ESCOLA DE GUERRA NAVAL

CC RICARDO PENEDO GONÇALVES

A PRIMEIRA GUERRA CIBERNÉTICA:

os ataques cibernéticos contra a Estônia, em 2007, à luz da teoria dos cinco anéis do Coronel John Warden.

Rio de Janeiro

2018

CC RICARDO PENEDO GONÇALVES

A PRIMEIRA GUERRA CIBERNÉTICA:

os ataques cibernéticos contra a Estônia, em 2007, à luz da teoria dos cinco anéis do Coronel John Warden.

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

Orientadores: CMG (FN-RM1) William Alves Rosa e CF Eugenio Campos Huguenin

Rio de Janeiro

Escola de Guerra Naval

2018

AGRADECIMENTOS

À Deus, por me permitir superar este desafio.

À minha esposa, Cristiana Targino Silvestre Penedo, e aos meus filhos, Isabela Targino Silvestre Penedo e Arthur Targino Silvestre Penedo, pelo amor incondicional e apoio durante o curso.

À minha mãe, Maria Cecília Amorim Penedo, pelos ensinamentos que me permitiram chegar até aqui.

Aos meus orientadores, CMG (FN-RM1) William Alves Rosa e CF Eugenio Campos Huguenin, pelas orientações e apoio durante a elaboração deste trabalho.

RESUMO

O objetivo deste trabalho é analisar se os ataques cibernéticos contra a Estônia (2007) tiveram aderência ao modelo teórico dos cinco anéis do Coronel John Warden (1943-), no que concerne à paralisia estratégica. Elaborada com as ideias oriundas do poder aéreo, a teoria selecionada foi empregada na Operação Tempestade no Deserto (1991), Iraque. O desenho de pesquisa escolhido foi a comparação da teoria com a realidade. Por meio desse confronto, concluímos que apesar da aderência parcial ao modelo estudado, um ataque cibernético, empregado contra as vulnerabilidades críticas de um Estado dependente da Internet e que não possua um sistema de defesa eficaz contra as ameaças cibernéticas, contribui para obtenção pelo atacante de vantagens estratégicas. Esse ataque tem seu efeito potencializado quando utilizado em conjunto com as armas convencionais, tendo assim, maior possibilidade de paralisar estrategicamente o oponente. Finalmente, este trabalho sugere o desenvolvimento e aprimoramento de doutrinas de guerra cibernética que aperfeiçoem o uso do espaço cibernético, bem como destaca a importância do bom relacionamento entre os setores público e privado nos assuntos ligados à Tecnologia da Informação e Comunicação (TIC) e a realização exercícios cibernéticos entre os Estados aliados, de forma a mitigar um possível ataque cibernético.

Palavras-chave: Ataques Cibernéticos. Estônia. John Warden. Paralisia Estratégica. Guerra Cibernética.

LISTA DE ABREVIATURAS E SIGLAS

C2	Comando e Controle
CG	Centro de Gravidade
DCiber	Defesa Cibernética
DDoS	*Distributed Denial of Service* - Distribuído de Negação de Serviço
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicações
STIC3	Sistemas de Tecnologia da Informação e Comunicações, Comando e Controle

SUMÁRIO

1 INTRODUÇÃO

O presente estudo foi pautado nos ataques cibernéticos contra Estônia em 2007, tendo como base teórica a paralisia estratégica utilizando o modelo teórico dos cinco anéis apresentada pelo Coronel John Warden.

O estudo é oportuno por ser a guerra cibernética uma nova atividade especializada de guerra, quando comparada com os métodos convencionais, e a sua crescente relevância em um mundo globalizado, onde a busca por conhecimento humano, associado ao o surgimento de recursos tecnológicos, torna a sociedade e os Estados cada vez mais dependentes de tecnologia, principalmente dos sistemas que fazem uso da *Internet*. Dessa maneira, o propósito deste trabalho é analisar se os ataques cibernéticos contra Estônia, em 2007, tiveram aderência ao modelo teórico dos cinco anéis do Coronel John Warden, no que concerne à paralisia estratégica.

Quando comparado à quantidade de conflitos armados convencionais ocorridos no mundo, o número de conflitos cibernéticos existentes é reduzido, tendo a Rússia, teoricamente envolvida nos poucos ocorridos. A população e o governo da Estônia são muito dependentes da *Internet* para condução das suas atividades diárias. O ataque contra a Estônia, em 2007, foi o primeiro caso em que supostamente tiveram dois Estados envolvidos, despertando o mundo para a importância dos conflitos cibernéticos. Por isso, consideramos que a análise dos ataques cibernéticos contra Estônia (2007), à luz da teoria do Coronel John Warden, pode melhor contribuir para o objetivo deste trabalho.

Para nortear o desenho de pesquisa, será utilizada a abordagem realística, comparando o objeto em estudo com o modelo teórico.

Visando atingir o propósito, o trabalho se desenvolve em cinco capítulos. Após esta introdução, segue-se o segundo capítulo, em que exibiremos o modelo teórico dos cinco anéis do Coronel John Warden, que foca em realizar uma paralisia completa do inimigo

utilizando ataques simultâneos em seus pontos mais vulneráveis visando atingir os líderes de um Estado, e os principais conceitos de guerra cibernética.

No terceiro capítulo, abordaremos os ataques cibernéticos contra a Estônia (2007), analisando quais foram os setores estonianos atingidos pelos ataques, os resultados, efeitos psicológicos gerados e seus impactos.

No quarto capítulo, confrontaremos os ataques cibernéticos contra Estônia na moldura temporal estabelecida com o modelo teórico estudado, a fim de verificar se tiveram aderência à teoria.

Finalmente, no quinto capítulo, apresentaremos as conclusões e indicaremos possíveis linhas de investigação futuras que não puderam ser detalhadas, a fim de ampliar a pesquisa de outras variáveis que não foram abordadas neste trabalho. Ressaltaremos, também, a importância do assunto dentro da Marinha do Brasil.

A seguir será apresentada a ideia de paralisia estratégica, o modelo teórico dos cinco anéis do Coronel John Warden e os principais conceitos de guerra cibernética.

2 A TEORIA DO CORONEL JOHN WARDEN E CONCEITOS DE GUERRA CIBERNÉTICA

Neste capítulo serão apresentados os conceitos de paralisia estratégica e de guerra cibernética e o modelo teórico dos cinco anéis do Coronel John Warden, utilizado na operação Tempestade no Deserto.

Warden é dos grandes teóricos do poder aéreo. Sua teoria tem como foco paralisar estrategicamente o sistema do inimigo. O choque com o oponente deve ser evitado sempre que possível. Atingir a liderança de um Estado é o objetivo a ser buscado.

Visando realizar uma futura comparação da teoria com os ataques cibernéticos contra a Estônia (2007), serão estudadas as principais variáveis que compõem os cinco anéis da teoria: liderança, elementos orgânicos essenciais, infraestrutura, população e forças militares no terreno. Além disso, serão abordados os conceitos de ataques paralelos e da interdependência entre os anéis.

2.1 A paralisia estratégica

Para uma melhor compreensão da teoria do Coronel John Warden, é importante que, incialmente, seja feita uma análise do que consiste à paralisia estratégica e como foi seu processo evolutivo.

Há dois mil anos, o guerreiro Sun Tzu[1] (1995, citado por FADOK), divulgou suas bases teóricas, as quais serviram de referência para os estrategistas que se seguiram. Para Sun Tzu, a regra geral para o emprego das forças armadas consistia na preferência de manter uma Estado intacta do que destruí-la. Os vencedores das batalhas não são os mais habilidosos, mas sim, os que tornam os exércitos inimigos indefesos sem ter que lutar. O mérito da guerra é

[1] Sun Tzu, *The Art of War*, tradução Thomas Cleary (Boston and London: Shambhala Publications, Inc., 1988), 66–67 p.

vencer o inimigo sem lutar. Além disso, Sun Tzu sustentava uma rápida incapacitação do rival.

Com o objetivo de paralisar o inimigo, logo após o término da Primeira Guerra Mundial (1914-1918), John Frederick Charles Fuller (1878-1966) e Basil H. Liddell Hart (1895-1970), dois veteranos britânicos, pensaram a respeito da paralisia estratégica. Em 1919, Fuller desenvolveu o que talvez tenha sido o primeiro plano operacional moderno com o propósito de paralisar o inimigo. Além disso, Fuller defendia que a maneira mais eficiente de se destruir a força militar inimiga era por meio da guerra psicológica. Similarmente, Liddell Hart assumia que a maneira mais potente e econômica da guerra era paralisar o oponente por meio da incapacitação em vez de aniquilá-lo (FADOK,1995).

Sete anos após o término da Primeira Guerra Mundial, o livro publicado por Liddell Hart intitulado *Paris; Or Future of war*, dentre os diversos livros sobre estratégia militar e guerra moderna, publicados por Liddell Hart, foi o primeiro. O livro nos faz recordar a derrota mítica sofrida por Aquiles para seu adversário Paris, através de um golpe preciso com uma flecha certeira. Como o próprio título indica, Liddell Hart defende que os novos ataques deveriam ser realizados sobre as vulnerabilidades do inimigo, podendo vir a servir de modelo para a condução da guerra nos próximos anos (FADOK,1995).

Adicionalmente, as mortes ocorridas nos campos da Primeira Guerra Mundial, associadas ao aparecimento das tecnologias dos voos e da mecanização, contribuíram pela preferência do emprego da estratégica de Paris. Assim, procurou-se explorar as vulnerabilidades inimigas que estavam protegidas por suas forças armadas. Dessa forma, os teóricos do poder aéreo reintegraram a noção de paralisia no dicionário da estratégia militar. Isso levou as pessoas a especularem que o poder aéreo poderia derrotar o oponente e suas forças armadas, atacando as vulnerabilidades inimigas pela retaguarda, conhecido como “calcanhar-de-Aquiles”, de forma a provocar sua paralisia ou incapacitação a um custo

relativamente baixo em termos de vidas e danos materiais (MEILINGER, 1997).

Segundo Fadok (1995), mesmo no plano inferior da guerra, o estrategista deve pensar em paralisar, não em matar o inimigo, pois um homem alterado é portador e transmissor do medo, podendo espalhar pânico para todas as pessoas nas suas proximidades. A pressão psicológica, quando direcionada contra o alto escalão adversário, pode impactar em todos os recursos sob o seu comando, anulando assim, a vontade de lutar das tropas subordinadas.

2.2 O modelo teórico dos cinco anéis do Coronel John Warden

O Coronel John Warden concebeu o modelo dos cinco anéis no transcorrer da Guerra do Golfo, em 1991, aplicando-o contra as forças iraquianas que invadiram o Kuwait (ROSA, 1995).

Warden (1988) apresenta a ideia de que o mundo passa por transformações revolucionárias na área de tecnologia, nos sistemas de produção e nos assuntos militares. A velocidade com que essas mudanças ocorrem aumenta a cada dia, enquanto a guerra de atrito[2] perde força. As operações militares devem ser programadas e executadas de forma a atingir os objetivos da política e com custo aceitável. A guerra de hoje não está mais focada na destruição total do inimigo, mas sim em fazer com que o oponente concorde com os interesses do atacante e que vão de encontro às suas vontades. Similarmente, é necessário se resguardar da vontade inimiga contrária aos seus objetivos.

Segundo Warden (1995), o Centro de Gravidade (CG) é o ponto onde o inimigo é mais vulnerável e quando atacado, a possibilidade de ser decisivo é elevada, provocando vantagens significativas para o atacante. Raciocinando estrategicamente, o inimigo deve ser

[2] Guerra de atrito - As forças são diretamente dirigidas sobre o centro de gravidade adversário. Buscam-se a consecução dos efeitos desejados por meio da destruição cumulativa dos meios físicos inimigos, tanto de pessoal quanto de material, trabalhando basicamente no campo físico, ou o confronto direto com as unidades de combate inimigas de modo a neutralizá-las (BRASIL, 2007).

entendido como um sistema composto de diversos subsistemas, sendo o atingimento dos objetivos a chave para o sucesso da guerra estratégica. Esses objetivos estratégicos vão além da simples submissão do inimigo e a destruição das suas forças militares. Buscamos justamente o oposto, provocar o menor número de baixas possíveis. Os objetivos são alcançados quando os ataques provocam uma paralisia no sistema inimigo, impossibilitando-o de oferecer resistência.

Ademais, Warden busca aproximar o modelo dos cinco anéis ao mundo real, comparando-o ao corpo humano; Por isso, divide a organização em cinco anéis concêntricos, da parte interna para externa, da seguinte forma: liderança, sistemas orgânicos essenciais, infraestrutura, população e forças militares no terreno (WARDEN, 1995).

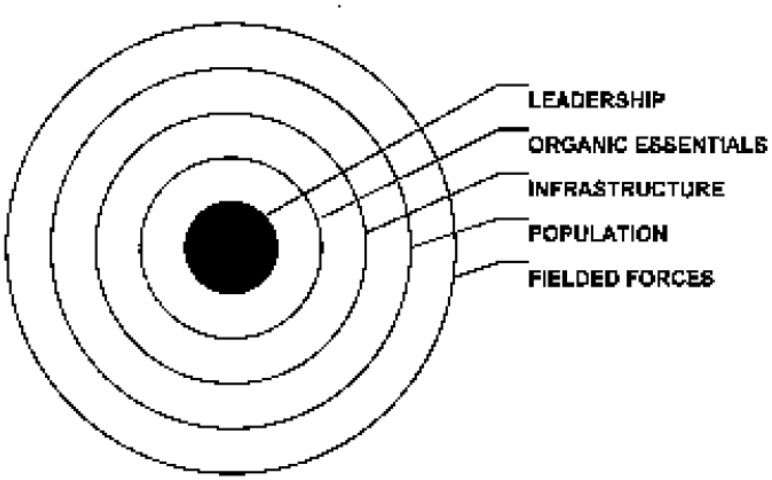

FIGURA 1 – Modelo dos cinco anéis estratégicos de John Warden
Fonte: FADOK, DAVID S, 1995, p. 25.

Outrossim, os anéis que compõem o sistema são interdependentes entre si, ou seja, cada anel possui uma função e mantém certo grau de relacionamento com os demais (WARDEN,1995)

Dessa forma, podemos comparar a liderança ao nosso cérebro, sendo considerado o anel central e o mais crítico, responsável por controlar as demais partes do corpo. Cada estado ou organização militar é detentor de um conjunto de vulnerabilidades críticas. As

pessoas que desempenham os cargos de líderes são os responsáveis por tomar decisões que podem alterar o rumo de uma guerra. No mundo contemporâneo, o domínio das comunicações é fundamental para um perfeito Comando e Controle (C2). Entretanto, as comunicações estão sujeitas a ataques e quando essas são severamente afetadas, os líderes não conseguem gerenciar de forma precisa seus esforços de guerra, dificultando a manutenção do moral elevado do Estado. Quando a liderança não puder ser afetada diretamente, buscamos aplicar pressão indireta nos demais anéis de modo a afetar o psicológico da liderança e levá-la a avaliar que a continuação da guerra não é mais vantajosa, obrigando-a a fazer concessões que favorecem o atacante (WARDEN,1995). Nesse contexto, Fadok expõe que

> A mensagem implícita é que a destruição ou neutralização do CG da liderança(s) produzirá paralisia física total do sistema, enquanto que o ataque bem sucedido no CG dos outros anéis produzirá paralisia física parcial, mas insuportável pressão psicológica sobre a liderança (FADOK, 1995, p. 23, tradução nossa).[3]

A destruição das infraestruturas de telecomunicações e informação é uma forma de dificultar o exercício da liderança.

Além disso, Warden (1995) apresenta que o modelo dos cinco anéis é eficaz no plano estratégico quando empregado prioritariamente contra a liderança militar. Adicionalmente, como o líder é quem pode ser convencido, todos os esforços devem ser voltados direta ou indiretamente para ele, de modo a transformar sua forma de pensar. Levar a liderança inimiga agir de acordo com a nossa vontade é o objetivo da guerra.

Os sistemas orgânicos essenciais são os órgãos vitais, tais como coração, fígado e pulmão, responsáveis por transportar ou converter os alimentos e o ar para uso do corpo. Sem eles, a liderança não desempenhará a função estratégica. É o anel onde são encontrados os recursos ou processos imprescindíveis para que o Estado ou organização se mantenha e não estão ligados, necessariamente, ao combate. O crescimento das cidades no mundo tem provocado uma dependência cada vez maior da eletricidade e de produtos derivados do

[3] No original: “The implicit message is that destruction nor neutralization of the leadership COG(s) will produce total physical paralysis of the system, where as successful attack upon COGs within the other rings will produce partial physical paralysis, but unbearable psychological pressure upon the leadership”.

petróleo, tornando-as *commodities* essenciais para os Estados. Caso esses produtos sejam destruídos, os estados ficarão impossibilitados de fazerem uso de armas modernas, sendo obrigados a atenderem o desejo do inimigo. Da mesma forma, a depender do tamanho do Estado e da importância que ele atribui aos seus objetivos, mesmo os pequenos danos às indústrias consideradas essenciais podem levar a liderança a ceder. Normalmente, os principais motivos das concessões são os danos nos sistemas orgânicos essenciais que levam ao colapso do sistema, pois provocam repercussões políticas ou econômicas internas que são muito difíceis de suportar (WARDEN, 1995). As telecomunicações e informação estão inclusas nesse anel.

Logo em seguida, surge a infraestrutura, representada pelos ossos, músculos e vasos sanguíneos. É o anel responsável por movimentar todos os bens e serviços civis, tais como portos, aeroportos, estradas, companhias aéreas, pontes, linhas férreas e demais sistemas semelhantes. Quando comparado com o anel dos sistemas orgânicos essenciais, exige um esforço maior, por parte do atacante, para que o ataque alcance o efeito desejado, em virtude de haver um número maior de facilidades de infraestruturas redundantes (WARDEN, 1995).

A população desempenha papel similar às células sanguíneas, transportando o alimento e oxigênio pelo corpo. A realização de ataque diretamente contra a população é mais difícil devido à diversidade de alvos e as incertezas que essas ações podem provocar considerando a imprevisibilidade humana. Uma abordagem indireta contra a população talvez surta o efeito esperado. Todavia, não devemos contar com isso. Como exemplo de ataque indireto sobre a população, observamos como as ações do Vietnã do Norte contra os Estados Unidos podem ser efetivas se o Estado alvo tiver interesse relativamente baixo no resultado da guerra. As ações norte-vietnamitas nos mostraram como é possível criar condições que levem a população civil do inimigo a pressionar o seu governo a mudar as políticas do Estado.

Contudo, em um Estado policial[4] a população pode estar disposta a ter maior aceitação do ataque antes de se voltar contra seu próprio governo (WARDEN, 1995). Vale lembrar que a população é protegida por regras internacionais.

No quinto e último anel estão as forças militares no terreno de um Estado, onde o corpo se protege por meio das células brancas dos ataques dos vírus e parasitas. As forças militares no terreno não são o que há de mais importante em uma guerra. Elas na verdade são os meios para um fim, tendo a função de proteger os anéis internos ou para ameaçar e comprometer os anéis do inimigo. Um Estado com forças militares reduzidas pode ser levado a realizar concessões e, se essas forças forem destruídas, talvez seja necessária uma cessão final porque a liderança reconhece que seus anéis internos estão indefesos e passivos de aniquilação. Atualmente, a tecnologia moderna possibilita diversas opções politicamente poderosas que permite situar as forças em uma categoria de fins e não de meios, diferentemente do ocorrido no passado, em que as forças militares eram empregadas em batalhas (WARDEN,1995).

Além disso, no interior de cada anel existe um CG que se for neutralizado ou destruído cessa o funcionamento do respectivo anel, impactando diretamente nos demais anéis e afetando o funcionamento do sistema com um todo. A gravidade dos danos será maior quanto mais próximo do centro for o anel atingindo (FADOK, 1995).

Segundo Rosa (2015), a defesa dos anéis deve ser feita pelas forças militares, porém elas não são a essência do sistema. Por isso, não devemos ter como objetivo aniquilar as forças militares inimigas, mas sim, os CG de cada anel.

Ao longo dos anos, a importância relativas dos quatros anéis exteriores tem passado por alterações. Outrossim, a depender do sistema social e período histórico analisado,

[4] Estado policial – Tipo de organização estatal que controla de maneira intensa a sua população, em especial os opositores aos detentores do poder, seja por meio da força, seja por meio da repressão política. Disponível em: <https://saviogreco.jusbrasil.com.br/artigos/414090945/vivemos-em-um-estado-policial>. Acesso em: 18 jun. 2018.

as vulnerabilidades também se modificam (WARDEN, 1995).

De acordo com Warden (1995), as forças militares também se subdividem em cinco anéis. Os CG existem tanto no nível estratégico como no nível operacional e são bastante semelhantes. No nível operacional, o objetivo é induzir os comandantes a fazerem concessões, tais como: desistir de uma ofensiva, recuar ou até mesmo se render. Do mesmo modo, o comandante operacional também possui nas suas proximidades seus CG. A estrutura no nível operacional é distribuída na seguinte forma:

- Primeiro anel – liderança – O CG é o comandante, sendo o alvo principal das operações, haja vista que é o encarregado de tomar as decisões. Junto ao anel central, encontra-se localizada sua estrutura de comando e controle (C2) de vital importância para transmissão de ordens e recebimento de informações de seus subordinados.
- Segundo anel – sistemas orgânicos essenciais – Semelhante à logística, pois contém os itens primordiais para o combate, tais como combustível, munição e alimentos.
- Terceiro anel – infraestrutura – Localiza-se a estrutura necessária para movimentar os itens encontrados nos sistemas orgânicos essenciais e os utilizados pela própria força militar. Compõe-se de estradas, oleodutos, linhas de comunicações, vias aéreas e todo arranjo fundamental para o emprego das forças.
- Quarto anel – população – Constitui-se das pessoas utilizadas para operação e apoio nos três anéis anteriores.
- Quinto anel – Forças militares – São as tropas, aeronaves, navios e os militares responsáveis pela defesa. É o anel mais resistente de todos. O ataque que tem como prioridade esse anel é suscetível a ser um conflito

> sangrento. Entretanto, às vezes, se faz necessário a concentração de esforços nesse anel.

Quando surge uma necessidade de se levar ao nível desejado ou paralisar o sistema inimigo, precisamos compreendê-lo previamente. Esse entendimento é considerado o requisito fundamental do ataque estratégico. O Ataque paralelo é a melhor maneira de reduzir a duração da guerra, a menos que existam motivos contrários convincentes que justifiquem um prolongamento (WARDEN, 1995).

Além do mais, a simultaneidade de ataques na guerra paralela faz com o sistema inimigo seja incapaz de se defender ou ser reparado. A guerra paralela consiste em atacar o CG do inimigo em ritmos maiores do que sua capacidade de se defender (ROSA, 2015).

Conforme afirma Warden (1995), os Estados possuem um reduzido número de alvos estratégicos e que tendem a serem de tamanhos reduzidos, de elevados valores, existência de poucos substitutos e difíceis de serem reparados quando atingidos. Ataques paralelos contra uma porcentagem significativa desses alvos tornam os danos insuperáveis. Diferentemente, no ataque sequencial, a investida contra os alvos são espaçadas ao longo do dia. Os efeitos de um ataque sequencial podem ser aliviados por dispersão pelo inimigo ao longo do tempo, permitindo-o elevar o nível de proteção dos possíveis alvos, realizar reparos nos alvos danificados e contra-atacar. A tecnologia é grande motivadora por permitir a realização de ataques simultâneos em níveis estratégicos e operacionais, proporcionando atacar em todos os lugares e ao mesmo tempo. Quanto maior for a quantidade de alvos atingidos simultaneamente, menor será a capacidade do inimigo responder eficazmente.

No futuro, o cerne da guerra será realizar tudo que se deseja em reduzido espaço de tempo, instantemente, quando possível (ROSA, 2015).

A seguir serão apresentados os principais conceitos de guerra cibernética necessários a compreensão do objeto em estudo.

2.3 Conceitos de guerra cibernética

Incialmente, para uma melhor compreensão dos conceitos relacionados à guerra cibernética, precisamos entender seu significado.

Conforme o pensamento de Clausewitz (1979), a guerra é um combate de grande proporção na qual cada lutador obriga o oponente a fazer a sua vontade, por meio do uso da força física.

Por sua vez, após o término da Segunda Guerra Mundial (1939-1945), Nobert Wiener criou o termo "Cibernética" derivado da palavra grega *Kubernetes* para definir um conjunto de ideias para um campo ligado à informação. Para que isso fosse possível, Nobert Wiener desenvolveu um estudo da mensagem como meio de controlar as máquinas e a sociedade, o que chamou de teoria da mensagem. Nesse processo, dar uma ordem para uma pessoa ou a uma máquina era indiferente (WIENER,1973).

Dessa forma, seu estudo permitiu o aperfeiçoamento das linguagens e técnicas necessárias para solucionar o problema do controle e comunicação, em que a troca de informações é essencial. Isso proporcionou o desenvolvimento de computadores, comandos eletromagnéticos e sistemas de comunicações.

Por tudo isso, a Guerra Cibernética[5] são as ações relacionadas às ferramentas de Tecnologia da Informação e Comunicações (TIC) para obtenção de vantagens dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC3) do oponente e defesa dos próprios STIC3, onde estão contidas as Ações Cibernéticas (BRASIL, 2014).

Essas ações são realizadas com o propósito de se obter vantagens tanto na área militar quanto na área civil (BRASIL, 2014). Por isso, quanto maior for o grau de dependência do oponente por TIC, maior será a possibilidade de emprego de ações

[5] Guerra Cibernética – Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C2 do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar (BRASIL, 2014).

cibernéticas contra os seus sistemas, exigindo assim, maior esforço do oponente para prover proteção aos seus ativos de informação[6]. Assim, a defesa dos Ativos de Informação é o principal objetivo da guerra cibernética. A sua proteção requer investimentos no sentido de prover segurança física e lógica e adestramentos dos seus utilizadores quanto aos procedimentos doutrinários a fim de reduzir os riscos cibernéticos[7].

Além disso, é necessário abordarmos os principais conceitos empregados pelo Ministério da Defesa em sua Doutrina Militar de Defesa Cibernética[8]: Espaço Cibernético, Defesa Cibernética (DCiber), Infraestrutura Crítica da Informação e Infraestruturas Críticas, Resiliência Cibernética.

Espaço Cibernético[9] é o mundo virtual onde os computadores estão interconectados e ocorre o estabelecimento de comunicações entre os diversos dispositivos digitais.

Ademais, as ações desenvolvidas no domínio do espaço cibernético podem impactar nos domínios aéreo, terrestre, marítimo e espacial, pois são interdependentes (BRASIL, 2014).

Segundo Nye Junior (2012), o espaço cibernético possui camadas físicas e virtuais. Os ataques originados da camada virtual possuem custos baixos e podem ser direcionados contra o domínio físico, onde os recursos são elevados e variam de acordo com as leis econômicas de cada Estado.

Dessa forma, as ações cibernéticas podem ser empregadas contra as instalações físicas de um Estado mais desenvolvido, mesmo que o atacante tenha poucos recursos para o

---

[6] Ativos de informação − Meios de armazenamento, transmissão e processamento de dados e 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).

[7] Riscos cibernéticos − É a probabilidade de ocorrência de um incidente cibernético associado à magnitude do dano por ele provocado (BRASIL, 2014).

[8] BRASIL, Ministério da Defesa. MD31-M-07, Doutrina Militar de Defesa Cibernética, Brasília, DF, 2014.

[9] 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).

desenvolvimento das ações. Caso sejam utilizadas em paralelo com atividades de outro domínio, elevam a intensidade do ataque e proporcionam uma melhor proteção dos seus ativos de informação.

A Defesa Cibernética[10] são as ações que têm como propósito realizar a proteção dos sistemas de informação de interesse da Defesa Nacional e obter informações do oponente de modo a comprometer os seus sistemas de informação bem como proporcionar a produção de conhecimento de inteligência a seu respeito (BRASIL, 2014).

Por sua vez, a Infraestrutura Crítica da Informação[11] é subconjunto dos ativos de informação avaliados como críticos para o funcionamento do sistema de modo seguro e confiável. Sua degradação compromete a segurança da sociedade e continuidade da missão do Estado (BRASIL, 2014).

Adicionalmente, as Infraestruturas Críticas[12] são as instalações, serviços, bens e sistemas que caso sejam afetados produzirão efeitos econômico, político, internacional ou à segurança do Estado e da sociedade. Normalmente, estão associados aos pontos de vulnerabilidade do inimigo (BRASIL, 2014). No tocante às infraestruturas críticas, foram escolhidas seis áreas prioritárias no Brasil, a saber: energia, telecomunicações, transportes, água, finanças e informação. Esta última permeia todas as anteriores, pois as Infraestruturas Críticas dependem cada vez mais de redes de informação para a sua gerência e controle (BRASIL, 2011).

Logo, os danos provocados na Infraestrutura Crítica fornecem vantagens estratégicas ou táticas ao atacante, a depender da magnitude e importância da infraestrutura

---

[10] Defesa Cibernética − Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa (BRASIL, 2014).

[11] Infraestrutura Crítica da Informação − Subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (BRASIL, 2014).

[12] 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).

investida. Além disso, os ataques são altamente potencializados quando executados de forma coordenada contra os pontos de vulnerabilidade do oponente.

A seguir, estudaremos os ataques cibernéticos contra a Estônia (2007) a fim de identificarmos os setores atingidos e seus efeitos sobre a população e o governo.

3 OS ATAQUES CIBERNÉTICOS CONTRA A ESTÔNIA (2007)

Devido à inexistência de informações quantitativas, este capítulo será analisado com foco maior nos dados qualitativos. Dessa forma, o capítulo será divido em sete seções. A primeira seção apresentará a história e as motivações dos ataques cibernéticos.

A partir da segunda seção será realizada uma análise dos ataques cibernéticos contra a Estônia (2007), de maneira a evidenciar a origem dos ataques, a relação existente entre conectividade e vulnerabilidades, os setores e serviços alvos dos ataques, os danos porventura provocados e os efeitos psicológicos gerados sobre a população e o governo. Além disso, será verificado como os ataques foram combatidos e suas implicações.

3.1 A história e as motivações dos ataques

Os conflitos envolvendo Estônia e Rússia existem há mais de 100 anos. Após os Estados Bálticos serem anexados em 1940 a então União das Repúblicas Socialistas Soviéticas (URSS) e durante o período da Guerra Fria (1947-1991), a URSS movimentou parte da sua população para a Estônia com objetivo de criar uma base cultural soviética e formar um bloco oriental coeso (HERZOG, 2011).

Além disso, após a Segunda Guerra Mundial, uma grande estátua de bronze de um soldado soviético foi instalada na capital Tallinn, de forma que a Estônia não se esquecesse do empenho do Exército Soviético por retirá-la do domínio nazista. O monumento possuía um significado diferente para os estonianos nativos e os russos étnicos que viviam na região, sendo motivo de crescentes tensões entre ambos os Estados. Para os estonianos, o soldado de bronze simbolizava um opressor e para os russos representavam a liberdade. Após o fim da Guerra Fria, a queda da URSS fez com que a Estônia se tornasse independente novamente (CLARKE; KNAKE, 2015).

Então, a Estônia começou a adotar políticas contrárias aos russos com o propósito de reduzir o legado soviético em seu Estado. Como, por exemplo, a adesão à Organização do Tratado do Atlântico Norte (OTAN), em 2004. Isso contribuiu, ainda mais, para elevar a insatisfação russa (HERZOG, 2011).

Em 26 em abril de 2007, a Estônia removeu a estátua para um cemitério, gerando descontentamento russo, e consequentemente, uma série de ataques cibernéticos foram desencadeados contra seu Estado (CLARKE; KNAKE, 2015). Os ataques cibernéticos ocorreram no período de 27 de abril a 18 de maio de 2007 e tiveram como alvo os sistemas da Estônia ligados à *Internet* (OTTIS, 2008).

Segundo Aaviksoo (2008), Ministro da Defesa da República da Estônia (2007-2011) durante as ações cibernéticas, os ataques foram diferentes dos anteriores. Para Ruus (2008), os ataques cibernéticos tiveram motivações políticas, pois foram diferenciados. Foi distinto de se proteger das tentativas de invasões de ataques limitados e restritos, provenientes em sua maior parte de *hackers*[13] amadores ou ações cibernéticas específicas com o objetivo de interromper ou afetar os sistemas de comando e comunicações militares.

Similarmente, conforme afirma Aaviksoo (2008), os ataques foram contra as empresas e *sites* pessoais com possíveis motivações políticas.

Dessa forma, a retaliação da Rússia contra a transferência da estátua de lugar foi motivada pelo histórico de desentendimentos entre ambos os Estados. Associado a isso, a independência da Estônia e sua aproximação com os Estados capitalistas do Bloco Ocidental, despertou sobre a Rússia um sentimento de perda de influência e poder sobre a Estônia, diminuindo assim, sua área de influência nas proximidades do leste europeu. Por isso, os ataques cibernéticos contra a Estônia não foram direcionados contra as forças militares como todos estavam acostumados.

---

[13] *Hacker – P*essoa especializada no uso de computadores. Normalmente aquele que obtém acesso ilegal a sistemas de computadores (tradução nossa). Cambridge Dictionary. Disponível em: <http://dictionary.cambridge.org/us/dictionary/english/hacker>. Acesso em: 10 jul. 2018.

3.2 Origem dos Ataques

De acordo com Brenner (2011), os ataques foram originados da Rússia e direcionados contra as autoridades que perseguiam cidadãos russos e estonianos com descendência russa.

Da mesma forma, o governo da Estônia considerou que os ataques cibernéticos partiram do território russo. Por isso, solicitou ajuda da OTAN, alegando enquadramento no Artigo V do tratado da OTAN. O Artigo V cita que os Estados integrantes da OTAN são obrigados a prestar ajuda em legítima defesa coletiva ao Estado que tem seu direito violado, equiparando o ataque cibernético a um ataque armado (GREEN, 2015).

Todavia, em 2007, ainda não havia resolução que legitimava a defesa coletiva contra um ataque cibernético (GREEN, 2015).

Por outro lado, a Rússia negou qualquer envolvimento nos ataques (LANDLER; MARKOFFMAY, 2007). Além disso, não demonstrou interesse em investigar os atacantes e não auxiliou no combate aos ataques. Seis meses após, nenhum grupo ou Estado havia assumido a responsabilidade pelos ataques (OTTIS, 2008).

Assim, com a entrada da Estônia para a OTAN, uma intervenção russa sobre a Estônia se tornou mais difícil, pois poderia vir a sofrer retaliações da OTAN. Além disso, possibilitou a OTAN expandir sua área de influência para as proximidades do território russo. Logo, a forma encontrada pelos russos para atacar e ocultar sua reponsabilidade foi o emprego de ataques cibernéticos visando atingir a soberania estoniana.

3.3 Conectividade e vulnerabilidades

Devido a Estônia ser um Estado altamente conectado, grande parte das atividades é realizada por meio da *Internet*, tais como: o voto[14], o recolhimento de impostos, sistema de identificação, transmissão de televisão ao vivo e acesso aos bancos (GREEN, 2015). A Estônia é tão conectada que ficou conhecida como e-estonia.

Da mesma maneira, Clarke e Knake (2015) entendem que a Estônia é um dos Estados mais conectado do planeta, superior inclusive aos Estados Unidos e similar à Coréia do Sul, possuindo assim, elevada dependência da *Internet* para poder fazer o uso de sistemas e aplicativos. Em dezembro de 2017, 97,7% da população possuía acesso à *Internet*.[15] Consequentemente, a população necessita de banda larga para o acesso ao conteúdo. Assim, a *Internet* é essencial para estabelecimentos de relações comerciais, estabelecimento de comunicações e acesso à informação.

De acordo com Aaviksoo (2008), apesar dos Estados mais conectados à *Internet* serem mais vulneráveis do que os que possuem infraestruturas digitais menos desenvolvidas, todos os Estados dependentes de tecnologia moderna estão sujeitos a ataques cibernéticos.

Nesse contexto, o Presidente da Estônia durante os ataques, expõe que "quanto mais digitalizado for um Estado, maior será a sua vulnerabilidade aos ataques cibernéticos"[16] (ILVES, 2016, p. 176, tradução nossa).

Assim, apesar da *Internet* facilitar a realização de diversas tarefas, em especial as relacionadas às atividades econômicas, um Estado com elevada dependência da rede mundial de computadores e com reduzida segurança cibernética possui diversos pontos de

---

[14] A Estônia foi a primeiro Estado da história a oferecer votação pela *internet* na eleição de 2005. O sistema *i-Voting* permite que os cidadãos votem de qualquer lugar do mundo, uma vez que o voto pode ser feito de qualquer computador conectado à *internet* (tradução nossa). Disponível em: <https://e-estonia.com/>. Acesso em: 28 jun. 2018.

[15] Internet World Stats. Disponível em: < https://www.internetworldstats.com/stats4.htm>. Acesso em: 21 jul. 2018.

[16] No original: "the more digitized a country is, the more vulnerable it is to cyber attacks."

vulnerabilidade nos seus ativos de informação. Dessa maneira, os Estados estão sujeitos a ataques cibernéticos que podem afetar seus ativos de informação e, mais gravemente, suas infraestruturas críticas que, porventura, estejam ligadas à *Internet* sem a devida proteção, podendo a vir a comprometer a sua segurança e da sociedade.

3.4 Operações de informação conduzidas por meio da guerra cibernética

Podemos considerar que os ataques se desenvolveram em duas fases. A primeira, com o propósito de afetar o psicológico das pessoas, *hackers* invadiram o *site* do partido político líder do governo da coalização e publicaram uma falsa carta de desculpas, do então Primeiro-Ministro da Estônia (2005-2014), Andrus Ansip (1956-), por ter movido a estátua para o cemitério (RUSS, 2008). De modo similar, Aaviksoo (2008) ratifica que os ataques tinham como propósito atingir o psicológico da população.

Além do mais, *hackers* divulgavam instruções por meio da *Internet* de como saturar o *site* do governo da Estônia com mensagens. Os *sites* foram pichados com propaganda desmoralizante, sendo desenhado sobre a foto dos integrantes do partido do Primeiro-Ministro Andrus Ansip um bigode de Hitler (KAMPMARK, 2007).

Desse modo, inicialmente, os ataques cibernéticos buscaram afetar a população que apoiava a retirada do monumento por meio de operações de informação. A divulgação da falsa carta de desculpas do Primeiro-Ministro pelos *hackers* e a pichação da fotografia com o bigode de Hitler tinham como finalidade alcançar o psicológico da população e do governo. Demonstrando, assim, para a população e para o mundo, que a movimentação do monumento para o cemitério havia sido um erro cometido pelo governo da Estônia.

3.5 Setores e serviços alvos dos ataques

A segunda fase teve início em 30 de abril e término em 18 de maio, dia em que os ataques cessaram. Em busca de vingança, os russos utilizaram uma estratégia com o objetivo de destruir os sistemas eletrônicos estonianos. Por isso, forneceram instruções complementares, por meio dos *sites*, de como se realizar um ataque de *Distributed Denial of Service (DDoS)*[17]. Os atacantes reforçaram a investida assumindo o controle de diversos computadores a fim de aumentar o volume de informações necessárias para saturar e causar a paralisia no sistema da Estônia (RUUS, 2008).

Dessa forma, os ataques de DDoS, por meio de *botnets*[18], dominaram a Estônia. A começar pelos servidores responsáveis por hospedar os mais importantes *sites*, os quais receberem, quase que simultaneamente, milhões de pedidos de acesso, ficando sobrecarregados (CLARKE; KNAKE, 2015).

Os ataques de DDoS degradaram vários servidores comerciais e governamentais. Em muitos deles, ocorreram perdas de serviço ou intermitências (OTTIS, 2008).

Da mesma maneira, o escritório do presidente e os principais servidores do governo foram severamente afetados pelos ataques. Os fax e telefones celulares de membros do parlamento estoniano foram sobrecarregados com informações e chamadas (GREEN, 2015).

Apesar de os ataques visarem os servidores web, servidores de e-mail, servidores e roteadores, o governo, o presidente, o parlamento, polícia, bancos,

---

[17] DDoS – Abreviação de *Distributed Denial of Service* - Ataque Distribuído de Negação de Serviço: uma ocasião em que uma rede de computadores ou um site é intencionalmente impedido de funcionar corretamente, por um número muito grande de usuários que enviam requisições ao mesmo tempo (tradução nossa): Disponível em: <https://dictionary.cambridge.org/pt/dicionario/ingles/ddos>. Acesso em: 10 jul. 2018.

[18] *Botnets* – Um grupo de computadores que são controlados por software contendo programas prejudiciais, sem o conhecimento de seus usuários. (tradução nossa): Disponível em: <https://dictionary.cambridge.org/pt/dicionario/ingles/botnet?q=botnets>. Acesso em: 15 jun. 2018.

Internet Service Provider (ISP)[19], mídia *online*, bem como muitas pequenas empresas e *sites* governamentais locais, os que mais afetaram a população foram os ataques feitos contra os servidores web (OTTIS, 2008).

A maioria dos ataques teve como objetivo os *sites* públicos e e-mail, todos considerados como serviço não críticos. Contudo, determinados ataques foram concentrados sobre os alvos vitais, tais como os servidores de *Domain Name System* (DNS)[20] e dos bancos *online* (OTTIS, 2008).

Somente a infraestrutura crítica civil foi alvo dos ataques na Estônia. Os principais foram contra os ISP, responsáveis por fornecer conectividade com a *Internet*. Caso não exista conectividade, toda infraestrutura deixa de funcionar. A *Internet* é tão importante quanto à água potável para Estônia (EVRON, 2007; MARK, 2007).

Além disso, o setor bancário também é considerado uma infraestrutura crítica, pois grande parte das transações bancárias é realizada por meio da *Internet*. A interrupção dos serviços *online* afetaria outros serviços, ocasionando uma paralisia no Estado. Outra infraestrutura crítica é a imprensa, representada pelos jornais *online* (EVRON, 2007).

Para Ruus (2008), os ataques partiram do território russo e foram realizados de forma sustentados e direcionados contra toda a infraestrutura digital da Estônia, afetando principalmente a infraestrutura civil e a econômica, com propósito de paralisar a sociedade de um Estado extremamente conectado e dependente das redes de computadores.

Grande parte dos ataques foram contra os *sites* dos governantes e seus servidores, contra os portais dos principais meios de comunicação, contra a maioria dos bancos

---

[19] *Internet Service Provider* – Provedor de Serviços de Internet – Denominam-se por ISP as empresas que fornecem comercialmente o acesso à Internet a particulares e/ou outras empresas, por qualquer meio, como a linha telefônica, cabo ou wireless. ISP in Artigos de apoio Infopédia. Disponível em: <https://www.infopedia.pt/apoio/artigos/$isp>. Acesso em: 17 jul. 2018.

[20] *Domain Name System* – O DNS é um dos principais serviços do TCP/IP e é responsável pela tradução de nomes IP em endereços IP. DNS em Artigos de apoio Infopédia. Disponível em: <2https://www.infopedia.pt/apoio/artigos/$dns>. Acesso em: 17 jul. 2018.

comerciais, incluindo os dois bancos mais importantes da Estônia. Os ataques cibernéticos tiveram implicações sobre o Estado da Estônia. Em virtude do momento de tensões, provocado pela transferência do monumento de localidade e os conflitos ocorridos na rua, a população estava carecendo de notícias. Muitas pessoas não conseguiram acessar os *sites* de notícias (AAVIKSOO, 2008).

Segundo Aaviksoo (2008), os ataques não tiveram como o objetivo atingir a infraestrutura crítica classificadas do Ministério da Defesa. Entretanto, colocou em risco a soberania da Estônia. Para Green (2015), os ataques visavam elementos da infraestrutura crítica, ao mesmo tempo em que procuravam manter a origem dos ataques ocultas.

Como afirma Aaviksoo (2008), a maioria das infraestruturas críticas do Ministério da Defesa estava preparada para combater as ameaças cibernéticas, pois as classificadas possuem mecanismo de proteção mais rígido quando comparado às infraestruturas críticas ligadas às redes privadas. Entretanto, os sistemas de informação e de redes dos setores público e privado estão interligados, podendo o privado servir de porta de entrada para os ataques.

Apesar de parte dos ataques terem sido contra as infraestruturas críticas civis, não tiveram a intensidade suficiente para paralisar o Estado. Os poucos ataques que tiveram como objetivo paralisar a infraestrutura crítica não foram eficazes devido ao elevado grau de segurança cibernética apresentados pelos setores atacados.

No dia 03 de maio, os *sites* dos bancos tiveram que ser isolados do exterior. Isso possibilitou o governo da Estônia ganhar tempo para reavaliar o ocorrido e, paralelamente, elaborar um plano para realizar um contra-ataque (RUUS, 2008).

De acordo com Kampmark (2007), as medidas adotadas pelo governo da Estônia de restringir o acesso aos *sites* do exterior foram potencialmente piores do que as demais sanções impostas pela Rússia. Para Herzog (2011), o ataque cibernético foi parecido com um bloqueio naval, pois isolou digitalmente a Estônia do mundo.

Para Ottis (2008), grande parte dos ataques era originada de fora da Estônia. Por isso, para impedir que os ataques atingissem os alvos, o governo resolveu interromper temporariamente o acesso externo. Dessa forma, diversos serviços ficaram indisponíveis para as pessoas localizadas no exterior. O acesso só foi possível para os clientes que se encontravam na Estônia.

Devido à reduzida dependência dos servidores externos, o bloqueio dos servidores externos, adotada pela Estônia, foi uma medida inteligente. Entretanto, os empresários estonianos que se encontravam no exterior não conseguiram ter acesso as suas respectivas contas bancárias (LANDLER; MARKOFFMAY, 2007). Desse fato, é possível concluirmos que o mesmo procedimento não é a melhor solução para um Estado altamente dependente de servidores externos, pois a desconexão degradaria diversos serviços que dependem da *Internet* para seu funcionamento.

A medida adotada pelo governo de desconectar a Estônia do exterior diminuiu a intensidade dos ataques, visto que os ataques originados do exterior foram imediatamente bloqueados. Isso proporcionou o restabelecimento dos serviços digitais à população em reduzido tempo. Além do mais, permitiu ao governo reavaliar o ocorrido e adotar medidas de forma a garantir a proteção dos sistemas atingidos. Apenas os clientes que se encontravam no exterior não conseguiram, inicialmente, acessar suas contas por meio dos *sites*. Todavia, os ataques aos bancos foram pouco sentido pelo público interno. Assim, os ataques sobre as infraestruturas críticas não obtiveram o sucesso almejado pelos atacantes.

A partir de 9 de maio, os ataques foram mais intensos e sofisticados. Com o objetivo de sobrecarregar os servidores da Estônia, *botnets* foram instalados nos computadores das pessoas espalhadas pelo mundo, transformando-os em robôs que transmitiram milhões de mensagens simultaneamente para os servidores estonianos. A taxa de tráfego disparou e os servidores não foram capazes de processar o alto volume de dados e

eram derrubados (RUSS, 2008).

Os *botnets* foram direcionados para os endereços dos servidores interligados aos sistemas dos cartões de crédito e da parte da rede de telefonia e dos serviços de diretório da *Internet*, degradando o funcionamento do comércio e dos serviços de comunicação do Estado. O Hansapank, considerado um dos maiores bancos do Estado, também foi afetado com os ataques. Com o passar dos dias, os ataques aumentavam de intensidade e retiravam do ar centenas de *sites*, impossibilitando o acesso ao seu conteúdo (CLARKE; KNAKE, 2015).

As perdas do Hansapank foram de mais de US$ 1 milhão. Além disso, os serviços *online* do banco ficaram inacessíveis por mais de uma hora (LANDLER; MARKOFFMAY, 2007).

Dessa forma, os ataques sobre o comércio e serviços de comunicações atingiram a população que é usuária dos serviços ofertados. Porém, o tempo de indisponibilidade dos *sites* dos bancos foi pequeno para provocar reflexos significativos nos setores dependentes dos serviços online bancários.

3.6 Resultado dos ataques

Para um Estado que possui 97% das operações bancárias realizadas pela *Internet* e 60% da população conectada, depois de três semanas sob ataque, os danos foram considerados relativamente baixos. Os principais danos foram no sistema de e-mail do parlamento que ficou inacessível por quatro dias; os *sites* da mídia e noticiais, incluindo o Postimees, o maior jornal diário, ficaram temporariamente impedidos de serem acessados (RUSS, 2008).

Segundo o especialista Jim Lewis, membro sênior do Centro de Estudos Estratégico e Internacionais (CSIS), localizado em Washington, os ataques foram realizados com o objetivo de investigar o sistema de defesa cibernética estoniano com fins futuros

desconhecidos, sendo mais uma “demonstração”, e que os atacantes não empregaram toda sua força durante o ataque, justificando o reduzido abalo na infraestrutura da Estônia (RUSS, 2008).

Dessa forma, os ataques não tiveram condições de paralisar os sistemas estonianos e foram pouco sentido pela população e pelo governo. Entretanto, um ataque realizado de forma coordenada, sustentada e de grande escala, contra infraestrutura crítica de um Estado altamente dependente da *Internet*, tem grandes possibilidades de causar uma paralisia nos sistemas atingidos e gerar reflexos em outros setores que tenham certo grau de dependência.

3.7 A mobilização para combater os ataques

Segundo Aaviksoo (2008), os ataques não provocariam maiores prejuízos à Estônia a longo prazo, haja vista que os especialistas neutralizaram os ataques rapidamente.

Durante as três semanas, a guerra cibernética ocasionou uma mobilização de emergência de toda ordem, especialmente de recursos humanos especializados, bem como de assistência internacional, para tentar defender a sua infraestrutura digital dos ataques cibernéticos russos. Os principais especialistas de segurança cibernética da Estônia, dos provedores de serviço de *Internet*, bancos, mídia e do governo se uniram rapidamente para combater os ataques. A maioria dos especialistas em TIC eram amigos e se falavam rotineiramente por meio das redes sociais, compartilhando informações (RUSS, 2008).

Entretanto, apesar do grupo no início dos ataques ter bloqueado o tráfego das mensagens oriundos do estrangeiro, impedindo o acesso do exterior aos *sites* estonianos, e aumentar a capacidade dos servidores, essas ações não foram suficientes para fazer frente aos ataques, sendo necessária ajuda de outros Estados e da OTAN, a qual enviou representantes para auxiliar (RUSS, 2008).

As infraestruturas críticas teriam deixado de operar se não fossem os esforços e o

compartilhamento de informações de forma aberta pelos especialistas estrangeiros e da Estônia (EVRON, 2007).

Segundo Aaviksoo (2008), para um combate eficaz é necessário a cooperação entre os setores privado e público. Nesse contexto, Ilves expõe que

> Na Estônia, investimos consideravelmente na cooperação entre os setores público e privado. O governo ajuda as empresas de infraestrutura crítica a avaliar e testar os seus sistemas de informação, organiza exercícios e tem sido bem sucedido na criação e suporte de comunidades de provedores de segurança cibernética. Aumentando cada vez mais a conscientização sobre ameaças cibernéticas, bem como desenvolvendo habilidades e conhecimento para usar a tecnologia com segurança tornaram-se um aspecto central para garantir a segurança cibernética na Estônia (ILVES, 2016, p. 176, tradução nossa).[21]

Os danos motivados pelos ataques foram atenuados pelo fato do governo ter realizado elevados investimentos na Estônia em segurança cibernética durante as eleições ocorridas em março de 2007, especialmente em conhecimento técnico e em mecanismos de defesa modernos para resguardar o processo eleitoral contra fraudes e invasões por hackers (RUSS, 2008).

Segundo Almann (2013), subsecretário permanente do Ministério da Defesa na época dos ataques, em virtude dos esforços em segurança cibernética despendidos durante as eleições eletrônicas de 2007, a Estônia estava preparada para reconhecer a possibilidade de estar sob ataque. Isso permitiu aos líderes do governo identificar rapidamente o ocorrido em vez de despender tempo em rever as convicções sobre uma possível guerra cibernética. Além do mais, assim que ocorreu o ataque cibernético, o governo da Estônia resolveu torná-lo público. Essa atitude possibilitou que os cidadãos compreendessem a indisponibilidade de alguns serviços, permitindo assim, melhor conter os ataques e estabelecer uma confiança mútua entre o Estado e a população.

Levando em conta o que foi observado, entendemos que a aliança dos principais

[21] No original: “In Estonia, we have invested considerably in cooperation between the public and private sector. The government helps critical infrastructure companies assess and test their information systems, organizes exercises, and has been successful in the creation and support of communities of cybersecurity providers. Increasingly, raising awareness about cyber threats as well as developing skills and knowledge to use technology safely have become a central aspect of ensuring cybersecurity in Estonia”.

especialista em TIC da Estônia, juntamente com os representantes de outros Estados e da OTAN, o bom relacionamento existente entre os setores público e privado, os altos investimentos em segurança cibernética e a preocupação do governo em proteger os sistemas digitais do seu Estado durante as eleições de 2007 foram fundamentais para conter os ataques, minimizar os danos nos ativos de informação e proteger as infraestruturas críticas da Estônia.

Simultaneamente aos ataques cibernéticos, outras ações foram adotadas pela Rússia contra o governo estoniano. Segundo Kampmark (2007), a Rússia utilizou medidas desfavoráveis à economia da Estônia, tais como o corte do transporte entre Tallinn e São Petersburgo. Para Green (2015), a guerra cibernética parece ser mais eficaz quando utilizada em conjunto com as operações militares convencionais.

Além do mais, o transporte de carvão e petróleo da Rússia para a Estônia foi suspenso pela estatal *Russian Railways*[22] sobre a alegação de que havia a necessidade de se realizar manutenção na linha férrea (STIENNON, 2010).

Outrossim, a embaixada da Estônia na Rússia foi atacada por um grupo de jovens russos. O problema só foi resolvido depois que a Alemanha auxiliou nas negociações e conseguiu libertar o embaixador.

Segundo Aaviksoo (2008), o nível de organização, a maneira como foram coordenados os ataques, o elevado volume e direcionado contra um Estado relativamente pequeno como a Estônia teve o objetivo de comprometer a segurança nacional. O que mais chamou a atenção de Aaviksoo foram o elevado nível de coordenação dos ataques e as ações que ocorreram de forma paralela, em especial as manifestações e bloqueio da embaixada da Estônia em Moscou. Os ataques foram precisamente sincronizados.

---

[22] Russian Railways – É uma empresa de transporte russa que gerencia infraestrutura e opera serviços de trem de carga e passageiros, processa 39% de todos os movimentos de carga, incluindo oleodutos e mais de 43,2% de todas as viagens de passageiros na Rússia. Fica localizada em Moscou, Rússia (tradução nossa). Disponível em: <https://www.crunchbase.com/organization/russian-railways#section-overview>. Acesso em: 28 jun. 2018.

Assim, analisamos que os ataques cibernéticos quando empregados sobre vários ativos de informação em curto intervalo de tempo e de forma sustentada, exige que o Estado atacado faça um esforço bem maior para poder reestabelecer os serviços de maneira mais rápida possível. Os ataques cibernéticos quando utilizados juntamente com armas convencionais ou com a adoção de medidas de caráter econômico potencializam o efeito sobre o inimigo.

No próximo capítulo, os resultados obtidos serão confrontados com o modelo teórico dos cinco anéis do Coronel John Warden, no que concerne à paralisia estratégica.

4 CONFRONTO ENTRE O MODELO TEÓRICO DE WARDEN E OS ATAQUES CIBERNÉTICOS CONTRA A ESTÔNIA (2007)

No capítulo dois, foram descritos conceitos sobre o modelo teórico dos cinco anéis de Warden e de guerra cibernética e no Capítulo três foi feita uma análise dos ataques cibernéticos contra a Estônia sobre a ótica do modelo teórico em estudo.

Neste capítulo será realizado um confronto entre a teoria e a realidade a fim de concluirmos se houve ou não aderência dos ataques cibernéticos contra a Estônia (2007) ao modelo teórico. Para facilitar a comparação, este capítulo será subdividido em seis seções. As cinco primeiras seções representarão os cinco anéis da teoria e a última os ataques paralelos propostos por Warden.

4.1 Liderança

Conforme mencionado no capítulo dois, a liderança é considerada o anel mais crítico, pois os líderes são responsáveis por tomar as decisões. O gerenciamento de todo o sistema fica comprometido quando ocorrem inutilizações dos meios de comunicações do governo, haja vista que os líderes não conseguem gerenciar suas ações corretamente.

Como os ataques tiveram motivações políticas, o principal alvo dos atacantes era desestimular a liderança do governo a adotar medidas políticas e econômicas desfavoráveis ao bloco oriental. Logo, foi necessário gerar efeitos psicológicos sobre a população, governo e o partido de oposição visando à substituição dos atuais líderes por políticos com uma posição mais favorável aos interesses russos ou pressionar os atuais membros do governo estoniano a ceder aos interesses dos atacantes.

Por isso, foram realizados ataques diretos e indiretos sobre governo. Os ataques diretos foram contra os *sites* e servidores do governo e e-mails dos membros do parlamento

com o propósito de desmoralizar os líderes. Os ataques indiretos foram efetuados contra os ativos de informação da Estônia, tais como, os *sites* dos bancos, cartões de crédito e *sites* dos principais jornais. Esses ataques tinham por objetivo alcançar o psicológico da população que se sentiu prejudicada pela indisponibilidade dos serviços e exerceu pressão sobre os líderes do governo, visando o imediato restabelecimento dos serviços digitais.

Porém, a atitude do governo de informar imediatamente à população que o Estado se encontrava passando por um ataque cibernético permitiu a compreensão da situação pelos cidadãos. Além disso, os ataques foram rapidamente combatidos pelos especialistas em TIC.

Apesar dos ataques diretos e indiretos terem sido direcionado e influenciado a liderança do governo, eles não alcançaram o objetivo dos atacantes. Pois, o governo não retornou com a estátua para o local de origem. Assim, a aderência à teoria foi parcial.

4.2 Elementos orgânicos essenciais

Segundo Warden, ataques sobre elementos orgânicos essenciais geram colapso no sistema, pois provocam repercussões políticas e econômicas internas difíceis de serem suportadas pelo governo. Sem eles o governo não conseguirá exercer a função estratégica. A fim de proporcionar uma análise fidedigna, à luz da teoria de Warden, as infraestruturas críticas de telecomunicações e informação serão consideradas como sendo elementos orgânicos essenciais.

Devido a Estônia ser dependente da *Internet e* ser considerada um dos Estados mais conectados do mundo possui diversos pontos de vulnerabilidade na sua infraestrutura crítica, onde se encontram inseridas as telecomunicações e informação que, quando atacadas, comprometem a segurança do Estado e da sociedade.

Conforme analisado no capítulo três, os ataques tiveram motivações políticas e foram direcionados contra as vulnerabilidades das infraestruturas críticas civis, de modo a

atingir indiretamente a liderança do Estado e a população.

Os principais ataques contra as infraestruturas críticas foram direcionados aos servidores ISP, responsáveis por prover *Internet* para a Estônia, e aos bancos online. Pelo fato dos ataques contra o sistema bancário terem sido de grandes proporções, os especialistas que combatiam os ataques foram obrigados a desconectar temporariamente a *Internet* da Estônia com diversos Estados nacionais, de modo a bloquear imediatamente os ataques. Porém, ao longo do dia, a conexão com outros Estados foi restabelecida aos poucos.

Dessa forma, a Estônia ficou parcialmente isolada do exterior, inviabilizando o acesso aos *sites* dos dois maiores bancos pelas pessoas localizadas fora do Estado. O dano não foi maior pelo fato da Estônia não ser tão dependente de servidores externos. Isso possibilitou que os habitantes continuassem a ter acesso aos *sites* dos bancos. Os ataques não infligiram grandes danos aos bancos.

Outro setor atingindo, foram os jornais *online*. A população ficou sem acesso aos *sites* dos principais jornais, carecendo de informações. Isso dificultou o exercício do pleno comando e controle do governo, pois o governo ficou temporariamente com dificuldades para manter a população informada.

As infraestruturas críticas classificadas estavam melhores protegidas dos ataques do que as infraestruturas críticas civis e não foram alvo dos atacantes. Em função disso, não sofreram danos.

Os danos decorrentes dos ataques cibernéticos afetaram parcialmente e temporariamente apenas os ativos de informação. As infraestruturas críticas de telecomunicações e informação não foram comprometidas.

Entretanto, atingiram indiretamente a população. Essa por sua vez, pressionou o governo a reestabelecer rapidamente os serviços atingidos. Como mencionado no capítulo dois, os anéis são independentes. O ataque sobre um anel pode ter efeitos nos demais, em

especial sobre a liderança.

Apesar dos ataques não terem afetado diretamente as infraestruturas críticas, atingiram os ativos de informação, gerando impactos na população e na liderança. Assim, para o anel de elementos orgânicos essenciais, houve aderência parcial à teoria de Warden.

4.3 População

Devido à imprevisibilidade do comportamento humano, influenciada por diversos fatores, dificilmente teremos certeza de que os ataques surtirão o efeito esperado sobre a população. Todavia, os danos nos ativos de informação, particularmente nos sistemas de cartão de crédito, nos *sites* de notícias, nos *sites* dos bancos e nos sistemas de comunicações, afetaram indiretamente e temporariamente a população da Estônia. Apesar de não existirem evidências de ataques direto sobre a população, os cidadãos sentiram a indisponibilidade dos serviços. Esses fatos contribuíram para elevar a pressão exercida pela população contra os principais líderes do governo. Influência indireta na liderança, como já mencionado na seção 4.1.

Entretanto, a insatisfação da população foi minimizada devido ao rápido restabelecimento dos serviços e *sites* afetados pelas equipes que realizavam o combate aos ataques.

Adicionalmente, a transparência do governo em divulgar para a população que o Estado estava sendo atacado permitiu que as pessoas entendessem os motivos da ausência dos serviços. Além disso, possibilitou estabelecer uma confiança mútua entre o Estado e a população, criando um sentimento nacionalista na Estônia. Esses fatos contribuíram para redução da pressão psicológica gerada pelos ataques sobre a população e, consequentemente, desta sobre os líderes do governo.

Os impactos psicológicos produzidos pelos ataques cibernéticos não puderam ser

analisados isoladamente, pois a população também foi influenciada por outras ações não cibernéticas de cunho econômico, utilizadas em paralelo pela Rússia, em especial as relacionadas à interrupção do transporte de Tallinn para São Petersburgo e a suspensão do comércio de carvão e petróleo da Estônia com a Rússia.

Logo, concluímos que o impacto dos ataques sobre a população foi pequeno e sentido por poucos, minorando assim, a pressão da população sobre o governo. Os ataques sobre a população, por si só, não tiveram condições de paralisar a Estônia. Contudo, foram suficientes para influenciar o processo de tomada de decisão do governo, haja vista que diversos líderes e setores do governo atuaram diretamente no combate aos ataques, inclusive com ajuda internacional e do setor privado. Assim, o anel população teve aderência parcial à teoria.

.

4.4 Infraestrutura

Conforme mencionado no capítulo dois, a movimentação dos bens e serviços civis está contida no anel da infraestrutura, a qual está mais relacionada à infraestrutura física, tais como indústrias, pontes e ferrovias.

Nos ataques contra a Estônia não foram identificadas evidências de danos ou ataques direcionados às infraestruturas físicas. Dessa maneira, concluímos que não houve aderência dos ataques à teoria, relativo ao anel infraestrutura.

4.5 Forças militares no terreno

As forças militares no terreno são as responsáveis por realizar a proteção dos demais anéis. Similarmente ao anel infraestrutura, nos ataques contra a Estônia não foram identificadas evidências de danos ou ataques contra as forças militares no terreno. Portanto, não houve aderência dos ataques à teoria para o anel forças militares no terreno.

4.6 Ataques paralelos

Ataques simultâneos contra vários ativos de informação dificultam o reparo em tempo reduzido. Quanto maior for o número de alvos atingidos, maior será o tempo despendido para sanar todas as avarias e restabelecer o sistema avariado. A indisponibilidade do sistema inimigo é fundamental para a obtenção de vantagens estratégicas pelo atacante.

Dado o exposto, percebemos que os ataques concomitantes empreendidos contra as infraestruturas críticas e os ativos de informação da Estônia dificultaram o combate pelo governo. Os *sites* dos bancos, *sites* públicos, e-mails, pichação do *site* do governo, servidores DNS e sistemas de cartão de crédito foram afetados em curto período de tempo. No ataque com maior intensidade foi necessário, inclusive, desconectar temporariamente o Estado de parte do mundo para resolver o problema. Um esforço maior foi exigido do governo para combater os ataques simultâneos. Por isso, para que o combate fosse possível, a Estônia solicitou ajuda internacional a diversos Estados, a OTAN e dos especialistas em TIC que se encontravam no local durante o período dos ataques.

Dessa forma, verificamos que os ataques paralelos contra Estônia atingiram vários ativos de informação, exigindo um esforço maior do governo para combater os ataques. Além disso, contribuíram para elevar a pressão sobre a população e, consequentemente, sobre a liderança do governo.

De modo semelhante, as análises feitas nos anéis elementos orgânicos essenciais, população e liderança, os ataques paralelos também influenciaram no processo de tomada de decisão no nível político, mas não foram capazes de fazer com que os líderes cedessem. Assim, a aderência à teoria foi parcial referente aos ataques paralelos. Visando facilitar a compreensão se os ataques cibernéticos contra Estônia (2007) tiveram aderência ao modelo teórico dos cinco anéis de Warden, reunirmos os resultados do confronto no quadro abaixo:

QUADRO 1

Síntese da aderência dos ataques cibernéticos contra Estônia (2007) ao modelo teórico dos cinco anéis do Coronel John Warden.

Modelo de Warden	Esperado do modelo	Observado	Aderência	Observações
Liderança	Ataques diretos sobre a liderança e influência dos demais anéis. Objetivo: fazer a liderança ceder.	Ataques diretos sobre os e-mails, *sites* e servidores do governo. Pressão da população. Liderança não cedeu.	Parcial	Os ataques atingiram a liderança. Entretanto, não tiveram a força suficiente para fazer com que os líderes determinassem o retorno da estátua para o local de origem.
Elementos orgânicos essenciais	Paralisar as infraestruturas críticas de telecomunicações, informação e energia de modo a afetar os demais anéis e fazer a liderança ceder.	Ataques nos ISP e *sites* dos bancos. *Sites* dos bancos inacessíveis do exterior, mas não afetaram as infraestruturas críticas. Afetou a população e a liderança temporariamente. Liderança não cedeu.	Parcial	Os ataques não atingiram as infraestruturas críticas, devido às medidas de proteção adotadas pelo governo.
Infraestrutura	Ataques sobre as infraestruturas de transporte e industrial de modo a afetar os demais anéis e fazer a liderança ceder.	Não foram identificadas evidências de ataques cibernéticos.	Não houve	Não ocorreram danos nas infraestruturas físicas.
População	Os danos nos demais anéis geram efeitos psicológicos. População pressiona as lideranças.	Danos nos ativos de informação, tais como *sites*, cartões de crédito e jornais provocaram efeitos psicológicos sobre a população. Pressão sobre o governo. Liderança não cedeu.	Parcial	O efeito psicológico for minimizado devido ao rápido restabelecimento dos serviços afetados.
Forças militares no terreno	Danos nos subanéis das forças militares no terreno.	Não foram identificadas evidências de ataques.	Não houve	Os ataques tiveram motivações políticas.
Ataques paralelos	Ataques simultâneos sobre vários alvos dos anéis dificultando seu reparo imediato. Afetar os demais anéis de modo que a liderança ceda.	Ataques simultâneos sobre vários ativos de informação dificultaram o restabelecimento dos serviços pelo governo que solicitou ajuda internacional para combater os ataques. Liderança não cedeu.	Parcial	Outras medidas de ordem econômica foram adotadas em paralelo aos ataques.

Fonte: WARDEN, 1995.

Nota: O quadro foi elaborado pelo autor a partir da análise do capítulo quatro.

Assim, os ataques não conseguiram atingir os setores apresentados pelos anéis da teoria de Warden na sua integralidade, principalmente, pelo fato de que a intensidade dos ataques esteve aquém do necessário para provocar danos significativos nas infraestruturas críticas e nos ativos de informação que pudessem efetivamente paralisar a Estônia. Ademais, o elevado esforço dos especialistas cibernéticos, juntamente com apoio de outros Estados e organismo internacionais, e os investimentos feitos pelo governo durante as eleições nos anos anteriores, contribuíram para que não houvesse uma paralisia nos sistemas estonianos. Entretanto, os ataques cibernéticos conseguiram atingir psicologicamente a população e gerar reflexos sobre os líderes da Estônia, mostrando-nos a interpendência entre os anéis da teoria de Warden.

Levando em consideração o que foi observado, o autor infere que um ataque cibernético de grandes proporções realizado por pessoas capacitadas, de forma coordenada e sustentada nos diversos anéis é capaz de paralisar um Estado, especialmente quando usado em conjunto com ataques que utilizam armas convencionais. Contudo, algumas condições se fazem necessárias para que isso seja possível, tais como: Estado extremamente dependente da *Internet*, infraestruturas críticas gerenciadas por software que estejam interligadas à rede mundial de computadores, reduzida mentalidade de segurança cibernética e baixo grau de investimentos em TIC. Esses fatos não ocorreram em sua plenitude no objeto em estudo.

Assim, concluímos que os ataques cibernéticos contra a Estônia (2007) tiveram aderência parcial ao modelo teórico em estudo, no que concerne à paralisia estratégica.

5 CONCLUSÃO

Este estudo teve como propósito analisar se os ataques cibernéticos contra a Estônia (2007) tiveram aderência à teoria dos cinco anéis do Coronel John Warden, no que tange à paralisia estratégica. Para tal, foi utilizada a abordagem realística, comparando o objeto em estudo com a teoria.

Desse modo, buscamos responder a seguinte questão que serviu como referência para o estudo: os ataques cibernéticos contra Estônia, em 2007, tiveram aderência ao modelo teórico dos cinco anéis do Coronel John Warden, no que concerne à paralisia estratégica?

No capítulo dois, a fim de amparar a resposta para a questão, apresentamos a teoria de Warden que tem como propósito paralisar estrategicamente o sistema do inimigo. Suas ideias foram oriundas dos teóricos do poder aéreo, utilizadas na operação Tempestade no Deserto (1991), no Iraque. Ademais, defende que na guerra estratégica o choque pode ser utilizado, mas nem sempre é necessário, devendo sempre que possível, ser evitado. Adicionalmente, expomos informações atinentes à Doutrina de Guerra Cibernética com propósito de proporcionar um melhor entendimento dos ataques cibernéticos contra a Estônia (2007).

No capítulo três, abordamos um breve histórico e as motivações dos ataques, seguidos de uma análise dos ataques cibernéticos contra a Estônia (2007), de maneira a evidenciar os autores dos ataques, a relação existente entre conectividade e vulnerabilidades, os setores e serviços alvos dos ataques, os danos provocados e os efeitos psicológicos gerados sobre a população e o governo. Além disso, verificamos o resultado dos ataques e como foram combatidos.

No capítulo quatro, realizamos o confronto entre a teoria de Warden com os ataques cibernéticos contra a Estônia (2007) a fim de verificarmos se houve aderência à

teoria. Por isso, produzimos uma análise por anéis a fim de identificarmos os impactos em cada anel e de que forma influenciaram a população e os líderes do governo.

As principais conclusões desses capítulos serão explanadas a seguir:

No capítulo dois, diagnosticamos no modelo teórico que cada Estado deve ser visto como um sistema composto por cinco anéis concêntricos e interdependentes. Os anéis são divididos do centro para a periferia da seguinte forma: liderança, elementos orgânicos essenciais, infraestrutura, população e forças militares no terreno. Dessa maneira, os anéis devem ser prioritariamente atacados de dentro para fora. O que se busca é atingir a liderança, considerado o anel mais importante, realizando ataques diretos sobre a liderança ou sobre o CG dos demais anéis. A destruição das lideranças ou da sua capacidade de se comunicar compromete todo o sistema. Assim, quanto mais próximo estiver o anel atacado da liderança, maiores são as chances de levar o sistema ao colapso. Além disso, um ataque eficaz é aquele feito simultaneamente sobre diversos alvos, chamado de ataques paralelos.

No capítulo três, demonstramos que os ataques cibernéticos ocorreram devido à retirada da estátua para um cemitério. Mas as divergências de cunho político entre os Estados da Rússia e da Estônia já existiam desde a Segunda Guerra Mundial. Ademais, a independência da Estônia, sua reaproximação com os Estados ocidentais e sua entrada na OTAN geraram descontentamento da Rússia, sendo a transferência da estátua apenas o estopim para o início das ações no campo cibernético. Por isso, os ataques tiveram motivações políticas com o propósito de pressionar o governo da Estônia de modo que a estátua fosse devolvida ao seu local de origem, de forma a demonstrar a força política, ainda remanescente, da Rússia sobre a Estônia. Em relação aos responsáveis pelos ataques, apesar de existirem evidências sugerindo os autores, a Rússia não se considera a responsável. A entrada da Estônia para OTAN dificultou uma intervenção tradicional russa, haja vista que poderia sofrer retaliações da OTAN. A maneira encontrada para ocultar suas responsabilidades foi o

emprego da “arma cibernética”, comprovando assim, que os ataques cibernéticos possui um poder de ocultação dos atacantes superior aos ataques convencionais que se utilizam de armas cinéticas.

Adicionalmente, verificamos como um Estado extremamente dependente da *Internet*, na qual a maioria das atividades é realizada por meio de dispositivos digitais conectados à rede mundial de computadores, possui diversas vulnerabilidades nos seus ativos de informação passíveis de serem exploradas.

Além do mais, ficou demonstrado que os ataques realizados contra os ativos de informação da Estônia tinham por objetivo causar danos nas infraestruturas críticas civis de forma a provocar reflexos sobre psicológico da população e liderança do governo. No entanto, as infraestruturas críticas não foram paralisadas, em virtude do esforço e preparo do governo no combate aos ataques. Investigamos que os ataques de DDoS infligiram danos temporários nos ativos de informação da Estônia, afetando principalmente, o presidente, governo, a mídia e a economia. A população foi pouco afetada pelos ataques.

No capítulo quatro, verificamos que diversos ataques cibernéticos foram realizados de forma simultânea, contra os ativos de informação, de forma a dificultar o combate aos ataques pelos especialistas cibernéticos. Entretanto, as medidas adotadas pelo governo, visando mitigar os ataques cibernéticos, impediram que sérios estragos às infraestruturas ocorressem e, por conseguinte, não afetassem severamente a população e o governo da Estônia. Por isso, os impactos dos ataques foram pequenos e sentidos por poucos. Contudo, foram suficientes para afetar indiretamente a população e influenciar no processo de decisão das lideranças. Logo, a comparação realizada com os cinco anéis de Warden, apenas os anéis da liderança, elementos orgânicos essenciais, população e o conceito de ataques paralelos tiveram aderência parcial à teoria. Portanto, a Estônia não foi paralisada estrategicamente.

Dessa forma, respondendo a nossa questão, concluímos que os ataques cibernéticos contra a Estônia (2007) tiveram a aderência parcial ao modelo teórico dos cinco anéis de Warden, no que concerne à paralisia estratégica.

Apesar de não ter provocado a paralisia estratégica da Estônia, um ataque cibernético empregado contra as vulnerabilidades críticas dos ativos de informação, especialmente contra as infraestruturas críticas de um Estado muito dependente da *Internet* e sem a devida proteção, somado ao efeito gerado pela indisponibilidade de diversos serviços à população, contribui para obtenção de grandes vantagens estratégicas pelo atacante. Quando os ataques são realizados em conjunto com as armas convencionais seus efeitos são potencializados ao ponto de fazer com que o inimigo desista de lutar. Todavia, não conseguimos durante o estudo desenvolver sua serventia contra as forças militares. Por isso, sugerimos para pesquisas futuras que seja feito uma análise da aplicabilidade dos ataques cibernéticos contra as forças militares no terreno.

Ao término deste trabalho, concluímos que a análise dos conceitos relacionados ao ambiente cibernético tem grande aplicabilidade para a Marinha do Brasil. Em especial, no desenvolvimento e aperfeiçoamento de doutrinas de guerra cibernética que possibilitem aprimorar o uso do espaço cibernético e para realçar a importância da sinergia entre os setores público e privado, em âmbito nacional, bem como a realização de exercícios cibernéticos com os Estados aliados, visando mitigar um possível ataque cibernético.

REFERÊNCIAS

ALMANN, Lauri. *Turning around the 2007 cyber attack: lessons from Estonia*, 2013. Disponível em: <http://estonianworld.com/security/turning-around-2007-cyber-attack-lessons-estonia/>. Acesso em: 25 jun. 2018.

AAVIKSOO, J. *Cyber-Terrorism. Vital Speeches of the Day*. v. 74, n. 1, p. 28-32, Jan. 2008. Disponível em: <http://web.b.ebscohost.com>. Acesso em: 15 jun. 2018.

BRASIL. Ministério da Defesa. MD-35-G-01*: Glossário das Forças Armadas.* 5.ed. Brasília, 2015.

_____. Ministério da Defesa. MD31-M-07*: Doutrina Militar de Defesa Cibernética*, Brasília, 2014.

_____. Secretaria de Assuntos Estratégicos da Presidência da República, *Desafios estratégicos para segurança e defesa cibernética*, Brasília, 2011, 216 p. Disponível em: <http://www.biblioteca.presidencia.gov.br>. Acesso em: 12 jun. 2018.

BRENNER, J. *America the vulnerable: Inside the new threat matrix of digital espionage, crime, and warfare.* New York, Penguin, 2011. 320 p.

CLARKE, Richard A.; KNAKE Robert K. *Guerra Cibernética: A próxima ameaça à segurança e o que fazer a respeito.* Rio de Janeiro, Brasport, 2015. 242 p.

CLAUSEWITZ, Carl V. *Da guerra*. São Paulo: M. Fontes, Brasília: Ed. Univ. Brasília, 1979. 787 p.

EVRON, G. *Estonian cyber-war highlights civilian vulnerabilities*. *eWeek*. 24, 26, 34, Aug. 13, 2007. Disponível em: <http://web.b.ebscohost.com>. Acesso em: 13 jun. 2018.

FADOK, David S. John Boyd and John Warden Air Power's Quest for Strategic Paralysis. 61f. Dissertação - USAF School of Advanced Airpower Studies, Air University Press Maxwell Air Force Base, Alabama, 1995.

GREEN, James A. *Cyber Warfare: a multidisciplinary analysis*, New York, Routledge, 2015. 195 p.

HERZOG, S. *Revisiting the Estonian cyber attacks: digital threats and multinational responses, Journal of Strategic Security*, v. 4, n. 2, p. 49–60, 2011. Disponível em: <http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss>. Acesso em: 22 jun. 2018.

ILVES, Toomas H. - *The Consequences of Cyber Attacks. Journal of International Affairs.* v. 70, n. 1, p. 175-178, 2016. Disponível em: <http://web.b.ebscohost. com>. Acesso em: 27 jun. 2018.

KAMPMARK, B. *Cyber warfare between Estonia and Russia*. *Contemporary review. v.* 289, n. 1686, p. 288-293, Set. 2007. Disponível em: <http://web.a.ebscohost.com>. Acesso em: 27 jun. 2018.

LANDLER, Mark; MARKOFFMAY, John, *Digital Fears Emerge After Data Siege in Estonia*. 2007. Disponível em: <https://www.nytimes.com/2007/05/29/technology/29estonia.html>. Acesso em: 05 mai. 2018.

LEWIS, James A. *Cyber Attacks Explaine,* 2007. Disponível em: <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/070615_cyber_attacks.pdf>. Acesso em: 07 jun. 2018.

MEILINGER, P. S. *The paths of heaven: the evolution of airpower theory*. Alabama: Air University, 1997. 650 p.

NYE JUNIOR, Joseph S. *O Futuro do Poder.* São Paulo: Benvirá, 2012. 334 p.

OTTIS, R. *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective.* Plymouth, 2008, p 163-168. Disponível em: <https://www.etis.ee/Portal/Publications/Display/c269960c-2e40-44b1-aa43-a7c62e9caaa6>. Acesso em: 15 mai. 2018.

ROSA, Carlos Eduardo Valle. *Poder aéreo: guia de estudos*. Rio de Janeiro: UNIFA, 2015. 468 p.

RUSS, Kertu, *Cyber War I: Estonia Attacked from Russia*. *European Affairs*: v. 9, n. 1-2, inverno/primavera 2008. Disponível em: <https://www.europeaninstitute.org/>. Acesso em: 06 jun. 2018.

STIENNON, Richard. *Surviving Cyberwar*, Rockville, United States, Government Institutes, 2010, 181 p.

TEN years of Cyber Estonia: What will the Next Decade Bring? Direção e produção: *Center For Strategic And International Studies*. Seminário, 151'10''. Washington, DC. 2017. Disponível em: <https://www.csis.org/events/10-years-cyber-estonia-what-will-next-decade-bring>. Acesso em: 10 jun. 2018.

WARDEN, John A. *The air campaign: planning for combat.*. Washington, DC: National Defense University Press, 1988. 193 p.

WARDEN, John. A. *The enemy as a system. Airpower Journal,* Pensilvânia, EUA, v. 9. n. 1, p.41-55, primavera 1995. Disponível em: <http://web.a.ebscohost.com/>. Acesso em: 22 mai. 2018.

WIENER, Norbert. Cibernética e sociedade: o uso humano de seres humanos. 4. ed. São Paulo: Cultrix, 1973. 190 p.