ESCOLA DE GUERRA NAVAL

CEMOS 2018

A ASSIMETRIA NA GUERRA CIBERNÉTICA: estudo de caso sobre os ataques cibernéticos na Estônia 2007, Georgia 2008 e EUA 2009.

Rio de Janeiro

2018

CC DOUGLAS VICENTE HEMERLY

A ASSIMETRIA NA GUERRA CIBERNÉTICA: estudo de caso sobre os ataques cibernéticos na Estônia 2007, Georgia 2008 e EUA 2009.

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

Orientador: CMG(RM1-FN) William A. Rosa

Rio de Janeiro

Escola de Guerra Naval

2018

AGRADECIMENTOS

Agradeço a Deus por permitir-me, com saúde e disposição, superar os desafios que se apresentam.

À minha esposa, Vanessa, e minha filha, Luana, pelo amor e incondicional apoio ao longo de todo o curso.

Ao meu orientador CMG(RM1-FN) William A. Rosa e ao CF Eugenio C. Huguenin, pelos seus atributos pessoais e pela oportunidade de valer-me dos seus conhecimentos.

À Escola de Guerra Naval, bem como à Marinha do Brasil, por conceder-me esta oportunidade.

RESUMO

Atualmente, o mundo encontra-se digital e devido à criação da Internet e ao desenvolvimento tecnológico, as informações e dados são transportados com rapidez e compartilhados em quantidades cada vez maiores. Essas características encurtaram distâncias e permitiram maior fluidez nas relações pessoais e entre diversas organizações. Foi nesse ambiente que surgiu a guerra cibernética. Nesse estudo serão abordados seus princípios e fundamentos teóricos, bem como apresentados ataques cibernéticos com características de assimetria. Para tal, os conceitos de assimetria também foram estudados e suas características serviram de base para o estudo de caso, que é o objeto desse trabalho, em que foram observados alguns ataques cibernéticos, ocorridos a partir dos anos 2000 e que apresentaram características de assimetria. Por fim, buscou-se demonstrar a importância do tema para o Estado de forma geral.

Palavras-chave: Guerra Cibernética. Assimetria. Internet. Estônia. Georgia. Estados Unidos da América.

LISTA DE ABREVIATURAS E SIGLAS

ARPA	*Advanced Research Projects Agency*
DDoS	*Distributed Denial of Service*
EUA	Estados Unidos da América
MIT	*Massachusetts Institute University*
TI	Tecnologia de Informação
TIC	Tecnologia de Informação e Comunicação
URSS	União das Repúblicas Socialistas Soviéticas

SUMÁRIO

1 INTRODUÇÃO

Atualmente, a ameaça deixou de estar exatamente próxima ao inimigo e as fronteiras dos territórios já são penetradas sem o atacante ser detectado. As operações militares convencionais que ocorrem no espaço e no tempo, e de forma bem definida, estão sendo afetadas pelas ameaças assimétricas que são menos dispendiosas e podem causar grande impacto. O exemplo disso foi a utilização de aviões civis, como ocorrido no 11 de setembro de 2001, como meios para realizar um ataque, conduzido por grupos localizados a milhares de quilômetros de distância e com gastos relativamente pequenos, em relação ao prejuízo que infligiu.

Desde a década dos anos 1990, a Tecnologia de Informação e Comunicação (TIC) desenvolveu-se muito rapidamente. A TIC, de apenas uma ferramenta administrativa, cujo objetivo seria realizar processos administrativos, tornou-se um instrumento de alcance totalmente estratégico para a Indústria, a Gestão e, também, para a Defesa.

A partir desse desenvolvimento da TIC, surgiu a guerra cibernética que realiza um novo modo de conflito, onde é possível corromper as informações, sistemas e tráfego de dados. Foi a partir dos anos 2000 que as ações de guerra começaram a ser percebidas nos conflitos internacionais, em particular, na Estônia (2007), na Geórgia (2008) e nos Estados Unidos da América (EUA), em 2009. Vários Estados despertaram para a necessidade de desenvolver sua defesa cibernética e suas capacidades ofensivas neste novo ambiente operacional.

Outro ponto a ser destacado é a possibilidade de empregar a guerra cibernética estrategicamente, ou seja, atacar diretamente a infraestrutura estratégica de outros Estados, em que o mais fraco, utilizando métodos convencionais teria menos probabilidade de alcançar a vitória, porém, nada impede que o mais forte possa utilizar esse novo método de guerra (ARQUILLA,2013).

É nesse sentido que há a possibilidade em se estudar a guerra cibernética como uma guerra com características de assimetria, onde a introdução de um elemento de ruptura, tecnológico, estratégico ou tático, em termos operacionais, emprega novas capacidades que o oponente não percebe, nem compreende e nem espera.

Durante o conflito entre a Rússia e a Geórgia, em 2008, ataques maciços a servidores governamentais na Geórgia não causaram danos físicos robustos, entretanto, enfraqueceram a estrutura governamental da Geórgia durante o conflito e prejudicaram a sua capacidade de realizar a comunicação com um público nacional e mundial.

A questão a ser investigada é a assimetria, que remete à ideia de desbalanceamento, na qual um oponente obtém resultados muito superiores em relação aos meios empregados, sugerindo haver relação entre as guerras cibernética e assimétrica.

O presente estudo tem como propósito realizar um estudo de caso e demonstrar a assimetria na guerra cibernética, principalmente se forem observadas as características de alguns ataques cibernéticos.

Portanto, a pesquisa será estruturada em uma introdução, três capítulos de análise e uma conclusão. O segundo capítulo abordará os conceitos e fundamentos teóricos de modo a prover uma melhor compreensão do que venha a ser guerra cibernética. Observará não só a definição, mas analisará as suas características e as principais ameaças no ciberespaço. O terceiro capítulo complementará os conceitos apresentados, aprofundando o tema com relação a assimetria no nível operacional. No quarto capítulo, a partir do estudo dos ataques cibernéticos, da Estônia (2007), da Georgia (2008) e dos EUA (2009), verificar-se-á a presença de características de assimetria e no último capítulo, será realizada a conclusão.

2 GUERRA CIBERNÉTICA

Neste capítulo serão examinados os fundamentos teóricos da guerra cibernética que permitirão a compreensão da pesquisa, bem como os conceitos nela adotados. Será composto por seis seções. Na primeira seção será analisada a origem da internet, a qual sem ela, a guerra cibernética não teria existido. Na seção seguinte serão mostrados os conceitos da guerra cibernética.

Na terceira e quarta seção deste capítulo, serão considerados o campo de atuação e as ameaças cibernéticas, respectivamente e na sequência, os objetivos externos. E em sua última seção, será mostrado um exemplo como a guerra cibernética poderia ser utilizada para compensar a inferioridade militar de um Estado.

2.1 ORIGEM DA INTERNET

A Internet[1], criada acidentalmente, foi destinada à resposta do governo norte-americano ao Projeto Sputnik da ex-União das Repúblicas Socialistas Soviéticas (URSS), durante a Guerra Fria, em 1957. Foi chamada de Arpanet e teve como finalidade, preservar as comunicações das bases militares dos Estados Unidos da América (EUA) (GILES, 2010).

O intuito era prover um sistema de comunicação confiável em rede e de informação. O que se pretendia era que ambos os sistemas deveriam proteger-se a um ataque nuclear e que não houvesse perda de informações entre os centros de produção científica. Julgava-se que todo o tipo de informação estaria vulnerável a um ataque nuclear, se houvesse apenas uma central de computação, em vez de vários pontos conectados em rede (GILES,2010).

Caso os Estados Unidos da América tivessem somente uma central de

[1]A Internet é conhecida como uma grande rede que conecta computadores de vários pontos do mundo e também é chamada de a rede mundial de computadores.

comunicação e informação, e se a então ex-URSS violasse a comunicação da defesa norte americana, a comunicação entraria em colapso, tornando os EUA extremamente frágil a ataques subsequentes.

O início se deu com o departamento de defesa dos EUA, que empregou recursos em pesquisa e desenvolvimento, e com a parceria de universidades de computação criou-se a *Advanced Research Projects Agency* (ARPA[2]), que seria Agência de Projetos de Pesquisa Avançada, em 1958. Essa Agência criou o Arpanet, por meio de um programa conhecido como *Information Processing Tecniques Office*, Gabinete de Técnicas de Processamento de Informação, em 1962 (CASTELLS, 2003).

O propósito era incentivar a pesquisa em computação participativa. No ano de 1969, as Universidades da Califórnia, situadas em Los Angeles e Santa Bárbara e a Universidade de Utah se conectaram ao Arpanet. Imediatamente nos dois anos seguintes, em 1971, esses centros já possuíam 15 nós de conexão (CASTELLS, 2003).

Por conseguinte, os alunos do Departamento de Computação da *Massachusetts Institute University* (MIT) utilizavam esses terminais e aproveitavam esse compartilhamento, pois permitia a comunicação entre os usuários, formando uma coletividade, que provavelmente foi o início da Internet que se conhece hoje (DERTOUZOS, 1997).

Com o passar do tempo, a conexão da Arpanet foi cedida para outras pessoas que não pertenciam a comunidade acadêmica, no intuito de proporcionar a utilização de correio eletrônico o que possibilitou a troca de arquivos e comunicações (DERTOUZOS, 1997).

Então, a partir de um projeto militar de comunicação, utilizando uma rede de computadores e depois liberado para uso de civis, se iniciou o que conhecemos de internet.

[2] A ARPA foi criada em 1958 com a finalidade de mobilizar recursos de pesquisa, particularmente do mundo universitário, com o objetivo de alcançar superioridade tecnológica militar em relação à União Soviética na esteira do lançamento do primeiro Sputnik em 1957 (CASTELLS, 2003, p.82).

2.2 CONCEITO DA GUERRA CIBERNÉTICA

De acordo com Clausewitz (1996), a guerra é mais do que um animal que se adequa rapidamente suas características ao meio que se encontra. Seus aspectos dominantes sempre fazem da guerra uma tríade composta da violência primitiva, ódio e inimizade. Esses fatores devem ser julgados como uma força natural cega; do jogo de chance e probabilidade em que o espírito criativo está livre para vagar.

Com o passar do tempo e com a liberdade de criação e utilização da informática, surgiram novas ameaças e vulnerabilidades comprometendo a paz e a segurança internacional. Inevitavelmente, em 1969 surgiu a primeira rede de computadores, Arpanet. Era um programa militar de comunicação e, tendo em vista que era manipulado por instituições não militares, acabou evoluindo para a criação de uma grande rede, conhecida como a Internet.

Os autores Knake e Clarke (2015) conceituam a guerra cibernética como aquelas ações realizadas por Estados para ingressar em computadores e redes de outro Estado com a finalidade de causar danos ou neutralizá-la. Destaca-se, ainda que sejam concreta, veloz e universal, ultrapassa o campo de batalha e já iniciou. Esse termo de guerra cibernética pode ser utilizado para apontar ataques, retaliações e intrusão não ilícita num computador ou numa rede.

De acordo com o glossário das Forças Armadas Brasileiras (MD35-G-01), o conceito de guerra cibernética é o seguinte:

> GUERRA CIBERNÉTICA - Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de Comando e Controle do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar…(BRASIL, 2015, p.134).

De acordo com Barros (2015), a guerra cibernética é bastante complexa e especialmente voltada pela realidade da assimetria e refere-se à ideia de que, por meio de uma ataque cibernético, atores com recursos limitados podem alcançar grandes resultados com

seus ataques. E, ao contrário dos conflitos que ocorrem no mar, no ar e na terra, os guerreiros cibernéticos não usam uniformes e nem bandeiras estampadas. Também pode ser atribuída uma vantagem é a facilidade do desaparecimento do rastro do ataque, gerando a impunidade.

Adicionalmente, a guerra cibernética distingue-se da Guerra Convencional pois caracteriza-se por ações realizadas no espaço cibernético, com consequências no mundo real e no virtual. Pode ser empregada no contexto da guerra da informação, cuja função é buscar dados sobre os pontos fracos do inimigo para atacá-lo (BARROS, 2015).

Como foi visto nesta seção, foram citadas algumas definições sobre a guerra cibernética, porém, tendo em vista que todas as definições são complementares umas das outras e o objeto desse estudo engloba a assimetria, podemos resumir que a guerra cibernética pode ser: as ações realizadas por Estados para ingressar em computadores e redes de outro Estado com a finalidade de causar danos ou neutralizá-la; ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de Comando e Controle do adversário; bastante complexa e especialmente voltada pela realidade da assimetria e refere-se à ideia de que, por meio de uma ataque cibernético, atores com recursos limitados podem alcançar grandes resultados com seus ataques.

2.3 CAMPO DE ATUAÇÃO

Exatamente como outras guerras, a guerra cibernética também tem seu local de atuação e desenvolve-se no chamado Espaço Cibernético. Os elementos que o constitui são os *hardware*[3]*, software*[4] e redes, conectados à internet por qualquer sistema de telecomunicação. Estes elementos juntos transformam-se em uma realidade virtual a qual pode ser dominada

[3]Hardware é a parte física de um computador formada pelos componentes eletrônicos.
[4]Software é uma sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas.

por uma pessoa especializada, conhecida como *hacker*[5] ou Guerreiro Cibernético (BARROS, 2015).

Também, de acordo com Brasil (2014), o espaço cibernético pode ser composto por dispositivos computacionais conectados em redes ou não, em que as informações digitais transitam, são processadas e/ou armazenadas.

Existente em todas as redes de computadores e em tudo aquilo onde se encontram conectadas, ou por elas controladas, o espaço cibernético, ou comumente chamado de ciberespaço, inclui a Internet e várias outras redes de computadores que possivelmente não deveriam estar acessíveis. Esse meio eletrônico, por meio do qual informação é criada, transmitida, recebida, armazenada e processada, pode ser apagada e manipulada, por pessoal especializado.

O ciberespaço é complexo e formado de um ambiente de informações, que consiste de redes interdependentes, de infraestruturas de tecnologias de informação, Internet, redes de telecomunicações, sistemas computacionais, processadores embutidos e controladores (BARROS, 2015).

Outros integrantes do ciberespaço são as chamadas redes transacionais, que desempenham, por meio do envio de dados, fluxos de dinheiro, operações de mercado de ações, transações de cartão de crédito e controle de máquinas. Essas redes privadas são basicamente semelhantes a Internet, mas estão, pelo menos teoricamente, isoladas. Algumas dessas redes possuem um rigoroso sistema de controle que permitem o acesso, somente, às máquinas registradas.

A comunicação com outras máquinas, por exemplo, painéis de controle com bombas hidráulicas, elevadores e geradores, tornam essas redes um local em que os militares podem atuar. Ademais, guerreiros cibernéticos podem utilizar dessas redes para invadir,

[5]*Hacker* é uma palavra em inglês, no âmbito da informática, a qual identifica uma pessoa que possui interesse e um bom conhecimento nessa área, sendo capaz de fazer *hack* (uma modificação) em algum sistema informático.

controlar ou destruir esses equipamentos (CLARKE e KNAKE, 2015).

Em face do ciberespaço consistir de muitos nós e redes diferentes e apesar de nem todos os nós e redes estarem globalmente conectados e acessíveis, é fácil transpor fronteiras geográficas utilizando a Internet. Entretanto, podem ser isoladas utilizando-se protocolos, firewalls[6], criptografia e separação física de outras redes.

Atualmente, informações também trafegam em redes que interligam aeronaves, embarcações, bases locais de apoio e centros estratégicos de controle, podendo estar localizados no país de origem, ou não. Empenhar-se em invadir essas redes com a finalidade de coletar ou buscar informações sensíveis ou confidenciais estão dentro dos objetivos do que se chama "Guerra Cibernética".

O Ciberespaço pode ser considerado um domínio peculiar, ainda não compreendido em toda sua extensão, porém, similarmente igual aos domínios comuns da guerra como no mar, na terra e no ar, e sendo diferente por ser um domínio físico encontrado na natureza, permite a liberdade de conexões, se tornando imprevisível (BARROS, 2015).

2.4 AMEAÇAS CIBERNÉTICAS

Com o desenvolvimento da tecnologia, o mundo está cada vez mais dependente da informática e consequentemente utilizando o ciberespaço para suas tarefas. A chamada "nuvem"[7], também componente do ciberespaço, tornam as negociações, controle de sistemas mais velozes e descomplicados. Mas, concomitantemente, essa interação digital também se observa o aumento da exposição e do risco de ataques, assim como os custos gerados pela violação de dados.

As informações podem ser violadas pela perda da integridade a qual está

[6]Um firewall (em português: parede de fogo) é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
[7]O conceito de computação em nuvem (em inglês, cloud computing) refere-se à utilização da memória e da capacidade de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da Internet

relacionada diretamente com a conversão indesejada dos dados dos sistemas de informação, resultando em ambiguidade ou imprecisão. A perda de disponibilidade também pode ser uma violação, pois torna indisponível para os usuários autorizados aquela informação necessária naquele momento. A confidencialidade, uma outra violação, poderá ser perdida também quando ocorre o acesso não autorizado nos sistemas de informação. Essa ameaça pode até afetar a segurança nacional, quando informações importantes são colhidas pelo inimigo (CLARKE e KNAKE, 2015).

No ciberespaço, as ameaças não são originárias apenas de aficionados da informática que dominam os sistemas de Tecnologias de Informação (TI) em busca do conhecimento ou de se tornarem celebridades, normalmente denominados de *hackers*, mas de oponentes mais eficientes, ou, pelo menos, com uma estrutura e experiência robusta. As ameaças mais perigosas provêm de criminosos, terroristas e Estados competidores, motivados por interesses políticos, ideológicos e financeiros (BOLENG; SCHWEITZER; GIBSON, 2008).

Portanto, faz-se necessário conhecer os principais atores que vivem no ciberespaço, para que seja possível aferir o grau de ameaça que cada um representa.

O elemento mais relevante que atua no espaço cibernético, em função de sua insuperável capacidade de recursos, é o Estado. Comparando com os demais atores, o Estado é o único que possui grande capacidade de atuar nesse ambiente. Pode ser considerado o único elemento com grande capacidade de desenvolver ferramentas para se contrapor a ataques com elevado grau de sofisticação, em face dos elevados custos envolvidos (BARROS, 2015).

Na guerra cibernética, existe também o ativismo cibernético, conhecido também por seu nome em inglês – *hacktivism*, sendo compreendido como a utilização das ações cibernéticas a fim de promover uma mudança política ou social (LACHOW, 2009).

De acordo com Lachow (2009), esses atos de ativismo cibernético buscam resultados idênticos aos obtidos pelo ativismo regular ou atos de desobediência civil, provenientes de ataques de recusa de serviço ou por meio de alteração de sítios da Internet.

Um *hacker* moderno está intimamente conectado à exploração de erros e/ou falhas que existem em código de sistemas operacionais de um computador, de modo a alcançar o acesso a sistemas, a exploração e ataque dos mesmos.

A última ameaça a ser analisada é o elemento interno que introduz uma vulnerabilidade operacional, como por exemplo o acesso ao *hacker* por meio de um projeto, desenvolvimento, teste, distribuição, operação ou manutenção de um software (CSIS, 2008).

2.5 OBJETIVOS EXTERNOS

A guerra cibernética pode ser usada para vários motivos e o que se deve ter em mente é de que o propósito mais abundante é a conquista de efeitos que transcendam o domínio cibernético, de forma que a guerra cibernética contribuía para a condução de operações militares. A guerra cibernética poderá ser usada para se alcançar efeitos nos domínios físico e cognitivo da guerra.

De acordo como Manual de Campanha de Operações de Informação do Exército Brasileiro (EB20-MC-10.213),

> O ambiente operacional é a composição de condições, circunstâncias e influências que afetam o emprego de recursos e apoiam as decisões do comandante, abrangendo áreas físicas e fatores relativos aos domínios marítimo, terrestre e aereoespacial, aspectos humanos, bem como a dimensão informacional, que inclui o espaço cibernético. Tradicionalmente, o foco da análise do ambiente operacional era concentrado na dimensão física, considerando a preponderância dos fatores terreno e condições meteorológicas nas operações. As variações no caráter e na natureza do conflito, resultantes das mudanças tecnológicas e sociais, impõem uma visão que também considere as influências das dimensões humana e informacional nas operações militares e vice-versa (BRASIL, 2014, p.13).

Segundo Nye (2010), em função da diminuição dos custos de processamento e da

transmissão de dados, houve uma revolução da informação, com aumento da velocidade do fluxo de informações trafegadas. Em decorrência desse fato, atores iniciaram as suas ações, considerados até pouco expressivos, o acesso ao ciberespaço e a capacidade de manipular informações.

Complementando, a análise do comportamento caracterizou o poder cibernético pela utilização dos recursos informacionais, conectados por meio de redes, através do ciberespaço, para atingir um determinado objetivo além dos resultados apenas utilizados no ciberespaço (NYE, 2010).

Com isso, pode se entender que o controle dos recursos do poder cibernético concede a manipulação de recursos de poder, tanto no ciberespaço e tanto nas dimensões físicas (mar, ar e terra), bem como na dimensão informacional e humana, que poderá facilmente decidir uma vantagem de uma operação militar e beneficiar ao atingimento dos seus objetivos.

2.6 DESPERTAR DA CHINA APÓS A TEMPESTADE DO DESERTO

Nesta seção será descrito um exemplo de uma nação que verificou a necessidade de se implementar e estar atenta às mudanças tecnológicas no campo da guerra e a assimetria a seu favor.

Sabe-se que a primeira Guerra do Golfo (1991-91) foi a seguinte grande guerra em que os EUA participaram desde o Vietnã. Conhecida como Tempestade no Deserto, outros 30 Estados se juntaram para combater Saddam Hussein, reunindo quase quatro mil aeronaves, 12 mil tanques e dois milhões de militares. Esta guerra foi considerada também como o despertar de um novo tipo de guerra, dominada por computador e por outros dispositivos de alta tecnologia.

Apesar de os militares dos EUA não estarem prontos para usarem a guerra

cibernética contra o Iraque, utilizaram as redes de computadores para atingir o inimigo. Além disso, estavam armados com uma nova geração de armas, tal como as bombas inteligentes, que tinham o propósito de reduzir o número de missões, ao acertarem com precisão o alvo.

A China ao assistir a vários documentários sobre a utilização dessas bombas inteligentes, a aniquilação de seu arsenal utilizado pelo Iraque, provou que estavam atrasados em tecnologia. Por um período de vários anos, observaram que a estratégia em derrotar os EUA por superioridade numérica não seria interessante e por este motivo, começaram a reduzir as suas forças armadas e investir em novas tecnologias.

A nova tecnologia estudada foi a rede de computadores e o principal argumento utilizado seria que o país inimigo pode receber um golpe paralisante por meio da Internet e que a força superior que perder o domínio da informação será esmagada, enquanto a inferior aproveitá-la será capaz de vencer (CLARKE e KNAKE, 2015).

Os estrategistas chineses descobriram que a melhor ideia seria convergir para a guerra cibernética para compensar as deficiências qualitativas militares. Os chineses poderiam desafiar o controle norte americano através da criação de meios que derrubassem satélites e invasões das redes de computadores. A ideia seria possibilitar tirar proveito de fraquezas de um inimigo com aparente capacidade superior, que ignore as tradicionais de conflito.

Em 2009, o Almirante Mike Mullen, Chefe do Estado Maior Conjunto à época, num discurso na Liga da Marinha, informou que a China estaria se desenvolvendo em capacidades, tanto no ambiente aéreo, como no marinho. Apesar de terem desenvolvido radares de longo alcance, mísseis antinavios mais rápidos que os sistemas de defesa, aquisição de porta-aviões e possuírem mais de dois mil mísseis posicionados ao longo de sua costa, não é suficiente para combater as forças dos EUA. A perspectiva é de que a China está no mínimo a uma década de atraso, sendo capaz de apenas derrotar de forma convincente apenas um inimigo de tamanho moderado, como o Vietnã (CLARKE e KNAKE, 2015).

A vitória então, nesse pensamento, poderia ser conseguida ao menos que sejam capazes de progredir na guerra cibernética, contra equipamentos militares, tais como um porta-aviões americano. Seria a maneira de contornar o campo de batalha, não com armas convencionais, mas sim de forma assimétrica.

3 AMEAÇA ASSIMÉTRICA

Para um melhor entendimento do que se pretende nesse estudo, a assimetria deverá ser estudada e neste capítulo serão examinados os fundamentos teóricos e será dividido em três seções as quais tratarão de seus conceitos iniciais, suas principais características e a assimetria em rede.

3.1 ASSIMETRIA

De acordo com Visacro (2009), desde o fim da Segunda Guerra Mundial, em 1945, ocorreram mais de 80 guerras de natureza assimétrica e 96% dos conflitos transcorridos durante a década de 1990 foram assimétricos. Com grande frequência, esse tipo de guerra desenvolve-se sem que seja declarada, reconhecida ou sequer percebida. Muitas vezes é oculta, porém é invariavelmente não compreendida pelo Estado e por diferentes segmentos da sociedade civil.

O glossário das Forças Armadas Brasileiras (MD35-G-01) define o conceito de Ameaça Assimétrica como sendo:

> AMEAÇA ASSIMÉTRICA - Ameaça decorrente da possibilidade de serem empregados meios ou métodos não ortodoxos, que incluem terrorismo, ataques cibernéticos, armas convencionais avançadas e armas de destruição em massa para anular ou neutralizar os pontos fortes de um adversário, explorando suas fraquezas, a fim de obter um resultado desproporcional (BRASIL, 2015, p.25).

A guerra assimétrica pode naturalmente ser realizada entre dois Estados com recursos militares e econômicos diferentes, bem como um combate entre indivíduos, grupos e comunidades. Geralmente, os conflitos assimétricos se caracterizam pela inferioridade bélica convencional, principalmente na fase inicial de organização e expansão.

Em termos gerais, esta é a percepção comum, especialmente a ideia do desbalanceamento extremo das forças entre os combatentes. No entanto, este entendimento não tem forte sustento, pois nem sempre foi o recurso do mais fraco.

É provável que o combate bíblico assimétrico entre David e Golias seja o responsável por essa percepção, porém, a assimetria não estava sustentada na diferença de forças. O que ocorreu foi a maneira não ortodoxa de emprego da funda[8] contra a espada e a armadura, o que permitiu ao israelense atingir diretamente o centro de gravidade de Golias através da única vulnerabilidade crítica: sua cabeça não protegida.

Outra oportunidade da assimetria é o ataque fulminante, numa campanha rápida, a qual permite atingir seu propósito, sem contar em seus estágios de desenvolvimentos com os meios necessários para a uma guerra longa (VISACRO, 2009).

3.2 PRINCIPAIS CARACTERÍSTICAS

As assimetrias utilizadas em conflitos apenas não se distinguem das guerras convencionais pelo simples comportamento e pelos hábitos bélicos, como uso de uniformes, disciplina e hierarquia. Podem ser consideradas várias características, como a seguir:

Disposição não militar

A guerra irregular, cercada de assimetria, é considerada a forma mais antiga de se combater e, desde a década dos anos de 1950, pode se dizer que é a mais usual. Muitos analistas políticos e militares manifestaram-se estimando que esse tipo de luta predominará sobre os tradicionais métodos beligerantes (VISACRO, 2009).

[8]arma de arremesso constituída por uma correia, ou corda dobrada, em cujo centro é colocado o objeto que se deseja lançar.

Segundo Cambeses (2003), existe uma predisposição, por parte das potências dominantes, em conduzir os combates armados como uma guerra regular. No entanto, o inimigo pode não ser um Estado constituído e muito menos completamente visível, dando lugar à assimetria como o principal meio de se chegar ao desejado.

Corroborando com o citado anteriormente, Bishara (2001) cita que um país, ao possuir superioridade de forças, de riquezas, de tecnologia e outras formas que lhe possibilite uma vantagem competitiva estratégica, geralmente, optará pelo tipo de guerra regular para solucionar os seus conflitos. Porém, ao contrário, o seu adversário poderá explorar as formas de luta não convencionais. A assimetria será utilizada para combatê-lo, concentrando as ações de ataque nos seus pontos vulneráveis, assim evitando as suas forças.

A exemplo, Visacro (2009) discorre que no ano 73 a. C. um gladiador chamado de Spartacus comandou uma das mais importantes lutas da Roma Antiga. Liderou um exército de escravos contra seus mestres e acabou derrotando sete expedições militares destinadas a sufocar a revolta que havia perdurado por anos. Spartacus havia se tornado um símbolo da revolta armada e para derrotá-lo, Pompeu necessitou mobilizar um contingente de dezenas de milhares de legionários.

Em termos operacionais, um conflito pode ter características de assimetria quando for conduzido por uma força que não dispõe de organização militar formal e de legitimidade jurídica institucional.

Preponderância dos processos indiretos

Quase sempre, o oponente que utiliza a assimetria possui uma inferioridade bélica em relação ao que utiliza meios convencionais, especialmente em sua fase de inicial de organização. Lutar e combater unidades regulares, que muitas das vezes possuem um poder de combate muito superior ou até mesmo tentar destruir objetivos vitais do inimigo, se torna

impossível obter sucesso.

Grupos que se utilizam de assimetria conservam suas energias não combatendo diretamente, tendo em vista que não gozam de poder superior em relação as forças regulares. Adotam a postura de atacar e fugir, principalmente nos estágios finais onde o declínio do inimigo está se tornando evidente (VISACRO, 2009).

Essas forças assimétricas também atuam por processos indiretos quando investem na educação de jovens e crianças em escolas próprias, como pode ser exemplificado, o Hamas e o Hezbolla, em que são passadas para essas gerações as ideologias de seu partidismo.

Estratégia prolongada

De acordo com as ideias de Clausewitz (1996) o objetivo de qualquer guerra é desarmar o inimigo, colocando-o em uma situação permanentemente desfavorável para que ele se submeta à nossa vontade.

Na guerra assimétrica, o objetivo central é a imobilização operacional do inimigo, visando a minimizar as diferenças que lhe são favoráveis, abalando-o moralmente, exaurindo as suas forças, desgastando-o internamente, até que esteja enfraquecido, não só fisicamente como psicologicamente, se tornando incapaz de reagir.

É natural que a sociedade esteja disposta a apoiar a campanha militar em virtude de possuir a credibilidade que poderá vencer com uma certa rapidez. Porém, quando esse conflito se torna prolongado, com o consumo grande de recursos orçamentários e também com vidas humanas, começa a se tornar impopular. Isso faz com que o Estado comece a perder o apoio da opinião pública.

Ao contrário, as forças que utilizam a assimetria procuram fazer do tempo um aliado principal. Dependendo da situação tática ou do cenário político-militar, as forças

podem utilizar de um período de inatividade, de acordo com sua conveniência, sem prejuízo à sua credibilidade junto a opinião pública.

Alguns exemplos de guerras desumanas que a opinião pública incidiu junto ao Estado foram a retirada dos norte-americanos do Vietnã e os portugueses abrissem mão de suas colônias na África (VISACRO, 2009).

Ações táticas efêmeras

Se no campo estratégico a assimetria tem como característica um aspecto de desgaste prolongado, no campo tático constitui de ações de ataque fulminante, apesar de demandarem um razoável tempo de planejamento e preparação.

Como por exemplo, um ataque a bomba ou um assassinato ocorre em frações de segundo. Ainda que nesses exemplos, apesar de se desenvolverem em um curto espaço de tempo, essas ações podem causar um grande impacto se a natureza do alvo possuir grande valor psicológico e se ainda for empregada a mídia, os efeitos poderão ser potencializados (VISACRO, 2009).

Não-linearidade

Uma outra característica da assimetria é a inexistência de frentes de batalhas, flancos ou retaguarda, tendo em vista que os combates são realizados em função da forma do terreno, da postura da população civil e da disposição espacial das forças do inimigo. Por vários anos, ocorria também operações somente em determinadas áreas restritas, não muito distantes de suas bases de operação (VISACRO, 2009).

Somente a partir dos anos 1960, com o surgimento do terrorismo internacional palestino, as forças assimétricas inciaram os seus ataques em alvos localizados em locais distantes de sua origem. Devido ao desenvolvimento da era digital e pela liberdade das

sociedades abertas, terroristas foram capazes de realizar ataques ignorando distâncias e fronteiras, a exemplo como ocorrido com os atentados de 11 de setembro, contra as torres gêmeas do World Trade Center, em Nova Iorque e contra o Pentágono, em Washington.

Difícil detectabilidade

As forças assimétricas são militarmente frágeis, principalmente em seus estágios de desenvolvimento e para preservarem inicialmente a estrutura organizacional e poucos meios que possuem, desenvolvem suas ações clandestinamente sem serem declaradas. Com mensagens simples e examinando contradições políticas e sociais, formulando reivindicações por justiça e equidade, trabalhando na proximidade de qualquer arcabouço jurídico, esses grupos tendem a legitimar o discurso com aquiescência popular (VISACRO, 2009).

Pode se dizer que os elos políticos existentes nesse tipo de força são obscuras e por conseguinte são difíceis de serem detectáveis. Por não existirem também frentes de batalhas, tampouco uma declaração formal de guerra, o conflito assimétrico torna-se indefinido no tempo e no espaço. Como por exemplo, guerrilheiros, terroristas e outros milicianos, vivendo na clandestinidade ou até mesmo possuindo uma vida normal, podem ser confundidos com a população civil.

Busca de resultados psicológicos

Ações assimétricas estão ligadas na capacidade de provocar forte impacto psicológico e grande repercussão. O evento 11 de setembro nos EUA pode ser considerado um exemplo. A assimetria não está ligada somente ao terrorismo em si, mas sim pelo potencial valor político e psicológico (VISACRO, 2009).

Um outro exemplo ocorreu no ano de 2005, quando forças insurgentes iraquianas realizaram bombardeios noturnos empregando morteiros contra escolas, sem pessoas estarem

presentes. Essas escolas seriam utilizadas como locais de votação e a finalidade desses ataques seria transmitir uma mensagem política de que a população seria compelida a não votar.

Ausência de padrões rígidos de planejamento e execução

Diferentemente da atuação dos soldados profissionais, na assimetria predominam a informalidade de táticas, de técnicas e de procedimentos. Os princípios que caracterizam o planejamento militar não funciona nesse tipo de ameaça. Na assimetria, as ações descentralizadas são concebidas no planejamento mais flexível onde se valoriza a iniciativa da liberdade de ação e da responsabilidade compartilhada.

Taticamente, as ações existem da necessidade de neutralizar o poder superior de combate das forças convencionais. Ainda no começo, as forças assimétricas contam com o poderio bélico pequeno e somente tornará possível a superioridade relativa, quando essa força bélica inferior adquirir a capacidade de realizar uma ação decisiva em um local definido, com tempo limitado (VISACRO, 2009).

De acordo com Visacro,

> As ações assimétricas seguem os seguintes princípios gerais: ataque a pontos fracos; maior familiaridade com ambiente operacional e prévia preparação do terreno; oportunidade da ação obtido pela inteligência e uma rede de informantes estruturada; surpresa obtida pelo sigilo e da manobra; manobra simples e breve; rapidez da ação seguida de uma retirada rápida e planejada; capacidade de inserir efeito psicológico; e motivação de seus militantes (VISACRO, 2009, p.248).

Insubordinação a restrições legais

No conflito assimétrico pode se dizer que não se aplica o direito internacional humanitário e atualmente os exércitos regulares são diretamente ligados às normas legais da guerra, enquanto a assimetria não se sujeita a nenhum tipo de restrição jurídica (VISACRO, 2009).

Individualidade

Por inúmeros anos, as forças regulares combateram em tipo de formação em que seus homens são inseridos lado a lado. Invariavelmente, em face da revolução tecnológica e o contínuo aperfeiçoamento dos sistemas de armas, a guerra tem se tornado mais letal e seus combatentes foram obrigados a vestirem uniformes para se confundirem com um terreno e fugirem da concentração do fogo inimigo. Apesar de ser observada essa evolução e mudança, os combatentes regulares concentram um sentimento de coletividade e espírito de corpo, diferentemente na guerra assimétrica, em que na maior parte das situações, o combatente fica isolado ou opera em grupos pequenos (VISACRO, 2009).

Economia de forças

O combate assimétrico pode ser empregado com intuito de complementar, apoiar ou ampliar operações militares convencionais. A exemplo disso, foi no contexto em que os rebeldes árabes liderados pelo príncipe Faissal tomaram parte da campanha britânica contra os turcos no Oriente Médio durante a Primeira Grande Guerra (VISACRO, 2009).

Um Estado que possua interesse em conduzir uma campanha de conflito poderá obter economia de meios e evitar uma confrontação militar regular, quando patrocinar um grupo que se proponha a realizar uma guerra que possua assimetria. A sua campanha será menos onerosa, arriscada e politicamente desgastada, se comparando com uma guerra convencional.

Desenvolvimento em fases

Visacro (2009) define que a guerra que utiliza a assimetria como base é formada por várias fases, divididas em dois fatores: o nível de maturação das forças e o grau de

deterioração dos cenários político, social e militar:

- ênfase nos trabalhos de organização e expansão;
- primazia de ações clandestinas;
- apoio inconsistente da população; e
- carência de sistema de abastecimento.

Subordinação dos objetivos militares aos objetivos políticos

De acordo com Visacro (2009), independentemente de ser uma guerra assimétrica, guerra é uma guerra e todos os objetivos militares devem se sujeitar integralmente a objetivos políticos. Os aspectos militares são considerados de menor importância e os guerreiros ou combatentes deverão ter consciência disso.

3.3 ASSIMETRIA EM REDE

Nos dias de hoje, as pessoas vivem num mundo rodeado de informações. As informações que dependiam unicamente da boca para serem passadas, foram se modificando e sendo passadas por meio de jornais, revistas, rádio, televisão, e-mails, telefones e que na maioria das vezes são utilizadas ondas de micro-ondas, fibras óticas e satélites para o seu envio.

Nos conflitos modernos, as organizações militares para reunir e controlar uma massa maior e com agilidade necessitam de um incremento de suas comunicações. A Guerra Civil Norte Americana e a Guerra Franco-Prussiana, só foram possíveis terem sido realizadas com dinamismo, graças à utilização do telégrafo. Sem a Internet e satélites, a recente Guerra do Golfo não seria tão favorável aos EUA (THORNTON, 2007).

Entretanto, a utilização dessas novas tecnologias torna o senso de vulnerabilidade incrementado tendo em vista que a maioria dos sistemas de informações são abertos e o

principal meio de condução é pela internet. Para ser eficaz e eficiente, é preciso estar conectado e acessível, e essa característica pode, tanto na esfera civil e militar, permitir efeitos maléficos se forem utilizadas por agentes mal intencionados.

E essa transformação de forças em vulnerabilidades é obviamente o que o guerreiro cibernético está a procura. Esses envolvem como alvo as redes de computadores, sistemas eletrônicos e outras infraestruturas que passam informações de apoio.

De acordo com Thornton (2007), os ataques sobre infraestruturas podem ocorrer em ataques virtuais e físicos e as fontes poderão ser individuais, por grupos e estados:

Ataques visuais - Esse é considerado o mais familiar de todos, pois é travado sobre a internet. Os principais participantes são os hackers que manipulam e perturbam os sistemas de informações para influenciar as percepções dos adversários e o comportamento por meio da interrupção de suas redes de computadores e bancos de dados, com a utilização de vírus de computadores.

Destruições físicas - Usualmente utilizada por militares ou ações terroristas que utilizam armas explosivas que degradam os sistemas de computadores ou fontes de informação.

Fonte individual - nunca houve um tempo em que a guerra estivesse aberta a indivíduos anônimos que estivessem em locais distantes armados com computadores e outros dispositivos eletrônicos e haverá, sem dúvida, indivíduos mais esclarecidos na área de cibernética nos próximos anos que intencionalmente testarão suas habilidades na forma de um ladrão.

Grupos - grupos sub-estatais, como gangues criminosas e organizações terroristas, podem lançar ataques mais coordenados e mais problemáticos, em teoria. Esses podem causar tantos danos quanto qualquer indivíduo, mas suas motivações podem causar distúrbios muito maiores.

Estados - Assim como os EUA, seus aliados encontram-se avançando rapidamente em termos de domínio no campo da informação, no intuito de se tornarem menos suscetíveis a ataques cibernéticos.

De acordo com Barros (2015), os Estados encontram-se preparando e percebendo, uns mais do que os outros, de que o poder cibernético pode ajudar na atuação, no âmbito das relações internacionais, pela busca da dominação da informação, no espaço cibernético e, também, em outros domínios, que se encontram fora do mundo cibernético.

4 ATAQUES CIBERNÉTICOS

A primeira parte deste capítulo consistirá em estudar as características de um ataque cibernético e posteriormente, nas seções seguintes, apresentar três estudos de casos dos ataques cibernéticos ocorridos na Estônia (2007), Georgia (2008) e EUA (2009). Adicionalmente, serão identificados os padrões e os comportamentos dos ataques a fim de possibilitar uma análise de semelhança aos padrões de assimetria e se poderiam ser considerados, esses tipos de ataques, como mais uma arma no arsenal tático da guerra moderna.

4.1 TIPOS DE ATAQUES

De acordo com a Doutrina Militar de Defesa Cibernética (BRASIL, 2014), o ataque cibernético compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente.

Um dos ataques mais conhecidos é o Ataque Distribuído de Negação de Serviço, *Distributed Denial of Service* (DDoS), porém não é uma das mais importante arma do arsenal cibernético, pois simplesmente é gerado um enorme fluxo de tráfego na Internet para derrubar ou congestionar uma rede.

O ataque é realizado de forma a acionar a centenas ou dezenas de milhares de computadores para enviar requisições a um único alvo. Os computadores que são utilizados para atacarem as redes são denominados de *botnet*, podendo ser considerados de zumbis pois são controlados remotamente. Esses zumbis realizam instruções sem os seus proprietários terem o conhecimento. Um indicador que o computador possa estar infectado com esse tipo de vírus é que se torna lento ao acessar páginas da internet e a provável infecção possa ter

ocorrido ao acessar inocentemente uma página ou ter acessado algum programa que possui o referido vírus (CLARKE e KNAKE, 2015).

Muitas das vezes, o computador infectado não inicia automaticamente o envio de requisições a fim de sobrecarregar o site definido e fica aguardando pelas ordens de início pelo guerreiro cibernético ou até mesmo inicia a infecção para outros computadores.

Uma outra vulnerabilidade em que o guerreiro cibernético pode atacar é a aptidão de propagar, pela Internet, tráfego malicioso para o ataque em computadores. Esse tráfego malicioso é composto por vírus e worms[9], que coletivamente são chamados de malware. Pode se aproveitar de uma falha do usuário ou até de fabricante de algum software/hardware. O usuário poderá acessar algum site de internet e por descuido abrir algum programa recebido por e-mail e infectar o computador.

Os worms citados acima, não necessariamente precisam que um usuário passe para outro computador, muitas das vezes eles podem autorreplicar automaticamente para outros computadores, se propagando.

4.2 ESTÔNIA 2007

Um dos ataques cibernéticos bastantes comentados na literatura sobre o assunto foi a série de ataques ocorridos na Estônia em 2007. Esses ataques iniciaram em 27 de abril e afetaram sites de variadas instituições e organizações da Estônia. Todos os bancos comerciais, empresas de telecomunicações, jornais e rádios comerciais foram atacados. Foram causados vários problemas à população e foi considerado como o primeiro ciberataque de grandes proporções (CLARKE e KNAKE, 2015).

Tudo começou quando o Governo da Estônia decidiu remover uma estátua de um soldado de bronze, um sinal das cinco décadas de opressão, pelas quais o povo foi obrigado a

[9] Worms são programas de computador que facilitam a intrusão em sistemas de hardware e roubam informação desses.

passar, pela Rússia. Os ex-soviéticos tinham construído a estátua em 1947 para comemorar os seus mortos em combate depois de terem expulsado as tropas alemãs no final da Segunda Guerra Mundial. Após a guerra, a Estônia transformou-se numa república soviética dirigida por Moscou.

Após ao final da Guerra Fria, a pequena nação Estônia declarou a sua independência e a retirada dessa estátua motivou a Rússia alegar que essa remoção difamaria os heróis mortos, incluindo aqueles enterrados ao redor da estátua. A estátua foi removida e instalada em uma nova localização, protegida em um cemitério militar, o que gerou uma revolta entre os grupos étnicos existentes no país.

A Estônia era um país que apostou e aderiu fortemente às tecnologias da informação. Cerca de 49% da população acessava diariamente jornais online. Mais de 90% das transações bancárias eram realizadas pela internet. Existiam muitos pontos Wi-Fi gratuitos. Os telefones celulares podiam ser utilizados para pagar estacionamentos ou refeições (CLARKE e KNAKE, 2015).

Esta característica do país ter se tornado digital, também o tornou fortemente dependente da Internet, o que motivou os Russos a atuarem no espaço cibernético.

Depois da noite da retirada da estátua de bronze, vários servidores que hospedavam as páginas de internet mais utilizadas na Estônia foram inundadas com pedido de acesso. Alguns dos ataques foram de DDoS, ataques Distribuído de Negação de Serviço. Os hackers usaram várias máquinas comprometidas, chamadas de "*zombis*" e inundaram as referidas páginas com milhares de pedidos por segundo, aumentando enormemente o tráfego. Fundamentalmente, esse tipo de ataque é considerado como uma das armas da guerra cibernética, onde é um dilúvio pré-programado de tráfego para se congestionar uma rede.

Os ataques à Estônia foram efetuados proritariamente por computadores que são estimulados a enviar requisições a várias páginas. Como citado na seção anterior, os

computadores que atacaram são conhecidos por *botnet* ou zumbis os quais atacam sem o conhecimento de seu proprietário.

No início dos ataques, o povo da Estônia achava que a queda das páginas da internet eram resultados de aborrecimento de alguns russos, mas quando alguns dos serviços de cartão de crédito e serviços bancários estavam sendo atingidos, semana após semana, e sendo incapazes de retornarem a operar, a Estônia encaminhou o assunto à apreciação do Conselho do Atlântico Norte a fim de que pudessem ser tomadas medidas para exterminar os ataques(CLARKE e KNAKE, 2015).

Alguns dos ataques foram originados da Rússia, incluindo um do gabinete administrativo do próprio Presidente Putin. Foram observadas que existiam muitas provas circunstanciais que apontavam para a Rússia. Entretanto, a Rússia sempre negou que estivesse acionado esses ataques.

Finalmente, de acordo com a Agência Routers (2009), em 10 de março de 2009, Konstantin Goloskokov, um "comissário" da juventude do grupo Nashi, declarou que era responsável pelo ataque. Os peritos estão céticos quanto a essas variadas assunções de responsabilidade por parte de cidadãos russos.

4.2.1 Análise comparativa

De acordo com o caso apresentado, tudo começou com o entendimento pela Rússia que o governo da Estônia havia realizado uma provocação ao Estado, com a retirada de uma estátua de um soldado de bronze, considerado como um símbolo.

Após esse ocorrido, foram verificados, com características de assimetria, alguns ataques no ciberespaço, tais como o congestionamento de algumas páginas da internet e negação de alguns serviços de cartão de crédito e de serviços bancários. Dentre elas, podemos citar:

- a ausência de padrões rígidos foi verificada quando predominou a informalidade de táticas e ações descentralizadas quando foram atacadas várias páginas da internet e alguns serviços;

- a economia de forças é observada quando, a fim de evitar o confronto numa operação regular, utilizaram hackers, sendo menos oneroso e arriscado;

- a utilização de ações efêmeras e a busca de resultados psicológicos pode ser verificada quando ocorreu a negação de alguns serviços de cartão de crédito e de banco causando aborrecimento à população;

- a não linearidade e adicionalmente a difícil detectabilidade foi observada pela provável suspeita de que os ataques no ciberespaço tenham sido provenientes da Russia, porém não há provas que apontam para essa suspeita;

- a disposição não militar e a individualidade pode ser verificada pela suspeita da participação de um civil, um "comissário" da juventude do grupo Nashi.

4.3 GEORGIA 2008

Ao sul da Rússia e junto ao Mar Negro, fica localizada a República da Geórgia e que em função de sua localização, era considerada como uma área de influência de Moscou. No território da Geórgia encontrava-se a Ossétia do Sul que, em meio a conflitos, tornou-se independente em 1991. Entretanto, a comunidade internacional continuou a reconhecer a Ossétia do Sul como parte da Geórgia. Apesar de ter ocorrido um cessar fogo e numerosos esforços de paz, o conflito continuou sem solução.

No mês de agosto de 2008, a Geórgia e a Ossétia do Sul voltaram a se confrontar. Com a intensificação dos ataques dos georgianos, a Rússia interveio no conflito a favor da Ossétia do Sul, deslocando o seu exército e expulsando os georgianos da Ossétia do Sul. Igualmente ao ataque ocorrido, houve também uma grande movimentação de ataques

cibernéticos contra a Geórgia. Desta forma, tornou-se o primeiro caso em que um conflito internacional político e militar, foi acompanhado, ou mesmo precedido por uma ofensiva de ataques cibernéticos (CLARKE e KNAKE 2015).

Na Geórgia, os ataques ocorreram num contexto de conflito que envolveu russos, georgianos e a Ossétia do Sul. Apesar de estarem entre um ambiente militar real, os ataques foram similares aos da Estônia em 2007, acompanhados de DDoS que acabaram bloqueando sites oficiais como o da página oficial do presidente e do Ministério do Exterior. Sites russos também foram atingidos, assim como páginas da Ossétia do Sul (WATTS, 2008).

De acordo com Melikishvili (2008, 2009), os primeiros ataques cibernéticos ocorreram antes do início da guerra. O site do presidente georgiano (president.gov.ge) sofreu um ataque de negação de serviço, em 20 de julho de 2008, deixando-o inoperante por 24 horas. Esse ataque foi considerado como o precursor de outros ataques de maior envergadura.

Os efeitos destes ataques tiveram grande poder de destruição. Os roteadores que requisitavam as redes da Geórgia, com dados oriundos da Rússia e Turquia, praticamente ficaram inoperantes em virtude dos imensos números de pacotes nas redes, todos criados pelos ataques DDoS com utilização de *botnets*. Os ataques também tiveram como alvo os roteadores de internet que se encontravam na Geórgia e fizeram com que a população não tivesse o acesso à comunicação com o mundo externo, sendo impossível o recebimento de e-mails, notícias e acesso à rede de dados. Foram realizadas tentativas de defesa que não foram eficazes e novos ataques eram realizados a partir de qualquer tentativa de bloqueio (CLARKE e KNAKE, 2015).

Pode se dizer que ataques cibernéticos apresentaram algumas características próprias, relativamente diferentes aos ocorridos à Estônia. Apesar de terem sido utilizados os ataques DDoS, os quais são baseados em *botnets,* no intuito de tornar a identificação mais

difícil, foram substituídos por ataques de injeção SQL[10], uma vez que utilizaram uma quantidade inferior de computadores conectados (SUTTON, 2013).

A proteção cibernética teve como uma de suas ações a de bloquear o tráfego oriundo da Rússia, porém ocorreu o redirecionamento dos ataques pela China. A Georgia transferiu os seus servidores do governo para a Califórnia, nos EUA, para a tentativa de restabelecimento da operação, mas mesmo assim os servidores continuaram a serem alvos de ataques contínuos. A rede bancária foi praticamente neutralizada, além das redes de cartões de crédito e sistemas de telefonia móvel (CLARKE e KNAKE 2015).

Não há provas conclusivas de quem esteve envolvido nos ataques DDoS, tal como no caso dos ataques realizados na Estônia, entretanto a Rússia é apontada como sendo a origem dos ataques. Existe um consenso de que os ataques foram coordenados e os autores estavam devidamente instruídos do que se ia fazer e se deduz que as ações orquestradas nos ataques não seriam possíveis de serem realizadas por patriotas cibernéticos somente baseada no protesto popular (CLARKE e KNAKE 2015).

No ataque cibernético descrito, houve o emprego massivo de DDoS que, somados aos demais métodos primitivos de ataque, permitiram conceber um cenário consideravelmente hostil com a participação de hackers com armas cibernéticas capazes de deteriorar as infraestruturas e atentar contra a Segurança Nacional de um Estado.

Criou-se o desenvolvimento de ações contra os ataques cibernéticos, tal como bloquear o tráfego oriundo de uma região e transferir os servidores para outros locais onde havia redes mais seguras para a normalidade de operação.

[10]A Injeção de SQL (do inglês *SQL Injection*) é um tipo de ameaça de segurança que se aproveita de falhas em sistemas que interagem com bases de dados, em que o atacante consegue inserir instruções SQL personalizadas e indevidas dentro de uma consulta (*SQL query*), por meio da entradas de dados de uma aplicação (ex. formulários).

4.3.1 Análise comparativa

Conforme observado, após um ambiente de conflito entre russos, georgianos e Ossétia do Sul, similarmente aos ataques no ciberataque da Estônia, a Georgia foi atacada e algumas páginas oficiais do governo, páginas de internet e serviços bancários foram negados.

Da mesma forma, características de assimetria foram observadas, dentre elas, podemos citar:

- a ausência de padrões rígidos foi verificada quando predominou a informalidade de táticas e ações descentralizadas, pois foram atacadas várias páginas da Internet e alguns serviços;

- a economia de forças é observada quando, a fim de evitar o confronto numa operação regular, utilizaram hackers, sendo menos oneroso e arriscado;

- a utilização de ações efêmeras e a busca de resultados psicológicos pode ser verificada quando ocorreu a negação de alguns serviços de cartão de crédito e de banco causando aborrecimento à população;

- a não linearidade, adicionada à difícil atribuição da responsabilidade pelo ataque foi observada, pela provável suspeita de que os ataques no ciberespaço tenham sido provenientes da Russia, tendo em vista que as provas não foram conclusivas e a Russia não assumiu o ataque;

- a subordinação dos objetivos militares aos objetivos políticos foi observada quando da possível suspeita de que a Rússia estaria envolvida e os ataques seriam provenientes daquele Estado.

4.4 EUA 2009

Em 2009, no feriado de 04 de julho, um satélite dos EUA detectou um lançamento de foguetes pela Coreia do Norte. Computadores no Colorado informaram que eram de curta distância e que foram lançados do mar e que, ao todo, foram detectados sete foguetes. Esses lançamentos foram uma demonstração de poder ou apenas um grito de atenção?

Saindo da ação no ambiente aéreo, dias antes desse feriado, a ameaça virou-se para o ciberespaço. Uma mensagem codificada foi enviada por meio de um agente norte-coreano para cerca de 40 mil computadores em todo o mundo, realizando a infecção com um vírus *botnet*.

De acordo com Clarke e Knake (2105), esse vírus possuía um conjunto de instruções que ordenava aos computadores infectados iniciar o envio de requisições para uma lista de sites de governo dos EUA, Coreia do Sul e de empresas internacionais. Foi considerado como outro ataque DDoS realizado por zumbis de uma *botnet*. Os EUA perceberam que os sites “dhs.gov” e “state.gov” estavam indisponíveis e cada um dos computadores zumbis inundavam outros servidores do Tesouro Federal, do Serviço Secreto, da Comissão Federal de Comércio e do Departamento de Transporte.

Como forma de se defender do ataque, os EUA transferiu o DDoS para próximo da fonte atacante, fazendo com que apenas os servidores da Ásia que hospedavam o site da Casa Branca ficassem inoperantes e utilizaram os provedores de serviços de Internet para filtrar os ataques, porém no dia 10 de julho de 2009, após perceberem que os ataques aos sites americanos não estavam obtendo sucesso, os guerreiros cibernéticos migraram os ataques para a Coreia do Sul com cerca de 166 mil computadores, em 74 países, inundando sites de bancos e agências governamentais, porém não foi observado que o controle de nenhum sistema do governo foi afetado.

O governo dos EUA não atribuiu diretamente os ataques à Coreia do Norte,

embora a Coreia do Sul aprovou por meio da empresa Vitnamita, Bach Khoa Internetwork Security, que indicou que oito servidores foram controlados por um servidor localizado em Brighton, no Reino Unido da Grã-Bretanha e Irlanda do Norte. Também houve a suspeita do envolvimento de um instituto de pesquisa militar norte-coreano, criado para destruir infraestruturas de comunicações da Coreia do Sul.

Curiosamente, de acordo com Clarke e Knake (2105), a Coreia do Norte possui uma rede elétrica precária e apenas 10% da população possui telefone celular e rádios e televisões que são utilizados apenas para sintonizar canais do governo e que, em sua pesquisa, verificou que de acordo com a avaliação de 2006 da revista New York Times, indicou que a Coréia do Norte estava absolutamente isolada do mundo virtual. Porém, a Coréia do Norte envidava esforços em desenvolver sua infraestrutura para a realização de ataques cibernéticos em outros Estados.

Suspeitas indicam que essa unidade de guerra cibernética estava localizada no Shanghai Hotel, na cidade chinesa de Dandong.

4.4.1 Análise comparativa

No caso citado acima, similarmente aos dois ataques da Estônia e Georgia, apesar de não haver um estímulo para o desencadear de um conflito, o ciberespaço dos EUA foi atacado, tais como servidores do governo.

Algumas características de assimetria foram observadas. Dentre elas, podemos citar:

- a ausência de padrões rígidos foi verificada quando predominou a informalidade de táticas e ações descentralizadas quando sites do governo foi atacado;

- a economia de forças é observada quando, a fim de evitar o confronto numa operação regular, foram utilizados hackers, menos oneroso e arriscado;

- a utilização de ações efêmeras e a busca de resultados psicológicos pode ser verificada quando computadores zumbis inundaram servidores do governo causando temor às Forças Armadas dos EUA;

- a não linearidade, adicionada à difícil atribuição da responsabilidade pelo ataque foi observada, pela provável suspeita de que os ataques no ciberespaço tenham sido provenientes da Coreia do Norte, porém não há provas que apontam para essa suspeita;

- adicionalmente, a assimetria pode ser verificada, tendo em vista que provavelmente foi realizada entre dois Estados com recursos militares e econômicos diferentes, entre os EUA e a Coreia do Norte, forte e fraco, respectivamente.

5 – CONCLUSÃO

A guerra cibernética, travada no ciberespaço, pode ser considerada como uma nova modalidade de guerra. No intuito de entender melhor, foram estudados os seus princípios, a origem e os campos de atuação. Foi verificado que os ataques DDoS, tipos de ataques mais utilizados na guerra cibernética, são instrumentos poderosos e podem restringir, corromper e até mesmo destruir equipamentos que estejam ligados à internet.

Entendeu-se também que o poder cibernético, através do ciberespaço, pode-se atingir um determinado objetivo, além do esperado, podendo estender o controle e facilmente decidir uma vantagem de uma operação militar e beneficiar ao atingimento dos seus objetivos.

Foi seguindo esse entendimento, que nesse estudo também foi verificada a assimetria. A definição e suas características foram descritas e num mundo onde a maioria das guerras ocorridas desde o fim da Segunda Guerra Mundial, foram de natureza assimétrica, a possibilidade de serem empregados meios ou métodos não ortodoxos, os ataques cibernéticos, considerado como um método de assimetria, podem anular ou neutralizar os pontos fortes de um adversário, explorando suas fraquezas, a fim de obter um resultado desproporcional.

A assimetria naturalmente é realizada entre dois Estados com recursos militares e econômicos diferentes, bem como por indivíduos, grupos e comunidades e contabilizam com inferioridade bélica convencional. Às vezes, a disposição não militar, a ausência de padrões rígidos, a economia de forças, a utilização de ações efêmeras e a busca de resultados psicológicos, a não linearidade e a difícil detectabilidade são armas obviamente utilizadas pelo guerreiro cibernético.

Neste trabalho, foi possível verificar, a partir dos ataques cibernéticos citados no estudo, que a guerra cibernética é cercada de características de assimetria. Verificou-se que, durante o ataque da Coreia do Norte, um país que possui uma rede de energia elétrica precária, poucos habitantes possuem telefone celular, rádios e televisões são utilizados apenas

para sintonizar canais oficiais do governo e a internet ainda é considerado como um mito, podendo ser considerada como uma nação fraca tecnologicamente em informática, conseguiu inundar os servidores dos Estados Unidos da América, país relativamente muito mais forte do que o atacante, tais como os servidores do Tesouro Federal, do Serviço Secreto, da Comissão Federal de Comércio e do Departamento de transporte.

Observado também que os ataques da Estônia e da Georgia foram similarmente parecidos, com ausência de padrões rígidos, ações descentralizadas, ações efêmeras e a busca de resultados psicológicos, mostrando características de assimetria utilizadas na guerra cibernética.

O estudo verificou indícios que ajudam a compreender como os ataques cibernéticos são assimétricos e utilizados na guerra:

- podem ser usados como vetores de agressão contra outros Estados ou outras entidades de direito privado;

- são uma forma moderna de guerra e complementar às operações de guerra convencional;

- podem ser consideradas como afirmações de forças políticas e ideológicas;

- aproveitam das vulnerabilidades do inimigo a seu favor;

- com o aumento do desenvolvimento tecnológico e da dependência das informações, o seu potencial destrutivo será incrementado.

Concluindo, neste estudo foi observado que a assimetria encontra-se presente na guerra cibernética e como sendo uma característica importante, os Estados, e principalmente a Marinha do Brasil, deverão estar preparados para enfrentá-la, adotando novos conceitos e estando presentes na defesa do novo domínio operacional, que é o espaço cibernético.

REFERÊNCIAS

ARQUILLA, John. **Twenty years of cyberwar.** Journal of Military Ethics, 17 abr. 2013. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/15027570.2013.782632>. Acesso em: 04 abr. 2018.

BARROS, Renata Furtado de. **Guerra cibernética:** os novos desafios do direito internacional. Belo Horizonte: D'plácido Editora, 2015. 178p.

BISHARA, Marwan. **Era das Guerras Assimétricas:** Um inimigo difuso. Rio de Janeiro, 1º out. 2001. Disponível em <http://diplomatique.org.br/um-inimigo-difuso/>. Acesso em 19 abr. 2018.

BOLENG, Jeff; SCHWEITZER, Dennis; GIBSON, David S. **Developing Cyber Warriors**. EUA: U.S. Air Force Academy, 2008. Disponível em: <file:///C:/Users/DVL/Desktop/C-EMOS%202018/DISSERTAÇÃO/Artigo%20Developing%20Cyber%20Warriors..pdf>. Acesso em: 15 mai. 2018.

BRASIL. Ministério da Defesa. **MD35-G-01:** Glossário das Forças Armadas. 5. ed. Brasília. 2015. 288 p.

_____. Ministério da Defesa. **MD31-M-07:** Doutrina militar de defesa cibernética**.** 1. ed. Brasília. 2014. 36 p.

_____. Exército Brasileiro. **EB20-MC-10.213:** Manual de Campanha de Operações de Informação do Exército Brasileiro**.** 1. ed. Brasília. 2014. 106 p.

CAMBESES JÚNIOR, Manuel. **O Conflito Assimétrico e o Confronto Entre Nações.** Rio de Janeiro, ago. 2002. Disponível em: <http://www.reservaer.com.br /est-militares/ assimetri co.html>. Acesso em: 19 abr 2018.

CASTELLS, Manuel. **A galáxia da Internet:** Reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: ed. Jorge Zahar Editor Ltda, 2003. 244 p.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética**: A próxima ameaça a segurança o que fazer a respeito. Rio de Janeiro: ed. Brasport, 2015. 241 p.

CLAUSEWITZ, Carl V. **Da guerra.** 2. ed. São Paulo: Editora Martins, 1996.

CSIS, Threat Working Group of the CSIS Commission on Cybersecurity for the 44th Presidency. **Threats Posed by Internet**. CSIS: EUA, 28 out. 2008. Disponível em:<. https:// csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs 081028_threats_ working_group.pdf>.Acesso em: 22 mai. 2018.

DERTOUZOS, Michael. **O que será:** como o novo mundo da informação transformará nossas vidas. São Paulo: ed. Companhia das Letras, 1997. 416 p.

GILES, David. **Psycology of the media.** New York: ed. Macmillan Education, 2010. 200p.

LACHOW, Irving. Cyber Terrorism: Menace or Myth? In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. **Cyberpower and National Security**. 1. ed. Dulles, EUA: National Defense University Press and Potomac Books, 2009. 664 p.

MELIKISHVILI, Alexander. **The Cyber Dimension of Russia's Attack on Georgia**, *The Jamestown Foundation*, September 12th, 2008. Disponível em: < www.jamestown.org/single/ ?no_cache=1&tx_ttnews%5Btt_news%5D=33936 >. Acesso em: 04 mai. 2018.

NYE, Joseph S. **Cyber Power**, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010. Disponível em: <https://www.belfercenter.org/sites/default/files /legacy/files/cyber-power.pdf> Acesso em: 08 jun.2018.

ROUTERS, Agência. **Kremlin loyalist says launched Estonia cyber-attack.** Disponível em: <https://www.reuters.com/article/us-russia-estonia-cyberspace/kremlin-loyalist-says-launched-estonia-cyber-attack-idUSTRE52B4D820090313>. Acesso em: 23 mai. 2018.

SUTTON, Walter S. **Cyber Operations and the Warfighting Functions**. 2013. 32 f. Dissertação (Mestrado em Estudos Estratégicos) – U.S. Army War College, Philadelphia, 2013.

THORNTON, Rod. **Asymmetric warfare:** threat and response in the twenty-first century. Cambridge, Ma: Polity, 2007. VIII, 241 p.

VISACRO, Alessandro. **Guerra Irregular:** Terrorismo, guerrilha e movimentos de resistência ao longo da história. São Paulo: ed. Contexto, 2009. 380 p.

WATTS, Mark. **Cyberattacks Became Part of Russia-Georgia War**. In Computer Weekly, EUA,2008. Disponível em <http://www.computerweekly.com/Articles/2008/08/13/231812 /Cyberattacks-became-part-of-Russia-Georgia-war.htm>. Acesso em: 30 maio 2018.