ESCOLA DE GUERRA NAVAL

CC (FN) MARCUS ZARATH

A PRIMEIRA GUERRA CIBERNÉTICA:

os ataques cibernéticos russos contra a Geórgia (2008), analisando três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica

Rio de Janeiro
2019

CC (FN) MARCUS ZARATH

A PRIMEIRA GUERRA CIBERNÉTICA:

os ataques cibernéticos russos contra a Geórgia (2008), analisando três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica

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

Orientador: CF Alexander Thomaz Arruda

Rio de Janeiro

Escola de Guerra Naval

2019

AGRADECIMENTOS

A Deus por me dar saúde e muita força para superar todas as dificuldades e concluir esta pesquisa.

À minha esposa, Monique, e a minha filha, Sophia, pela compreensão durante todos os momentos de ausência, pelo amor incondicional e pelas alegrias do dia a dia, que me deram força durante todo o curso.

Aos meus pais, Gilberto e Sonia, por todo o amor que me deram, além da educação, ensinamentos e apoio.

Ao meu orientador, CF Thomaz, pela orientação precisa e oportuna, durante momentos de convivência amistosa e enriquecedora.

Aos meus companheiros de turma no curso de 2019, pelo clima agradável e participativo e pelo incentivo constante.

A Escola de Guerra Naval e todo seu Corpo Docente, que me proporcionaram as condições necessárias para que eu alcançasse meus objetivos.

Aos servidores, militares e civis, da Escola de Guerra Naval pelo excelente suporte administrativo às atividades do Curso de Estado-Maior para Oficiais Superiores.

Enfim, a todos que contribuíram para a realização deste trabalho, seja de forma direta ou indireta, fica registrado aqui, o meu muito obrigado.

RESUMO

O presente trabalho avalia como a guerra cibernética impacta a conduta da guerra contemporânea. O enfoque principal do estudo são os ataques cibernéticos russos à Geórgia durante o conflito entre esses dois países ocorridos em 2008. Analisam-se três tendências com diferentes níveis de modificação das formas de beligerância advindos do ciberespaço. A primeira delas se refere à criação de um novo domínio, o cibernético. A segunda vislumbra a incorporação do ciberespaço à guerra enquanto arma combinada, ou seja, incorporando-a aos instrumentos de força convencionais para produção de efeitos cinéticos. E a terceira estipula o uso da guerra cibernética como uma arma estratégica. Em termos metodológicos, a pesquisa se baseia, em primeiro plano, na revisão bibliográfica da literatura de segurança internacional e guerra cibernética e, secundariamente, na análise histórica dos ataques cibernéticos russos na Guerra Rússia-Geórgia (2008). Objetiva-se assim construir um quadro de análise para melhor compreender como o fenômeno da guerra cibernética afeta a conduta da guerra do século XXI.

Palavras-chave: Guerra Cibernética. Ciberespaço. Conduta da Guerra. Segurança Internacional.

LISTA DE SIGLAS E ABREVIATURAS

ADA –	Artilharia de Defesa Aérea
CCDCOE –	Cooperative Cyber Defense Centre of Excellence
CPS –	Sistema Físico Cibernético
C2 –	Comando e Controle
DDoS –	Ataque Distribuído de Negação de Serviço
DoD –	Departamento de Defesa dos Estados Unidos da América
EUA –	Estados Unidos da América
IP –	Internet Protocol
I&W –	Indicações e Avisos
JFC –	Comando de Força Conjunta
JFHQ-C –	Joint Forces Headquarters-Cyber
OTAN –	Organização do Tratado do Atlântico Norte
RAM –	Revolution Military Affairs
RBN –	Rede Negócios Russa
SCADA –	Supervisory Control and Data Acquisition
SQL –	Structured Query Language
TIC –	Tecnologia de Informação e Comunicação
TO –	Teatro de Operações
UK –	Reino Unido
URSS –	União das Repúblicas Socialistas Soviéticas
USB –	Porta Universal

USCCU –	Unidade de Consequências Cibernéticas dos EUA
USCYBERCOM –	United States Cyber Command
1ªGM –	Primeira Guerra Mundial
2ªGM –	Segunda Guerra Mundial

SUMÁRIO

1 INTRODUÇÃO

Ao avaliar o mundo e o seu panorama após a Guerra Fria (1947-1991) observa-se que surgiram novos desafios explanatórios e disciplinares, de maneira especial os que se referem a segurança internacional e aos estudos estratégicos. Hoje em dia, ressalta-se o crescente interesse por pesquisas sobre o ciberespaço[1] dentro das relações internacionais, sobretudo em seu aspecto securitário. No aspecto do debate sobre modificações na condução da guerra, os conceitos sobre a "redução da fricção" e o "distanciamento do front" são de grande relevância na chamada Revolução dos Assuntos Militares (RAM), ou Revolution Military Affairs (RMA)[2], na qual destaca-se a guerra cibernética como partidária. Atualmente, alguns países e organizações estão considerando o ciberespaço como um domínio combatente, provocando, desta forma, mudanças estratégicas, doutrinárias e institucionais. Podemos citar como exemplo de inclinação de pensamento estratégico-militar o United States Cyber Command (USCYBERCOM), o Cooperative Cyber Defense Centre of Excellence (CCDCOE) da Organização do Tratado do Atlântico Norte (OTAN) e a preocupação da China em combater no espaço cibernético.

Considerando a concepção mais ampla de poder cibernético, a guerra cibernética pode ser definida como uma conjuntura de fatos em que o poder militar utiliza estratégias, ferramentas e meios no espaço cibernético para alcançar seus objetivos. Por essa ótica, a guerra cibernética é uma modalidade beligerante de atuação e uso predominantes do ambiente cibernético para desestabilizar sistemas computadorizados e obter informações privilegiadas de um país[3].

---

[1] No presente estudo, considera-se, que a palavra ciberespaço possui o mesmo significado de espaço cibernético. Por isso, ao longo do texto, os termos são utilizados de modo intercambiável.

[2] Revolução em Assuntos Militares (RMA) é uma teoria sobre a evolução da guerra ao longo do tempo. Uma RMA é baseada no casamento de novas tecnologias com reformas organizacionais e conceitos inovadores de operações. O resultado é frequentemente caracterizado como uma nova forma de guerra.

[3] No presente estudo considera-se, nessa definição de guerra cibernética como domínio, seus efeitos e empregos são ligeiramente diferentes, quando considerada enquanto arma combinada ou estratégica.

O presente trabalho tem a finalidade de realizar uma análise descritiva para compreender como o fenômeno da guerra cibernética afetou a campanha Russa contra a Geórgia em 2008. Nesse sentido, o problema indaga: os ataques cibernéticos[4] russo influenciaram na condução da campanha da Rússia contra a Geórgia em 2008? A hipótese levantada é que militarmente, os ataques cibernéticos ajudaram no objetivo estratégico geral dos militares russos e a vida civil da Geórgia não foi prejudicada por esses ataques durante a guerra.

Essa reflexão impõe três grandes problemas aos estudos estratégicos e de segurança internacional, no sentido de que o ciberespaço:

1. Revolucionaria a conduta da guerra, mitigando a relevância dos domínios clássicos da terra, mar, ar e espaço sideral;

2. Permitiria alcançar a vitória militar sem dispêndio de muita energia cinética; e

3. Faria emergir uma mudança paradigmática na própria conduta da guerra, semelhante ao emprego dissuasório das armas nucleares.

Para isso, será feita uma análise de três tendências com diferentes níveis de modificação das formas de beligerância advindos do ciberespaço. A primeira delas se refere à criação de um novo domínio, o ciberespaço. A segunda vislumbra a incorporação do ciberespaço à guerra enquanto arma combinada, ou seja, incorporando-a aos instrumentos de força convencionais para a produção de efeitos cinéticos. A terceira estipula o uso da guerra cibernética como uma arma estratégica.

No que tange à metodologia, a pesquisa irá se basear na revisão bibliográfica da literatura de segurança internacional e guerra cibernética e na análise histórica dos ataques cibernéticos russos na Guerra Rússia-Geórgia (2008).

Cabe, por fim, apontar que o presente estudo se encontra estruturado a partir de cinco capítulos. O primeiro capítulo consiste nesta introdução. O capítulo 2, por sua vez, aborda os

[4] No presente estudo considera-se, que a palavra ciberataque possui o mesmo significado de ataque cibernético. Por isso, ao longo do texto, os termos são utilizados de modo intercambiável.

aspectos atinentes as considerações atuais sobre utilização operacional, quais sejam: o campo de batalha da idade da informação, o ciberespaço como uma arma, o ciberespaço como componente, a força de missão cibernética e o requerimento de integração entre as operações cibernéticas com as operações em outros ambientes.

O capítulo 3 realiza um estudo acerca do conflito entre a Rússia e a Geórgia (2008), focado na guerra cibernética, considerando como o primeiro em que ocorreu o uso do domínio cibernético em paralelo com o domínio físico. Já o capítulo quatro, apresenta uma análise da pesquisa apresentando os seguintes aspectos: a guerra cibernética como uma ferramenta silenciosa, as indicações e avisos da guerra cibernética integrada, ferramentas e táticas cibernéticas, os domínios integrados na guerra, a capacidade do adversário na área cibernética e quais foram às áreas de interesse dos ataques cibernéticos.

Por fim, o último capítulo traz as principais conclusões do trabalho, fundamentando-se nas análises dos capítulos anteriores. Por isso, nesse capítulo, busca-se responder à pergunta proposta e também se reflete sobre a possibilidade de futuras pesquisas que não foram o foco deste estudo.

2 CONSIDERAÇÕES ATUAIS SOBRE UTILIZAÇÃO OPERACIONAL

Neste capítulo apresenta-se, na seção 2.1, o espaço cibernético como um novo domínio dentro do campo de batalha além dos domínios terrestre, marítimo, aéreo e espacial. Na seção 2.2, apresenta-se o espaço cibernético como uma arma estratégica. Na seção 2.3, analisa-se o componente do ciberespaço como um componente do Comando de uma Força Conjunta. Por sua vez, na seção 2.4, avalia-se como o Departamento de Defesa dos Estados Unidos da América (DoD) incluiu um componente de ciberespaço dentro de um Comando de uma Força Conjunta. Por fim, na seção 2.5, analisa-se a importância da integração do espaço cibernético com os outros domínios.

2.1 O campo de batalha da idade da informação

Os campos de batalha do século XX e XXI tem apenas semelhanças superficiais. Há uma diferença fundamental na forma como as guerras são travadas e na luta na era da informação devido à velocidade e profundidade do espaço cibernético. Os avanços na tecnologia da informação podem muito bem limitar a tradicional guerra de manobras que luta nos domínios Terrestre, Marítimo, Aéreo e Espacial (REILLY, 2016). Em reconhecimento da importância do espaço cibernético às guerras modernas, o DoD definiu o espaço cibernético como um domínio à parte e realçou a sua importância para alcançar seus interesses nacionais[5] (UNITED STATES, 2010). O Estado-Maior Conjunto declarou que a guerra na era da informação será definida pela dependência de operações integradas e sincronizadas do ciberespaço.

O reconhecimento de que o ciberespaço é um domínio e que é parte integrante da

[5] O DoD define o domínio do ciberespaço como um "domínio global dentro do ambiente de informações que consiste na rede interdependente de infraestruturas de tecnologia da informação e dados residentes, incluindo a Internet, redes de telecomunicações, sistemas de computador e processadores e controladores integrados," U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, (Washington, DC: U.S Joint Chiefs of Staff, November 8, 2010 (As Amended Through February 15. 2016)), 58. (Tradução nossa).

guerra não significa nada a menos que possa ser incorporado ao nível operacional da guerra e que possa ser empregado na arte operacional do comandante. Planejadores conjuntos precisam entender como esta revolução da informação equivale a uma mudança na guerra no nível operacional, e como os Comandantes das Forças Conjuntas podem planejar operações no campo de batalha. Assim como o advento da mecanização, comunicação sem fio e aeronaves mudaram a guerra no nível operacional nas décadas após 1918, o ciberespaço também mudou a guerra no século XXI. Essa mudança na guerra requer uma conceituação apropriada do ciberespaço.

Este capítulo analisará essa conceituação. Ao examinar o debate sobre uso do domínio do ciberespaço para fornecer armas exclusivas, o capítulo examinará o Comando e Controle (C2) atual direcionado para o ciberespaço, argumentando que o domínio feito pelo homem deve ser centralmente gerenciado. Em contraste, exemplos históricos serão apresentados para diminuir a visão de que novas tecnologias servem para remediar a guerra. Tal abordagem raramente alcança objetivos operacionais e estratégicos. Uma conceituação adequada da guerra do século XXI e o papel do ciberespaço trará uma compreensão de que o ciberespaço está mais bem integrado em operações conjuntas como uma função conjunta.

2.2 O ciberespaço como uma arma

No espírito dos defensores do poder aéreo no início do século XX, os entusiastas do ciberespaço são rápidos para organizar um quadro de operações no ciberespaço, rapidamente paralisando um país. Richard Clarke, que foi assessor especial do presidente dos Estados Unidos da América (EUA) para assuntos referente ao ciberespaço (1998-2003), trabalhou tanto para o presidente Bill Clinton quanto para o presidente George W. Bush e visualizou armas do ciberespaço derrubando mais de 157 cidades dos EUA em menos de quinze minutos, incapacitando infraestruturas e impedindo uma resposta militar (CLARKE e KNAKE, 2015). A velocidade e o poder do domínio do ciberespaço parecem ser quase inimagináveis. A teoria é

que, como muitas sociedades se tornaram dependentes do ciberespaço para comunicações, comércio e conforto, e que ataques a ele poderiam comprometer os padrões de vida mais efetivamente do que bombardeios aéreos ou de artilharia (MYERS, 2011).

Na opinião de Clarke e outros, o ciberespaço tornou-se a plataforma de entrega para a próxima grande arma, que pode deter adversários, e se necessário, pode ser a única arma para alcançar objetivos de interesses nacionais (RAMSBY e YANNAKOGEORGOS, 2016). Em 1921, Giulio Douhet supôs uma teoria sobre a capacidade destrutiva do poder aéreo. Douhet acreditava que o poder aéreo tinha a capacidade de infligir "graves danos a ponto de provocar o colapso completo de suas forças em muitos poucos dias" (DOUHET, 1983). Os entusiastas do poder aéreo pensaram que aviões ofensivos sozinhos poderiam forçar decisivamente a rendição de um adversário. Para entusiastas como Douhet, a aeronave sozinha dominaria o campo de batalha. William Mitchel expôs na teoria de Douhet que marinhas de superfície e forças terrestres não eram mais necessárias desde que o poder aéreo poderia defender-se contra ameaças aéreas inimigas e navios, bem como projetar poder em alvos terrestres vitais (MITCHEL, 2010).

A história mostrou que Douhet e Mitchell estavam enganados. O poder aéreo sozinho não poderia encontrar decisivamente um estado final desejado na guerra. Em vez disso, utilizando-se no ar, na terra e no mar forças sincronizadas e integradas no nível operacional se tornou a fórmula vencedora para a guerra de manobra do século XX. Da mesma forma, a integração e sincronização do ciberespaço com armas aéreas, terrestres e marítimas demonstrará o verdadeiro potencial na guerra da era da informação. Análogo ao poder aéreo, o poder do ciberespaço deveria ser entendido como outro recurso que um Comandante de uma Força Conjunta poderia usar em combinação com outros recursos para alcançar um resultado decisivo (SINGER, 2014). Assim como a eficácia real do poder aéreo foi demonstrada como uma capacidade integrada, a história indica o mesmo papel para o ciberespaço.

Os fiéis defensores do ciberespaço têm, em uma única capacidade, uma lembrança

na dependência do tanque como a única resposta para o impasse na Frente Ocidental entre 1916 e 1918. O major-general alemão Heinz Guderian (1888-1954) descobriu em sua análise de táticas blindadas na Primeira Guerra Mundial que o excesso de confiança dos Aliados em sua nova arma - o tanque - fez com que desperdiçassem sua vantagem tática e estratégica. Os primeiros usos do tanque em 1916 provocaram indecisões (GUDERIAN, 1999).

Os Aliados, por meio da tentativa e erro, desenvolveram uma abordagem combinada de armas um ano mais tarde, em Cambrai, que sincronizou o movimento da infantaria, cavalaria, aeronave e artilharia para integrar fogo, manobra e proteção (GUDERIAN, 1999). A Batalha de Cambrai (1917) foi considerada um sucesso operacional pelos comandantes britânicos e franceses no campo de batalha não visto nos três anos anteriores da Primeira Guerra Mundial (1ªGM) (1914-1918). Guderian usou as lições deste campo de batalha e outros que seguiram para desenvolver um conceito moderno de guerra de manobra que abriu um novo capítulo na história da guerra (GUDERIAN, 1999).

O domínio do ciberespaço não deve ser considerado como uma capacidade separada e decisiva das partes modernas, assim como em 1916 acreditavam que o tanque era a resposta para mudança no campo de batalha decisivamente. Da mesma forma, as imprecisas avaliações de Duohet e Mitchell a respeito do poder aéreo como o único instrumento necessário para uma ação decisiva no campo de batalha, deve fazer com que defensores do ciberespaço façam uma reflexão.

A categorização do ciberespaço como uma arma única decisiva representa um erro de acordo com as lições aprendidas com a evolução das guerras do século XX. A história demonstra que o melhor caminho para o sucesso operacional e estratégico é integrar e sincronizar recursos no nível operacional. Há defensores do ciberespaço que entendem a necessidade de se integrar, mas acreditam que o controle e a direção do ciberespaço devem ser removidos do

comandante operacional e colocados somente nas mãos de especialistas adequados que podem empregar essa capacidade de forma eficaz a pedido do comandante.

2.3 O ciberespaço como componente

Os teóricos do ciberespaço acreditam que a singularidade do ciberespaço requer um modelo C2. O USCYBERCOM defende seu papel de agir como apoiado ou apoiando o comando para integrar o ciberespaço na gama mais ampla das operações militares; Porque esse ponto de vista reflete a ideia de que o ciberespaço é equivalente aos domínios físicos e os proponentes argumentam que a melhor maneira de integrar o ciberespaço é organizar as forças do ciberespaço como as dos domínios físicos são organizadas, por um modelo de componente. Acredita-se que um componente do ciberespaço pode assessorar um Comando de Força Conjunta (JFC) com perícia consolidada que resultará em operações ciberespaciais integradas[6]. Outros têm defendido que um único comando, por exemplo o USCYBERCOM, pode direcionar as tarefas e a distribuição das forças do ciberespaço e assumir temporariamente o controle tático dos Comandantes dos Teatros de Operações de uma missão em particular (FITZGERALD e WRIGHT, 2014).

O USCYBERCOM centralizou o controle do ciberespaço ao se posicionar no Joint Forces Headquarters-Cyber (JFHQ-C) em um papel de suporte direto. O JFHQ-C atribuiu ao USCYBERCOM a capacidade de manter autoridade sobre as forças no ciberespaço e de enviar um elemento de coordenação a cada comando combatente para sincronizar as ações do ciberespaço. Em teoria, tal modelo oferece ao USCYBERCOM a capacidade de apoiar os comandos combatentes e simultaneamente apoiar missões mais estratégicas. Essa estrutura reflete o desejo do USCYBERCOM de centralizar e controlar as operações no ciberespaço. O

[6] Operações ciberespaciais integradas é o emprego das capacidades do ciberespaço onde o objetivo principal é alcançar objetivos no ciberespaço ou através dele (FITZGERALD e WRIGHT, 2014. p.5).

controle centralizado da USCYBERCOM permite que as forças e capacidades no ciberespaço funcionem como um componente separado não integradas ou sincronizadas com as operações do JFC. Na melhor das hipóteses, esse modelo de controle próximo permite executar operações coordenadas com os JFCs (FITZGERALD e WRIGHT, 2014).

Os modelos C2 do século passado foram baseados na capacidade de coordenar ações entre domínios. As operações do ciberespaço, ofensivas ou defensivas, ocorrem mais rápidas do que os modelos C2 tradicionais podem coordenar com outros elementos do poder militar. A filosofia atual do ciberespaço de que ele deve ser controlado centralmente como um pacote de capacidade entregue ao comandante, viola os princípios doutrinários da unidade de comando e simplicidade para operações conjuntas[7] (UNITED STATES, 2011a). O USCYBERCOM e os defensores do controle centralizado do ciberespaço caíram em uma mentalidade semelhante à dos defensores do poder aéreo no período entre guerras. Comandantes do Ar se recusaram a integrar forças que funcionavam separadamente e ofereceram suporte limitado a outros Comandantes com limitações estritas no emprego e comando das autoridades. O resultado durante esse período da Segunda Guerra Mundial (2ªGM) (1939-1945) foi a falta de compreensão entre forças aéreas e terrestres para interagirem suas capacidades, o produto de uma estrutura C2 bifurcada, que se mostrou ineficaz na campanha inicial dos EUA em 1942 no Norte de África[8] (STARBUCK, 1992). As lições das estruturas de C2 ineficazes e limitadas de

[7] A-I - A-5- Estabelece 12 princípios de operações conjuntas: objetivo, ofensivo, massa, manobra, economia de forças, unidade de comando, segurança, surpresa, simplicidade, contenção, perseverança e legitimidade, JP 3.0 states. "O propósito da unidade de comando é assegurar a unidade de esforços sob um comandante responsável para cada objetivo. Unidade de comando significa que todas as forças operam sob um único comandante com a autoridade necessária para direcionar todas as forças empregadas em busca de um propósito comum." Simplicidade é definida como um princípio, "aumentar a probabilidade de que os planos e operações serão executados como pretendido. Preparando planos claros e descomplicados e ordens concisas" (UNITED STATES, 2011).

[8] Sua tese não é uma análise histórica aprofundada da Operação Torch, mas uma análise na estrutura de treinamento e de comando e controle da operação. Ao longo da tese, Starbuck aponta as limitações de coordenação entre comandantes distantes, falta de entendimento entre forças terrestres e aéreas devido a cadeias separadas de comando e falta de treinamento e lacunas na doutrina que foi formulada fora do conceito Douhet de bombardeio estratégico. Starbuck ilustrou como o comandante de teatro acabou mudando o modelo C2 para integrar melhor o poder aéreo ao plano operacional, removendo assim a noção da força aérea "guarda-chuva" e a missão de bombardeio estratégico fora de sincronia com o tempo e o tempo operacionais (STARBUCK, 1992, 13-14, 32-33).

1942 podem ser hoje aplicadas à exigência de um ciberespaço integrado e sincronizado em um campo de batalha do Século XXI. O USCYBERCOM parece reconhecer a limitação do uso central controlado do ciberespaço que está geograficamente separado do ambiente operacional; e, em uma tentativa de simplificar as operações do ciberespaço, o USCYBERCOM adaptou-se a um novo modelo de C2, uma Força de Missão Cibernética.

2.4 A Força de missão cibernética

O Departamento de Defesa dos Estados Unidos (DoD) investiu em mão-de-obra, tempo e recursos para criar a Força de Missão Cibernética como a base de C2 do ciberespaço e da estrutura de força para suportar um Comando de Forças Conjuntas (UNITED STATES, 2014a). A Força de Missão Cibernética está dividida em três partes: Equipes de Proteção Cibernética, Equipes de Missão de Combate e Forças Missionárias Nacionais. As Equipes de Missão de Combate e a Equipes de Proteção Cibernética são as partes da Força de Missão Cibernética que são projetadas para apoiar os comandantes de nível operacional. As Equipes de Proteção Cibernética são organizadas para "defender redes e sistemas do DoD prioritários contra ameaças prioritárias" (UNITED STATES, 2011b). No Nível Operacional o suporte ofensivo do ciberespaço é fornecido através das Equipes de Missão de Combate.

USCYBERCOM vê a Força de Missão Cibernética como uma capacidade de fornecer apoio no ciberespaço em tempo real aos Comandantes das Forças Conjuntas (UNITED STATES, 2016a). A Força de Missão Cibernética segue o modelo de apoio direto controlado pelo respectivo serviço principal JFHQ-C (UNITED STATES, 2014a). O Almirante Michael Rogers, comandante USCYBERCOM à época, considerou o modelo de suporte direto como essencial para fornecer aos comandantes de nível operacional a expertise e as ferramentas

necessárias para executar sua respectiva missão no domínio do ciberespaço[9]. O suporte direto fornece missões no ciberespaço centralmente planejadas e executadas em estreita coordenação com um Comando de Força Conjunta. A Força de Missão Cibernética também bifurca operações ofensivas e defensivas do ciberespaço separando as funções em diferentes equipes estáticas: Equipes de Proteção Cibernética para defesa e Equipes de Missão Cibernética para ofensiva.

Ao escrever sobre o domínio marítimo há cerca de um século, Sr. Julian Corbett argumentou que as operações ofensivas e defensivas são mutuamente complementares e que as guerras não são apenas ofensivas ou defensivas (CORBETT, 2004) O argumento de Corbett também pode ser aplicado aos bens comuns globais do ciberespaço.

Como Corbett apontou,

> "Nunca há, de fato, uma escolha clara entre ataque e defesa. Em operações agressivas a questão é sempre, até que ponto a defesa deve entrar nos métodos que empregamos para nos permitir fazer o máximo dentro de nossos recursos para quebrar ou paralisar a força do inimigo"[10] (CORBETT, 2004).

Como no domínio marítimo, as operações no domínio do ciberespaço exigem uma capacidade de planejar, sincronizar e transitar rapidamente entre missões ofensivas e defensivas (TATE, 2016). Isso claramente não pode ser feito sob a construção de uma Força de Missão Cibernética.

A análise de Corbett das operações ofensivas e defensivas no domínio marítimo levou a sua dissecação da capacidade de comandar o mar. Um estado não poderia conquistar o mar, mas, em vez disso, precisava olhar para o que o Estado precisava para "garantir para ele mesmo e o que poderia negar ao inimigo" (CORBETT, 2004). Para Corbett, a importância do mar era a capacidade de controlar o acesso às linhas de comunicações marítimas e, assim, levar a uma estratégia para negar o inimigo essas linhas de comunicações, enquanto habilitava o estado a explorar seu acesso. Corbett via o domínio do mar de uma maneira global comum, cujo "ataque

[9] An Interview with Michael S. ROGERS. Joint Force Quarterly no. 80 (2016 1st Quarter 2016, 82).
[10] CORBETT, Julian S.. *Some Principles of Maritime Strategy*, (New York: Dover Publications, 2004, 14).

e defesa tendiam a se fundir de uma maneira desconhecida em terra" (CORBETT, 2004).

O ciberespaço é análogo ao domínio global do mar, exigindo assim que um Comando de Força Conjunto tenha capacidade de agir ofensivamente e defensivamente no ciberespaço simultaneamente, e planejar operações sincronizadas em todos os domínios. A principal diferença entre o domínio marítimo e domínio do ciberespaço é a velocidade. O controle e a distribuição centralizados não são mais úteis para as forças navais do que para as capacidades do ciberespaço. Como força distribuída a um Comando de Força Conjunto, a Força de Missão Cibernética terá dificuldade para coordenar as operações de duas equipes separadas porque as operações ocorrem à alta velocidade.

Como Corbett apontou, com o domínio marítimo,

> "[...] a preocupação primordial ... é determinar a relação mútua entre o exército e a marinha em um plano de guerra"[11] (CORBETT, 2004).

Mais uma vez, o ciberespaço requer a mesma abordagem que Corbett levou com o mar e se concentrar na relação para empregar as capacidades do ciberespaço em todo o plano operacional.

Um Comando de Força Conjunta tem confiança no ciberespaço e requer que os líderes de nível operacional precisem "integrar as operações do ciberespaço ao planejamento e execução de operações conjuntas." (UNITED STATES, 2013). No entanto, o atual modelo de suporte direto do ciberespaço centralizado planeja em coordenação com um Comando de Força Conjunta e torna o planejamento integrado em um empreendimento difícil. Planejadores bem-intencionados, separados pelas habilidades ofensivas ou defensivas e sob uma cadeia de comando operacional diferente tendem a perder a relação entre efeitos e objetivos (BENDER, 2013). O projeto de uma Força de Missão Cibernética controlada centralmente em apoio direto aos comandantes de nível operacional baseia-se na crença de que o ciberespaço afeta todas as regiões simultaneamente. Infelizmente, a Força de Missão Cibernética de C2 inibe a flexibilidade

[11] CORBETT, Julian S.. *Some Principles of Maritime Strategy*, (New York: Dover Publications, 2004, 2, 56, 62).

e a capacidade de um Comando de Força Conjunta de utilizar o ciberespaço totalmente.

Os Comandos de Forças Conjuntas exigem a capacidade de construir um plano de liberdade de manobra em todos os domínios, para incluir o ciberespaço, por meio de recursos integrados e sincronizados com efeito desejado em todos os alvos, independentemente do sistema de armas. No entanto, no relatório do Departamento de Defesa, "Análise da Missão para Operações Cibernéticas do Departamento de Defesa", o Departamento argumenta que o modelo de suporte da Força de Missão Cibernética deve ser apenas uma estrutura temporária de comando e controle até que o domínio amadureça (UNITED STATES, 2014b).

2.5 Requerimento de integração

Um ex-Oficial de Operações (J3) do USCYBERCOM (2012-2014), major-general Brett Williams, observou que há uma necessidade inerente de integrar as operações do ciberespaço para evitar limitar a flexibilidade de um Comando de Força Conjunta (WILLIAMS, 2011). Outros defensores do ciberespaço acreditam que a singularidade do ciberespaço requer estruturas de C2 e autoridades separadas para apoiar os comandantes de nível operacional que possam utilizar um domínio do ciberespaço sincronizado e integrado (BRETT REISTER, 2012). No entanto, de acordo com JP 3-12 (R) Cyberspace Operations, "o ritmo das operações do ciberespaço requer uma significativa colaboração, bem como vigilância constante sobre o início, para assegurar que as atividades do ciberespaço em todo o ambiente operacional sejam coordenadas e desconstruídas antecipadamente" (UNITED STATES, 2011). O planejamento das operações no ciberespaço é comparado ao planejamento de nível operacional de coordenação de fogos para o "rápido engajamento de alvos e, simultaneamente, fornece salvaguardas para forças componentes" (UNITED STATES, 2011).

A capacidade de um Comando de Força Conjunta sincronizar as operações do ciberespaço com os outros domínios é a chave para ocorrer operações eficazes no domínio do

ciberespaço. A comparação com o planejamento de apoio de fogo é útil, pois a mesma analogia pode ser feita para sincronizar os esforços do ciberespaço com inteligência, C2 e manobra do Comando da Força Conjunta. Como a doutrina conjunta indica, porque as capacidades do ciberespaço abrangem todas as operações conjuntas, um Comando da Força Conjunta requer uma capacidade de sincronizar com todos os processos operacionais de planejamento e execução.

O campo de batalha da era da informação apresenta um Comando da Força Conjunta com uma visão diferente do domínio de emprego, um de interdependência versus integração (REILLY, 2016). Dr. Jeffrey Reilly definiu interdependência de domínio como uma, "falha em um domínio tem efeitos em cascata em um ou mais dos outros" (REILLY, 2016). É essa interdependência de domínio que outras nações estão aprendendo para explorar e estão desenvolvendo métodos para integrar os domínios com sucesso enquanto negar essa oportunidade a outros (UNITED STATES, 2016b). Todas as forças militares modernas dependem da capacidade de integrar tecnologia nas operações; isso é especialmente verdadeiro para um Comando da Força Conjunta (UNITED STATES, 2016b). O entendimento de que a guerra do século XXI requer interdependência sobre a integração, exige um comando de nível operacional descentralizado e uma estrutura de autoridades para o ciberespaço.

Em razão do exposto, neste capítulo observou-se que a complexidade dos campos de batalha do século XXI exige que um Comando da Força Conjunta planeje, sincronize e integre o ciberespaço em todo o ambiente operacional. O Ciberespaço é um domínio único e capacitador para as guerras do século XXI. A guerra na era da informação requer uma mudança na tentativa de integrar as operações do ciberespaço em um teatro para entender que essas operações são fundamentais para o Teatro de Operações (TO). A estreita coordenação e integração são as técnicas letárgicas do século XX, a total sincronização das operações é o pré-requisito para as guerras deste século.

Em seguida, no capítulo 3, apresenta-se um estudo acerca do conflito entre a Rússia

e a Geórgia (2008) focado na guerra cibernética com uma breve explanação dos motivos que levaram ao conflito, seguido do desenrolar da considera primeira guerra cibernética e de uma análise sumária do resultado do conflito.

3 RÚSSIA X GEÓRGIA (2008)

O presente capítulo é composto por quatro seções. Na seção 3.1, aborda-se o desenvolvimento do conflito entre a Rússia e a Geórgia (2008) sumariamente. Na seção 3.2, analisa-se os ataques cibernéticos russo que foram empregados, pela primeira vez, em paralelo aos domínios físicos. Na seção 3.3, observa-se o faseamento dos ataques cibernéticos russos. Na seção 3.4, analisa-se o resultado do conflito. Assim, ao desenvolver este capítulo, constitui-se a base necessária para a análise da guerra cibernética durante o conflito da Rússia X Geórgia (2008).

3.1 Desenvolvimento do conflito

A Geórgia tem uma história conturbada com a Rússia. Ex-integrante da União das Repúblicas Socialistas Soviéticas (URSS), a Geórgia tornou-se independente da dissolução da União Soviética em 1991. No ano anterior à queda da União Soviética, uma área no norte da Geórgia chamada Ossétia do Sul tentou se separar da Geórgia e declarar sua independência, uma ação que levou ao Conflito da Ossétia do Sul e da Geórgia (1990-1992). O resultado dessa guerra foi um cessar-fogo entre a Geórgia, a Rússia e os combatentes pró-russos na Ossétia do Sul.

Desde a declaração da independência da Ossétia em 1990 até a Guerra Russo-Georgiana de 2008, a Rússia efetivamente manteve seu domínio na área mantendo prontamente uma presença militar na fronteira com a Geórgia. Economicamente, manteve o envolvimento na Ossétia do Sul ao fornecer assistência monetária à população e permitindo que os Ossetianos do sul se registrassem como cidadãos da Federação Russa.

Pertinente na discussão a seguir é como o conflito finalmente irrompeu no que hoje é conhecido como a Guerra Russo-Georgiana. As tensões haviam sido lentamente construídas entre a Rússia e a Geórgia, em parte devido aos exercícios russos planejados para preparar as

tropas russas para uma ofensiva contra a Geórgia na Ossétia do Sul a fim de simular a retomada do controle definitivo da região (GEORGE, 2009). A tensão causada pelas políticas agressivamente desestabilizadoras da liderança georgiana em face a Região Ossétia do Sul não foi facilitada (GEORGE, 2009). Tudo isso levou à eventual erupção do conflito em 7 de agosto de 2008. Tropas georgianas, supostamente em resposta à agressão separatista na região, moveram-se para a Ossétia do Sul para restabelecer o controle e foram recebidas por tropas russas (TIKK, 2008).

3.2 A primeira guerra cibernética

Embora o conflito entre a Rússia e a Estônia tenha sido significativo por ser o primeiro caso conhecido de um país sendo atacado via ciberespaço, a guerra da Rússia contra a Geórgia é ainda mais significativa, pois é o primeiro uso cibernético conhecido em paralelo com o domínio físico de um conflito (HOLLIS, 2008). Curiosamente, poder-se-ia argumentar que a guerra começou antes que as tropas georgianas entrassem em contato com seu adversário. Pois três semanas antes do conflito no domínio físico, uma ofensiva cibernética de hackers russos já havia começado. Esses ataques foram coordenados e na maior parte vieram na forma de negação de serviço (DDoS), como foi visto na Estônia. Um ataque cibernético de negação de serviço é aquele que tenta impedir o uso legítimo de recursos de informática. Quando vários computadores são empregados para atingir esse objetivo, ele se torna um ataque distribuído de negação de serviço. Embora a guerra física tenha começado em agosto, um dos pesquisadores de segurança da Arbor Networks[12] verificou ataques DDoS em sites do governo da Geórgia em 20 de julho de 2008 (MARKOFF, 2008).

A campanha cibernética russa atacou um total de 38 sites georgianos e ocidentais

[12] A Arbor Networks é uma empresa de software fundada em 2000 e sediada em Burlington, Massachusetts, Estados Unidos, que vende software de segurança de rede e monitoramento de rede, usado por mais de 90% de todos os provedores de serviços de Internet (NETSCOUT, 2019).

sobre o surto da guerra, incluindo os do Presidente da Geórgia, do Ministério dos Negócios Estrangeiros, dos Bancos, do Parlamento, do Supremo Tribunal e os das Embaixadas dos Estados Unidos da América (EUA) e do Reino Unido (UK) na Geórgia. Esses ataques parecem ter sido direcionados centralmente e coordenado, a julgar pelo fato de terem iniciado e terminado defasados 30 minutos um do outro – começando aproximadamente às 05:15 da tarde no dia 8 de agosto de 2008 e terminando por volta das 12:45 da tarde em 11 de agosto de 2008, quando a Rússia anunciou seu cessar-fogo (ASMUS, 2010).

Pode-se olhar para esses ataques iniciais como provas de fraqueza ou exercícios iniciais para hackers do governo, no entanto, é tão provável que esses ataques antes do conflito físico fossem simplesmente "hactivismos"[13] desonestos de dentro da Rússia. De uma maneira que parecia perfeitamente sincronizada, as tropas russas marcharam para a Ossétia do Sul para proteger seus interesses na área e impedir que a Geórgia declarasse militarmente o poder sobre a região, enquanto mais ataques cibernéticos invadiam os sites georgianos. Os ataques DDoS foram eficazes para desativar sites segmentados e interromper a comunicação da Geórgia para o mundo exterior. Como foi o caso do site do Parlamento georgiano, alguns sites não foram fechados, mas sim confundidos com propaganda russa (JOHN MARKOFF, 2008).

Apesar desse fato, é improvável que os ataques tenham sido conduzidos diretamente pelo governo russo. A Rússia tem sido uma fonte de muitos ataques cibernéticos sofisticados nos últimos anos, a maioria se origina de uma organização chamada de Rede de Negócios Russa (RBN), que não foi definitivamente mostrado ter ligações com o Governo russo. Na verdade, o fato de a RBN não ser uma empresa registrada e de seus domínios da Internet estarem registrados em endereços anônimos torna as origens e a propriedade da RBN um desafio para a comunidade de inteligência. No caso, fica evidente que além de cometer crimes cibernéticos, como roubo de identidade, phishing, spam e distribuição de malware (código malicioso), a RBN também se

[13] Hactivismo: promover ou resistir a algum tipo de mudança política ou social, valendo-se de meios de protestos cibernéticos não violentos, mas, quase sempre, legalmente questionáveis (SINGER e FRIEDMAN, 2017).

especializou, entre outras ações ruins, em ataques distribuídos de negação de serviço (DDoS) que foram direcionados a sites georgianos durante a guerra (DAVID, 2008). Em uma briga anterior entre a Rússia e a Estônia sobre a remoção de um memorial de guerra soviético do governo estoniano capital, o governo da Estônia foi submetido a uma série semelhante de ataques cibernéticos também pensados terem sidos realizados pelo RBN. O cenário mais provável em ambos os casos é que a RBN realizou os ataques em nome de o governo russo, fornecendo ao governo o seu anonimato.

Os hackers russos, sancionados pelo governo ou não, pareciam ser bem coordenados e taticamente sensatos em suas ações. Assim como um ataque aéreo a um país inimigo visaria primeiro as capacidades defensivas do inimigo, como a Artilharia de Defesa Aérea (ADA), os ataques de agosto de 2008 começaram com a segmentação de fóruns frequentados de hackers georgianos (KEIZER, 2008). Ao efetivamente neutralizar o inimigo antes que eles pudessem combater os ataques, os hackers russos asseguraram seu domínio contra a já sobrecarregada infraestrutura da web da Geórgia. Outra tática sofisticada de capacidade de hackers russos foi o momento e a localização desses ataques cibernéticos.

Enquanto a Rússia afirma que apenas civis russos estavam envolvidos em atividades nefastas de hackers, os hackers pareciam saber onde os ataques russos ocorreriam antes que eles acontecessem e, em vez de atacar sites aleatoriamente, sites específicos e de importância militar eram alvos. Por exemplo, um relatório da Unidade de Consequências Cibernéticas dos EUA (USCCU) sobre os ataques apontou que um site georgiano desativado por hackers era usado para alugar geradores a diesel, um alvo altamente improvável para “hacktivistas” russos, com a intenção de reforçar os efeitos dos ataques físicos na rede elétrica georgiana” (BUMGARNER e BORG, 2009).

Curiosamente, os ataques cibernéticos à Geórgia foram menos eficazes do que poderiam ter sido contra um governo mais conectado. Embora a infraestrutura de internet

georgiana tenha se mostrado relativamente simples para os guerreiros cibernéticos russos, o governo georgiano provou ser capaz de voltar a ficar on-line. O site do presidente georgiano foi restabelecido como uma página no site do presidente da Polônia, que a Rússia se mostrou incapaz ou não queria atacar; outros sites do governo georgiano rapidamente se restabeleceram como blogs por trás da proteção do google.com, e novamente a Rússia não estava disposta ou incapaz de derrubá-los. O resultado foi uma explosão no tamanho e importância da blogosfera georgiana, que continua a ser um problema no lado da Rússia desde o fim da guerra (CORNELL e STARR, 2009). Uma razão final que os ataques cibernéticos russos foram limitados em sua eficácia é que, em agosto de 2008, a Geórgia tinha apenas recentemente criado contas de e-mail oficiais para seus governos e militares. No início da guerra, muitos, se não a maioria, funcionários georgianos ainda usavam suas contas pessoais (gmail, yahoo etc.) para comunicação oficial, o que significa que os ataques aos servidores de email do governo da Geórgia tinham pouco efeito sobre sua capacidade de comunicação.

Não só parece que os hackers estavam tomando as dicas dos militares russos, como também os militares pareciam estar prestando atenção aos alvos que haviam sido colocados off-line pelos hackers. A seleção de alvos russos na Geórgia parecia estar em coordenação com ataques no domínio cibernético; centros de comando e controle e meios de comunicação, alvos físicos que normalmente estariam no topo da lista para a Rússia atingir a fim de controlar a comunicação dentro da Geórgia, pareciam ser poupados, uma vez que já haviam sido neutralizados via cyber (BUMGARNER e BORG, 2009). Além disso, o envolvimento dos hackers com os militares também foi revelado pelos alvos que eles não atingiram. A USCCU notou que muitas infraestruturas críticas georgianas estavam acessíveis aos hackers durante os ataques, e que, se eles quisessem causar danos permanentes a alguns desses sistemas, isso estaria bem dentro das capacidades exibidas durante a guerra (BUMGARNER e BORG, 2009). Mais uma vez, em vez da natureza frenética e destrutiva que geralmente é notada em comunidades de

hackers desorganizadas, eles estavam demonstrando contenção e previsão em sua escolha de alvos.

3.3 As fases dos ataques cibernéticos russos

Especialistas em segurança identificaram duas fases na campanha cibernética russa contra a Geórgia. A primeira iniciou-se na noite de 07 de agosto de 2008, com ataque de *hackers* a sites do Governo da Geórgia e da mídia (BUMGARNER e BORG, 2009).

Na primeira fase, os hackers russos realizaram ataques distribuído de negação de serviço (DDoS - Distributed Denial of Service) como ação principal. Um ataque cibernético de negação de serviço é aquele que tenta impedir o uso autêntico de recursos de informática. Esses ataques podem ser categorizados de forma *semântica* quando se tira proveito de uma característica ou de uma distorção do software do sistema visado. Ou ataques que empregam *força bruta* (ou de "inundação") quando o sistema visado recebe, via internet, um volume de dados maior do que ele pode suportar esgotando os recursos de comando e controle do servidor fazendo com que ele fique indisponível (MIRKOVIC, 2004).

Durante essa fase, os ataques DDoS foram conduzidos a cabo por botnets (NAZARIO, 2008). *Botnet* é uma rede de computadores, conectados à internet, infectados por um aplicativo conhecido como *malware. Malware* é um código malicioso destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não). Normalmente, as *botnets* são utilizadas para lançar mensagens eletrônicas publicitárias conhecidas como *spam*, mas também podem ser usadas para realizar ataques DDoS em larga escala. As *botnets* russas empregaram os ataques DDoS por força bruta (NAZARIO, 2008). As redes georgianas, devido à sua natureza débil, estavam mais suscetíveis a inundações do que as redes estonianas, que haviam sido atacadas pelos *hackers* russos no ano anterior (BUMGARNER e BORG, 2009).

Já na segunda fase, os ataques aos sítios de internet da mídia e do governo georgianos continuaram, mas a operação cibernética russa foi ampliada de modo a infligir danos a mais alvos, incluindo instituições financeiras, empresas, instituições de ensino, mídia ocidental (BBC e CNN) e um sítio de internet de *hackers* da Geórgia (BUMGARNER e BORG, 2009). Esses servidores além de sofrerem ataques de negação de serviço, também tiveram seus sítios desconfigurados (um exemplo foi a "grafitagem" pró-Rússia nas páginas do governo, como o emprego de uma imagem comparando o Presidente georgiano Mikheil Saakashvili a Adolf Hitler). Além disso, vários *hackers* russos utilizaram endereços de correio eletrônico de políticos georgianos, disponíveis ao público, para iniciar uma campanha de proliferação de mensagens eletrônicas (*spam*) (DANCHEV, 2008).

Para executar as desconfigurações de sítios da internet, os *hackers* russos recorreram ao tipo de ataque conhecido como injeção de SQL (sigla em inglês para *Structured Query Language*, ou Linguagem de Consulta Estruturada), que se aproveita de um campo de texto em uma página da rede mundial para se comunicar diretamente com o banco de dados *back-end* (responsável por dinamizar os sites utilizando linguagens de programação, além de organizar todas as informações invisíveis aos olhos do usuário.). Em resumo, um sistema suscetível a esse tipo de vulnerabilidade confere ao *hacker* acesso total ao banco de dados em questão — que pode incluir todo tipo de informação, desde listas com as identificações de acesso dos usuários, até registros de transações financeiras, ou até mesmo o conteúdo integral de sítios da internet (ULLRICHA, 2008).

Organizações criminosas, como a RBN, alugam e usam *botnets* para uma variedade de propósitos (CARR, 2010). Conforme citado anteriormente neste capítulo, provavelmente os ataques realizados aos sítios de internet da Geórgia partiram da RBN.

A Geórgia reagiu aos ataques russos, primeiramente, filtrando os endereços de IP

(Internet Protocol)[14] russos. No entanto, os *hackers* russos se adaptaram rapidamente e usaram servidores não russos ou endereços de IP falsos. Os georgianos, então, transferiram muitos de seus sítios para servidores localizados fora do país (principalmente nos Estados Unidos). Não obstante, mesmo esses servidores, localizados no exterior, permaneceram suscetíveis à exploração por inundação, devido ao grande volume de força bruta empregado no ataque russo (BUMGARNER e BORG, 2009).

3.4 Resultado

Embora alguns desses ataques cibernéticos possam parecer semelhantes e ainda mais notórios do que os ocorridos na Estônia em 2007, a maioria da população georgiana não foi afetada por esses ataques cibernéticos. Militarmente, os ciberataques pareciam ajudar no objetivo estratégico geral dos militares russos, mas a vida civil da Geórgia não foi prejudicada pelos ciberataques durante a guerra. A Geórgia não era nem de longe tão dependente do espaço cibernético quanto a Estônia. Por volta da mesma época que este conflito, a Estônia tinha aproximadamente 57 em cada 100 cidadãos na web e a Geórgia tinha apenas 7 (TIKK, 2008). Dessa forma, a população geral da Geórgia não se sentia nem perto dos mesmos efeitos desses ataques cibernéticos como os cidadãos estonianos, fazendo um paralelo com os ataques cibernéticos russos à Estônia (2007).

Embora não seja surpreendente, é um pouco revelador que a Rússia ainda negue envolvimento no domínio cibernético, ainda que esteja obviamente envolvida em um conflito aberto com a Geórgia. Alguns dos ataques cibernéticos que ocorreram durante o conflito, incluindo a desconfiguração dos sites do Parlamento, foram preparados com bastante antecedência. Provavelmente não seria um bom momento para um hacker planejar ataques

[14] Internet Protocol - é um número que identifica um dispositivo em uma rede.

cibernéticos sem coordenação com outros componentes em meio a um conflito armado (BUMGARNER e BORG, 2009). A questão então se torna, o que é mais provável: a Rússia utilizando um meio de ataque barato e efetivo que é perfeitamente capaz de usar em uma guerra aberta contra a Geórgia, ou que um grande bando de hackers amadores russos planejou com bastante antecedência um ataque a Geórgia via ciberespaço de uma forma que coincidiu perfeitamente com os objetivos operacionais e táticos russos? A Rússia, sem dúvida, deseja manter suas capacidades no domínio cibernético "fora do radar", mas é, na melhor das hipóteses, ingênuo para a Rússia continuar a negar qualquer envolvimento em tais ataques.

Também deve ser notado que, embora a Geórgia estivesse muito mais atrasada do ponto de vista tecnológico do que a Estônia, os hackers georgianos retomavam o acesso aos serviços de informática quando possível, já a Estônia simplesmente cortou o acesso externo a seus sites, tornando-se efetivamente uma intranet. Atualmente, a Ossétia do Sul permanece sob contenção, com presença de militares russos, mas geralmente ainda reconhecida pela comunidade internacional como parte da Geórgia (TIKK, 2008).

Feitas estas observações, cabe apontar, portanto, que no próximo capítulo serão feitas considerações da pesquisa realizada sobre a guerra cibernética, particularmente sobre os ataques cibernéticos russos à Geórgia durante o conflito armado entre as partes, ocorrido em 2008.

4 CONSIDERAÇÕES DA PESQUISA

O presente capítulo aborda as considerações da pesquisa realizada sobre a guerra cibernética, particularmente os ataques cibernéticos russos à Geórgia durante o conflito armado entre as partes (2008). Para tanto, este capítulo é composto por cinco seções. Na seção 4.1, relata basicamente o tamanho da amostragem da pesquisa. Na seção, 4.2, verifica-se o efeito de observador referente a capacidade russa de realizar uma guerra cibernética. Na seção 4.3 são analisados os ataques cibernéticos como ferramenta silenciosa, as indicações e avisos da guerra cibernética integrada, as táticas que foram empregadas e as que poderiam ter sido empregadas no conflito e os domínios integrados do conflito. Na seção 4.4, observa-se a necessidade de se avaliar a capacidade do adversário na área cibernética. E por fim, na seção 4.5, ressalta-se as áreas de interesses dos ataques cibernéticos.

4.1 Tamanho da amostragem

A guerra cibernética é uma fronteira relativamente nova, os exemplos do mundo real são poucos e distantes entre si. Portanto, é necessário enfatizar que as cibertáticas empregadas pela Rússia não foram testemunhadas com muitas repetições; isto é, essa pesquisa só pode tirar conclusões com base no que foi visto, e provavelmente ainda há muito a ser feito nessa área de pesquisa que só pode ser feita quando mais conflitos tiverem ocorrido.

4.2 Efeito de observador

A Rússia demonstrou um padrão de utilização da guerra cibernética em compromisso com um adversário. No entanto, um estrategista conservador precisa considerar todas as possibilidades ao defender-se contra um possível ataque. O efeito observador sustenta que observar um processo pode mudá-lo. Apenas em virtude da Rússia estar ciente de que suas táticas

cibernéticas foram observadas em um cenário mundial, significa que ela pode estar mudando suas táticas para possíveis conflitos futuros. Com isso, pode-se chegar à conclusão de que a Rússia já “mostrou suas cartas”, confirmando sua capacidade de realizar uma guerra cibernética.

4.3 Análise da guerra cibernética

Passando agora para uma análise mais aprofundada das táticas cibernéticas russas utilizadas durante o conflito acima mencionado, esta seção cobrirá o comportamento dos hackers russos para atingir objetivos políticos e militares. Para os objetivos desta pesquisa, o conflito entre a Rússia e a Geórgia é o mais significativo, pois fornece exemplos concretos de táticas cibernéticas e como elas podem ser usadas em conjunto com os outros domínios. Embora os domínios físicos supostamente não tenham sido integrados nesse conflito, eles podem fornecer contexto para aqueles que visualizam o domínio cibernético como uma arma sem efeitos cinéticos.

4.3.1 Uma ferramenta silenciosa

Esta seção destaca algo que pode ser considerado como uma “cibernética apatia” ou a aceitação dos ataques cibernéticos por parte da comunidade internacional. Ao fazer uma breve comparação entre dois conflitos cibernéticos envolvendo a Rússia, contra a Estônia (2007) e contra a Geórgia (2008), é mais fácil reconhecer essa resposta no caso da Estônia, já que não houve uma guerra física para desviar a atenção, ou seja, no caso da Geórgia, pode não fazer sentido citar ataques cibernéticos quando os tanques russos estavam atuando pela fronteira. No coração dessa apatia está a questão da eficácia.

Como diz Rehman,

> "...existe sempre, entretanto, a questão de como identificar se um ataque cibernético é uma arma de destruição em massa ou simplesmente uma arma de distração e inconveniência em massa" (REHMAN, 2014).

O que Rehman cita é como a população em geral não sabe como classificar ataques cibernéticos. Além disso, o mundo ainda tem que testemunhar ataques cibernéticos realmente danosos. Na maioria dos casos, os ataques cibernéticos nos noticiários tendem a ser mais transitórios por natureza.

Como foi citado anteriormente, a guerra cibernética é tão nova que a comunidade internacional não testemunhou o verdadeiro potencial dos ataques cibernéticos. Esses ataques, embora não necessariamente cinéticos, podem ter efeitos secundários e terciários que poderão ser realmente devastadores. Por exemplo, se a Rússia o desejasse, poderia ter ensinado à Geórgia uma lição muito mais dolorosa ao visar suas infraestruturas críticas. As sociedades tecnologicamente avançadas têm uma infinidade do que é conhecido como Sistema Físico Cibernético (CPS)[15], normalmente referindo-se à integração de sistemas físicos e infraestruturas com sistemas de computador. Esses tipos de ataques utilizados contra redes de energia, instalações de tratamento de água ou gás, as instalações de distribuição de petróleo, podem rapidamente se tornar mortais. Devido à falta de exemplos do mundo real, a comunidade internacional, ao contrário, classifica os ataques ao CPS como “alarmistas e irrealistas” (APPLEGATE, 2013). É evidente que a Rússia contava com essa apatia ao entrar em conflito

[15] Sistema Físico Cibernético (CPS) são sistemas automatizados que permitem a conexão das operações da realidade física com infraestruturas de computação e comunicação (GOMES, 2016).

cibernético com a Geórgia e respondeu com as negativas que normalmente acompanham os ataques cibernéticos alegando não ter participado dos mesmos.

4.3.2 As indicações e avisos da guerra cibernética integrada

Talvez o aspecto mais impressionante da ofensiva cibernética da Rússia à Geórgia tenha sido o modo como ela processou sua campanha aérea em conjunto com sua campanha cibernética. Como a Unidade de Consequências Cibernéticas dos EUA (US-CCU)[16] observou em seu relatório sobre a guerra russo-georgiana, o principal objetivo das campanhas cibernéticas era apoiar uma invasão russa, e "... os ataques cibernéticos se encaixam perfeitamente no plano de invasão" (BUMGARNER e BORG, 2009). Os alvos cibernéticos foram entrelaçados com os ataques terrestres e aéreos de tal maneira que os alvos não foram atingidos desnecessariamente. Se uma capacidade georgiana não estivesse disponível para ser atacada via ataque cibernético, talvez devido à falta de dependência tecnológica da Geórgia e o mínimo de CPS, então a Rússia a atingiria fisicamente. Por outro lado, se um alvo tivesse sido efetivamente neutralizado via ciberespaço, a Rússia não desperdiçaria recursos físicos para atingi-lo fisicamente, como no exemplo dos meios de comunicação da Geórgia (BUMGARNER e BORG, 2009).

Além das situações em que as metas eram divididas por capacidade, também existiam casos em que um ataque físico em um ativo georgiano era apoiado por um ataque cibernético subsequente virtual, como no caso do site de aluguel de geradores georgiano discutido anteriormente. Embora aparentemente inconsequente, este exemplo demonstra a coordenação prévia envolvida nesta campanha como também táticas russas sofisticadas. Acertar o site depois de ataques físicos na rede elétrica georgiana efetivamente neutralizava uma possível

[16] A Unidade de Consequências Cibernéticas dos EUA (US-CCU) é um instituto de pesquisa independente, sem fins lucrativos. Ele fornece avaliações das consequências estratégicas e econômicas de possíveis ataques cibernéticos e ataques físicos cibernéticos. Também investiga a probabilidade de tais ataques e examina a relação custo-eficácia de possíveis contramedidas (EUA, 2019).

tática de mitigação do alvo. Além disso, alvos cibernéticos foram mantidos no mesmo local na Ossétia do Sul, onde a luta física estava ocorrendo, outro possível indicador e alerta para aqueles que estavam acompanhando o conflito (HOLLIS, 2008).

A campanha da Rússia contra a Geórgia e, de certa forma, a Estônia também, forneceu aos especialistas em inteligência desses países Indicações e Avisos (I&W), termo comum na comunidade de Inteligência Norte-Americana. Se um adversário foca seus ataques cibernéticos em uma determinada área, isso pode fornecer indicações e avisos úteis para um analista de inteligência. Isso pode indicar que os ataques no domínio físico também serão focados nessa região, o que, por sua vez, também podem ser úteis de outras maneiras. Como dito anteriormente, os analistas podem olhar para os alvos que eles esperam que sejam atingidos por ciberataques e não foram. Isso pode indicar uma área que teria que ser focada no domínio físico. Algo tão simples quanto olhar para onde o ataque está sendo focalizado ainda pode dizer algo ao analista, se o inimigo está usando o direcionamento errado ou não. Sem listar todas as possibilidades, deve ficar claro que, ao entender como uma guerra cibernética é processada, pode-se tirar proveito desse conhecimento e usá-lo no futuro.

4.3.3 Ferramentas e táticas

Existem inúmeras ferramentas cibernéticas que um estado pode usar contra um adversário, e elas podem ser usadas de várias maneiras para negar o acesso de um adversário a seus próprios sistemas, interromper suas comunicações, degradar suas capacidades e até mesmo destruir sistemas por completo. Exemplos desse intervalo, do vírus Stuxnet inserido no CPS nuclear iraniano, supostamente por hackers norte-americanos e israelenses. Existe a possibilidade de hackers militares chineses estarem estabelecendo uma “cabeça de ponte digital” em computadores militares dos EUA pelo do uso de uma USB “infectada” (FARWELL e ROHOZINSKI, 2011). Na Rússia, os ataques preferidos, parecem ser principalmente os DDoS.

Esta é uma boa e má notícia para aqueles que antecipam a possibilidade de ter que lidar com hackers russos.

A boa notícia é que tanto os casos Estônia quanto da Geórgia apontam o DDoS como a cibertática russa preferida. Para ter certeza, havia outras táticas, como postar propaganda em sites do governo da Geórgia, mas o DDoS parece ser a “ponta da lança”. A má notícia é que o DDoS, embora tipicamente brutal e sem sofisticação, pode ser uma tática eficaz. No espectro de efeitos cibernéticos ofensivos, os "cinco D's", Deny, Degrade, Disrupt, Destroy, and Deceive[17] (UNITED STATES, 2008). O DDoS pode se enquadrar nas várias categorias de negação, degradação ou interrupção, dependendo da eficácia do ataque. A eficácia do ataque depende muito do tamanho do recurso DDoS.

Em relação aos ataques realizados pela Rússia no espaço cibernético da Geórgia foram considerados de pequena capacidade, 1Gbps era de fato um ataque DDoS comparativamente pequeno no momento. No entanto, era suficientemente necessário para superar a largura da banda das redes menores usadas pela Geórgia. A discrição foi utilizada na forma de quais sites atacar e quais deixar de lado e a Rússia parecia estar usando apenas o que era necessário para derrubar a rede. Se fosse o caso, então um ataque maior não faria nada além de não usar uma capacidade melhor deixada oculta.

Além disso, enquanto os ataques DDoS russos eram pequenos, eles eram sofisticados. A maioria dos ataques DDoS podem ser mantidos por horas ou até mesmo um dia se os hackers forem persistentes, mas eventualmente o alvo é capaz de corrigir o sistema ou utilizar filtros que manterão as solicitações incorretas. Como exemplo, no caso dos ataques DDoS na Estônia foram mantidos por semanas (SCHMIDT, 2013). Isso faz com que um hacker ativo e persistente trabalhe em volta dos filtros colocados pelo alvo para bloquear o ataque. De

[17] Deny, Degrade, Disrupt, Destroy, and Deceive - Negam, Degradam, Rompem, Destroem e Enganam (UNITED STATES,2008, tradução nossa)

acordo com o Relatório da US-CCU sobre a Campanha Cibernética da Geórgia, os ataques DDoS contra a Geórgia levaram bastante tempo para serem planejamento e serem realizados.

No caso da Geórgia, no entanto, vemos que as comunicações georgianas não só foram afetadas, como também foram tornadas cegas do ponto de vista da rede por uma combinação de ataques aéreos e cibernéticos em suas estruturas C2. Embora isso pareça debilitante para os leitores de estados tecnologicamente avançados, observar como a Geórgia foi afetada, ou melhor, não afetada, é significativo em comparação com a Estônia.

Não há dúvida de que a rede da Geórgia foi fortemente afetada. Vale ressaltar a falta de efeitos adversos para os militares georgianos. Das várias redes e sites afetados pelos ataques cibernéticos à Geórgia, os militares georgianos saíram praticamente ilesos. Embora a Geórgia tenha percorrido um longo caminho desde 2007 em termos de suas Tecnologias de Informação e Comunicação (TIC), ainda tem um longo caminho a percorrer (WORLD ECONOMIC FORUM, 2015). Embora o Fórum Econômico Mundial não avalie a dependência militar das TICs, se a participação do governo da Geórgia em TICs pode ser usado como um parâmetro comparável, a Geórgia é classificada como a 60ª do mundo, em oposição ao ranking da Estônia de 22ª geral (WORLD ECONOMIC FORUM, 2015). No entanto, essa falta de TICs teve a vantagem de proteger os efeitos potenciais da ofensiva cibernética sobre as forças armadas georgianas. Se houvesse uma dependência maior, sua eficácia no campo poderia ter sido afetada de maneira mais adversa. O exemplo mais citado do Stuxnet se aplica aqui. Se as centrífugas iranianas não fizessem parte de um CPS, seus sistemas físicos não seriam capazes de ser alvos dessa maneira. Isso ilumina os aspectos positivos e negativos da dependência cibernética.

Além de utilizar o DDoS para tentar cegar e arrochar seus alvos, a Rússia pareceu usando o DDoS como uma distração em alguns casos, causando uma grande paralisação em um setor enquanto realizava esforços de infiltração cibernética em outro, semelhante a como o DDoS era usado durante o Violação de dados da Sony em 2011(JOSHUA, 2014). A ideia por trás dessa

tática é que enquanto os esforços defensivos estão sendo concentrados para filtrar o fluxo de dados dos ataques DDoS, outros hackers estão migrando para importar vírus e spyware nocivos, ou explorar dados protegidos de os sistemas de destino. Dependendo da natureza das informações exploradas, elas podem assumir a forma de espionagem ou até mesmo auxiliar em ataques futuros, fornecendo aos hackers um esquema da infraestrutura da rede de destino e de outros CPS para os quais ela pode estar conectada. O site mais popular de hackers da Geórgia, www.hacking.ge, também foi alvo de hackers russos antes do conflito principal (TIKK, 2008). Parte da degradação do oponente é garantir que ele não consiga atacar ou responder em espécie.

4.3.4 Domínios integrados da guerra

Por meio de uma análise cuidadosa do estudo de caso georgiano, demonstrou-se que os russos são proficientes na integração dos domínios díspares da guerra. Exemplos demonstraram como um ataque aéreo russo foi apoiado por um ataque cibernético de alvos secundários ou terciários. Além disso, ataques aéreos e terrestres foram retidos de alvos que foram neutralizados por um ataque DDoS e vice-versa. Assim, durante um conflito aberto e declarado com um estado inimigo, deve-se esperar que um adversário tecnicamente simétrico empregue uma campanha sofisticada de guerra cibernética que seja ativamente integrada com os domínios aéreo, espacial, terrestre e marítimo de guerra.

4.4 Capacidade do adversário na área cibernética

Independentemente de o governo russo estar ou não envolvido nos ataques cibernéticos, eles foram claramente benéficos às operações russas, como um todo. Dessa forma, talvez devamos passar a considerar as capacidades cibernéticas como um sistema operacional do campo de batalha, assim como o são a manobra, a artilharia, a defesa antiaérea etc. Conhecer

adequadamente as capacidades cibernéticas do inimigo é parte importante de qualquer análise. O *hacker* inimigo pode assumir várias formas: indivíduos em laboratórios patrocinados pelo governo, militares integrantes de Unidades cibernéticas, membros de organizações criminosas e *hacktivistas*. Distinguir os diferentes participantes que estão no espaço cibernético é algo frequentemente difícil ou mesmo impossível. No entanto, entender quais desses soldados cibernéticos fazem parte da ordem de batalha do inimigo pode trazer esclarecimentos sobre suas ações. Com a ordem de batalha estabelecida, podemos então aplicar "padrões doutrinários" cibernéticos. No exemplo do conflito na Geórgia, incluiríamos as organizações criminosas russas na ordem de batalha, embora não soubéssemos precisamente quais eram suas relações com as Forças convencionais. A partir de sua inclusão na ordem de batalha, poderíamos considerar o padrão doutrinário associado à atuação dos criminosos. Isso poderia indicar a possibilidade de emprego de *botnets* e *hacktivistas*, com a missão de isolar e silenciar o inimigo, mas não para afetar a infraestrutura ou o SCADA[18] permanentemente.

4.5 Áreas de interesse dos ataques cibernéticos

Outra lição, que talvez possamos extrair do caso georgiano, é que os comandantes não devem apenas considerar a segurança de redes militares, mas também das redes civis. Ainda que não estivessem direcionados a alvos militares, de modo geral, os ataques cibernéticos russos na Geórgia produziram efeitos psicológicos e de informação significativos. Uma consideração adicional: alguns ataques cibernéticos, como os que foram desencadeados em julho, contra sítios internet do governo georgiano, podem ser indicativos não apenas de ataques cibernéticos em grande escala, mas também da proximidade do início de operações terrestres. Assim, um

[18] Controle de Supervisão e Aquisição de Dados (*Supervisory Control and Data Acquisition — SCADA*). Sistemas SCADA são aqueles que coletam dados, controlam e monitoram, em tempo real, estações que fazem parte da infraestrutura crítica, incluindo usinas, oleodutos, refinarias e sistemas de tratamento e distribuição de água (FERNANDEZ, 2005).

comandante talvez queira levantar elementos essenciais de informações que sejam cibernéticos, por natureza. Para ajudar na proteção da população local, talvez seja imperativo garantir a sobrevivência das redes de computadores civis.

5 CONCLUSÃO

O propósito do presente trabalho foi analisar três tendências com diferentes níveis de modificação das formas de beligerância advindos do ciberespaço. A primeira delas se refere à criação de um novo domínio, o cibernético. A segunda vislumbra a incorporação do ciberespaço à guerra enquanto arma combinada, ou seja, incorporando-a aos instrumentos de força convencionais para produção de efeitos cinéticos. E a terceira estipula o uso da guerra cibernética como uma arma estratégica. Nesse sentido, o enfoque principal do estudo foram os ataques cibernéticos russos à Geórgia durante o conflito entre esses dois países ocorridos em 2008.

Dessa maneira, procurou-se responder à seguinte pergunta: os ataques cibernéticos russo influenciaram na condução da campanha da Rússia contra a Geórgia em 2008? Ratificando a hipótese inicial, o estudo atestou que a guerra tinha começado bem antes que as tropas georgianas entrassem em contato com as tropas russas, pois três semanas antes do conflito no domínio físico, uma ofensiva cibernética de hackers russos já havia começado. Os ataques cibernéticos foram eficazes para desativar sites segmentados e interromper a comunicação da Geórgia para o mundo exterior contribuindo para a campanha militar, de modo que os ciberataques foram bem efetivos ajudando na conquista do objetivo estratégico geral dos militares russos.

Para alcançar o que foi proposto, a pesquisa foi estruturada em três capítulos de desenvolvimento. No capítulo dois foi estudado as considerações atuais sobre a utilização operacional do ciberespaço. Foi abordado o reconhecimento de que o ciberespaço é um domínio e que é parte integrante da guerra podendo ser incorporado ao nível operacional da guerra e ser empregado na arte operacional do Comandante. Além disso, foi considerado como uma arma que deve atuar de forma integrada e sincronizada com as armas aéreas, terrestres e marítimas demonstrando o verdadeiro potencial na guerra da era da informação.

No capítulo seguinte, fez-se necessário preceder à análise do conflito ocorrido entre a Rússia e a Geórgia (2008). Para tal, foi realizado um apanhado histórico relacionando os motivos que levaram ao desenvolvimento do conflito. Foi abordado como os russos realizaram os ataques cibernéticos antes e durante o conflito sendo considerado como a primeira guerra cibernética da história ocorrendo em paralelo com a guerra cinética.

No capítulo quatro foram feitas considerações sobre a pesquisa fazendo uma análise mais profunda das táticas cibernéticas russas utilizadas na guerra entre a Rússia e a Geórgia (2008), como podem ser empregadas em conjunto com as táticas empregadas nos conflitos físicos. Analisou-se a guerra cibernética como uma ferramenta silenciosa pois até os dias atuais não se utilizou ataques cibernéticos para causarem grandes efeitos, como por exemplo fazer ataques as estruturas críticas. No caso da Geórgia só causaram efeitos secundários e terciários. Apontou-se a elevada relevância da ofensiva cibernética integrada com as campanhas aérea e terrestre. Demonstrou que a Rússia, dentre as inúmeras ferramentas de ataques cibernéticos, tem preferência pela tática de negação de serviços (DDoS), pois fez uso tanto na guerra cibernética contra a Estônia (2007) quanto na guerra contra a Geórgia (2008). Dessa forma, é interessante que se observe a capacidade do adversário no campo cibernético bem como suas áreas de interesses para realizar ataques cibernéticos.

Assim, conclui-se que uso estratégico-militar do ciberespaço vem provocando alterações na conduta da guerra. Entretanto, a criação de um novo domínio, o cibernético, não ocorre em desconexão com as dimensões materiais, em que os conflitos armados já se processam.

Ao chegar ao final deste trabalho, pode-se afirmar que, até o momento, a literatura não apresenta relatos plausíveis de que ataques cibernéticos tenham produzido danos em larga escala contra estruturas estratégicas ou centros de C2. Entretanto, apesar de não se atestar vínculos causais, o acontecimento aqui analisado — envolvendo, Rússia e Geórgia — permite apregoar que as atuais guerras cibernéticas estão ligadas a retaliações ou antecedem, sem efeitos

cinéticos comprovados, ofensivas terrestres contra Estados. É possível ainda declarar, em favor da guerra cibernética, que, quanto mais um país estiver “plugado” ao ciberespaço, especialmente no que tange a suas estruturas estratégicas, mais vulnerável estará para ataques originados no ciberespaço.

Finalmente, em virtudes das limitações expostas nesse estudo sobre o impacto revolucionário da guerra cibernética, chama-se atenção para a importância de se pensar, de forma crítica, a incorporação do ciberespaço como novo domínio. Em contrapartida, argumenta-se aqui que tal ceticismo não deve produzir o efeito de negar a realidade da guerra no ambiente cibernético ou de não o levar em conta em suas estratégias, especialmente no que toca as potencialidades de emprego como arma combinada.

REFERÊNCIAS

APPLEGATE, Scott D.. *The Dawn of Kinetic Cyber*. Center for Secure Information Systems. Fairfax, VA [or V.A.]. 2013. Disponível em: <https://www.academia.edu/2376951/The_Dawn_of_Kinetic_Cyber>. Acesso em: 05 abr. 2019.

ASMUS, Ronald D. *A Little War That Shook the World*. New York: Palgrave-MacMillan, 2010. 167.

BENDER, Jason M.. *The Cyberspace Operations Planner: Challenges to Education and Understanding of Offensive Cyberspace Operations.* Small Wars Journal 9, no. 11 (November2013). Disponível em: <https://smallwarsjournal.com/jrnl/art/the-cyberspace-operations-planner>. Acesso em: 27 abr. 2019.

BRETT REISTER. *Cyberspace: Regional and Global Perspectives.* Strategic Research Project, (Carlisle Barracks, PA: U.S. Army War College), 2012. Disponível em: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a561780.pdf>. Acesso em: 27 abr. 2019.

BUMGARNER, John; BORG, Scott. *Overview by the USCCU of the Cyber Campaign Against Georgia in August of 2008*. U.S. Cyber Consequence Unit Special Report, Aug. 2009.

CARR, Jeffrey. *Inside Cyber Warfare* (Sebastopol, CA, O'Reilly Media, Inc., 2010), p. 121-30. Disponível em: <https://wikileaks.org/sony/docs/05/docs/eBooks/Inside_Cyber_Warfare.pdf>. Acesso em: 20 mai. 2019.

CLARKE, Richard A.; KNAKE, Robert K.. *Guerra Cibernética: A próxima ameaça à segurança e o que fazer a respeito*. Tradução de Bruno Salgado Guimarães, Davidson Rodrigo Boccardo, Rafael Soares Ferreira, Raphael Carlos Santos Machado e Ricardo Salvatore. Brasport Livros e Multimídia Ltda., 2015. Título original: Cyber War: The next threat to national security and what to do about it.

CORBETT, Julian S.. *Some Principles of Maritime Strategy*. New York: Dover Publications, 2004.

CORNELL, Svante; STARR, S. Frederick. Eds.. *The Guns of August 2008: Russia's War in Georgia*, London, UK: M. E. Sharpe, 2009. 166-168.

DAVID Bertold's son. *Interview*, August 2008.

DAVIS, Joshua. *Hackers Take Down the Most Wired Country in Europe*. *WIRED*. 21 August 2007. Disponível em: <http://www.wired.com/2007/08/ff-estonia/>. Acesso em: 05 abr. 2019.

DANCHEV, Dancho. *Coordinated Russia vs. Georgia Cyber Attack in Progress*. *ZDNet*, 11 Aug. 2008. Disponível em: <https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/>. Acesso em: 27 jun. 2019.

DOUHET, Giulio. *The Command of the Air*. Translated by Dino Ferrari. Washington, DC: Office of the Air Force History, 1983. Disponível em: <http://www.airforcemag.com/MagazineArchive/Documents/2013/April%202013/0413keeperfull.pdf>. Acesso em: 25 abr. 2019.

FARWELL, James P.; ROHOZINSKI, Rafal. *Stuxnet and the Future of Cyber War Online*. IISS. London, England. International Institute for Strategic Studies. 28 January 2011. Disponível em: <https://pdfs.semanticscholar.org/b09a/12b798cf0a4613eceee0e506e8a844fee089.pdf>. Acesso em: 05 abr. 2019.

FERNANDEZ, John D.; FERNANDEZ, Andres E. "SCADA systems: vulnerabilities and remediation*", Journal of Computing Sciences in Colleges* 20, no. 4 (April 2005): p. 160-68.

FITZGERALD, Bem; WRIGHT, Parker. *Digital Theaters: Decentralizing Cyber Command and Control*. Disruptive Defense Papers, (Washington, DC: Center for a New American Security, April, 2014), 9-10. Disponível em: <https://www.cnas.org/publications/reports/digital-theaters-decentralizing-cyber-command-and-control>. Acesso em: 25 abr. 2019.

GEORGE, Julie A.. *The Politics of Ethnic Separatism in Russia and Georgia*. New York, NY [or N.Y.]: Palgrave Macmillan, 2009. 181.

GUDERIAN, Heinz. *Achtung-Panzer!, The development of Tank warfare*. Translated by Christopher Duffy. London: Brockhampton Press, 1999.

HOLLIS, David. *Cyberwar Case Study: Georgia 2008*. Small Wars Journal. Small Wars Foundation, (6 January, 2011): 1-10.

JOSHUA, Davis. "Hackers Take Down the Most Wired Country in Europe." *WIRED*. 21 August 2007. Disponível em: <http://www.wired.com/2007/08/ff-estonia/"DDoS Attack Timeline: The History and Changing Nature of DDoS Attacks." Defense.net. 2014>. Acesso em: 05 mai. 2019.

KEIZER, Gregg. *Russian Hacker 'Militia' Mobilizes to Attack Georgia*. *Network World*. 13 August 2008. Disponível em: <https://www.computerworld.com/article/2532365/russian-hacker--militia--mobilizes-to-attack-georgia.html>. Acesso em: 02 abr. 2019.

MARKOFF, John. *Before the Gunfire, Cyberattacks*. New York Times, 12 August 2008. Disponível em: <http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1>. Acesso em: 02 abr. 2019.

MITCHELL, William E.. *Winged Defense: The Development and Possibilities of Modern Air Power—Economic and Militaty*, 2d ed., Tuscaloosa, AL: University of Alabama Press, 2010.

MIRKOVIC, Jelena; REIHER, Peter. *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM SIGCOMM* Computer Communication Review 34, no. 2, April 2004, 1-12. Disponível em: <https://www.isi.edu/~mirkovic/publications/ucla_tech_report_020018.pdf>. Acesso em: 05 mai. 2019.

MYERS, Elizabeth A.. *Cyber as a "Team Sport": Operationalizing a Whole-of-Govermnent Approach to Cyberspace Operations. Master's Thesis*. (Norfolk, VA: Joint Advanced Warfighting School, 2011).

NAZARIO, Jose. *Georgia DDoS Attacks—A Quick Summary of Observations*. Arbor SERT (Security engineering and response team), 12 Aug. 2008.

RAMSBY, Corey M.; YANNAKOGEORGOS, Panayotis A.. *A Reality Check on a Cyber Force*. Strategic Studies Quarterlj 10, no. 2: 116-133. International Security & Counter TerrorLcnz Reference Center, EBSCOhost (accessed September 1, 2016). Disponível em: <https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-10_Issue-2/Yannakogeorgos.pdf>. Acesso em: 25 abr. 2019.

REHMAN, Scheherazade. "Estonia's Lessons in Cyberwarfare." *US News & World Report*. January 2014. Disponível em: <http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare>. Acesso em: 05 mai. 2019.

REILLY, Jeffrey M.. *Multidomain Operations: A Subtle but Significant Transition in Military Thought*. Air and Space Power Journal 30, Issue I (Spring 2016): 61-73. Disponível em: <https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-30_Issue-1/ASPJ-Spring-2016.pdf>. Acesso em: 28 abr. 2019.

RICH, Paul. Ed.. *Crisis in the Caucasus: Russia, Georgia and the West*, Oxon. UK: Routledge, 2010.

RICHARD J. Bailey, Jr.. *Dilating Pupils: The Pedagogy of Cyber Power and the Encouragement of Strategic Thought*. Air and Space Power Journal Africa & Francophonie,7, Issue 3 (Fall 2016).

ROGERS, Michael S.. *An interview with Michael S. Rogers*. JFQ: Joint Force Quarterly. no. 80 (2016, 1st Quarter 2016), 78-85. Disponível em: <https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643105/an-interview-with-michael-s-rogers/>. Acesso em: 25 abr. 2019.

SCHMIDT, Andreas. *The Estonian Cyberattacks*. In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Edited by Jason Healey. Cyber Conflict Studies Association, 2013. Disponível em: <https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks>. Acesso em: 25 abr. 2019.

SINGER, Peter W.. *The War of Zeros and Ones*. Popular Science, September, 2014, 40-46. Disponível em: <https://www.popsci.com/article/technology/war-zeros-and-ones/>. Acesso em: 25 abr. 2019.

SINGER, Peter W.; FRIEDMAN, Allan. *Segurança e Guerra Cibernéticas: o que todos precisam saber*. Tradução de Geraldo Alves Portilho Junior. Biblioteca do Exército, 2017. Título original: Cybersecurity and Cyberwar: what everyone needs to know, 2014.

STARBUCK, F. Randall. *Outlines the challenges of the different C2 architectures for U.S. airpower during Operation Torch in his thesis, Airpower in North Africa, 1942- 43: An Additional Perspective*, (Carlisle Barracks, PA: U.S. Army War College, 1992). Disponível em: <https://www.scribd.com/read/259900391/Air-Power-In-North-Africa-1942-43-An-Additional-Perspective#>. Acesso em: 25 abr. 2019.

TATE, Ryan. *Maximizing Flexibility: Mitigating Institutionalized Risk in the Cyber Mission Force*. The Cvber Defense Review (June, 2016).

TIKK, Eneken. et al. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Cooperative Cyber Defense Center of Excellence, Tallinn, Estonia, November 2008. Disponível em: <http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf. 4>. Acesso em: 02 abr. 2019.

UNITED STATES. Air Force. *Air Force Cyber Command Strategic Vision*. Air Force Cyber Command (Barksdale AFB, LA [or L.A.], February 2008).

_____. Chairman of the Joint Chiefs of Staff. *Joint Operations*. Joint Publication 3-0. Washington. DC: U.S. Joint Chiefs of Staff, August 11, 2011a. Disponível em: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910>. Acesso em: 25 abr. 2019.

_____. Congress. Senate. Armed Services Committee. *Statement of Admiral Michael S. Rogers, USN. Commander*, United States Cyber Command. 114th Cong., 2nd sess., April 5, 2016a. Disponível em: <https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf>. Acesso em: 25 abr. 2019.

_____. *Cyberspace Operations*, Joint Publication 3-12 (R). Washington, DC: U.S. Joint Chiefs of Staff, February 5, 2013. IV-9.

_____. Department of Defense. *Quadrennial Defense Review*, Washington DC: U.S. Department of Defense, 2014a, 33. Disponível em: <https://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf>. Acesso em: 25 abr. 2019.

_____. Department of Defense. *Mission Analysis for Cyber Operations of Department of Defense*. Washington, DC: U.S. Department of Defense, August 2014b. Disponível em: <https://info.publicintelligence.net/DoD-CyberMissionAnalysis.pdf>. Acesso em: 25 abr. 2019.

_____. *Departament of Defense Strategy for Operating in Cyberspace*, (Washington, DC: U.S. Department of Defense), July 2011b. Disponível em: <https://csrc.nist.gov/presentations/2011/department-of-defense-strategy-for-operating-in-cy>. Acesso em: 25 abr. 2019.

_____. *Join Operating Environment 2035*. Washington, DC. Joint Chiefs of Staff, July 14, 2016b. 15. Disponível em: <https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917>. Acesso em: 28 abr. 2019.

_____. Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*, (Washington, DC: U.S Joint Chiefs of Staff, November 8, 2010 (As Amended Through February 15, 2016)). Disponível em: <https://fas.org/irp/doddir/dod/jp1_02.pdf>. Acesso em: 25 abr. 2019.

ULLRICHA, Johannes B.; LAMB, Jason. *Defacing websites via SQL injection*. *Network Security*, vol. 2008, issue 1, January 2008, p. 910.

WILLIAMS, Brett T. *The Propositions Regarding Cyberspace Operations*. JFQ: Joint Force Quarterly. no. 61 (2nd Quarter), 2011. 10-17. Disponível em: <https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-61.pdf>. Acesso em: 27 abr. 2019.

WORLD ECONOMIC FORUM. *Network Readiness Index*. 2015. Disponível em: <http://reports.weforum.org/global-information-technology-report-2015/network-readiness-index/>. Acesso em: 05 abr. 2019.