho de 2017, os funcionários da Maersk[22] começaram a ter seus respectivos laptops inutilizados. Alguns liam “O sistema de arquivos em C: está em reparo” e minutos depois “... seus arquivos foram criptografados”, exigindo o pagamento de US$ 300 em bitcoin[23] para descriptografar. A propagação foi tão rápida que em poucos minutos todos os computadores em uma mesma sala da Maersk apresentaram a mesma tela (GREENBERG, 2018).

Em questões de instantes, a sede na Dinamarca entrou em crise e pelos corredores funcionários corriam para desligar todos os computadores e retirar da rede, antes que o software malicioso infectasse mais unidades porque a cada minuto dezenas de computadores se tornavam corrompidos (GREENBERG, 2018).

Houve a necessidade de desconectar toda a rede global da Maersk e a maioria dos funcionários foi para casa, entretanto, a equipe de tecnologia da informação (TI) iniciou uma grande jornada para entender e restabelecer o sistema (GREENBERG, 2018).

Esse ataque fez com que as operações da Maersk fossem paralisadas, destacando se os megaportos de Nova York, Nova Jersey, Los Angeles e Roterdã. Todos os dados de localização e conteúdo dos contêineres foram apagados por meio do ataque (CLARKE; KNAKE, 2021).

Durante um período de dez dias, a Maersk realizou a reinstalação de 4.000 servidores, 45.000 computadores pessoais e 2.500 aplicativos, graças ao trabalho árduo da sua equipe de TI. Durante esse tempo, a empresa enfrentou uma redução de 20% em seu volume de operações, sendo que os outros 80% restantes foram executados manualmente (e-mail e telefone) até que os sistemas fossem restaurados ao pleno funcionamento. O custo total da interrupção das operações foi de US$ 300 milhões (ZDNET, 2018).

No relato apresentado, percebemos o que muitas empresas e instituições sofrem quando ocorre um ataque de *ransomware*. Além do aspecto financeiro, a reputação da

---

[22] Maior empresa de transportes marítimos de contêineres do mundo, movimentando 12 milhões de contêineres por ano (MAERSK, 2023).

[23] Tipo de moeda digital, ou criptomoeda, gerado por redes de computadores para substituir as moedas tradicionais (KASPERSKY, 2023).

empresa fica abalada diante de seus parceiros e clientes. Assim, após um grande incidente, mesmo que haja grandes investimento para evitar a repetição dessas situações desastrosas, como relatado, a reconquista da confiança exigirá um grande esforço e dedicação.

3.3 O Ataque Realizado na Ucrânia

No dia 27 de junho de 2017, véspera do feriado nacional do Dia da Constituição da Ucrânia[24], em uma pequena empresa familiar de software, sediada em Kiev, chamada Linkos Group, seus servidores enviaram algumas atualizações de rotina para um software de contabilidade fiscal chamado MeDoc. Esse produto era popular e amplamente utilizado por pessoas e instituições na Ucrânia para declaração de seus impostos ou fazer negócios. Contudo, em algum momento, essas máquinas foram o marco-zero para o ataque cibernético mais devastador desde a criação da internet, no qual uma nação foi atacada por uma outra (GREENBERG, 2018).

Na tentativa de contextualizar a importância do MeDoc para a Ucrânia, podemos inferir que ele teria o mesmo grau de importância que o Programa Gerador de Declaração do Imposto sobre a Renda no contexto brasileiro, cujo número de declarações enviadas no ano de 2023 foi de 41.151.515 (BRASIL, 2023).

Em maio de 2017, hackers militares russos conseguiram o acesso aos servidores da Linkos Group e implantaram o NotPetya em um pacote de atualização do MeDoc. Então, em 27 de junho de 2017, quando a atualização foi disponibilizada, o malware foi propagado para todos os computadores que tinham esse programa (GREENBERG, 2018). Ou seja, muitas pessoas físicas e jurídicas que pagavam os seus impostos e que utilizavam o MeDoc tiveram os seus computares criptografados de forma irreversível.

Após a "infecção" na máquina, o malware conseguia se propagar de forma automática e indiscriminada entre os computadores que estavam na mesma rede, sendo considerado o ataque mais rápido da história até então (GREENBERG, 2018).

---

[24] No dia 28 de junho de 1996, a Verkhovna Rada (o Parlamento) da Ucrânia aprovou uma nova Lei no país – primeira Constituição do Estado moderno ucraniano. Essa constituição, além de consolidar os princípios fundamentais da democracia, independência, direitos humanos e liberdades fundamentais, determina que a política externa da Ucrânia é destinada a assegurar os seus interesses nacionais e sua segurança, mantendo a cooperação pacífica e mutuamente benéfica com a comunidade internacional com base em princípios e normas do direito internacional universalmente reconhecidos (UCRÂNIA, 2013).

Além da implementação do EternalBlue *c*om as informações vazadas da NSA no início do ano de 2017, o NotPetya incorporou uma invenção mais antiga chamada Mimikatz, desenvolvida pelo pesquisador em segurança francês Benjamin Delpy em 2011. Ele demonstrou que o Windows® deixava as senhas dos usuários em texto claro na memória dos computadores. Assim, os hackers conseguem obter acesso inicial a um computador e o Mimikatz pode extrair as senhas da memória RAM e usá-las também para invadir outras máquinas em rede com as mesmas credenciais. Com as senhas de administrador obtidas pelo Mimikatz e com as vulnerabilidades do EternalBlue, em questão de minutos o computador era criptografado de forma irreversível e o NotPetya transferido para outros computadores em rede (GREENBERG, 2018).

Mantendo a falha em segredo por aproximadamente 5 anos (CLARKE; KNAKE, 2021), o EternalBlue era a ferramenta mais poderosa do arsenal cibernético da NSA. Com o vazamento em 2017, a NSA fez contato com a Microsoft Corporation informando da vulnerabilidade de dia zero, o que a fez lançar a atualização de segurança MS17-010 para o Windows®, em 14 março de 2017 (MS17-010, 2017). Sabendo que muitos usuários ainda utilizavam versões antigas, como o Windows XP®, que ficou sem suporte em 08 de abril de 2014 (TECHTUDO, 2014), em maio de 2017 foi lançado as correções críticas de segurança para o software (MS17-010, 2017). Somente em 14 abril de 2017, o Shadow Brokers confirmou, por meio de uma conta do Twitter, que tinha obtido a ferramenta (BURDOVA, 2020).

Analisando os estragos realizados pelo NotPetya, consideramos que houve a falta de uma comunicação mais efetiva por parte da Microsoft Corporation, informando que o mundo estaria em perigo se medidas não fossem tomadas com relação às atualizações críticas. Além disso, houve também o descaso por parte de administradores e usuários em manter os seus sistemas operacionais atualizados.

Conforme divulgado por TechTudo (2022), acreditamos que o grande sucesso da disseminação do NotPetya, em 27 de junho de 2017, foi pelo fato de 98% dos usuários não manterem os seus softwares atualizados, segundo pesquisa da associação norte-americana de profissionais de TI, também conhecida como USENIX.

Ademais, a própria equipe de segurança da Maersk confessou que utilizavam em alguns servidores da corporação o Windows 2000®, que tinha terminado o suporte da

Microsoft Corporation em 13 de julho de 2010 (GREENBERG, 2018). De acordo com a ESET[25], de todas as infecções causadas no mundo por malware em junho de 2017, 80% delas aconteceram em território Ucraniano e 9%, em segundo lugar, na Alemanha (WAKEFIELD, 2017).

Foi por meio de um único computador com o MeDoc instalado, em um escritório em Odessa, na Ucrânia, utilizado por um executivo financeiro, que toda a infecção se tornaria fatal para Maersk (GREENBERG, 2018). O malware se alastrou pelas empresas globais que operavam naquele país por meio das redes privadas virtuais (VPN) e conexões de fibras alugadas (CLARKE; KNAKE, 2021).

Em virtude do acima exposto, verificamos que todas as instituições conectadas com a internet possuem uma superfície exposta suscetível a ataques. Essa Insegurança Latente, uma das características da Defesa Cibernética, nos obriga a pensar sobre outras formas de lidar com o problema.

No caso Maersk, a empresa levou 10 dias para se recuperar do ataque. Mesmo que se busque fechar todas as portas, os hackers sempre encontrarão alguma brecha. Dessa forma, chegamos à conclusão de que além da importância da proteção cibernética, as empresas e instituições precisam fortalecer a resiliência cibernética, diminuindo o tempo de recuperação após um evento catastrófico.

No dia 15 de fevereiro de 2018, o governo dos EUA responsabilizou a Rússia pelo ataque (CHALFANT, 2018) e, logo em seguida, os demais membros da Aliança Five Eyes[26] fizeram o mesmo. De acordo com o ex-conselheiro de Segurança Interna da Casa Branca Tom Bossert, a arma cibernética usada pela Rússia contra a Ucrânia foi desproporcional porque o mundo todo foi afetado, comparando o uso de uma bomba nuclear para ter apenas uma pequena vitória tática. Afirmou também que o resultado foi mais de 10 bilhões de dólares de prejuízo, o mais destrutivo já registrado, no qual esse valor é apenas um piso e não um teto (GREENBERG, 2021).

Em escala nacional, Greenberg afirma que:

> Em resumo, no final de 27 de junho, o NotPetya havia atingido pelo menos quatro

---

[25] Empresa de software eslovaca especializada em cibersegurança que fornece software de segurança em mais de 200 países e territórios em todo o mundo. É uma das pioneiras em cibersegurança na Europa e é administrada pelos mesmos engenheiros que iniciaram a empresa há três décadas (ESET, 2023)

[26] Aliança de inteligência composta por Austrália, Canadá, Nova Zelândia, Reino Unido e Estados Unidos (DNI, 2020)

> hospitais apenas em Kiev, junto com seis companhias elétricas, dois aeroportos e mais 22 bancos ucranianos, caixas eletrônicos, sistemas de pagamento com cartão e praticamente o governo federal inteiro. De acordo com a ISSP[27], pelo menos trezentas empresas foram atingidas, e mais tarde um oficial sênior do governo ucraniano faria a estimativa de que um total de 10% de todos os computadores do país foram apagados; a internet do país foi literalmente dizimada (GREENBERG, 2021, p. 183).

Em escala mundial, ele elenca as seguintes organizações afetadas pelo NotPetya:

> Ele prejudicou empresas multinacionais, incluindo a Maersk; a gigante farmacêutica Merck; a subsidiária europeia da FedEx, TNT Express; a empresa francesa de construção Saint-Gobain; a empresa-mãe do ramo industrial alimentício da Cadbury e da Nabisco, Mondelēz; e a fabricante inglesa Reckitt Benckiser, cujos produtos incluem as camisinhas Durex e o desinfetante Lysol. Em cada um desses casos, ele causaria centenas de milhões de dólares de prejuízo. Espalhou-se até mesmo para a Rússia — o principal suspeito imediato da comunidade de cibersegurança para a origem do NotPetya —, atingindo vítimas como a empresa petrolífera Rosneft, a siderúrgica Evraz, a empresa de tecnologia médica Invitro e o Sberbank (GREENBERG, 2021, p. 177).

Apesar do esforço em qualificar e quantificar as perdas financeiras, não encontramos estudos para contabilizar as possíveis perdas humanas, pois toda a infraestrutura de um país foi paralisada, incluindo os serviços de saúde, o abastecimento de energia, o sistema financeiro, sem contar os diversos medicamentos e equipamentos médicos que tiveram as suas entregas atrasadas em virtude do ataque. Desse modo, concluímos o presente capítulo abordando as causas do conflito Rússia-Ucrânia e como foram os acontecimentos do ataque cibernético. No próximo capítulo, abordaremos a aderência entre a teoria exposta no segundo capítulo com os fatos apresentados no terceiro capítulo.

---

[27] ISSP - Empresa que realiza pesquisa e ciência forense em Kiev (GREENBERG, 2021).

4 ADERÊNCIA ENTRE A TEORIA E O ATAQUE CIBERNÉTICO NOTPETYA

Neste capítulo, iremos verificar a aderência dos seguintes aspectos teóricos relacionados à Defesa Cibernética: níveis de decisão, princípios de emprego, características, tipos de ações, as camadas do espaço cibernético, a classificação das vulnerabilidades e as estratégias aplicadas.

Como já foi abordado, não foi possível analisar efetivamente todas as ações de planejamento militar realizadas pela Rússia, em virtude de não terem sido divulgadas. Entretanto, realizaremos o esforço para inferir esse planejamento baseado nas investigações de Greenberg (2018, 2021) para confrontar com a teoria apresentada.

4.1 Análise do Nível de Decisão

Nesta seção verificaremos se as ações adotadas pela Rússia tiveram aderência com os níveis de decisão político e estratégico, conforme detalhado na subseção 2.2.1 com as atribuições de cada nível.

No nível estratégico, assim como o Exército Brasileiro foi designado para coordenar o setor cibernético em termos de Defesa Nacional, realizando a integração com diversas entidades e instituições, percebemos que a GRU também realiza a mesma tarefa ao coordenar os diversos grupos hackers, como o SandWorm que desenvolve armas cibernéticas e realiza ataques sob autoridade russa.

Já no nível político, não é possível concluir se o governo russo autorizou o ataque ou se já existia uma liberdade de ação para ataques cibernéticos russos contra a Ucrânia. Percebemos que o malware retornou para a Rússia, afetando a empresa petrolífera Rosneft, a siderúrgica Evraz, a empresa de tecnologia médica Invitro e o Sberbank. Além dessas consequências negativas para o país, verificamos que o ataque ao sair do teatro de operações[28] ucraniano atingiu diversas partes do mundo. Isso poderia gerar retaliações de outros países com graves consequências diplomáticas.

É de se esperar que o nível político conheça essas consequências negativas e que tenha

---

[28] Teatro de Operações - Parte do teatro de guerra necessária à condução de operações militares de grande vulto, para o cumprimento de determinada missão e para o consequente apoio logístico (BRASIL, 2015, p. 265).

capacidade de autorizar ou não esse tipo de ataque cibernético que pode ter graves efeitos no âmbito interno e externo do país. Assim, conseguimos evidenciar que a Doutrina Militar de Defesa Cibernética, com os seus níveis de decisão, estabelece que esse tipo de ataque em um período de não guerra só pode ser autorizado pelo nível político. Concluímos assim, que houve aderência apenas no nível estratégico para o conflito analisado.

Com relação à lição aprendida, podemos perceber a importância da captação de recursos humanos fora do âmbito das Forças Armadas para enfrentar os desafios emergentes no espaço cibernético. Assim como a GRU tem estreitas relações com o SandWorm, o Sistema Militar de Defesa Cibernética[29] precisa identificar e recrutar especialistas e profissionais do setor privado, universidades e instituições de pesquisa para cooperarem com a Defesa Cibernética Brasileira, garantindo maior resiliência e proteção contra ameaças externas.

4.2 Análise dos Princípios de Emprego

Na subseção 2.2.2 apontamos os seguintes Princípios de Emprego: Efeito, Dissimulação, Rastreabilidade e Adaptabilidade. Nesta seção, iremos analisar os fatos com relação a esses princípios.

Com relação ao Princípio do Efeito, percebemos que houve aderência, visto que o ataque produziu consequências devastadoras no cotidiano, na economia e na segurança nacional ucranianas. Além disso, diversas empresas e organizações no mundo foram afetadas incluindo empresas de transporte, bancos, hospitais e sistemas governamentais, levando a graves impactos na economia, na saúde pública e nos sistemas de infraestrutura crítica.

Como exemplo podemos apontar: a Maersk relatou um prejuízo de US$ 300 milhões em virtude de interrupções das operações; hospitais na Ucrânia tiveram os atendimentos médicos afetados; e impactos no fornecimento de energia e transportes afetaram o dia a dia do cidadão ucraniano.

O Princípio da Dissimulação também está presente, uma vez que a autoria do ataque não foi conclusiva. Podemos verificar outra aderência a esse princípio em virtude da rápida e

---

[29] O Sistema Militar de Defesa Cibernética é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de defesa no Espaço Cibernético, assegurando, de forma conjunta, o seu uso efetivo pelas FA, bem como impedindo ou dificultando sua utilização contra interesses da Defesa Nacional (BRASIL, 2014, p.25).

silenciosa propagação com a criptografia irreversível dos dados dos sistemas. Também podemos apontar a tática de dissimulação ao ser classificado inicialmente como um *ransomware*, porém foi verificado que o único objetivo era apenas destruir, pois o pagamento não resgatava os dados.

Tudo no ciberespaço pode ser rastreado para a obtenção de provas com o intuito futuro de responsabilizar judicialmente o atacante. No caso em questão, o NotPetya não deixou rastros que confirmassem efetivamente a autoria russa. Apenas foi verificado a semelhança do código do NotPetya com outros malwares de autoria do grupo SandWorm. Algo que nos chama a atenção é que o ataque aconteceu na véspera de um feriado nacional, o Dia da Constituição, que é a celebração da independência e da soberania do país com relação à Rússia, provável autora do ataque que teria a intenção de causar uma desmoralização nacional. Então, de certa forma, o Princípio da Rastreabilidade teve aderência parcial ao apontar para a Rússia como possível autor do ataque.

O Princípio da Adaptabilidade trata da capacidade do atacante ser proativo e capaz de se adaptar rapidamente às mudanças no ciberespaço. Esse ataque foi altamente sofisticado e destrutivo, espalhando rapidamente por todo o mundo. Ao tomar conhecimento da vulnerabilidade de dia zero, conhecida como EternalBlue, o grupo SandWorm conseguiu realizar o ataque antes que a vulnerabilidade fosse corrigida pela maioria das entidades. Portanto, o atacante conseguiu ter uma capacidade de adaptação maior que a do adversário, confirmando a aderência ao referido princípio.

Analisando os Princípios de Emprego acima, percebemos que a maioria deles teve aderência com o ataque NotPetya.

4.3 Análise das Características

Na subseção 2.2.3 apontamos como principais características da Defesa Cibernética: Alcance Global, Vulnerabilidade das Fronteiras Geográficas, Insegurança Latente, Mutabilidade, Incerteza e o Paradoxo Tecnológico. Nesta seção, iremos analisar as seguintes características e a sua aderência aos fatos:

a) Alcance Global: o ataque teve alcance global, já que o ciberespaço não tem fronteiras. Algumas empresas atacadas na Ucrânia estavam conectadas com o resto do mundo por meio de VPN ou conexões de fibras alugadas;

b) Vulnerabilidade das Fronteiras Geográficas: o SandWorm conseguiu atuar fora de seus limites geográficos, conseguindo atacar a Ucrânia e diversas organizações em todo o mundo;
c) Insegurança Latente: em virtude de todo sistema computacional possuir vulnerabilidades, o NotPetya explorou essa característica em sistemas desatualizados, sendo disseminado por meio da atualização do MeDoc;
d) Mutabilidade: essa característica está associada à rápida capacidade de se adaptar ao ambiente cibernético. Percebemos que o NotPetya utilizou de forma eficiente as novas vulnerabilidades descobertas, incorporando técnicas avançadas de propagação e alta capacidade de se multiplicar em rede;
e) Incerteza: em algum momento, o ataque pode gerar efeitos indesejados. O ataque foi realizado na Ucrânia, mas acabou se espalhando ao ponto de atingir empresas e organizações russas; e
f) Paradoxo Tecnológico: essa característica ficou clara na Ucrânia quando a maioria das empresas e instituições dependia do software MeDoc para declarar impostos ou fazer negócios. Mesmos essas empresas e instituições com avançadas infraestruturas de TI podem ser vulneráveis aos ataques cibernéticos. Quanto maior a dependência tecnológica, mais suscetível a ataques se encontrará.

Assim, verificamos que as características definidas na doutrina encontraram aderência com os fatos conhecidos.

4.4 Análise dos Tipos de Ações Cibernéticas

Na subseção 2.2.4 discorremos sobre os três tipos de ações no espaço cibernético: exploração, proteção, e ataque cibernéticos. Nessa seção, iremos analisar os tipos e a sua aderência aos fatos:

a) Ataque Cibernético: o NotPetya é um grande exemplo de ataque cibernético automatizado com a atualização de um software, o MeDoc, que foi programado para ocorrer no dia 27 de junho de 2017. Ele destruiu informações armazenadas em dispositivos e redes computacionais;
b) Proteção Cibernética: a Defesa Cibernética Ucraniana não foi efetiva com relação à proteção desse ataque. Após iniciado, a única forma encontrada pelas

instituições para mitigar sua ação foi o desligamento dos computadores e desconexão das redes. Um aspecto que levantamos é que houve uma baixa resiliência cibernética, pois o restabelecimento de alguns sistemas levou dias;

c) Exploração Cibernética: podemos afirmar que essa foi a principal ação realizada pelo SandWorm, visto que buscou e coletou informações em sistemas de TI de interesse, identificando a dependência tecnológica de uma nação relacionada à apenas um software de contabilidade de cálculo de imposto. Além disso, a exploração cibernética foi realizada na empresa Linkos Group para implantar o malware no servidor de atualização.

Concluímos que os três tipos de ações no espaço cibernético podem ser observados comprovando a aderência à doutrina.

4.5 Análise das Camadas do Espaço Cibernético

De forma didática, apresentamos na subseção 2.3.1 as camadas existentes no espaço cibernético, conforme o contido na Doutrina Cibernética da Marinha. No estudo em questão, verificamos que a primeira camada, o estrato físico, e a terceira, o estrato das identidades virtuais, não eram o objetivo do NotPetya.

Esse não destruiu equipamentos e nem obteve ou vazou dados. O único objetivo foi a destruição da segunda camada, o estrato lógico, uma vez que todos os computadores com Windows® atacados tiveram os seus respectivos discos rígidos criptografados irreversivelmente.

Concluímos que a divisão em camadas do espaço cibernético tem aderência com os fatos apresentados.

4.6 Análise da Classificação das Vulnerabilidades Técnicas

Na subseção 2.3.3 apontamos que as vulnerabilidades mais utilizadas em ataques cibernéticos são as conhecidas e não divulgadas, também chamada de vulnerabilidade de dia zero. Como exemplo, tratamos que o EternalBlue era uma vulnerabilidade conhecida pela NSA, porém não divulgada pela falta de conhecimento da Microsoft Corporation. Com o vazamento das informações, logo em seguida, a Microsoft Corporation disponibilizou as atualizações

críticas. Dessa forma, a vulnerabilidade foi reclassificada como conhecida, divulgada e corrigida.

Pelo exposto, concluímos que a classificação das vulnerabilidades técnicas possui aderência com os fatos apresentados.

Ademais, aqui evidenciamos mais uma lição aprendida que não há como evitar a exploração cibernética, caso sejam utilizadas vulnerabilidades similares às que foram utilizadas pela NSA em suas atividades de inteligência. Nesse caso, a capacidade de detecção é muito baixa e de identificação torna-se ainda mais difícil.

4.7 Análise das Estratégias Aplicadas

Como abordado na seção 2.4, com a falta de teóricos estrategistas do quinto domínio, é natural a utilização, em uma abordagem inicial, de teóricos de outros domínios da guerra. Desse modo, iremos abordar as principais contribuições dos Coronéis Warden e Boyd ao caso em questão.

4.7.1 Análise do Modelo dos Cinco Anéis Concêntricos do Coronel Warden

Apesar do pensamento estratégico do Coronel Warden ser subdividido em várias formas de aplicação da força contra o inimigo, o nosso trabalho focou em abordar apenas um aspecto que é a capacidade de um ataque cibernético atingir os cinco anéis concêntricos por ataques paralelos, causando a paralisia estratégica em virtude de uma destruição tamanha que impõe o adversário a desistir de seus objetivos.

Não obstante, analisando todas as entidades atacadas pelo NotPetya, podemos realizar as seguintes divisões dos anéis concêntricos afetados:

a) Lideranças Nacionais: esse é o núcleo das tomadas das decisões. Praticamente todas as organizações do governo federal ucraniano foram afetadas, desorganizando a capacidade de planejar e responder ao incidente;
b) Funções Orgânicas Essenciais: essas funções são críticas para a sobrevivência de um país. No ataque, foram afetados os sistemas de energia, bancários e de transportes. A interrupção de energia afetou empresas, hospitais, serviços públicos e a população em geral. Os sistemas de TI dos bancos foram criptografados,

paralisando as operações bancárias. As empresas de transportes marítimos tiveram interrupções significativas porque todos os dados sobre os contêineres foram perdidos;

c) Infraestrutura: esse já tem como atribuição apoiar a sobrevivência do país, como os serviços de saúde. O ataque realizado a hospitais colocou em risco a segurança e a qualidade dos atendimentos médicos. Foram bloqueados o acesso a registros médico eletrônicos, sistemas de agendamento, resultados de exame e outras informações essenciais;
d) População: além dos grandes impactos psicológicos de um ataque na véspera de feriado nacional, a população sofreu interrupções nos serviços essenciais, perdas de dados pessoais e financeiros, prejuízos econômicos e intensa desconfiança com relação à segurança cibernética de seu país; e
e) Forças Desdobradas: não foram verificados relatos de ataque nesse subsistema com a propagação do NotPeyta para os sistemas operacionais utilizados pelas forças em campo.

Pelo exposto, concluímos que dos cinco círculos concêntricos quatro tiveram o ataque confirmado, demonstrando, assim, que houve aderência à teoria dos ataques paralelos do Coronel Warden.

4.7.2 Análise do Ciclo OODA do Coronel Boyd

Com relação ao ciclo OODA (observar, orientar-se, decidir e agir) do Coronel Boyd, iremos verificar se é possível aplicar ao referido ataque cibernético:

a) Observar: podemos associar a atividade de observar com a exploração cibernética, que tem como missão coletar informações sobre potenciais vulnerabilidades do sistema alvo. No caso específico, foi verificada a dependência de todo um país com relação a apenas um software de contabilidade, o MeDoc, e por meios das ações de exploração, o atacante identificou falhas de segurança para realizar a invasão aos servidores do Linkos Group;
b) Orientar-se: nessa etapa, após analisada as informações coletadas e verificadas as vulnerabilidades do sistema alvo, é realizada a seleção de alvos e identificado as melhores táticas e estratégia para realizar o ataque cibernético. Entre essas táticas,

podemos apontar a utilização do EternalBlue e do Mimikatz para potencializar os efeitos catastróficos causados pelo NotPetya;

c) Decidir: aqui é tomada a decisão sobre qual será o alvo e o método de ataque. Além disso, será preciso verificar a infraestrutura necessária, o planejamento sequencial do ataque e a coordenação de recursos para a execução; e
d) Agir: após a decisão é realizado o ataque cibernético. No caso em questão, houve a inserção do NotPetya nos arquivos de atualização do MeDoc, os quais estavam armazenados nos servidores da Linkos Group. Observa-se que a propagação do malware foi realizada de forma automatizada no dia 27 de junho de 2017.

Por conseguinte, concluímos que o Ciclo OODA do Coronel Boyd possui aderência ao referido ataque. Em adição, também, concluímos que as principais teorias e doutrinas apontadas possuem aderência com os fatos relatados. Encerramos dessa forma o desenvolvimento do trabalho e no próximo capítulo realizaremos as devidas conclusões com as respectivas oportunidades de melhoria.

5 CONCLUSÃO

Quando o referido trabalho se propôs a estudar o ataque cibernético do NotPetya e as doutrinas militares brasileiras, buscávamos responder à seguinte pergunta: o planejamento das ações do ataque cibernético do malware NotPetya, realizado em 27 de junho de 2017, tem aderência com a atual Doutrina Militar de Defesa Cibernética e a Doutrina Cibernética da Marinha?

Uma das dificuldades da pesquisa foi que não encontramos esse planejamento de forma clara e detalhada para comparar com as doutrinas. Entretanto, conseguimos consultar os diversos artigos e livros que descreveram as consequências nefastas, os procedimentos adotados para se restabelecer os sistemas destruídos e as investigações forenses para descobrir o que tinha acontecido. É por meio deles que inferimos como foi feito o planejamento militar, tendo como as principais referências as obras de Greenberg (2018, 2021).

Com relação ao ataque, percebemos que ele está inserido em uma disputa geopolítica por áreas de influência entre a civilização ocidental e a civilização ortodoxa oriental, segundo a teoria de Huntington (1997). Além disso, a Guerra Cibernética travada entre Rússia e Ucrânia é apenas uma das operações de uma Guerra Híbrida em curso.

Concluímos que o Brasil, nas últimas décadas, passou a ter novas vulnerabilidades, uma vez que os Estados estão adquirindo uma maior capacidade de Guerra Cibernética, como observado nesse ataque. Podemos também, em qualquer momento, estar em risco diante de personagens não estatais que podem realizar ações de pequeno vulto no espaço cibernético por meio de uma equipe de hackers.

Como lição aprendida, podemos apontar que essas novas vulnerabilidades farão com que as nossas HE sejam revisadas com maior frequência, o que levará, consequentemente, à revisão contínua das nossas doutrinas cibernéticas. Além disso, o Sistema Militar de Defesa Cibernética precisa estar em constante cooperação com o setor privado, universidades, instituições de pesquisa e outros órgãos governamentais para garantir que ameaças externas não venham a impactar a segurança e soberania do país.

Na falta de teóricos cibernéticos, essa pesquisa abordou apenas alguns aspectos das teorias dos Coronéis Boyd e Warden, atestando uma aderência parcial dessas com relação ao ataque. Dessa forma, sugerimos que as próximas pesquisas busquem aprofundar essa questão

para verificar a possibilidade de aderência do ataque aos outros aspectos desses teóricos.

Outra lição aprendida é sobre a importância da resiliência cibernética, visto que não é possível ter uma proteção cibernética totalmente efetiva por causa da Insegurança Latente, uma das características da Defesa Cibernética. Ou seja, mais importante do que a proteção, é a capacidade de se recuperar rapidamente e continuar operando. Em um mundo onde os ataques cibernéticos se tornam mais frequentes e devastadores, vulnerabilidades como EternalBlue irão surgir de uma forma ou de outra, portanto os aspectos da resiliência cibernética não podem ser negligenciados.

Ao longo deste trabalho, afirmamos diversas vezes sobre essa importância, contudo não foi objeto da nossa análise apontar como atingir tal capacidade. Assim, destacamos a necessidade da realização de novos estudos para verificar como é possível obter esse importante requisito para os sistemas de compõem a Defesa Cibernética Brasileira.

No nível tático e operacional, verificamos que lições podem ser aprendidas ao debruçarmos sobre a História. Assim como a aeronave se tornou um elemento chave para a condução das guerras no mar, percebemos que haverá a gradual elevação da importância das ações de Guerra Cibernéticas pelas Forças Navais. Logo, a Doutrina Cibernética da Marinha terá um grande papel relevante na disseminação de conhecimentos do quinto domínio da guerra no âmbito da nossa Força.

O nosso objeto de pesquisa demonstrou que as nações e instituições mais protegidas podem sofrer ataques maliciosos e que o Princípio do Efeito estará mais evidente a cada dia. Nesse sentido, o aspecto da resiliência cibernética deverá ser buscado com mais intensidade em nossos sistemas. Por fim, chegamos à conclusão de que os objetivos do trabalho foram cumpridos, pois foi possível verificar a aderência do ataque cibernético NotPetya na maior parte do conteúdo exposto das doutrinas militares cibernéticas e propor oportunidades de melhoria para a Defesa Cibernética Brasileira.

REFERÊNCIAS

APARECIDO, Julia Mori; AGUILAR, Sergio Luiz Cruz. A Guerra entre a Rússia e a Ucrânia. *Série Conflitos Internacionais*, v. 9, n. 1, 2022. Disponível em: <https://www.marilia.unesp.br/Home/Extensao/observatoriodeconflitosinternacionais/v.-9-n.-1fev.-2022.pdf>. Acesso em: 17 jun. 2023.

BELCIC, Ivan. Ransomware Petya: Como funciona e como se proteger. *AVAST*, 2023. Disponível em: <https://www.avast.com/pt-br/c-petya>. Acesso em: 09 ago. 2023.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020a. *Aprova a Estratégia Nacional de Segurança Cibernética*. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419?ref=blog.ecoit.com.br>. Acesso em: 14 de jun. de 2023.

_____. Exército. Estado-Maior do Exército. *Glossário de termos e expressões para uso no Exército*. Brasília-DF, 2018. Disponível em: <https://bdex.eb.mil.br/jspui/handle/1/1148>. Acesso em: 21 jun. 2023.

_____. Força Aérea Brasileira. Estado-Maior da Aeronáutica. *Doutrina Básica da Força Aérea Brasileira - Volume 1*. Brasília-DF, 2020b. Disponível em: <https://www.sislaer.fab.mil.br/terminalcendoc/Busca/Download?codigoArquivo=6535>. Acesso em: 21 jun. 2023.

_____. Marinha do Brasil. Comando-Geral do Corpo de Fuzileiros Navais. *CGCFN-0-1 - Manual Básico dos Grupamentos Operativos de Fuzileiros Navais.* Rio de Janeiro-RJ: CGCFN, 2020c.

_____. _____. Estado-Maior da Armada. *EMA-419 - Doutrina Cibernética da Marinha*. Brasília-DF: EMA, 2021.

_____. Ministério da Defesa. *MD51-M-04 - Doutrina Militar de Defesa. Brasília*: MD, 2007. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/File/legislacao/emcfa/publicacoes/md51a_ma_04a_doutrinaa_militara_dea_defesaa_2aa_ed2007.pdf>. Acesso em: 21 jun. 2023.

_____. _____. Estado-Maior Conjunto das Forças Armadas. *Política Cibernética de Defesa*. MD31-P-02. Brasília-DF, 2012. Disponível em: <https://redectidc.com.br/assets/files/ 2012 - Política Cibernética de Defesa MD 31.pdf>. Acesso em: 17 jun. 2023.

_____. _____. _____. *Glossário das Forças Armadas*. Brasília-DF, 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>. Acesso em: 17 jun. 2023.

_____. _____. *MD31-M-07 - Doutrina Militar de Defesa Cibernética*. Brasília: MD, 2014. Disponível em: <https://www.gov.br/defesa/pt-

br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_07a_defesaa_ciberneticaa_1a_2014.pdf>. Acesso em: 21 jun. 2023.

_____. *Política Nacional de Defesa e a Estratégia Nacional de Defesa*. [Online] Encaminhadas, em 22 de julho de 2020d, para apreciação do Congresso Nacional. Disponível em: <https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/politica-nacional-de-defesa>. Acesso em: 27 maio 2023.

_____. Presidência da República. Gabinete de Segurança Institucional. Portaria nº 93, de 26 de setembro de 2019. *Aprova o Glossário de Segurança da Informação*. Sessão de 01/10/2019. Diário Oficial da União, Brasília, DF, 01 out. 2019. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>. Acesso em: 17 jun. 2023.

_____. Receita Federal. *Meu Imposto de Renda*, 31 maio 2023. Disponível em: <https://www.gov.br/receitafederal/pt-br/assuntos/meu-imposto-de-renda>. Acesso em: 05 jul. 2023.

BRZEZINSKI, Z. K. *The grand chessboard: American primacy and its geostrategic imperatives*. New York: Basic Books, 1997.

BURDOVA, Carly. O que é o EternalBlue e por que o exploit MS17-010 ainda é relevante?, *AVAST*, 18 jun. 2020. Disponível em: <https://www.avast.com/pt-br/c-eternalblue>. Acesso em: 18 jun. 2023.

CAPIROTO. [In]Segurança Nacional? *Exército é hackeado e tem 7 mil contas crackeadas.* Tecmundo. Brasil, 09 nov 2015. Disponível em: <https://www.tecmundo.com.br/ataque-hacker/89110-in-seguranca-nacional-exercito-hackeado-tem-7-mil-contas-crackeadas.htm>. Acesso em: 15 jun. 2023.

CARVALHO, Guilherme Almeida Matos de, *A teoria de Warden aplicada na Guerra Cibernética: a aderência do ataque do Stuxnet a Estrategia da Paralisia e a Teoria dos Cinco Anéis*, Escola de Guerra Naval (EGN), 2020. Disponível em: <https://www.repositorio.mar.mil.br/handle/ripcmb/845275>. Acesso em: 15 jun. 2023.

CHALFANT, Morgan. Trump admin blames Russia for massive global cyberattack. *The Hill,* 2018. Disponível em: <https://thehill.com/policy/cybersecurity/374104-trump-admin-blames-russia-for-global-cyberattack-warns-of-international/>. Acesso em: 24 jun. 2023.

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

_____. *O Quinto Domínio, defendendo nosso país, nossas empresas e nós mesmos na era das ameaças cibernéticas*. Rio de Janeiro: Alta Books, 2021.

COUTAU-BÉGARIE, Hervé. *Tratado de Estratégia*. Rio de Janeiro: Escola de Guerra Naval, 2010.

COUTINHO, Alexandre Nunes, *A Guerra Cibernética entre Rússia e Geórgia de 2008: uma análise dos ataques cibernéticos sob a ótica da teoria de John Warden*, Escola de Guerra Naval (EGN), 2020 Disponível em: <https://www.repositorio.mar.mil.br/handle/ripcmb/845279>. Acesso em: 15 jun. 2023.

DE OLIVEIRA, Marcos Aurelio Guedes; PORTELA, Lucas Soares. As camadas do espaço cibernético sob a perspectiva dos documentos de defesa do Brasil. *Revista Brasileira de Estudos de Defesa*, v. 4, n. 2, 2017. Disponível em: <https://rbed.abedef.org/rbed/article/view/75014>. Acesso em: 17 jun. 2023.

DNI. Five Eyes *Intelligence Oversight and Review Council (FIORC),* 15 jun. 2020. Disponível em: <https://www.dni.gov/index.php/who-we-are/organizations/enterprise-capacity/chco/chco-related-menus/chco-related-links/recruitment-and-outreach/217-about/organization/icig-pages/2660-icig-fiorc>. Acesso em: 24 jun. 2023.

ESET, *Quando a tecnologia permite o progresso, a ESET o protege*, 01 jul 2023. Disponível em: <https://www.eset.com/br/sobre/>. Acesso em: 24 jun. 2023.

EUA, *About the Space Force*, 10 jun 2023. Disponível em: <https://www.spaceforce.mil/About-Us/About-Space-Force/> Acesso em: 29 jun. 2023.

FADOK, David S. *John Boyd and John Warden*: Air Power´s Quest for Strategic Paralysis. 61 f. Dissertação – USAF School of Advanced Airpower Studies, 1995. Disponível em: <https://media.defense.gov/2017/Dec/27/2001861508/-1/-1/0/T_0029_FADOK_BOYD_AND_WARDEN.PDF>. Acesso em: 30 jul. 2023.

GAMA NETO, R. B. Guerra cibernética / guerra eletrônica – conceitos, desafios e espaços de interação. *Revista Política Hoje*, v. 26, n. 1, p. 201 – 217, 2017.

GOMES, Mauro Guedes Ferreira Mosqueira; CORDEIRO, Sandro Silva; PINHEIRO, Wallace Anacleto. A Guerra Cibernética: exploração, ataque e proteção cibernética no contexto dos sistemas de Comando e Controle (C2). *Revista Militar de Ciência e Tecnologia*, Rio de Janeiro, v. 33, n. 2, p. 11-18, 2016. Disponível em: <https://rmct.ime.eb.br/arquivos/RMCT_3_tri_2016_web/RMCT_275.pdf> Acesso em: 14 de jun. de 2023.

GONÇALVES, Ricardo Penedo. *Primeira Guerra Cibernética:* os ataques cibernéticos contra a Estônia, em 2007, à luz da teoria dos cinco anéis do Coronel John Warden, Escola de Guerra Naval (EGN), 2018. Disponível em: <https://www.repositorio.mar.mil.br/handle/ripcmb/844934>. Acesso em: 20 jun. 2023.

GREENBERG, Andy. *The untold story of NotPetya, the most devastating cyberattack in history*. Wired, 22 ago. 2018. Disponível em: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world>. Acesso em: 15 jun. 2023.

_____. *Sandworm*: Uma nova era na Guerra Cibernética e a caça pelos hackers mais perigosos do Kremlin. Rio de Janeiro: Alta Books, 2021

KASPERSKY LAB. *O que é roubo de dados e como evitá-lo*. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/data-theft>. Acesso em: 15 jun. 2023.

KORYBKO, Andrew. *Guerras híbridas*: das revoluções coloridas aos golpes. São Paulo, SP: Expressão Popular, 2018.

LATTO, Nica. Exploits: Tudo que você precisa saber, *AVAST*, 29 set. 2020. Disponível em: <https://www.avast.com/pt-br/c-exploits>. Acesso em: 17 jun. 2023.

LIND, William S. *Maneuver Warfare Handbook*. Bolder: Westview Press, 1985. 147 p.

LISKA, Allan; GALLO, Timothy. *Ransomware*: defendendo-se da extorsão digital. Novatec Editora, 2019.

MAERSK, *Serviços de Transporte*. 2023. Disponível em: <https://www.maersk.com/transportation-services>. Acesso em: 17 jun. 2023.

MANDARINO, Raphael, Jr. *Segurança e Defesa do Espaço Cibernético Brasileiro*. Recife: Cubzac, 2010.

MS17-010: Atualização de segurança para o servidor Windows SMB. *MICROSOFT*, 14 mar 2017. Disponível em: <https://support.microsoft.com/pt-br/topic/ms17-010-atualiza%C3%A7%C3%A3o-de-seguran%C3%A7a-para-o-servidor-windows-smb-ter%C3%A7a-feira-14-de-mar%C3%A7o-de-2017-435c22fb-5f9b-f0b3-3c4b-b605f4e6a655>. Acesso em: 25 jun. 2023.

PAGLIUSI, Paulo Sergio. Guerra Cibernética russo-ucraniana: lições para o Brasil e para o mundo. *Revista do Clube Naval*, v. 2, n. 402, p. 74-79, 2022. Disponível em: <http://portaldeperiodicos.marinha.mil.br/index.php/clubenaval/article/view/3189>. Acesso em: 15 jun. 2023.

RABOCZKAY, Tibor. *A Ucrânia e as minorias étnicas na atual guerra*. 11 abr. 2022. Disponível em: <https://jornal.usp.br/?p=507288>. Acesso em: 15 jun. 2023.

RIBEIRO, António Silva. *Teoria geral da estratégia*: o essencial ao processo estratégico. Coimbra: Almedina, 2010. 258 p.

SEGUIN, Patrick; LATTO, Nica. Guia básico sobre ransomware, *AVAST*, 24 set. 2021. Disponível em: <https://www.avast.com/pt-br/c-what-is-ransomware>. Acesso em: 09 ago. 2023.

TECHTUDO. *Dez coisas que você precisa saber sobre o fim do suporte ao Windows XP*, 08 abr. 2014. Disponível em: https://www.techtudo.com.br/noticias/2014/04/dez-coisas-que-voce-precisa-saber-sobre-o-fim-do-suporte-ao-windows-xp.ghtml>. Acesso em: 15 jun. 2023.

UCRÂNIA, Embaixada no Brasil. *Dia da Constituição da Ucrânia*, 27 jun 2013. Disponível em:

<https://brazil.mfa.gov.ua/pt/news/13152-deny-konstituciji-ukrajini> Acesso em: 29 jun. 2023.

VIDIGAL, Armando A. F. *A Evolução do Pensamento Estratégico Naval Brasileiro*. Rio de Janeiro: Biblioteca do Exército, 3ª Edição, 1985.

_____. A Evolução do Pensamento Estratégico Naval Brasileiro – meados da década de 70 até os dias atuais. Rio de Janeiro: Clube Naval, 2002.

WAKEFIELD, Jane. BBC. *Tax software blamed for cyber-attack spread*, 28 jun. 2017. Disponível em: <https://www.bbc.com/news/technology-40428967> Acesso em: 29 jun. 2023.

ZDNET. *NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs*, 26 jan. 2018. Disponível em: <https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/>. Acesso em: 24 jun. 2023.

ANEXO A - NÍVEIS DE DECISÃO

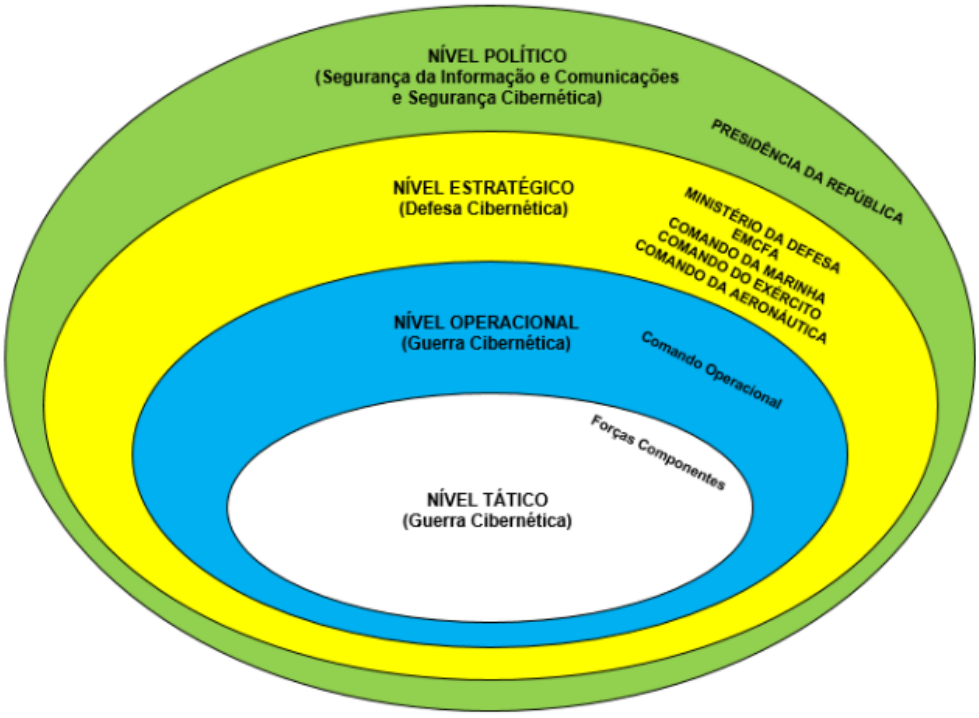

FIGURA 1 - Níveis de decisão
Fonte: BRASIL, 2014, p. 17

ANEXO B - O CICLO OODA - OPONENTE X NOSSAS FORÇAS

FIGURA 2 - O ciclo OODA - oponente x nossas forças
Fonte: BRASIL, 2020c, p. 3-2

ANEXO C - MODELO DOS CINCO ANÉIS CONCÊNTRICOS

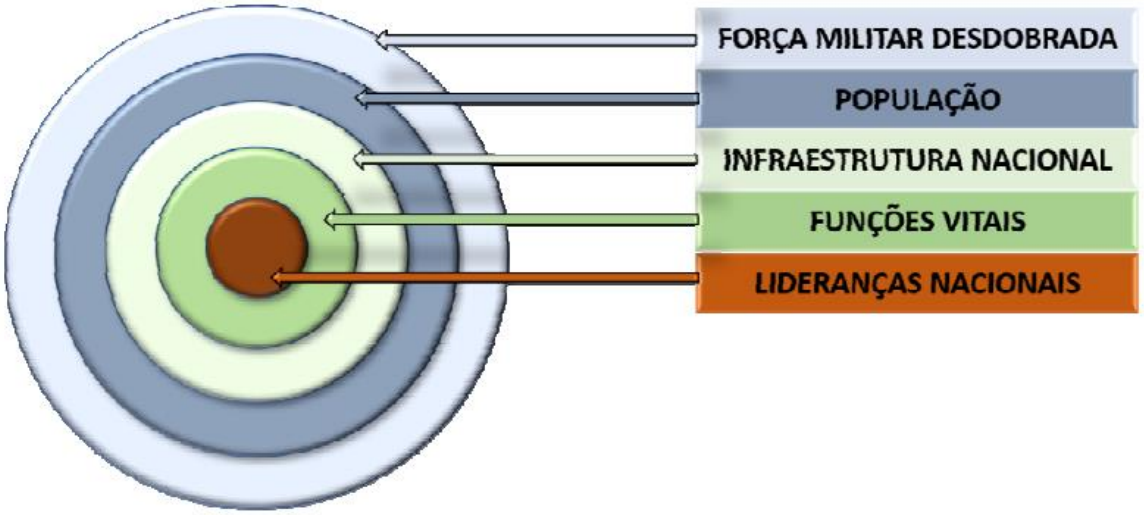

FIGURA 3 - Modelo dos cinco anéis concêntricos
Fonte: BRASIL, 2020b, p. 26