ESCOLA DE GUERRA NAVAL

ALEXANDRE NUNES COUTINHO

A GUERRA CIBERNÉTICA ENTRE RÚSSIA E GEÓRGIA DE 2008:

uma análise dos ataques cibernéticos sob a ótica da teoria de John Warden

Rio de Janeiro

2020

ALEXANDRE NUNES COUTINHO

A GUERRA CIBERNÉTICA ENTRE RÚSSIA E GEÓRGIA DE 2008:
uma análise dos ataques cibernéticos sob a ótica da teoria de John Warden

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.
Orientador: CC (CA) Daniel Barbosa da Silva Barabani

Rio de Janeiro

Escola de Guerra Naval

2020

AGRADECIMENTOS

À minha esposa, Ana Luiza e aos meus filhos, Ian, Caio e Laura, pelo apoio, motivação e carinho dispensados durante a realização deste trabalho.

À minha mãe, Ângela Maria Nunes Coutinho, pelo carinho e apoio até a conclusão deste trabalho.

Ao Capitão de Corveta Barabani, meu orientador, pelo incentivo em estudar este tema e pelas sugestões, sempre precisas e extremamente profissionais, que foram de grande valia para a conclusão deste estudo.

Ao Capitão de Fragata Nagashima, pelo suporte ao desenvolvimento da minha argumentação e pelas contribuições para a sofisticação do encadeamento lógico desta pesquisa.

Por fim, A Deus, por sua paciência e amor, e por ter me inspirado nos momentos de dificuldade para que pudesse concluir este trabalho da melhor forma possível.

“O problema para todos os estados na atual era da informação global é que mais coisas estão acontecendo fora do controle até mesmo dos estados mais poderosos”

(Joseph S. Nye Jr., 2011)

RESUMO

O objetivo deste trabalho é analisar se os ataques cibernéticos contra a Geórgia em 2008 tiveram aderência ao modelo teórico dos cinco anéis do Coronel John Warden, no que se refere à paralisia estratégica. A sua teoria foi formulada a partir do poder aéreo e com o passar dos anos, mais precisamente em 1988, procurando uma forma de relacionar os centros de gravidade com o poder aéreo, Warden desenvolve o "modelo dos cinco anéis". O modelo foi aplicado contra as forças iraquianas que invadiram o Kuwait em 1991, com grande sucesso. O desenho de pesquisa utilizado foi a comparação da teoria com a realidade. Fruto desse confronto, concluímos que os ataques cibernéticos tiveram aderência parcial ao seu modelo, contudo as evidências mostraram que os resultados dos ataques tiveram consequências graves para a Geórgia e que caso fossem realizados contra as infraestruturas críticas poderiam ter levado aquele Estado rapidamente a sua paralisia estratégica. Além disso, concluímos também, que os ataques cibernéticos quando utilizados de forma paralela com os meios convencionais de guerra, em um conflito armado, podem trazer grandes vantagens militares para o atacante. Finalmente, este trabalho mostra a importância da Marinha do Brasil manter seu poder cibernético, ofensivo e defensivo, em prol dos seus interesses e dos interesses nacionais, em consonância com a Política Nacional de Defesa e a Estratégia Nacional de Defesa.

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

LISTA DE ABREVIATURAS E SIGLAS

C2	Comando e Controle
CG	Centro de Gravidade
DDoS	*Distributed Denial of Service* - Distribuído de Negação de Serviço
ICS	*Industrial Control System* – Sistema de Controle Industrial
RBN	*Russian Business Network* – Rede de Negócios Russa
SCADA	*Supervisory Control and Data Acquisition* - Sistema de Supervisão e Aquisição de Dados
SQL	*Structured Query Language* - Linguagem de Consulta Estruturada
Op Info	Operações de Informação
CRI	Capacidades Relacionadas à Informação

SUMÁRIO

1 INTRODUÇÃO

A Revolução da Informação se baseia nos rápidos avanços tecnológicos em computadores, softwares e nas comunicações. Tais mudanças acarretaram alterações significativas no custo de criar, processar, transmitir e acessar as informações. À medida que os custos diminuíram ao longo dos anos e o acesso a essas tecnologias se difundiu entre praticamente todas as classes sociais, a Revolução da Informação vem reduzindo o poder dos grandes Estados e aumentando o poder dos pequenos e dos atores não estatais.

No mundo hodierno, é perfeitamente factível que um adversário mais fraco, porém com capacidade de realizar ataques cibernéticos, possa atacar ou ameaçar adversários mais fortes. Existe também a possibilidade de os Estados patrocinarem hackers para realizar ataques cibernéticos para fins diversos.

Em um mundo cada vez mais volátil, incerto, complexo e ambíguo (VUCA)[1] e ,também, globalizado, atores estatais e não estatais vêm se utilizando de ataques cibernéticos para conseguir vantagens, sejam elas no campo de batalha ou não. Os benefícios dos ataques cibernéticos são bem claros: anonimato e custo reduzido em relação aos ataques com armas convencionais. Assim, nas duas últimas décadas, estudos apontam que o número de ataques cibernéticos aumentou vertiginosamente, causando prejuízos incalculáveis para os Estados e empresas privadas.

É nesse contexto que escolhemos como objeto de estudo a guerra cibernética entre Geórgia e Rússia ocorrida no ano de 2008. Analisaremos os tipos de ataques cibernéticos utilizados, seus objetivos, uma breve análise sobre a autoria dos ataques e as suas consequências para o meio militar e civil. Este conflito se reveste de uma característica especial: foi o primeiro

[1] Acrônimo das palavras em ingês "*Volatility, Uncertainty, Complexityand Ambiguity."* O conceito foi empregado na década de 90 pelo *U.S Army War College* para explicar o mundo no cenário pós-Guerra Fria (1947-1991). <http://usawc.libanswers.com/faq/84869>.

conflito na história em que ataques cibernéticos ocorreram simultaneamente com ataques militares no campo de batalha. Assim, também, analisaremos se esses ataques paralelos trouxeram - ou não - vantagens militares para os russos.

O propósito deste trabalho é analisar se os ataques cibernéticos contra a Geórgia em 2008 tiveram aderência ao modelo teórico dos cinco anéis do Coronel John Warden, no que se refere à paralisia estratégica do inimigo. Para tal, utilizaremos a confrontação da teoria com o objeto aludido.

Para atingir o propósito, o trabalho foi dividido em cinco capítulos. Após esta introdução, segue-se o segundo capítulo, em que descreveremos o modelo teórico dos cinco anéis, cujo objetivo é permitir uma melhor visualização de como se distribui os centros de gravidade do inimigo nos níveis estratégico e operacional, permitindo atacar as suas lideranças com o objetivo de causar a sua paralisia estratégica. Também abordaremos o conceito de ataques paralelos e alguns conceitos considerados importantes sobre guerra cibernética.

No capítulo três, abordaremos os ataques cibernéticos contra a Geórgia em 2008, analisando os setores atingidos, as consequências dos ataques e uma breve análise sobre a autoria dos mesmos. Além disso, abordaremos se os ataques paralelos foram propositais ou não, levando em consideração evidências de estudiosos e especialistas no assunto. No quarto capítulo, confrontaremos os ataques cibernéticos contra a Geórgia com o modelo teórico selecionado para a pesquisa, a fim de verificar as aderências à mesma.

No quinto capítulo, apresentaremos as conclusões e indicaremos possíveis linhas de investigação futuras que não puderam ser comprovadas, devido à falta de evidências encontradas nas obras consultadas. A seguir será apresentada a ideia de paralisia estratégica, o modelo teórico dos cinco anéis do Coronel John Warden e alguns conceitos importantes sobre guerra cibernética.

2 TEORIA DE JOHN WARDEN E CONCEITOS DE GUERRA CIBERNÉTICA

Neste capítulo, abordaremos um breve histórico da vida do Coronel John Warden e os fatores que o levaram a formular, em 1998, a sua teoria sobre a "Estratégia da Paralisia" e seus principais fundamentos, concretizados em 1995, no modelo teórico dos cinco anéis. Além disso, apresentaremos alguns conceitos de guerra cibernética importantes para a compreensão dos ataques cibernéticos que serão descritos no capítulo 3.

Warden é um 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 a realizar uma comparação da sua teoria com os ataques cibernéticos contra a Geórgia em 2008, serão estudados os 5 anéis da sua teoria, os quais são liderança, elementos orgânicos essenciais, infraestrutura, população e forças militares. Além disso, será abordado o conceito de ataques paralelos, a fim de verificar se houve aderência com os ataques descritos no capítulo 3.

2 .1 Surgimento da estratégia da paralisia

As origens da estratégia da paralisia remontam há milênios. Sun Tzu (544 a.C. - 496 a.C.), um dos maiores estrategistas militares da história, entendia que uma boa estratégia não visa a ganhar várias batalhas, e sim vencê-las sem combater (SUNZI, 2007).

No primeiro volume da sua obra "*On War*", o atemporal Clausewitz (1780-1831) entende que a aniquilação das forças inimigas deve ser conduzida a um ponto em que o inimigo não tenha condições de prosseguir no combate (CLAUSEWITZ, 1918). Assim, observa-se que a concepção de destruição do inimigo está, de certa forma, alinhada com a estratégia da paralisia

do inimigo.

Após os ensinamentos da Primeira Guerra Mundial (1914-1918), em 1919, o inglês John Frederick Chales Fuller (1878-1966), um dos percussores da paralisia estratégica, defende que a força de um exército depende da sua organização, controle e cérebro. Segundo o autor, parando o seu cérebro, o corpo do exército também para de funcionar (FULLER, 1966).

Para um melhor entendimento da sua teoria, ele fez a seguinte analogia: assim como o corpo humano é constituído por corpo, mente e espírito, a guerra, como uma atividade humana, apresenta uma constituição similar. Assim, a estratégia da paralisia tinha o objetivo de atuar na dimensão física (elementos materiais que formam o poder combatente) do poder inimigo, procurando afetar sua capacidade mental (capacidade de planejamento, comando e controle) e, indiretamente, atingir a sua vontade moral (FULLER, 1966).

Na mesma linha de pensamento em relação à estratégia militar, seu conterrâneo e admirador, Liddell Hart (1895-1970), advogava que a mais eficiente e econômica forma de fazer a guerra seria paralisar o inimigo ao invés de destruí-lo ou aniquilá-lo. Hart argumentava que os estrategistas deveriam pensar em termos de paralisia em todos os níveis da guerra. Ele insistia que a forma de guerra mais potente e econômica era o desarmamento por meio da paralisia, e não a destruição por meio da aniquilação (FADOK, 1995).

Pelas ideias apresentadas, percebe-se que a paralisia estratégica evoluiu com o passar dos anos, obedecendo à moldura intelectual dos estrategistas citados. Dessa forma, entende-se que é uma opção que engloba os quatro níveis da guerra. No campo político e estratégico, o objetivo é incapacitar o inimigo, impedindo-o a ação. Nos níveis operacionais e táticos, busca-se a incapacitação física e mental dos combatentes, afetando o psicológico e, consequentemente, a sua vontade de lutar.

Baseado nas ideias apresentadas, os estrategistas contemporâneos desenvolveram novas teorias de emprego do poder aéreo, com foco na paralisia estratégica.

2.2 A paralisia estratégica e o modelo de cinco anéis

John Ashley Warden III nasceu em 21 de dezembro de 1943 na cidade norte-americana de Mckinney. Foi o quarto da família a ingressar nas Forças Armadas. Em 1965 formou-se na Academia da Força Aérea dos EUA, iniciando uma carreira militar que perduraria pelos próximos 30 anos (OLSEN, 2007).

O interesse pela estratégia e pela arte da guerra se intensificou entre 1974 e 1975, quando passou a fazer mestrado na Universidade do Texas. Ele aproveitou a oportunidade para ler amplamente e refletir sobre novos aspectos da Segunda Guerra Mundial e sua tese concentrou-se exclusivamente na tomada de decisões com base em uma estratégia de alto nível (OLSEN, 2007).

A partir desse momento, com base nos conceitos anteriores de paralisia estratégica, Warden desenvolve a sua teoria de emprego do poder aéreo no cenário das guerras atuais e futuras.

Em sua obra “The Air Campaign” (1988), defende que o poder aéreo é capaz de atingir objetivos estratégicos com custos operacionais mínimos. As características da força aérea como velocidade e penetração permitem, de forma rápida e decisiva, alcançar alvos além do alcance das forças de superfície: os centros de gravidade do inimigo (WARDEN, 1998).

A interpretação do conceito de Centro de Gravidade, na obra “The Air Campaign”, não se diferencia na essência de conceitos previamente estabelecidos por outros estrategistas. Com o passar dos anos, mais precisamente em 1988, procurando uma forma de relacionar os centros de gravidade com o poder aéreo, Warden desenvolve o “modelo dos cinco anéis”. O modelo foi aplicando contra as forças iraquianas que invadiram o Kuwait (ROSA, 1995).

De acordo com Warden (1995), no nível estratégico, os melhores modelos são aqueles que apresentam uma visualização do inimigo de uma forma macro; assim, para qualquer necessidade de detalhamento, basta expandir o modelo na área desejada, refinando as

informações. O modelo dos cinco anéis é o que melhor representa o mundo real por apresentar as características citadas.

A interpretação do inimigo como um sistema parte do princípio de que ele possui características de entidades estratégicas[2]. Para melhor compreensão do modelo, o autor utiliza o corpo humano como exemplo[3]. Vejamos a sua linha de raciocínio: o cérebro é o órgão central, sendo responsável por comandar o corpo. Além do cérebro, o centro do sistema também engloba receptores de informação, como olhos e outros órgãos responsáveis pela percepção. O corpo, sem o funcionamento do cérebro, deixa de ser uma entidade estratégica, pois ele é quem comanda o sistema todo (WARDEN, 1995).

O cérebro, para controlar as demais partes do corpo, depende das informações provenientes dos órgãos essenciais como o oxigênio e os alimentos. Estes, por sua vez, são convertidos pelos órgãos vitais que, a partir dessas fontes de energia, fornecem os elementos necessários ao bom funcionamento do corpo. Com esse processo funcionando em harmonia, o cérebro pode exercer a sua função de controlar o corpo através das outras partes constituintes do sistema, como ossos e músculos. Além disso, as células são responsáveis pelo transporte de nutrientes e oxigênio e, dentre elas, algumas têm a missão de proteção contra corpos estranhos, como um vírus (WARDEN 1995).

Neste ponto, são necessárias algumas observações importantes para ajudar a compreender a dependência entre os elementos que compõe o sistema proposto por Warden. Em primeiro lugar, apesar da importância do elemento central, o cérebro não é capaz de exercer o controle pleno sem o apoio dos órgãos essenciais, devido ao déficit de energia, faltando-lhe energia para distribuir para o corpo. Do mesmo modo, os demais órgãos não atuariam de forma eficiente sem os comandos do elemento central: o cérebro.

---

[2] Entidade estratégica é um sistema que funciona de forma autônoma para tomar decisões utilizando seus próprios meios (WARDEN, 1995).

[3] No texto original, o autor se aprofunda nas conexões entre as partes do sistema do corpo humano. Para não fugir ao propósito do trabalho, faremos um resumo da sua teoria, salientando as partes que interessam à pesquisa.

Em segundo lugar, o impacto causado pela falha de um de seus subsistemas vai depender da sua importância para o funcionamento do sistema como um todo. Por exemplo, o mau funcionamento do cérebro pode tornar o corpo inerte, ao passo que o mau funcionamento de uma célula, dependendo da sua função, não causa danos graves ao sistema.

A partir deste exemplo, Warden extrai os componentes do sistema que podem ser encontrados em outras entidades estratégicas. Conforme visto na figura 1, que também ilustra os subsistemas de cada componente, o anel central deste sistema engloba as lideranças e é envolvido pelos seguintes anéis, distribuídos do interior para o exterior: os elementos essenciais orgânicos, a infraestrutura, a população e os elementos responsáveis pela defesa do sistema e as forças militares.

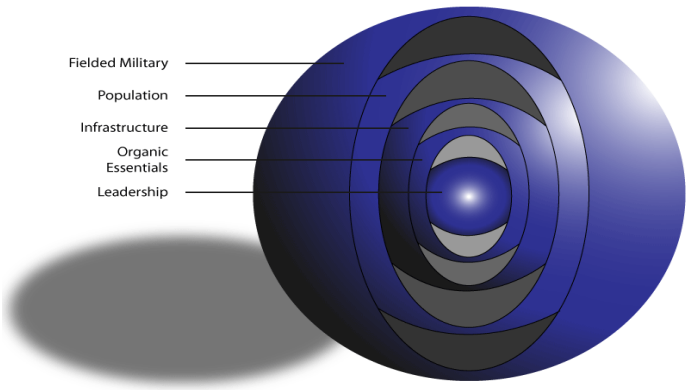

FIGURA 1 – Modelo dos cinco anéis estratégicos de John Warden. Fonte: (WARDEN, 1995, p. 47).

Além disso, Warden entende que, em sistemas mais complexos, existem dificuldades para manutenção da ordem quando ocorrem alterações em locais estratégicos, levando-os ao colapso, conforme descrito abaixo:

> No nível estratégico, nós atingimos nossos objetivos causando mudanças tão significativas a uma ou mais partes do sistema físico do inimigo que ele decide adotar nossos objetivos, ou tornamos fisicamente impossível para ele se opor. A essa última forma chamamos de “Paralisia Estratégica”. Que partes do inimigo atacamos (com uma variedade de armas, variando desde explosivos até **vírus de computador** não letais) dependerá de quais sejam nossos objetivos, da vontade do inimigo de resistir, de quão capaz ele é e de quanto esforço nós somos, fisicamente, moralmente e

politicamente, capazes de exercer (WARDEN, 1995, Pag.43, tradução e **grifo nosso**).[4]

No nível estratégico da guerra, os objetivos são distribuídos de acordo com o modelo dos cinco anéis por todo o sistema do inimigo. Assim, segundo Warden, tem-se uma visualização mais ampla das forças do inimigo, permitindo atacar os alvos prioritários a fim de desprover das forças militares o apoio das lideranças, dos suprimentos, da infraestrutura e da população.

No interior dos anéis existe um centro de gravidade (CG) que representa o "centro de todo poder e movimento". Eliminando ou neutralizando um ou mais CG, põe-se fim à efetividade desse componente do poder e o impacto no sistema como um todo dependerá da posição do anel: quanto mais interno, mais efetivo deverá ser o efeito.

Em relação às forças militares, Warden atenta que não se deve desconsiderar o ataque a elas pois, para atingir os centros estratégicos, pode ser necessária a sua neutralização ou destruição. Além disso, as forças militares também serão os alvos prioritários quando um militar não dispuser de meios para atingir diretamente os centros estratégicos.

Assim, Warden (1995) conclui que os centros de gravidade também são identificáveis no nível operacional e, para identificar precisamente os CG de cada anel, sugere o desmembramento em outros cinco "subanéis", conforme a Fig. 2 (com os mesmos componentes: liderança, órgãos essenciais, etc.) e sucessivamente, até encontrar o verdadeiro centro de gravidade: aquele que efetivamente afetará o cérebro do adversário.

[4]At the strategic level, we attain our objectives by causing such changes to one or more parts of the enemy's physical system that the enemy decides to adopt our objectives, or we make it physically impossible for him to oppose us. The latter we call strategic paralysis. Which parts of the enemy system we attack (with a variety of weapons ranging from explosives to non lethal computer viruses) will depend on what our objectives are, how much the enemy wants to resist us, how capable he is, and how much effort we are physically, morally, and politically capable of exercising (WARDEN, 1995, p.43, tradução nossa).

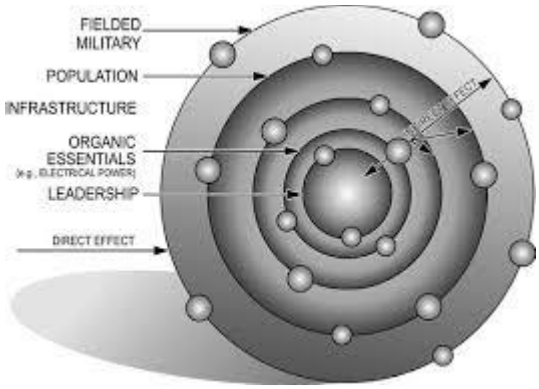

FIGURA 2 – Modelo dos cinco anéis com subsistemas Fonte: (WARDEN,1995, p. 48).

O anel central do modelo - a liderança - é considerado crítico pois, segundo Warden (1995), este é o componente do sistema responsável por definir as decisões de um Estado, ou seja, o responsável por nortear as forças em um conflito e fazer concessões. Capturar ou matar um líder de Estado, atualmente, tornou-se uma tarefa difícil; no entanto, monitorar ou destruir as comunicações do elemento central se tornaram fundamentais, uma vez que elas são vulneráveis a um ataque. Assim, quando as comunicações do comando sofrem danos, como no caso do Iraque, a liderança do sistema tem dificuldade em nortear seus esforços de guerra.

Quando a liderança do sistema não pode ser ameaçada diretamente, deve-se fazê-la indiretamente, até o inimigo concluir racionalmente que é apropriado realizar concessões e desistir da guerra. Tal conclusão é advinda da constatação do grau de danos impostos aos anéis vizinhos, levando-o a uma grande pressão psicológica para manter o esforço de guerra. Assim, o inimigo será levado à paralisia estratégica.

O próximo anel crítico contém os elementos orgânicos essenciais. Tais elementos referem-se às facilidades ou processos cujas ausências impedem a sobrevivência de uma organização ou de um Estado. No nível estatal, com crescimento das cidades em tamanho ao redor do mundo, a necessidade por eletricidade e petróleo colocou essas commodities como prioridades. Um ataque severo a estas dificultaria a vida da população, além de impedir o uso de armamentos modernos que necessitem destes recursos. Dependendo do tamanho do Estado e da importância que atribui aos seus objetivos, mesmo pequenos danos a indústrias essenciais

podem obrigar as lideranças a fazerem concessões.

As concessões podem vir pelos seguintes motivos: os danos aos elementos orgânicos essenciais levam ao colapso do sistema; danos aos elementos orgânicos essenciais tornam fisicamente difícil ou impossível manter uma determinada política ou esforço de guerra; os danos aos elementos orgânicos essenciais têm repercussões políticas ou econômicas internas que são muito caras para suportar.

O terceiro anel mais crítico é o anel da infraestrutura inimiga. Ele contém o sistema de transporte, responsável por movimentar bens e serviços, tanto civis quanto militares, em toda a área de atuação do Estado. Inclui linhas ferroviárias, linhas aéreas, rodovias, pontes, aeródromos, portos e uma série de outros sistemas similares. Os produtos industriais situam-se neste anel, pois uma parcela da produção não é considerada como elemento orgânico essencial.

Para a manutenção dos propósitos civis e militares de um Estado, é necessário o movimento de mercadorias, serviços e informações de um ponto até outro; assim, caso ocorra interrupção nessa dinâmica de movimentação, o Estado perde capacidade de resistir às exigências do seu adversário. Em comparação aos elementos orgânicos essenciais, existem mais facilidades de infraestrutura e redundâncias; assim, um grande esforço pode ser requerido para atingir o efeito desejado sobre o inimigo.

O quarto anel refere-se à população. Sem levar em consideração os aspectos morais, Warden (1995) afirma que existem dificuldades em atacá-la, em virtude da variedade e quantidade de alvos. Além disso, há sua vontade em resistir aos ataques. Contudo, Warden considera a possibilidade de um ataque indireto à população, como no caso da guerra do Vietnã, em que os guerrilheiros norte-vietnamitas elevaram o número de baixas norte-americanas além do esperado, impactando na opinião pública estadunidense para a saída dos Estados Unidos da América do conflito, alterando assim, a sua política de Estado.

Nesse sentido, Warden (1995) entende que os resultados deste tipo de ataque são difíceis de serem calculados devido à imprevisibilidade da natureza humana, entretanto os

ataques indiretos podem fazer parte de um esforço geral para causar alterações no sistema inimigo, porém os resultados, como já dito, podem ser imprevisíveis.

O último anel engloba as forças militares de um Estado. Warden (1995) afirma que há uma tendência em pensar que as forças militares são vitais em um conflito; na verdade, elas são os meios para se pôr fim a ele. Assim, sua função é proteger seus próprios anéis internos ou ameaçar os do inimigo. Ainda em relação às forças militares, o autor entende que um Estado pode ser levado a fazer concessões ao reduzir o seu componente militar e, caso toda ela seja destruída, a rendição será a única solução, pois a liderança do país atacado sabe que seus anéis internos se tornaram indefesos e passíveis de destruição.

Nos dias atuais, a tecnologia moderna permite novas possibilidades e opções de políticas mais eficientes, situando as forças em campo como um fim, e não um meio, em contraste com a visão clássica em que as forças militares eram o meio para se chegar ao fim da guerra (WARDEN, 1995).

“Os Centros de Gravidade são estratégicos porque são a principal parte do sistema inimigo. Um comandante deve sempre tentar atacar os centros de gravidade mais próximos possíveis do círculo central, ou seja, da liderança do sistema inimigo” (WARDEN,1995, p.48).

Nesse sentido, o autor explica que, por vezes, uma força militar não é capaz de atingir a liderança do inimigo, devido a sua inferioridade em termos militares ou restrições advindas da política. Nesses casos, as forças militares do inimigo devem ser analisas da mesma forma como se fosse um Estado pois, segundo o autor, a sua teoria não fica restrita ao nível estratégico, podendo ser aplicada ao nível operacional também. Assim, neste nível, o objetivo é induzir os líderes a fazerem concessões em um conflito, como desistir de uma ação ofensiva, recuar ou mesmo procurar uma retratação. A seguir, veremos a distribuição dos centros de gravidade deste nível.

O primeiro anel trata da liderança ou do próprio comandante, pois ele é o responsável por tomar decisões que afetam diretamente ou indiretamente o seu adversário.

Além dele, encontra-se inserido o sistema de Comando e Controle (C2), que é vital para a disseminação e coleta de informações. Sem o correto funcionamento deste, um comandante perde a sua capacidade de gerenciar uma situação de crise. O segundo anel engloba os elementos orgânicos essenciais que - no nível operacional - são representados pelos materiais logísticos, por conterem os elementos essenciais para uma guerra como munição, combustível e comida.

A infraestrutura é o elemento essencial do terceiro anel, pois tem a função de possibilitar o transporte dos elementos orgânicos essenciais para as forças militares. É composta por estradas, vias aéreas, vias marítimas, ferrovias, linhas de comunicação, gasodutos e todo aparato necessário para o esforço de guerra. Nenhum dos três anéis internos funcionará sem pessoal especializado; dessa forma, esses profissionais constituem o quarto anel operacional; o quinto anel é representado pelas forças militares. É o anel mais difícil de combater pelas suas características: uma campanha que se concentra nesse anel tem a tendência de ser longa e sangrenta para ambos os lados. Entretanto, às vezes, é apropriado concentrar esforços contra esse anel ou reduzir a sua capacidade até certo ponto com o objetivo de atingir o anel representado pelas lideranças no nível operacional ou estratégico (WARDEN, 1995).

2.3 Ataques paralelos

Ao finalizar a sua teoria, Warden reforça que o requisito mais importante do ataque estratégico é a compreensão do sistema inimigo. Com esse requisito atendido, o próximo passa a ser o problema de como reduzir as forças inimigas a um nível desejado ou, até mesmo, paralisá-las, caso necessário. Os ataques paralelos serão normalmente a abordagem, a menos que haja alguma razão convincente para prolongar a guerra.

Os Estados, normalmente, possuem um pequeno número de alvos vitais que estão no nível estratégico. Tais alvos são de tamanho reduzido, não possuem redundância e são difíceis de serem reparados; assim, caso sejam atingidos em paralelo, os danos se tornam

irreversíveis. Diferente do ataque paralelo, os ataques sucessivos focam as suas ações em uns dois alvos diferentes em um período relativamente curto, normalmente um ou dois dias. Neste caso, o inimigo pode minimizar os efeitos através da dispersão das suas forças pelos alvos que, provavelmente, serão atacados em sequência, concentrando recursos para reparar e realizar contra-ataques. O ataque paralelo priva o inimigo de reagir efetivamente, uma vez que diversos alvos são atingidos de forma simultânea, dificultando a sua reação (WARDEN, 1995).

A tecnologia tornou possível o ataque paralelo nos níveis estratégico e operacional, afetando diretamente a vulnerabilidade do inimigo nesses níveis. Esse processo de ataques simultâneos, em oposição à antiga forma de atacar os alvos em série, aproxima-se da ideia de Clausewitz que a chamou de forma ideal da guerra, o golpe dos golpes em todos os lugares ao mesmo tempo (WARDEN, 1995).

A seguir serão apresentados alguns conceitos atinentes à guerra cibernética, necessários para a compreensão de como essas ferramentas podem ser utilizadas no espaço cibernético para causar prejuízos a uma terceira parte, ou até mesmo causar a sua paralisia estratégica.

2.4 Difusão de poder e revolução da informação

Dois tipos de deslocamento de poder estão presentes atualmente: a transição de poder de um Estado mais poderoso para outro e a difusão de poder. O primeiro é visto como um processo cíclico ao longo da história e o segundo é um processo mais recente, subjacente da Revolução da Informação[5] (NYE, 2012). Segundo o autor, o problema para todos os Estados na era da informação é que muitos eventos estão ocorrendo fora do controle dos Estados,

[5] Revolução da Informação, às vezes chamada a "Terceira Revolução Industrial", baseia-se nos rápidos avanços tecnológicos em computadores, comunicações e softwares que, por sua vez, tem conduzido a reduções enormes no custo de criar, processar, transmitir e buscar informações (NYE, 2012).

incluindo os mais poderosos.

Alguns estudiosos interpretam essa tendência como o marco do declínio do Estado soberano, que tem sido a instituição global dominante desde a Paz de Vestfália, em 1648. Analisando as suas interpretações sobre o assunto, observamos que existe um senso comum no qual eles preveem que a Revolução da Informação vai achatar as hierarquias burocráticas e substituí-las por organizações em rede. Tal assertiva é materializada nas palavras de Nye: “Os Estados vão se tornar menos importantes para a vida das pessoas. Estas vão viver por múltiplos contratados voluntários e entrar e sair das comunidades ao click de um mouse” (NYE, 2012, p.152).

A característica fundamental da Revolução da Informação é o barateamento no custo da transmissão da informação, assim a quantidade de informação que pode ser processada e transmitida para o mundo tornou-se virtualmente infinita, resultando em uma explosão de informações. “O poder sobre as informações está muito mais amplamente distribuído hoje do que apenas algumas décadas atrás” (NYE, 2012, p.154). Assim, conforme o seu pensamento, as informações têm a capacidade de proporcionar um poder fundamental; além disso, mais pessoas têm acesso a mais informações do que jamais visto na história.

Neste sentido, com a queda do custo da computação e da comunicação, os entraves para se ter acesso a essas tecnologias declinaram vertiginosamente. Assim, indivíduos, ONGs, organizações privadas e até mesmo terroristas estão capacitados para desempenhar papéis diretos na política mundial.

2.5 Poder cibernético

O poder baseado em recursos de informações não é uma novidade, pois assim já pensava o filósofo francês Francis Bacon (1561-1626), considerado o pai da ciência moderna:

“O conhecimento em si mesmo é um poder”. Contudo, o poder cibernético é um conceito novo. Existem diversas definições de espaço cibernético, mas, em geral, o termo “cibernético” está associado a atividades eletrônicas associadas a computador (NYE, 2012).

Antes de conceituar o poder cibernético, é importante entender em que ambiente este atua: o espaço cibernético. Richard Clarke apresenta a seguinte definição:

> Ciberespaço. Lembra outra dimensão, talvez como no filme *Matrix*, com a iluminação verde e coluna de números e símbolos piscando no ar. Na verdade, o ciberespaço é muito mais prosaico. É o laptop que você ou seu filho leva para a escola, o computador do seu trabalho. É um monótono edifício sem janelas no centro da cidade. Está em toda parte, em todos os lugares onde existir um computador, um processador ou um cabo se conectando a um (CLARKE, 2012, p. 60).

Nesse sentido, o ciberespaço é, antes de tudo, um ambiente informativo, composto por dados digitalizados que são criados, armazenados e, o mais importante, compartilhados. Isto significa que não é apenas virtual, ele compreende os computadores que armazenam os dados, softwares, sistemas e toda a infraestrutura que permite o funcionamento harmônico entre estes elementos. Inclui também a internet, intranet, tecnologias celulares, cabos de fibra ótica e as comunicações baseadas no espaço (SINGER; FRIEDMAN, 2013).

Agora que consolidamos o conceito de ciberespaço, podemos compreender melhor a definição de poder cibernético na ótica de Joseph Nye: “O poder cibernético pode ser definido como um conjunto de recursos que se relacionam à criação, ao controle e à comunicação de informações eletrônicas baseadas em computador” (NYE, 2012. P. 161).

No capítulo 3 veremos com mais detalhes como os *hackers* russos utilizaram o poder cibernético para realizar ataques cibernéticos contra as infraestruturas georgianas.

2.5.1 Guerra cibernética

Na última década, surgiram diversas definições sobre guerra cibernética após o surgimento da internet como uma nova arma no espaço cibernético. A partir do momento em que a internet surgiu como uma nova arma no campo de batalha, surgiram também muitas teorias e definições sobre o tema. Assim, teorizar a guerra cibernética é complicado, devido à diversidade de definições no meio acadêmico.

No entendimento de Clausewitz, a guerra era uma extensão da política por outros meios. Nesta linha de raciocínio, Shakarian (2013) apresenta, inicialmente, um corolário da ideia de Clausewitz para definir guerra cibernética, descrevendo-a como "uma extensão da política por ações tomadas no espaço cibernético". Contudo, o autor entende que essa definição não é completa, por não abranger todas as situações envolvidas em uma guerra cibernética: por exemplo, as ações de atores não estatais sem motivações políticas.

Assim, o autor amplia seu entendimento anterior e passa a defender a ideia que a guerra cibernética é uma extensão da política através de ações tomadas no espaço cibernético por atores estatais ou não estatais que constituem ou não uma séria ameaça à segurança de uma nação ou são conduzidas em resposta a uma ameaça percebida contra a segurança de uma nação. Desse modo, o autor engloba aquelas situações em que não há necessariamente um objetivo político envolvido em um conflito cibernético.

2.5.2 Ataque cibernético

A informação se tornou um importante aspecto da vida moderna. Bancos, empresas e diversas outras instituições necessitam de um constante fluxo de informações para operarem e se manterem dentro de um padrão de qualidade esperado pela sociedade. Em uma situação de

conflito, a informação é fundamental para os comandantes manterem a consciência situacional do cenário da guerra, assim como é fundamental para a mídia transmitir seu ponto de vista para o resto do mundo. Um exemplo disso foi a atuação da mídia na guerra do Vietnã que alterou a opinião pública dos americanos sobre a manutenção do esforço de guerra estadunidense devido ao grande número de baixas de soldados americanos.

Shakarian (2013) entende que um ataque cibernético é utilizado para reduzir os efeitos da informação através da destruição ou redução do desempenho dos recursos de Tecnologia da Informação de uma entidade, por exemplo, colocando uma rede de computadores offline ou, de alguma forma, impedindo que outras pessoas tenham acesso a determinados recursos de TI. Um bom exemplo foi quando hackers[6] russos negaram à mídia georgiana divulgarem informações sobre a invasão das forças armadas russas no Cáucaso em 2008. Esse episódio abordaremos no capítulo 3 com mais detalhes.

Assim, os danos provocados em uma estrutura de comando e controle, por exemplo, podem favorecer vantagens ao atacante, a depender da magnitude e importância da infraestrutura afetada. Além disso, caso sejam realizados ataques paralelos, conforme descrito na teoria de John Warden, os efeitos podem ser potencializados e causar grandes perdas para o oponente.

2.5.3 Operações de Informações

Para finalizar os conceitos atrelados à guerra cibernética, é de suma importância entendermos o conceito de Op Info. Dentro do espaço cibernético, a manipulação das informações com objetivos políticos e militares vem tomando importância no cenário mundial

[6] Hacker – O termo tem sido utilizado para representar alguém com habilidades de ganhar acesso a um computador ou rede sem autorização (CLARKE, 2015).

nas últimas décadas. O objeto de estudo, descrito no capítulo 3, contempla ações efetuadas por hackers e simpatizantes russos em prol de objetivos militares e políticos. Tais ações, focaram basicamente nos meios da mídia causando grandes transtornos para a Geórgia.

As Op Info[7]são materializadas pelo emprego integrado das CRI, em apoio a outras operações ou mesmo sendo parte integrante do esforço principal, para informar e influenciar pessoas ou grupos hostis, neutros ou favoráveis, capazes de impactar positiva ou negativamente o alcance dos objetivos políticos e militares, bem como para comprometer o processo decisório dos oponentes ou potenciais oponentes, enquanto garantindo a integridade do nosso processo. Dentre as CRI, destacam-se como principais: Operações Psicológicas, Ações de Guerra Eletrônica, Guerra Cibernética, Comunicação Social e Assuntos Civis (BRASIL, 2020).

No próximo capítulo, abordaremos o objeto escolhido para a nossa pesquisa, conflito entre Rússia e Geórgia de 2008, com ênfase nos ataques cibernéticos.

[7] É o somatório de ações destinada a obter superioridade de informações, degradando as redes de comunicações de um adversário e as informações que servem de base aos processos decisórios do mesmo, bem como retirando-lhe a liberdade de ação, ao mesmo tempo em que garante as informações, os processos e a liberdade de ação amigos (BRASIL, 2020).

3 GUERRA CIBERNÉTICA ENTRE RÚSSIA E GEÓRGIA (2008)

O início das contendas entre as duas nações remonta há mais de um século. De um lado, a República da Geórgia, defendendo a sua independência e, do outro lado, a ex-União Soviética, buscando anexar a Geórgia aos seus domínios. Neste ínterim, ocorreram diversos eventos que, se fossem descritos, não acrescentariam substâncias argumentativas à pesquisa. Sendo assim, para não fugir ao propósito do trabalho, que é focado na guerra cibernética, este capítulo abordará - de forma sucinta - os antecedentes históricos e as ações da guerra cibernética serão descritas com detalhes.

3.1 Antecedentes

A Geórgia situa-se ao sul da Rússia, junto ao Mar Negro, e as duas nações mantiveram relações conturbadas por um longo período histórico. A Geórgia é geograficamente um estado pequeno e com uma população igualmente pequena. O Kremlin a considerava como parte dos seus domínios geográficos devido a sua proximidade. O desmoronamento do império original Russo, em 1918, foi a oportunidade para a Geórgia sair da esfera de influência russa e declarar a sua independência. Após o término das brigas políticas internas, os russos a invadiram e implementaram um regime títere; assim, ela passou a fazer parte da União das Repúblicas Socialistas Soviéticas (CLARKE, 2015).

Com a dissolução da União Soviética, em 1991, a Geórgia aproveitou a instabilidade política e declarou a sua independência novamente. Contudo, em 1993, os territórios da Ossétia do Sul e da Abecásia, com apoio de Moscou e suas populações locais russas, expulsaram a maioria dos georgianos, estabelecendo “governos independentes”. Embora as regiões fossem reconhecidas pela comunidade internacional como pertencentes à

Geórgia, as regiões dependiam de recursos financeiros e do apoio dos russos. Em julho de 2008, rebeldes da Ossétia do Sul realizaram diversos ataques com mísseis contra aldeias georgianas, incitando um conflito com a Geórgia. O exército georgiano respondeu aos ataques bombardeando a capital da Ossétia do Sul e posteriormente realizou a sua invasão em 07 de agosto. No dia seguinte, o exército russo expulsou o exército georgiano sem grandes dificuldades. Nesse dia se iniciaram os ataques cibernéticos russos contra a Geórgia (CLARKE, 2015).

3.2 Os ataques cibernéticos contra a Geórgia

Os ataques cibernéticos contra a Geórgia se concentraram em duas fases: A primeira fase teve início na noite de 7 de agosto, ocasião em que *hackers* russos realizaram ataques aos sites do governo e de agências de notícias georgianas (SHAKARIAN, 2013). O Coronel Anatoly Tsyganok, entende que essas ações iniciais foram uma resposta aos *hackers* georgianos que invadiram os sites da mídia da Ossétia do Sul na semana em que se iniciou os conflitos (TSYGANOK, 2010).

É importante observar que os supostos "contra-ataques" ocorreram um dia antes do início da guerra terrestre. Isso levou muitos estudiosos a sugerir que os hackers, pelo menos, sabiam o dia da invasão com alguma antecedência.

Na primeira fase, os hackers russos utilizaram-se de ataques do tipo *Distributed Deniel of Service* (DDoS)[8] realizados em sua grande maioria por *botnets*[9]. Os computadores

[8] Técnica básica de guerra cibernética frequentemente utilizada por criminosos e outros personagens não estatais em que um site da Internet, um servidor ou um roteador é inundado com mais solicitações de pacotes que o site pode responder ou processar. O resultado disso é que o tráfego legítimo não consegue acessar o site e esse fica em um estado desligado (CLARKE, 2015).

[9] Uma rede de computadores forçada a operar sob comandos de um usuário remoto não autorizado, geralmente sem o conhecimento de seu dono ou operador. Essa rede de computadores "robôs" é então utilizada para realizar ataques a outros sistemas. Uma *botnet* geralmente tem um ou mais computadores de controle, que estão diretamente associados ao operador por detrás da *botnet*, para o envio de ordens a dispositivos controlados secretamente (CLARKE, 2015).

"robôs" (*botnets*) usados na investida contra sites georgianos, segundo especialistas, foram associados a organizações criminosas russas, como a *Russian Business Network* (RBN). Os ataques foram dirigidos para sites do governo e da mídia georgiana. Inicialmente, eles pareciam triviais, até mesmo juvenis. (CLARKE, 2015).

Segundo Shakarian (2015), devido a sua segurança ser considerada fraca, as redes georgianas eram mais vulneráveis aos ataques do que o sistema de redes da Estônia, atacadas pelos russos um ano antes. Ainda segundo o autor, os ataques também tiveram como objetivo atingir a liderança georgiana. O site oficial do governo foi desfigurado com a inserção de fotos de Adolf Hitler na tentativa de associar a imagem do presidente georgiano Mikheil Saakashvili à imagem do ditador alemão (Fig.3). Ademais, *hackers* utilizaram os dados de e-mail públicos da classe política georgiana com intuito de causar a paralisação do funcionamento dos mesmos, tal ação é conhecida como "campanha de spam"[10] (DANCHEV, 2008).

Fig.3 – Site do governo da Geórgia com a foto de Hitler
Fonte: www.zednet.com

Além disso, com o objetivo de conduzir ataques para desfigurar e parar o funcionamento de outros sites da web, os *hackers* russos empregaram outra modalidade de ataque cibernético conhecida como injeção SQL[11] (*Structured Query Language*), em português conhecido como linguagem estruturada em dados. Uma rede vulnerável a esse tipo de ataque

[10] Spam é o termo usado para se referir às mensagens eletrônicas que são enviadas para você sem o seu consentimento e que, geralmente, são despachadas para muitas pessoas (CLARKE,2015).
[11] É um tipo de ataque cibernético que explora vulnerabilidades que são comumente encontradas em aplicações da WEB (SHAKARIAN, 2015).

fornece ao *hacker* acesso total ao sistema e ao seus dados armazenados, permitindo assim, que os dados sejam utilizados para fins diversos (SHAKARIAN, 2015).

Nesta fase, grande parte das ações no campo cibernético se deslocou para o recrutamento de usuários "patrióticos" de computadores russos, conhecidos como "hacktivistas". De acordo com divulgações, em alguns websites russos, muitos "hacktivistas" foram considerados membros da juventude russa (SHAKARIAN, 2015).

Neste sentido, segundo informações contidas no relatório do *Project Grey Goose Phase II*[12], o recrutamento foi realizado por meio de diversos websites; o mais atuante foi o "StopGeorgia.ru", criado ao início do conflito (GREYLOGIC, 2009).

De acordo com relatório, o site "StopGeorgia.ru" fornecia os procedimentos e orientações de como realizar um ataque DDoS a través de máquinas privadas. O site disponibilizava um botão chamado "FLOOD" que, ao ser clicado, disparava pacotes de dados com o fim de paralisar servidores georgianos. Além disso, possuía uma lista de servidores de alvos georgianos, incluindo a informação se estavam acessíveis ou não, e outras vulnerabilidades.

Pelas evidências apresentadas, nota-se o nível de profissionalismo dos *hackers* russos em instruir, de forma precisa, os "hacktivistas" para os ataques e em proteger os seus domínios de internet, sem sofrer qualquer tipo de interrupção.

Segundo Shakarian (2015), um bom exemplo foi a resposta dos administradores do site hacker russo "XAKEP.ru", que prontamente bloquearam as varreduras realizadas pelo projeto estadunidense chamado "*Projeto Grey Goose*", impedindo temporariamente o acesso de todos os endereços IP (Protocolo Internet) oriundos dos Estados Unidos da América.

[12] Uma iniciativa de Inteligência de Código Aberto (*Open Source Intelligence* - OSINT) criada pela empresa *GreyLogic* com a missão de examinar como a guerra cibernética russa foi conduzida contra sites georgianos e verificar se houve participação do governo russo ou se foi uma ação isolada de hackers patrióticos russos (Greylogic, 2009).

Dado o exposto, apesar de a Internet ser uma ferramenta poderosa, responsável pela globalização e seus efeitos magníficos, ela possui um lado obscuro que é a porta de entrada para pessoas mal intencionadas agirem de acordo com seus interesses próprios ou de terceiros. Incluem-se aí, também, os Estados-Nações que, nas últimas décadas, vêm explorando as fragilidades de segurança digital de outros Estados-Nações e outros atores não estatais, seja para obterem dados estratégicos ou para causarem algum tipo de dano ou destruição em suas infraestruturas críticas[13].

Assim, no mundo hodierno, pessoas e agentes, sejam eles estatais ou não, estão sujeitos a ataques cibernéticos que podem causar prejuízos de todas as ordens. Neste contexto, a defesa no ciberespaço é mandatória e deve ser levada tão a sério quanto os outros meios convencionais de defesa.

3.3 O silêncio imposto à Geórgia

Os ataques cibernéticos à Geórgia foram possíveis devido à fragilidade dos mecanismos de defesa no ciberespaço georgiano. Segundo Clarke (2015), a Geórgia se conectava à Internet por meio de roteadores localizados na Rússia e na Turquia que tiveram seu funcionamento interrompido com os ataques hackers do tipo DDoS; assim, as transmissões por esses roteadores foram completamente interrompidas. Ainda segundo o autor, os demais roteadores da Geórgia passaram a ser controlados pelos *hackers*.

Segundo Shakarian (2015), os georgianos não conseguiam se conectar a qualquer fonte de notícia ou informação externa e trafegar e-mails para fora do país. As consequências foram bem retratadas por Clarke: “A Geórgia efetivamente perdeu o controle sobre o domínio

[13] Trata-se de um mundo praticamente invisível ao cidadão, mas que sustenta a produção da indústria, a distribuição da energia, o funcionamento de sistemas de transportes e de comunicações e que responde, cada vez mais, a comandos emitidos por computadores (CLARKE, 2015).

"ge"[14] da nação e foi forçada a mudar diversos sites do seu governo para servidores fora do país".(CLARKE, 2015, p. 21)

Corbin (2009) entende que a finalidade principal dos ataques cibernéticos era segregar a Geórgia da coletividade internacional através do seu isolamento nos meios de comunicações, impedindo-a de contar ao mundo o que estava acontecendo. Ainda segundo o autor, o objetivo de isolar a Geórgia do mundo exterior também explica os ataques aos bancos georgianos em uma segunda onda de ataques cibernéticos. Na época, o sistema financeiro foi seriamente afetado pelos ataques cibernéticos.

3.4 Ataques ao sistema financeiro

Nesse contexto, deu-se o início da segunda fase das ações no espaço cibernético que procurou acarretar danos a uma lista expandida de alvos, incluindo instituições bancárias e a mídia ocidental, como a BBC e a CNN (CORBIN, 2009).

Para mitigar o ataque ao sistema financeiro, a Geórgia desligou seus servidores, supondo que a perda temporária do sistema bancário seria menos danosa que o risco de ver seus dados confidenciais nas mãos dos hackers. Inicialmente o plano funcionou; contudo, assim que os hackers perceberam que não tinham mais acesso ao sistema bancário georgiano, enviaram um alto fluxo de dados, através dos *botnets* para a comunidade bancária internacional, fingindo serem ataques cibernéticos provenientes da Geórgia.

Esses ataques desencadearam uma resposta automática da maioria dos bancos estrangeiros, que encerraram suas conexões com o setor bancário georgiano. Sem acesso ao sistema de compensação europeu, as operações bancárias da Geórgia ficaram paralisadas. O sistema de cartões de crédito ficou inoperante, bem como o sistema de telefonia móvel

[14] Um domínio é um conjunto de caracteres que é inserido em um navegador de internet para encontrar um determinado site. (SHAKARIAN, 2015).

(CLARKE, 2015).

Neste sentido, segundo Shakarian (2015), os bancos internacionais, na tentativa de mitigar os danos, pararam as operações bancárias no estado no país durante as contendas com a Rússia. Consequentemente, o sistema financeiro do país ficou inoperante por alguns dias.

Tendo em vista os aspectos observados, percebe-se que os russos detinham um poder cibernético capaz de realizar operações complexas no campo informacional. Os ataques aos meios de comunicação, incluindo o sistema bancário da Geórgia, isolando-a do mundo social e financeiro, são provas de como esse poder pode gerar prejuízos ou até mesmo levar seu oponente à rendição. Joseph Nye, ao definir poder cibernético no capítulo 2, descreveu com perfeição a capacidade desse poder de criar, controlar e manipular as informações eletrônicas. Foi exatamente o que os russos e seus simpatizantes fizeram durante o conflito.

3.5 Finalidades dos ataques cibernéticos

Corbin (2009) entende que o propósito dos ataques cibernéticos eram "isolar e silenciar" os georgianos, degradando os meios de comunicação e isolando o país do sistema internacional. As reportagens especializadas sobre a guerra e as relações de objetivos específicos fornecidos nos sites de *hackers* patrióticos dão credibilidade à sua teoria. Ademais, os residentes georgianos foram submetidos a efeitos psicológicos e informacionais significantes devido à impossibilidade de se comunicarem com o resto do mundo.

Embora tenha o cuidado de afirmar que o governo russo não teve participação nos eventos ocorridos no espaço cibernético, Tsyganok (2008) entende que as ações cibernéticas contra a Geórgia fizeram parte de uma guerra de informação contra a mídia georgiana e ocidental.

Segundo Shakarian (2015), os objetivos de "isolar e silenciar" a Geórgia foram de

escopo limitado. Não foram realizados ataques cibernéticos que causassem danos permanentes às infraestruturas críticas e aos seus sistemas associados, como os sistemas de controle industrial (ICS) e de supervisão de controle e aquisição de dados (SCADA). Tais sistemas são projetados para coleta, controle e monitoramento, em tempo real, de dados coletados de infraestruturas críticas como usinas elétricas, oleodutos/gasodutos, refinarias e sistemas de água.

Além disso, as conexões físicas de Internet que ligavam a Geórgia a outros países, como a Turquia e a própria Rússia, permaneceram intactas (CLARKE, 2015).

Em vista dos argumentos apresentados, entende-se que os ataques cibernéticos tiveram objetivos específicos, principalmente no que tange à interrupção dos sistemas de comunicações digitais. Os ataques não tiveram intenção de paralisar as infraestruturas críticas georgianas. Contudo, um ataque contra elas poderia levar um Estado à paralisia estratégica, pois, segundo Warden, trata-se de elementos orgânicos essenciais que são representados pelas facilidades ou processos cujas ausências impedem a sobrevivência de uma organização ou de um Estado.

Cabe ressaltar que atualmente diversas infraestruturas críticas são dependentes de tecnologia de ponta, controlada por softwares como o ICS e o SCADA*;* assim, a proteção no ciberespaço passa a ter uma importância talvez maior que os meios de proteção convencionais para infraestruturas críticas dependentes de softwares e acesso à Internet.

3.6 Coordenação com as forças convencionais

A coordenação dos ataques cibernéticos com as forças convencionais é polêmica. Alguns especialistas são fervorosos em afirmar que houve coordenação, todavia outros não concordam com essa linha de raciocínio. Faz-se necessário analisar as evidências para se chegar a um melhor entendimento sobre a questão.

Segundo Shakarian (2015), a coordenação dos ataques cibernéticos com as forças convencionais foi limitada. Alguns especialistas afirmam que os hackers russos sabiam quando as operações terrestres iriam começar, porém, após o início dos ataques cibernéticos, existem poucas evidências de coordenação. As duas principais razões são: o governo russo, desde o início do conflito, sempre fez questão de dissociar a sua imagem dos ataques cibernéticos e o alto escalão militar russo não havia chegado a um consenso sobre a utilização conjunta de operações cibernéticas e as forças convencionais (BIKKVOL, 2009 *apud* SHAKARIAN, 2015)[15].

Por outro lado, especialistas em segurança fizeram apontamentos que indicam coordenação entre os ataques cibernéticos e as ações terrestres. Segundo Shakarian (2015), os meios da mídia e os de comunicação não foram alvo dos ataques cinéticos, tal fato pode ser devido aos bem sucedidos ataques cibernéticos no início dos conflitos. Além disso, hackers russos atacaram um site especializado em locação de geradores elétricos a diesel, um alvo fora dos padrões para este tipo de ação. Esse ataque pode ter sido conduzido em apoio aos ataques convencionais contra a infraestrutura elétrica georgiana (BUMGARNER; BORG, 2009 apud SHAKARIAN, 2015).

Segundo Clarke (2015), um grupo de especialistas ocidentais em guerra cibernética concluiu que os sites usados para realizar os ataques cibernéticos tinham conexão com o aparato de inteligência russa.

Em virtude do que foi mencionado, percebe-se que existem poucas evidências concretas para afirmar se houve ou não coordenação com as forças terrestres convencionais. Apesar de o governo russo negar veemente a sua participação nos ataques cibernéticos, alguns fatos merecem destaque. O primeiro deles é que os ataques cibernéticos se iniciaram praticamente no mesmo dia das ações terrestres. O segundo fato é que os meios de

[15] BikkvolTor. Russia'smilitary performance in Georgia. Military Rev 2009.

comunicações e da mídia não foram alvos dos ataques terrestres e o terceiro foi o ataque cibernético a um site de aluguel de geradores de energia. Dessa forma, entendemos que fica patente alguma participação do governo russo, mesmo que de forma indireta nos ataques cibernéticos, concordando assim com a teoria de alguns especialistas ocidentais que afirmam que os sites usados para realizar os ataques cibernéticos tinham conexão com o aparato de inteligência russa.

No próximo capítulo, será realizada a comparação entre o modelo dos cinco anéis de John Warden e os ataques cibernéticos ocorridos no conflito entre Rússia e Geórgia de 2008. O objetivo é verificar se houve aderências à teoria de Warden.

4 CONFRONTO ENTRE O MODELO TEÓRICO DE WARDEN E OS ATAQUES CIBERNÉTICOS CONTRA A GEÓRGIA

Neste capítulo, será realizado o confronto entre a teoria e a realidade, a fim de verificarmos se houve ou não aderência dos ataques cibernéticos ao modelo teórico utilizado na pesquisa. Para facilitar o confronto, este capítulo será divido em seções correspondentes aos anéis de Warden, que são: liderança, elementos orgânicos essenciais, população, infraestrutura e Forças Militares. Para cada anel, será feita uma pequena síntese do que foi escrito no capítulo 2, de forma a facilitar o entendimento das comparações.

Por fim, será analisado também se os ataques cibernéticos e convencionais ocorridos no conflito tiveram aderência ao conceito de ataque paralelo de Warden.

4.1 Liderança

Conforme descrito na teoria de Warden, a liderança é crítica, está localizada no centro do modelo dos cinco anéis; sendo assim, é o principal elemento do sistema. Os líderes mais importantes localizam-se neste anel. São estes os responsáveis pelas decisões de um Estado-Nação que vão alterar o curso de um conflito a seu favor, sacramentar a sua derrota ou negociar a sua rendição. Neste ínterim, as comunicações são vitais para manutenção do funcionamento do sistema; uma vez perdidas, o funcionamento do sistema fica comprometido.

Os ataques cibernéticos contra a Geórgia tiveram como principais objetivos abalar a liderança política e infligir danos aos sistemas de comunicações digitais. A intenção inicial dos hackers foi bem clara: desmoralizar o presidente Mikheil Saakashvili perante a sua nação, desfigurando a sua imagem em vários sítios oficiais do governo na Internet. Além disso, os e-mails oficiais dos parlamentares georgianos foram inundados com mensagens do tipo spam com dizeres pró-Rússia e contendo *malwares* e críticas ao governo atual com o objetivo de

atingi-los psicologicamente.

No que diz respeito às comunicações, os estragos foram notáveis. Os servidores que conectavam a Geórgia ao mundo foram bloqueados, impedindo-a de transmitir para o mundo o que estava ocorrendo durante os cinco dias do conflito. Além disso, o sistema de telefonia móvel ficou inoperante. O objetivo dos hackers foi bem claro: destruir a capacidade de comunicação digital da Geórgia.

Apesar de a guerra cibernética ter causado graves danos aos principais meios de comunicações e ter atacado a liderança do país, os ataques cibernéticos, isolados, não levaram a Geórgia a sua paralisia estratégica que, segundo Warden, representaria a sua rendição ou derrota. Assim, a aderência à teoria foi parcial.

4.2 Elementos orgânicos essenciais

Segundo Warden, tais elementos se referem às facilidades ou processos cujas ausências impedem a sobrevivência de uma organização ou de um Estado. No nível estatal, por exemplo, a complexidade das cidades modernas torna certos insumos fundamentais, como a eletricidade e o petróleo. Os principais meios de comunicação de um Estado, como servidores do governo e o sistema bancário, também fazem parte desta lista. A ausência destes elementos afeta diretamente a vida da população, devido aos impactos econômicos, sociais, políticos e psicológicos.

Assim, danos causados nas indústrias essenciais podem gerar pressões sobre a liderança, obrigando-a a fazer concessões em um conflito. Ainda segundo Warden, os motivos para as concessões são os seguintes: os danos aos elementos orgânicos essenciais levam ao colapso do sistema, tornam fisicamente difícil ou impossível manter uma determinada política ou esforço de guerra e têm repercussões políticas ou econômicas internas que são muito caros para suportar.

Para examinar se houve aderência dos ataques cibernéticos aos elementos orgânicos essenciais, é imperioso entender se os alvos atacados eram essenciais para a sobrevivência da Geórgia. Conforme descrito no capítulo 3, os ataques cibernéticos focaram os meios de comunicações digitais com a finalidade de "isolar e silenciar" o país da comunidade global, colocando líderes daquele país e a sua população sob pressão psicológica. Além disso, o sistema bancário, responsável pelas transações internacionais e nacionais, devido aos ataques cibernéticos, ficou 10 dias paralisado, causando enormes prejuízos econômicos ao país; consequentemente, afetando o psicológico da população.

No que se refere às infraestruturas críticas, não foi observado nenhum ataque cibernético. Os Sistemas de Controles Industriais (ICS) e de Supervisão de Controle e Aquisição de Dados (SCADA), sistemas projetados para gerenciar equipamentos industriais, não foram afetados e nem houve registro de tentativa de invasão. Tais sistemas controlam usinas elétricas, oleodutos/gasodutos, refinarias e sistemas de água, por exemplo. Além disso, a conexão física da Geórgia à Internet permaneceu intacta durante todo o conflito, inclusive a estrutura física localizada na Rússia.

Analisando os dados apresentados, fica evidente que os ataques cibernéticos tiveram um escopo limitado. Os danos restringiram-se a servidores selecionados pelos hackers, contudo as infraestruturas críticas não foram afetadas pelos ataques. O silêncio imposto à Geórgia gerou impactos psicológicos na população e na liderança, porém na pesquisa não foram encontradas evidências que indicassem que a Geórgia realizou algum tipo de concessão aos russos, devido aos ataques cibernéticos. Assim, os ataques aos elementos orgânicos essenciais tiveram aderência parcial à teoria de Warden.

4.3 Infraestrutura

Segundo Warden, a infraestrutura inimiga consiste no sistema de transporte, responsável por movimentar bens e serviços, tanto civis quanto militares, em toda a área de

atuação do Estado. Inclui linhas ferroviárias, linhas aéreas, rodovias, pontes, aeródromos, portos e uma série de outros sistemas similares. Em comparação aos elementos orgânicos essenciais, existem mais facilidades de infraestrutura e redundâncias; assim, um grande esforço pode ser requerido para atingir o efeito desejado sobre o inimigo.

Na pesquisa não foram encontradas evidências de ataques cibernéticos contra infraestruturas. Os ataques ocorreram sim, mas na campanha terrestre; todavia, fogem ao escopo desta pesquisa que é direcionada para a guerra cibernética. Sendo assim, os ataques cibernéticos não foram aderentes ao anel da infraestrutura.

4.4 População

Segundo Warden, atacar a população constitui-se uma tarefa muito difícil, devido à variedade e à quantidade de alvos; além disso, a sua vontade em resistir aos ataques é um elemento intangível, pois depende de diversos fatores como cultura, religiosidade, crenças e outros valores intrínsecos aos seres humanos. Sendo assim, os efeitos esperados dos ataques à população são difíceis de serem estimados. Todavia, Warden considera a possibilidade de um ataque indireto à população, causando impactos psicológicos que contribuam para a mudança da política de um Estado em um conflito.

Conforme descrito no capítulo 3, os ataques cibernéticos foram orientados para atingir os meios de comunicação digital, ocasionando um impacto psicológico significativo em toda a Geórgia, pois reduziram a capacidade de comunicação com o mundo exterior não apenas para a mídia e o governo, mas também para o público em geral.

Além disso, os ataques cibernéticos fizeram com que a comunidade bancária internacional encerrasse as conexões com o setor bancário georgiano, impossibilitando o acesso ao sistema de compensação europeu, paralisando as transações bancárias. Assim, as transações com o sistema de cartões de crédito e o sistema de telefonia móvel ficaram inoperantes no país.

Esse episódio afetou diretamente a economia do país e, consequentemente, o psicológico da população.

Levando-se em conta o que foi observado, os ataques cibernéticos aos meios de comunicações e ao sistema econômico causaram impacto no psicológico da população, contudo na pesquisa não foram encontradas evidências que indicassem uma alteração de postura do governo no conflito devido somente aos efeitos psicológicos. Cabe ressaltar que o conflito durou apenas cinco dias; caso a duração fosse maior, os efeitos psicológicos provavelmente seriam mais impactantes na população, o que poderia levar uma pressão maior no anel liderança, levando assim, o governo a adotar medidas para alterar o curso do conflito como a sua rendição, por exemplo. Dado o exposto, o anel população teve aderência parcial à teoria.

4.5 Forças militares

Segundo Warden, a sua função é proteger seus próprios anéis internos ou ameaçar os do inimigo. Na pesquisa não foram encontradas evidências de ataques cibernéticos contra as forças convencionais russas. A intenção não era levar o país ao colapso total, e sim, parar ou prejudicar o funcionamento de setores específicos, como o setor financeiro e das comunicações. Os ataques tiveram um escopo limitado e restringiram-se ao setor civil.

Assim, não houve aderência à teoria de Warden no que se refere ao ataque as forças militares sob a ótica da guerra cibernética.

4.6 Ataques paralelos

Warden entende que os ataques paralelos têm como objetivo reduzir as forças inimigas a um nível desejado ou mesmo paralisá-las. O ataque paralelo priva o inimigo de reagir efetivamente, uma vez que diversos alvos são atingidos de forma simultânea, dificultando a sua

reação. Ainda segundo Warden, a tecnologia tornou possível o ataque paralelo nos níveis estratégicos e operacionais, afetando diretamente a vulnerabilidade do inimigo nestes níveis. Além disso, os Estados normalmente possuem um pequeno número de alvos vitais que estão no nível estratégico, são de tamanho reduzido, não possuem redundância e são difíceis de serem reparados; assim, caso sejam atingidos em paralelo, os danos se tornam irreversíveis.

A campanha cibernética russa sobre a Geórgia, em agosto de 2008, representa o primeiro ataque cibernético em larga escala que ocorreu simultaneamente com grandes operações militares convencionais. Para destruir instalações inimigas, já não são mais necessários apenas mísseis e bombas guiadas a lazer ou GPS, bastando somente, um computador e pessoal especializado e bem treinado.

Em que pese os impactos psicológicos e financeiros causados à Geórgia, os ataques paralelos não se mostraram tão efetivos para causar danos irreversíveis ao país. Porém, caso as infraestruturas críticas fossem atingidas ou a duração do conflito fosse maior, talvez as restrições às comunicações e ao sistema bancário fossem suficientes para levar a Geórgia a sua rendição. Assim, os ataques paralelos tiveram aderência parcial ao conceito de ataques paralelos de Warden.

No próximo capítulo, passa-se a tratar sobre as conclusões do trabalho, bem como sobre as reflexões acerca da utilização da guerra cibernética como ferramenta para neutralizar um adversário sem a utilização de forças convencionais. Serão apresentadas ainda, linhas futuras de pesquisa e implicações dos conhecimentos para a MB.

5 CONCLUSÃO

Este estudo teve como objetivo analisar os ataques cibernéticos contra a Geórgia em 2008. A comparação da realidade com a teoria foi a metodologia utilizada na pesquisa. Sendo assim, buscamos responder a seguinte questão: os ataques cibernéticos contra a Geórgia em 2008 tiveram aderência ao modelo teórico dos cinco anéis no que se refere à paralisia estratégica?

No capítulo dois, apresentamos a teoria de Warden, cujo propósito é pensar no sistema inimigo de forma macro e dividí-lo em anéis de forma a identificar os seus CG. Os ataques devem sempre buscar as lideranças dos seus respectivos anéis e, se possível, atacar os anéis mais próximos do anel central, de forma a aumentar as chances de causar a paralisia estratégica do inimigo. Além disso, Warden defende os ataques paralelos, pois privam o inimigo de reagir efetivamente, uma vez que diversos alvos são atingidos de forma simultânea, dificultando a sua reação. Salienta que a tecnologia tornou possível o ataque paralelo nos níveis estratégicos e operacionais, afetando diretamente a vulnerabilidade do inimigo nestes níveis.

No capítulo três, apresentamos um breve histórico e as motivações geopolíticas para os ataques. De forma mais detalhada, descrevemos os ataques cibernéticos contra a Geórgia em 2008, as técnicas utilizadas pelos hackers, os setores atingidos, os danos provocados na economia e nas comunicações e, por fim, uma breve análise sobre a questão se houve - ou não - coordenação entre as ações em terra e os ataques cibernéticos.

No capítulo quatro, realizamos o confronto da teoria com o objeto da pesquisa, de forma a verificarmos as aderências. Para tal, analisamos cada anel em separado, para facilitar a compreensão e posteriormente verificamos se os ataques cibernéticos foram aderentes à teoria de Warden.

Em que pese os ataques cibernéticos não terem causado a paralisia estratégica da Geórgia, as evidências mostraram que os resultados dos ataques tiveram consequências graves para o referido país, pois o mesmo ficou isolado da comunidade internacional e ficou com seu sistema eletrônico financeiro inoperante por 10 dias, causando um impacto psicológico significativo em toda a população. Contudo, mais uma vez ressaltamos que a duração do conflito foi muito curta e por isso, talvez os impactos psicológicos na população e nos governantes não tenham sido suficientes para levar a Geórgia a sua paralisia estratégica.

As evidências mostraram que, se um ataque cibernético for executado de forma bem planejada, as vantagens podem ser significativas em um conflito militar, principalmente se for executado contra infraestruturas críticas e seus sistemas controladores, como usinas elétricas, oleodutos/gasodutos, refinarias e sistemas de água. Essas Infraestruturas são elementos essenciais para um Estado manter a sua sobrevivência e, caso sejam perdidas, podem levá-lo a sua paralisia estratégica de forma abrupta.

Até a presente data, o governo russo nega a sua participação nos ataques cibernéticos, contudo as evidências do seu envolvimento, mesmo que de forma indireta, não deixam dúvidas da sua participação. Os ataques terrestres se iniciaram no mesmo dia dos ataques cibernéticos, deixando evidente que os hackers tinham informações privilegiadas. Na pesquisa não foram encontradas evidências sobre vantagens militares significativas dos ataques paralelos, devido os ataques cibernéticos terem sido de escopo limitado, ou seja, não tinham o objetivo de paralisar as infraestruturas críticas da Geórgia, e sim atingir servidores específicos.

Os impactos, no entanto, foram consideráveis. Não resta dúvida que se os ataques cibernéticos fossem realizados de forma paralela e dirigidos para alvos específicos de grande valor estratégico, as vantagens no campo de batalha seriam imensas. Assim, sugerimos, para pesquisas futuras, uma análise sobre a aplicabilidade de ataques cibernéticos em conjunto com as forças convencionais.

Pelas ideias apresentadas, concluímos que os ataques cibernéticos contra a Geórgia em 2008 tiveram a aderência parcial ao modelo teórico dos cinco anéis, no que se refere à paralisia estratégica.

Ao final dessa pesquisa, concluímos que os ataques cibernéticos sofridos pela Geórgia abarcam alguns aspectos importantes para a Marinha do Brasil. Como vimos, o espaço cibernético é um ambiente que apresenta vulnerabilidades e que, de alguma forma, pode oferecer ao adversário informações de grande importância, inclusive de valor estratégico para a segurança e defesa do país. Assim, torna-se importante que a Marinha do Brasil se mantenha capacitada para utilizar seu poder cibernético, ofensivo e defensivo, em prol dos seus interesses e objetivos nacionais, em consonância com a Política Nacional de Defesa e a Estratégia Nacional de Defesa.

REFERÊNCIAS

BRASIL. Estado-Maior da Armada. *Doutrina de Operações de Informação* (EMA-335). Brasília, 2018.

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 Von. On War. Tradução de Michael Howard. Princenton: Princenton university Press, 2008. 732 p. Título original: Vom Kriege.

CORBIN, Kenneth. Internet News.com: *Lessons From Russia- Georgia cyberwar,* março, 2009. Disponível em <http://www.internetnews.com/government/article.php/3810011/Lessons-From-the-Russia-Georgia-Cyberwar.htm> Acessado em: 03 junho.2020.

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.

FRANÇA, Lessa Júnia; VASCONCELLOS, Ana Cristina de. *Manual para Normalização de Publicações Técnico-Científicas*. 8. ed. Belo Horizonte: Editora UFMG, 2007. 255 p.

FULLER, John Frederick Charles. *A Conduta da Guerra.* Rio de Janeiro: Biblioteca do Exército, 1966.

GREYLOGIC. Project Grey Goose Phase II*: the evolving state of cyber warfare*; Março, 2009. Disponível em < http://www.fistfulofgold.com/Documents/ProjectGreyGoose.pdf> Acessado em: 02 junho. 2020.

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

OLSEN, John A. *John Warden and the Renaissance of American Air Power*. 1 ed. Washington, D.C. Potomac Books, Inc., 2007, 374 p.

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

SHAKARIAN, Paulo. Introduction to Ciber-Warfare. Manhattam: Elsevier, 2013. [11165] p. Ebook.

SINGER; FRIEDMAN, Cybersecurity and Cyberwar. New York. Oxford University Press, 2014. [6809] p. Ebook.

TSYGANOK, Anatoly. *Information Warfare a Geopolitical Reality*. Russia Beyond, 2008. Disponível em:<https://www.rbth.com/articles/2008/11/05/051108_strategic.html/>. Acessado em: 25 mai. 2020.

TZU, Sun. *A Arte da Guerra*. Tradução Cândida de Sampaio Bastos. Editora DPL. São Paulo,

2007, 190 p.

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.40-55,primavera1995. Disponível em: < https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf >. Acesso em: 10 mai. 2020.