UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE CIÊNCIAS HUMANAS
DEPARTAMENTO DE HISTÓRIA

ESTUDO DE CASO SOBRE O CONFLITO CIBERNÉTICO ENTRE A RÚSSIA E A GEÓRGIA

MICHEL GOMES NOGUEIRA

ORIENTADOR: PROFESSOR DOUTOR VIRGÍLIO CAIXETA ARRAES

BRASÍLIA - 2018

UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE CIÊNCIAS HUMANAS
DEPARTAMENTO DE HISTÓRIA

ESTUDO DE CASO SOBRE O CONFLITO CIBERNÉTICO ENTRE A RÚSSIA E A GEÓRGIA

MICHEL GOMES NOGUEIRA

DISSERTAÇÃO APRESENTADA AO PROGRAMA DE GRADUAÇÃO DO DEPARTAMENTO DE HISTÓRIA DA UNIVERSIDADE DE BRASÍLIA (UnB) COMO REQUISITO PARCIAL PARA OBTENÇÃO DE TÍTULO DE GRADUADO NO CURSO DE HISTÓRIA.

BANCA EXAMINADORA:

PROFESSOR Dr. VIRGÍLIO CAIXETA ARRAES
(ORIENTADOR)

PROFESSOR Dr. VICENTE DOBRORUKA
(MEMBRO)

PROFESSOR Dr. THIAGO GEHRE GALVÃO
(MEMBRO)

DATA: BRASÍLIA/DF, 29 DE NOVEMBRO DE 2018.

AGRADECIMENTOS

A Deus, meu louvor e gratidão.

Esta conquista só foi possível porque minha esposa Nara Fabiana e meu filho Pedro me envolveram de amor, compreensão, carinho e sacrifício. Sem o apoio de vocês, eu não teria conseguido.

Obrigado Dr. Virgílio Arraes por toda ajuda e apoio. Seus conhecimentos e orientações foram primordiais para o desenvolvimento deste trabalho.

A todos, os meus sinceros agradecimentos.

RESUMO

ESTUDO DE CASO DO CONFLITO CIBERNÉTICO ENTRE RÚSSIA E GEÓRGIA

O trabalho da dissertação apresenta um fenômeno ainda bastante recente, pouco conhecido e explorado no mundo informatizado; trata-se da questão dos conflitos cibernéticos que não envolvem somente nações, políticas governamentais e forças armadas; novos elementos foram incorporados às estratégias e táticas de guerra. Esses elementos estiveram presentes no que se pode entender como sendo um dos primeiros conflitos cibernéticos pós internet, que serviu de suporte para um confronto de natureza bélica. A guerra ocorrida entre Rússia e Geórgia em agosto de 2008 foi uma demonstração dos danos causados quando um país é submetido a um bloqueio digital, tornando-se incomunicável na perspectiva do espaço cibernético. Neste sentido, a proposta da monografia é analisar se a guerra cibernética deve ser entendida como um futuro desdobramento da guerra regular ou irregular.

Palavras-chaves: Rússia, Geórgia, Internet, Guerra Cibernética

ABSTRACT

CYBERWAR CASE STUDY BETWEEN RUSSIA AND GEORGIA

The dissertation work shows a phenomenon that is still very recent, little known and exploited in the computerized world. It deals with the issue of cybernetic conflicts, which do not only involve nations, government policies and armed forces, new elements have been incorporated into strategies and tactics of war. These elements were present in that can be understood as being one of the first cybernetic conflicts after internet that served as support for a confrontation of a war nature. The war between Russia and Georgia in August 2008 was a demonstration of the damage caused when a country is subjected to a digital lock, incommunicable from the perspective of cyber space. In this sense, the proposal of this work focused if cyber warfare should be understood as a future deployment of regular or irregular warfare.

Keywords: Russia; Georgia; Internet; Cyberwar.

SUMÁRIO

1. INTRODUÇÃO 6
2. ESTADO X GUERRA REGULAR e IRREGULAR 10
2.1. O ESTADO E A GUERRA 10
2.2. A EVOLUÇÃO DA COMPUTAÇÃO NO SÉCULO XX 18
3. ESTUDO DE CASO: RÚSSIA X GEÓRGIA 25
3.1. RÚSSIA E A GEÓRGIA 25
3.2. CONFLITO BÉLICO E A GUERRA CIBERNÉTICA 28
4. CONCLUSÃO 34

1. INTRODUÇÃO

À medida que a realidade se torna mais complexa, novos temas[1] são acrescentados aos estudos históricos; um deles é a tecnologia da informação e da comunicação. A tecnologia da informação está presente no cotidiano das sociedades e serve de base para o desenvolvimento técnico-científico, para as transformações sociais, econômicas, políticas, e de modo geral para a globalização do mundo contemporâneo.

Nesse contexto, o campo de estudo sobre a tecnologia se encaixa na história do tempo presente[2], impõe-se como uma nova possibilidade de memória, não submetida necessariamente aos documentos e à oralidade, e oferece uma capacidade de relacionar informações digitais. São relações que apresentam novas percepções sensoriais do espaço, do tempo, das imagens, nas dimensões da cultura histórica (RIBEIRO, 2004).

Para Almeida (2011, p.11), "a historiografia não pode se afastar da realidade que pretende estudar", principalmente a história do tempo presente. Existe a necessidade de se adaptar de forma rápida às novas tecnologias da informação.

> Para os historiadores que buscam compreender o presente, negligenciar as fontes digitais e a Internet significa fechar os olhos para todo um novo conjunto de práticas, de atitudes, de modos de pensamento e de valores que vêm se desenvolvendo juntamente com o crescimento e popularização da rede mundial de computadores (ALMEIDA, 2011, p.12).

O caminho trilhado desde a evolução dos computadores está fortemente atrelado à mudança da sociedade da informação; uma sociedade baseada na lógica binária, que pode ser entendida da seguinte forma:

> Isso simplesmente significa que ele lê as descargas elétricas, que são negativas ou positivas e tratadas como 0 ou 1. Ele usa uma série de números binários para representar coisas que simplesmente vimos como muito simples. Assim a letra A maiúscula é representada por 01000001. A letra a minúscula é 01100001. Essa série de números é reorganizada numa linguagem de máquina que por sua vez, é administrada por um código de computador escrito numa dentre várias linguagens, entre elas Basic, C++ e Java (FRIEDMAN, 2009, p. 82).

Desde o final do século XIX, o mundo nunca experimentou uma quantidade tão grande de novas descobertas. A tecnologia da informação é uma dessas invenções cujo

[1] A nova temática a que o autor se refere envolvem questões recentes no mundo digital, tais como: redes sociais, "*fake news*", *wikileaks*, *malwares*, crimes cibernéticos, etc.

[2] Segundo Almeida (2014, p. 53) o tempo não para e o presente está constantemente se tornando passado, em um fluxo constante de "agoras" em direção a "futuros" em aberto. Cada evento ocupa certa duração, sempre presente. O tempo mais curto é aquele que habitamos, ponto de encontro entre passado e futuro infinitos.

impacto é algo que a princípio parece não ter um fim em si mesmo, mas está sempre em evolução. Os conflitos entre as nações também passam por uma mudança em sua dinâmica. Até então, um dos pontos a serem estudados em termos de conflito ou mesmo guerras se referia ao poderio militar de cada Estado, seus armamentos bélicos, sejam nucleares ou não. Atualmente, o espectro se ampliou para pesquisa no campo de ataques cibernéticos entre os Estados.

Creveld (2004, p.540) declara que "a ascensão do Estado é inseparável da ascensão da tecnologia moderna". Isso significa que a informatização da sociedade está diretamente ligada à informatização do Estado. A busca pelo aprimoramento tecnológico perpassa pelos eixos econômico, comercial, educacional e também militar. Um Estado moderno precisa se preocupar com o nível de inserção tecnológica do seu arsenal bélico. Aviões, submarinos, drones, equipamentos de comunicação, tanques, mísseis e vários outros estão cada vez mais dependentes do aparato tecnológico.

Entende-se que o termo "guerra cibernética" é polêmico, segundo Maynard baseado em Clarke, o nome "cyberwar" ("ciberguerra" em tradução literal) refere-se a "iniciativas empreendidas por um Estado-nação para invadir computadores ou redes de informação com o propósito de causar danos ou distúrbios" (*apud* TEIXEIRA, 2017).

Em palestra no *Campus Party* Brasil 2017, Bernardo Wahl (*apud* TEIXEIRA, 2017) destaca que a Revolução Cibernética não mudou fundamentalmente a guerra, mas permitiu novas estratégias de ofensiva e de espionagem como o "*Stuxnet"*, um verme de computador (*worm*) utilizado por uma aliança ocidental (EUA, Grã-Bretanha e Israel) para atrasar o desenvolvimento do programa nuclear iraniano:

> As armas cibernéticas não são abertamente violentas, então é improvável que seu uso se encaixe no critério de guerra interestatal. Mas essa nova capacidade amplia a gama de possíveis danos e resultados entre os conceitos de guerra e paz. Interessa para muitos estados o quanto for possível que esses campos permaneçam nebulosos [quanto à sua regulamentação] (*apud* TEIXEIRA, 2017).

Ele relata que novos atores podem ganhar força com a difusão do poder pelo conhecimento cibernético, como entidades não estatais como o "Anonymus", grupo formado por *hackers* de todo o mundo que lançam ofensivas a alvos anunciados em casos específicos (TEIXEIRA, 2017). Em 2013, o Ministro da Defesa Celso Amorim comentou sobre as ações cibernéticas estatais:

> O monitoramento de dados e a guerra cibernética têm em comum o emprego de instrumentos de altíssima tecnologia para atividades que importam em graves violações de soberania. Quando o objeto do

> monitoramento vai além da mera observação, e visa a tomada de conhecimentos tecnológicos, a fronteira entre a espionagem e a guerra fica ainda mais difícil de ser determinada. Conceitualmente, não haveria diferença, salvo talvez no que diz respeito a danos imediatos, entre um ato de espionagem, de busca de informações econômicas e tecnológicas, e um ataque tradicional para a obtenção de um recurso econômico. O monitoramento e a guerra cibernética podem alvejar tantos países tidos como hostis ou como ameaças imediatas quanto países amigos e aliados. Já sabemos que esse foi o caso na interceptação de dados [do governo brasileiro pelos EUA descoberto neste mesmo ano]. Não se pode excluir que o mesmo ocorra com ataques cibernéticos, provenientes de qualquer quadrante. Essas duas atividades ilustram em tons muito fortes alguns dos novos desafios da segurança internacional (*apud* TEIXEIRA, 2017).

"Nos Estados Unidos, a guerra cibernética é considerada, hoje, a principal ameaça à segurança nacional, maior até mesmo que a rival Rússia, a ameaçadora China ou os extremistas islâmicos" (RUDZIT *apud* GUEDES, BRASIL e PAGANINE, 2012, p.38). O governo norte-americano tratou esta questão tão a sério, "que o Departamento de Defesa criou sua própria divisão de combate cibernético".

Segundo Rudzit, "a divisão emprega jovens ligados a essa nova realidade para buscar falhas e formas de minar os sistemas de defesa das potências adversárias". Os governos reconhecem que as ações militares estão cada vez mais dependentes do aparato tecnológico e os sistemas se tornaram o "calcanhar de aquilhes" das potências bélicas.

Na história, o tema também já aparece há algum tempo em trabalhos em eventos de grande porte. Na XXVI ANPUH, de 2011, Maynard explicou a atuação de grupos não estatais:

> Aquilo que os militares veem como ciberguerra (guerra de informação) pode ser melhor entendido como 'ciberativismo' ou 'hacktivismo'. Uma clara evidência disto está no fato de que os ataques dos hackers tiveram efeitos menores do que os desejados. O objetivo não era retirar as páginas do ar permanentemente, tampouco prejudicar a capacidade logística de um país. Não foram paralisados aeroportos, hospitais, estações de metrôs ou sistemas energéticos (*apud* TEIXEIRA, 2017).

Por se tratar de um tema tão recente e ligado a informações confidenciais, o acesso às fontes é muito restrito. O Café História solicitou a Wahl, na *Campus Party* 2017 indicar as fontes que ele utilizava em suas pesquisas:

> A sugestão é acompanhar as pesquisas das empresas que trabalham com segurança de computação como Symantec, a Kaspersky entre muitas outras que frequentemente elaboram relatórios que podem iluminar essa área que ainda é muito cinzenta. Além disso, temos os *think tanks*, centros de pesquisas, como o CPDOC da FGV e muitos outros, nos EUA, por exemplo, que produzem material sobre o assunto (*apud* TEIXEIRA, 2017).

Wahl alertou: “Nessa área de cibernética e nessa era de redes sociais existem muitas informações falsas. O papel do pesquisador é de ser muito rigoroso com suas fontes e com sua pesquisa. ”

Por isso a metodologia de trabalho se valeu da análise de fontes relacionadas à guerra cibernética; acessos a sítios especializados em segurança da informação e de normativos sobre a defesa cibernética do Brasil.

E para o enriquecimento do tema, apresentou-se o estudo de caso sobre a guerra entre Geórgia e Rússia, que completou em agosto de 2018 dez anos. É importante destacar que o desenrolar desse conflito apresentou-se como nova estratégia de guerra, deliberando-se um ataque cibernético prévio para posterior invasão russa no território georgiano, o que bloqueou os principais canais de comunicação do país.

A pesquisa também envolveu a questão se a guerra cibernética deve ser entendida como um futuro desdobramento da guerra regular ou irregular, cuja hipótese tratou de verificar se as transformações tecnológicas operadas na sociedade moderna afetam a forma de fazer a guerra.

Outro ponto relevante da pesquisa foi identificar a criação de forças militares cibernéticas entre diversas nações, inclusive o Brasil. O que é uma demonstração da visibilidade do tema nos assuntos internacionais. Além do que, conforme mencionado por Dutra (2007), existe a necessidade de um despertar do brasileiro para o assunto:

> É evidente que a Guerra Cibernética não se trata mais de uma ficção, na qual batalhas são irrompidas por comandantes por detrás de mesas, com simples acionamentos de botões (...) A preocupação demonstrada por países como a China e Taiwan, em criar unidades especialmente dedicadas ao assunto em suas forças armadas, e dos Estados Unidos da América, ao buscar desenvolver doutrina na área, indicam que não se pode mais desconsiderar essa vertente de emprego militar num teatro de operações moderno.

Portanto, o principal objetivo deste trabalho é a apresentação de um estudo sobre guerra cibernética como uma nova forma de conflito mundial, bem como suas implicações na invasão russa no território da Geórgia no ano de 2008.

O estudo tratou de avaliar os conceitos de guerra regular, irregular e cibernética; uma análise histórica da internet como um instrumento de guerra, o entendimento do que seja espaço cibernético e a atuação do Comando de Defesa Cibernética do Brasil.

Salienta-se que o assunto tratado tramita dentro do que pode ser considerada a 3ª revolução industrial que tem como característica sua forte dependência tecnológica, fato que se deve à miniaturização dos componentes eletrônicos e à sua utilização em

larga escala nos setores da economia, empresarial, comercial, acadêmico e militar, por meio de computadores, redes de dados e a interconexão do que se pode chamar de mundo globalizado. Segundo Coutinho (1992, p. 70) a aplicação da microeletrônica serviu de "base para tecnológica comum" para a descoberta de diversos produtos e serviços de uso industrial, o que permitiu o surgimento de segmentos e setores inovadores na forma de um "complexo eletrônico", vinculado à área de tecnologia da informação.

Desta forma, os capítulos foram organizados conforme o seguinte raciocínio. O primeiro trata da questão do relacionamento do Estado com a guerra regular e a guerra irregular cujo assunto envolve o conceito de guerra, sua arte, as gerações da guerra moderna e a guerra irregular e assimétrica. O segundo lida com o assunto sobre a guerra cibernética propriamente dita que se desencadeia na história da computação, da internet e do uso da força militar cibernética. No terceiro, descreve-se um estudo de caso sobre a guerra entre Geórgia e Rússia em agosto de 2008 e como ocorreram os preparativos para o início desse enfrentamento que é considerado como um dos primeiros conflitos cibernéticos desde o fim da Segunda Guerra Mundial e do início da internet.

2. ESTADO X GUERRA REGULAR E IRREGULAR

Este capítulo inicia com a revisão dos conceitos fundamentais para a compreensão de como a guerra cibernética relaciona-se com a questão de conflito entre Estados e o uso da internet como ferramenta militar. Em virtude disso, é essencial o entendimento de determinadas abordagens relacionadas ao tema guerra cibernética.

2.1. O ESTADO E A GUERRA

Para Creveld (2004, p.1) Estado significa "uma entidade abstrata que não se pode ver, ouvir nem tocar" e é semelhante a qualquer corporação, ou seja, necessita possuir uma *persona* jurídica própria, cujo atributo de soberania é reservado somente a ele, exercendo suas funções sobre um determinado território. Importante destacar que precisa da autorização de outros de sua espécie para ser reconhecido.

> "Após quatro séculos e meio de evolução, que começara por volta de 1300, o Estado talvez seja o mais poderoso construto político e todos os tempos. Contando com forças armadas permanentes – primeiro, os militares, depois a polícia e também o aparato carcerário -, impôs ordem à sociedade, chegando ao ponto em que as únicas organizações capazes de enfrenta-lo eram outras do mesmo tipo" (CREVELD, 2004, p. 260).

Em termos de deveres, o Estado possui dois que são considerados primordiais segundo Treitschke (*apud* Waltz, 2004, p. 120): "o duplo dever de manter o poder no exterior e a lei no interior". O primeiro dever diz respeito à questão que o Estado tem que ter o cuidado do seu exército e o segundo, que o Estado deve se ater à sua jurisprudência, "a fim de proteger e controlar a comunidade de seus cidadãos".

Adam Smith também se manifestara da mesma forma, no sentido do Estado se preocupar "externamente com a defesa e internamente com a justiça" (*apud* WALTZ, 2004, p. 120). Por assim dizer, Weber (2004, p. 527) entende o Estado como uma comunidade humana presente em um determinado território, que esse exerce o papel de "coação física" na medida do permitido.

> "É uma relação de dominação de homens sobre homens, apoiada no meio da coação legítima (quer dizer, considerada legítima). Para que ele subsista, as pessoas dominadas têm que se submeter à autoridade invocada pelas que dominam no momento dado. Quando e por que fazem isto, somente podemos compreender conhecendo os fundamentos justificativos internos e os meios externos nos quais se apoia a dominação".

Da mesma forma, Thomas Hobbes, no *Leviatã*, no capítulo XVII, descreve o poder soberano como homens que se unem, que concordam entre si em se submeterem-se a um homem ou a uma assembleia de homens, de maneira voluntária, "com a esperança de serem protegidos por ele contra os outros". A este poder soberano, Hobbes dá o nome de Estado Político ou um Estado por instituição.

Neste contexto, o ato de guerra[3] parece simples e fácil de se entender e remete seu entendimento a conflitos armados entre duas ou mais nações. E seguindo essa lógica de pensamento, a Doutrina de Defesa Militar Brasileira interpreta a palavra guerra como sendo um conflito no seu grau máximo de violência. A depender da magnitude do conflito, pode envolver a mobilização de todo o poder nacional, com predominância da expressão militar, para impor a vontade de um ator ao outro (MINISTÉRIO DA DEFESA, 2007, p.22).

[3] A etimologia da palavra guerra procede do germânico *werra*, a qual sua variância será *war* em inglês, cujo significado inicial não era de conflito sangrento, mas algo mais na linha da discordância, que podia nascer de uma simples discussão verbal e chegar, no máximo, a um duelo (Dicionarioetimologico, 2018).

Para Clausewitz[4] (2017, p.75) a guerra se baseava em um duelo em grande escala, algo como inúmeros duelos sendo travados, por pares de lutadores, formando uma imagem como um todo. Os lutadores se enfrentavam, com o objetivo de obrigar o outro a fazer a sua vontade. O propósito imediato é derrotar o seu inimigo de modo a torná-lo incapaz de oferecer qualquer outra resistência. É uma forma de impor a vontade do vitorioso ao derrotado. Este estado de impotência do inimigo é o verdadeiro intuito da guerra. "A guerra é, portanto, um ato de força para obrigar o nosso inimigo a fazer a nossa vontade".

A forma mais clássica de se entender o que é uma guerra é aquela aprendida nos bancos escolares, por meio dos livros e filmes tão disseminados nos meios de comunicação, que envolve a luta armada entre nações, povos, tribos ou até mesmo entre grupos internos; uma hostilidade declarada que também pode significar uma oculta, que ainda não eclodiu em conflito, exemplo da guerra fria entre a Rússia e os Estados Unidos.

Waltz (2004, p.50) destaca que "a maldade do homem, ou seu comportamento impróprio, leva à guerra; a bondade individual, se pudesse ser universalizada, significaria paz". Segundo os pessimistas, a paz é uma meta e um sonho utópico, que seria possível sim, uma reforma nos indivíduos para "trazer ao mundo uma paz duradoura". Duas condições de Duroselle (2000, p.283) para que haja um conflito internacional:

A primeira se traduz no interesse de considerar um certo objeto de interesse, que o adquirir é desejável e que vale à pena correr os riscos necessários para obtê-lo; a segunda diz respeito ao fato que essa decisão deve ser "acompanhada de reação emocional favorável ou desfavorável, pelo menos em uma parte da população que ele controla ou da população do campo adversário". No conflito entram em jogo, "uma ação e uma reação".

Afinal de contas, existe uma extensa literatura sobre a guerra, segundo Magnoli (2006); o ponto de partida retrocede séculos antes da era cristã, até o mais antigo tratado militar de que se tem registro: *A arte da guerra*, atribuído a Sun Tzu[5] e escrito possivelmente entre 320 e 400 a. C., aborda o surgimento da guerra verdadeira na China. Sun Tzu constata que a arte da guerra é importante para o Estado, que lida com a vida ou

[4] Um veterano prussiano das guerras napoleônicas que aproveitou seus anos de reserva para compor o mais famoso livro sobre a guerra – chamado justamente *Da guerra* (KEEGAN, 1993).

[5] Historiadores e comentaristas antigos e contemporâneos referem-se ao general Sun Tzu como um dos homens mais versados na arte militar e até na difícil técnica de bem-dispor dos recursos para fazer face às dificuldades (PUGLIESI *apud* TZU, 2005).

a morte; com a segurança ou a ruína. Portanto, é um objeto de investigação que não pode ser negligenciado.

> No sistema de Sun Tzu, o recurso às armas devia fazer parte de um programa mais amplo pelo qual o inimigo seria politicamente atingido, antes de ser militarmente batido. Era mister, por meio de agentes e espiões infiltrados, criar divergências entre o soberano inimigo e seus ministros, entre chefes e os subordinados, entre a elite e a massa de súditos, instilando a subversão e provocando a desmoralização da autoridade. A guerra como continuação da política (MAGNOLI, 2006).

O tratado delineado por Sun Tzu é tido como um dos mais antigos do gênero, sendo largamente apreciado, há séculos, entre os militares. O texto teria sido fonte inspiradora do livro vermelho de Mao Tsé-Tung (TZU a*pud* PUGLIESI, 2005, p.09).

> Quando o inimigo estiver unido, divida-o. Ataque onde ele estiver despreparado; invista quando ele não o estiver esperando. Estas são as chaves do estrategista para a vitória. Não é possível discuti-las antecipadamente (TZU, 2005, p.14).

Torres (MAQUIAVEL, 2011, p. 7) ressalta que o desdobramento do pensamento maquiaveliano perpassa pela questão que "não há nada menos afim entre si, nem tão dessemelhante quanto a vida civil da militar", que se levando em consideração as imprescritíveis lições dos antigos, deve-se se dar conta que "não se encontrariam coisas mais unidas, mais afins e que, necessariamente mais se amassem uma a outra" do que essas, pois tudo o que se fizer com vistas ao bem comum de uma cidade será vão "se suas defesas não forem bem preparadas." Isso explica que para Maquiavel o cuidado com a segurança é central e crítico para a vida civil, e que se negligenciado terá como consequência inevitável a ruína das cidades imprudentes, "das que não entenderam que Marte, o deus da guerra, é também – reconheça-se isso ou não – o deus da polis".

Em sua abordagem, Keegan (1993, p. 11) descreve a guerra como algo que "precede o Estado, a diplomacia e a estratégia por vários milênios". Para ele, "a guerra é quase tão antiga quanto o próprio homem e atinge os lugares mais secretos do coração humano, lugares em que o ego dissolve os propósitos racionais, onde reina o orgulho, onde a emoção é suprema, onde o instinto é rei". Para Clausewitz a guerra era o compromisso estabelecido pelos Estados dos quais ele conhecia, que perpassava pelo respeito à ética dominante, à soberania absoluta, à diplomacia ordenada e aos tratados legais, "ao mesmo tempo que se levava em conta o princípio superior do interesse de Estado".

Clausewitz é considerado um dos poucos teóricos militares, incluindo Sun Tzu, que conseguiu influenciar grandes nações em relação aos seus pensamentos modernos

sobre estratégia. Seu livro *"vom Kriege"* (Da guerra) é amplamente utilizado nas principais academias militares de guerra ao redor do mundo (CREVELD, 1991, p. 35).

Portanto, a condução da guerra consiste no planejamento e na condução da luta. Seu entendimento é que a luta não consiste em um único ato isolado, mas em um número maior ou menor de atos isolados, cada um deles completos em si mesmos, denominados "engajamentos". Essas atividades formam diferentes meios de planejar e executar esses engajamentos e de coordená-los, de modo a atingir o propósito da guerra. A esse "*modus operandi*", Clausewitz chama de tática e a outra de estratégia. "De acordo com a nossa classificação, portanto, a tática ensina o emprego das forças armadas no engajamento. A estratégia, a utilização dos engajamentos para atingir o propósito da guerra" (p. 138).

Ou seja, no entender de Clausewitz a tática se baseia no uso das forças armadas durante o confronto, e parte do princípio que o general fará o ordenamento e direção dessas forças, cujo principal objetivo é a vitória militar. Enquanto a estratégia fará o uso dos confrontos a serviço da guerra e envolver-se-á no estabelecimento da paz no pós-conflito, impondo a vantagens para o lado vencedor do conflito. Essa ação é desempenhada essencialmente pelo político. Segundo Lidell Hart (*apud* STORTI, 2009, p. 18), estudioso e crítico da obra de Clausewitz, a estratégia é "a arte de distribuir e aplicar os meios militares para atingir os fins da política e a tática como as medidas tomadas para o emprego e controle desta ação [da estratégia]". Hart define a tática como a aplicação da estratégia e a estratégia como parte de uma grande estratégia.

> A grande estratégia, por sua vez, preocupa-se não apenas com a delimitação do objetivo político, mas essencialmente com a garantia da paz em condições vantajosas no pós-guerra, assim, ela não se esgota na vitória militar, mas na consolidação da paz e no cumprimento do objetivo político. (...). Enquanto o horizonte da estratégia é limitado pela guerra, a grande estratégia olha mais para frente, preocupando-se com os problemas da paz subsequente. Utiliza os instrumentos necessários à conduta da guerra e procura evitar os danos, tendo em vista a paz, preocupando-se com a segurança e a prosperidade (LIDELL HART, 1982, p.407, *apud* STORTI, 2009, p.18 -19).

Creveld (p.97) mencionou que Clausewitz tinha uma grande admiração por Napoleão, considerado por ele, como o "deus da guerra", e para Napoleão a melhor estratégia, em primeiro lugar, é sempre ser mais forte que o adversário e ter conhecimento para atuar em pontos decisivos. Ademais, a estratégia consistia em dois elementos básicos: gerar a força em uma mão e usá-la contra o oponente com a outra mão (p. 116). Ou seja, partia-se do princípio que gerar a força era sempre representada por uma condição necessária para promover a guerra.

> Sun Tzu e Clausewitz estão unidos pela tese fundamental de que a gramática estratégica não só está ao serviço da lógica política, como o verdadeiro pensamento estratégico está possuído pelas três características que Max Weber atribuía ao político por vocação: paixão pela sua causa, sentido de responsabilidade no que toca às consequências concretas das suas decisões, e rápida capacidade de avaliação das situações, aperfeiçoada pela coragem de olhar para o perigo de frente, e mantendo uma serena distância perante as coisas e os homens (SOROMENHO-MARQUES, 2000, *apud* ABREU, 2006, p.12).

A visão de estratégia de Beaufre (1998, p. 28) se difere em certo aspecto da definição apresentada por Clausewitz e de Liddell Hart, que no seu entender a estratégia não se trata somente da arte de empregar as forças militares para atingir resultados fixados pela política, mas a arte de fazer a força concorrer para atingir os objetivos da política. Segundo Beaufre, a finalidade da estratégia "é atingir os objetivos fixados pela política, utilizando da melhor maneira os meios de que se dispõe". Esses objetivos podem ser considerados como ofensivos (conquista, impor condições onerosas), defensivos (proteção do território ou outros interesses) ou para manutenção do *status quo* político.

Storti (2009, p.19) descreveu a estratégia como algo que sofre mutações, não visto somente como uma tarefa a ser usada em campo de batalha, mas também com a inclusão de "planejamentos externos, que se vale de táticas que podem ser utilizadas em diferentes situações, como o uso de estratégias de fundo psicológico ou ideológico".

No caso da guerra relâmpago entre a Rússia e a Geórgia em agosto de 2008, assunto que será detalhado no próximo capítulo, uma das estratégias e táticas utilizada pela Rússia para subverter a Geórgia foi o uso de elementos cibernéticos. Segundo Hagen (2012, p.2) esse conflito foi considerado sem precedentes em termos de guerra, em razão dos ataques cibernéticos ofensivos realizados terem feito parte de um esforço que acompanhou as operações militares estratégicas e táticas em solo. "Este caso foi um dos primeiros atos evidentes de guerra cibernética na história recente após os eventos na Estônia em 2007", que sofreu um ataque de negação de serviço, impossibilitando o acesso aos sítios governamentais, bancos e mídia.

Independentemente se a guerra se dá em razão dos desígnios de um Estado ou dos desejos intrínsecos do homem em possuir poder e lutar por sua honra, os conflitos modernos evoluíram para a perda do monopólio do Estado e os militares se encontram

combatendo oponentes não estatais. Nesse sentido, Lind[6] (2005, p. 12) apresenta um modelo de evolução da arte da Guerra - "Quatro Gerações da Guerra Moderna":

- A Primeira Geração (Utilização da Massa) é a guerra de linha e coluna (*line-and column*) onde as batalhas eram formais e o campo de batalha era ordenado, com duração entre 1648 e 1860 aproximadamente. Criou-se uma cultura militar de ordem, cuja maioria das coisas que distingue o militar do civil (uniformes, continências, graus hierárquicos) eram produtos da primeira geração com a intenção de reforçar a ideia de ordem.
- A Segunda Geração (Concentração do Poder de Fogo) foi desenvolvida pelo exército francês na I Guerra Mundial, com objetivo de atrito, artilharia de conquista e infantaria de ocupação. O poder de fogo era cuidadosamente sincronizado (usando-se planos e ordens detalhados e específicos) para infantaria, carros de combate e artilharia em uma "batalha conduzida" onde o comandante era um condutor de orquestra.
- A Terceira Geração (Manobra) também foi um produto da I Guerra Mundial, desenvolvida pelo Exército alemão e conhecida como "*blitzkrieg*" ou guerra de manobra. Ela é baseada não no poder de fogo e atrito, mas na velocidade, surpresa e no deslocamento mental e físico. Ao invés de "aproximar e destruir", o lema é "passar e causar o colapso".
- A Quarta Geração (Conflitos irregulares e assimétricos) caracteriza-se pelo fato de o Estado perder o monopólio sobre a guerra. Em todo o mundo, os militares se encontram combatendo oponentes não estatais tais como a al-Qaeda, o Hamas, a Hezbollah e as Forças Armadas Revolucionárias da Colômbia. Quase em toda a parte o Exército está perdendo. Nessa guerra, a invasão de imigrantes pode ser tão perigosa quanto a invasão do exército inimigo.

Lind (2005, p.14) reconhece que os militares estatais talvez não possam lidar com os inimigos da Quarta Geração, não importa o que eles façam, e menciona que talvez a chave do sucesso na guerra da quarta geração seja "perder para vencer".

> Parte do motivo porque as guerras no Afeganistão e no Iraque não estão sendo vencidas é que as nossas invasões iniciais destruíram o estado,

[6] William S. Lind é diretor do Center for Cultural Conservatism of the Free Congress Foudation. Serviu de assistente legislativo das forças armadas para o Senador Robert Taft, Jr. e também para o Senador Gary Hart do Colorado. Escreve coluna semanal "On War" online no www.military.com. (LIND, 2005, p. 17).

> criando um feliz campo de caça para forças de Quarta Geração. Em um mundo onde o estado está em decadência, se for destruído, é difícil recriá-lo (LIND, 2005, p. 14).

Seguindo essa mesma linha de raciocínio, Costa (2017, parte 4, p.01) descreve que os fatores que definem as gerações da Guerra Moderna são a combinação do uso de tecnologias (armamentos, meios de transportes, equipamentos e logísticas) e o seu emprego tático e para cada alteração de tática pode-se impulsionar novas tecnologias e com isso uma nova geração da guerra poderá ser implementada.

Visacro (2009) destacou a existência de uma guerra irregular, uma forma antiga de se combater, que é considerada a mais comum desde meados do século passado. Para Visacro, terrorismo, guerrilha, insurreição, movimento de resistência, combate não convencional e conflito assimétrico, são exemplos de modalidades de guerra irregular.

> " Um breve olhar sobre as áreas de tensão e as áreas conflagradas em torno do planeta reforçará a ideia de supremacia das práticas qualificadas como "irregulares", pois grupos insurgentes, organizações terroristas e facções armadas romperam o pretenso monopólio estatal sobre a guerra, protagonizando os principais conflitos da atualidade. " (VISACRO, 2009)

O que difere a guerra regular da guerra irregular, é que a regular é travada entre exércitos de países organizados e estáveis, é baseada na separação clara entre civis e soldados e a sua maior característica é o conflito entre Estados. Enquanto que a irregular coloca o Estado frente a um grupo que quer derrubar um governo instituído, tomar o poder de forma revolucionária ou impor uma ideologia (COSTA, 2017, parte 5, p.02).

> Objetivos anteriores como destruição de forças inimigas, conquista e manutenção do terreno passam a ter valor secundário na guerra irregular, pois o principal agora é a conquista da opinião pública e o apoio às atividades dos grupos que lutam a guerra irregular. Toda a ação armada tem por finalidade, também, atingir um objetivo psicológico (COSTA, 2017, parte 5, p.02).

De acordo com o Exército brasileiro, a guerra irregular pode ser entendida como o conflito armado executado por forças não regulares ou por forças regulares empregadas fora dos padrões normais da guerra regular, contra um governo estabelecido ou um poder de ocupação, com o emprego de ações típicas de guerrilhas. E a guerra assimétrica como sendo o conflito armado que contrapõe dois poderes militares que guardam entre si marcantes diferenças de capacidades e possibilidades. Um enfrentamento cujo um dos lados é bem superior ao outro e o mais fraco adota majoritariamente técnicas, táticas e procedimentos típicos da guerra irregular (MINISTÉRIO DA DEFESA, 2007, p.25).

> Em termos práticos, guerra irregular é todo conflito conduzido por uma força que não dispõe de organização militar formal e, sobretudo, de legitimidade jurídica institucional. Ou seja, é a guerra travada por uma força não regular.
> É licito afirmar, portanto, que a guerra irregular é a mais antiga forma de guerra conhecida, pois estima-se que as primeiras forças armadas combinadas permanentes tenham surgido por volta de 3000 a.C., no Oriente Médio, e a prática guerreira dentro da coletividade humana, certamente, antecede esse período (VISACRO, 2009)

Costa (parte 5, p.05) destacou que após os atentados sofridos pelos Estados Unidos, em 11 de setembro de 2011, ocorreu um aumento nos embates assimétricos, cuja maior mudança se estabeleceu nas ações observadas nos meios utilizados na condução da guerra, que extrapolam as atividades militares. A guerra assimétrica manifesta-se em formatos diversos:

- Guerra psicológica; guerra econômica; guerra com armamentos variados e improvisados; guerra química, radiológica, nuclear ou radioativa; guerra biológica, bacteriológica ou virótica; guerra cibernética ou eletrônica; cooperação civil-militar; crime organizado, entre outras. Tendo em vista que nesse tipo de conflito se busca atingir a moral do adversário, a guerra psicológica é preponderante, sempre usando técnicas de terror como atentados e sequestros.

2.2. A EVOLUÇÃO DA COMPUTAÇÃO NO SÉCULO XX

Em 1935, a revolução do computador começou efetivamente a realizar-se com a participação de Alan Mathison Turing (1912 – 1954), na época estudante do King´s College em Cambridge. Turing desenvolveu diversos trabalhos importantes que resultou na fundamentação teórica da chamada "Ciência da Computação". Ele formalizou definitivamente o conceito de algoritmo (FONSECA FILHO, 2007, p.75). "Turing também desenvolveu um teste para comprovar se um computador possuía ou não inteligência artificial" (SARAIVA, 2009). Além disso, durante a II Guerra Mundial, Turing foi convocado pela Escola de Cifras e Códigos, cuja tarefa era decifrar mensagens codificadas do inimigo, mais conhecida como a "Máquina Enigma". "Quando a guerra terminou, Turing tinha ajudado a construir um computador, o Colossus, uma máquina inteiramente eletrônica com 1.500 válvulas (...)" (FONSECA FILHO, 2007, p.78).

O Colossus Mark 1 foi considerado o primeiro computador digital programável, cuja utilização ocorreu principalmente em consequência da II Guerra Mundial. O

computador Colossus Mark 2 se tornou o primeiro a ser produzido em série, com 10 unidades no total. No entanto, esse computador fazia parte de um projeto secreto do governo inglês, o que fez que seus inventores não recebessem crédito e o design também não pôde ser aproveitado em outros computadores. O projeto do Colossus acabou na obscuridade (MORIMOTO, 2011).

Mas os americanos foram mais liberais ao compartilhamento de informações e construíram o ENIAC (Electronic Numerial Integrator Analyzer and Computer) entre os anos de 1943 e 1945, mas sua operação ocorreu somente em 1946, encerrando suas operações em 1955. O ENIAC foi o primeiro computador digital eletrônico totalmente funcional a ser construído pela Escola Moore de Engenharia Elétrica da Universidade da Pensilvânia - Estados Unidos para atender um pedido do Departamento do Exército Americano. O computador foi idealizado por J. Presper Eckert[7] e John Mauchlye era um pouco semelhante ao Colosso, embora fosse maior e mais flexível. Foi projetado para realizar cálculos das tabelas usadas pela artilharia (COPELAND, 2006). Outros computadores foram construídos, como o UNIVAC I (Universal Automatic Calculator), em 1951, o primeiro computador comercialmente disponível.

Desde então, houve uma revolução do hardware e do software, diversas linguagens de programação foram desenvolvidas e as arquiteturas de máquinas, principalmente impulsionadas pela invenção do transistor (1948). Outros equipamentos eletrônicos passaram a ter espaço no ambiente computacional, tais como impressoras, as fitas magnéticas, os discos para armazenamento, etc. Segundo Fonseca Filho (p.123), "os computadores passaram a ter um desenvolvimento rápido, impulsionados principalmente por dois fatores essenciais: os sistemas operacionais e as linguagens de programação".

Todas as transformações do computador foram se aperfeiçoando ao longo do tempo, isso se deve ao avanço das áreas da matemática, eletrônica, engenharia da computação. Diana (2018) descreveu a história da computação em quatro períodos:

- Primeira Geração (1951 – 1959) – Computadores funcionavam por meio de circuitos e válvulas eletrônicas. Possuíam o uso restrito, além de serem imensos e consumirem muita energia.

[7] Eckert (1919-1995) e um pouco mais tarde John Mauchly (1907-1980), físico, e Herman H. Goldstine, matemático, acabaram por tornarem-se os principais protagonistas na construção do primeiro computador de uso geral que realmente funcionou como tal, o ENIAC (Electronic Numerical Integrator and Computer) (FONSECA FILHO, 2007, P.104).

- Segunda Geração (1959 – 1965) - Computadores funcionavam por meio de transistores, os quais substituíram as válvulas que eram maiores e mais lentas, mas ainda possuíam dimensões muito grandes.
- Terceira Geração (1965 – 1975) – Computadores funcionavam por circuitos integrados. Esses substituíram os transistores e já apresentavam uma dimensão menor e maior capacidade de processamento.
- Quarta Geração (1975 – até os dias atuais) – Computadores de tamanho menor e com muita capacidade e velocidade de processamento de dados. São incluídos os microprocessadores com gasto cada vez menor de energia. Nesse período, mais precisamente a partir da década de 90, há uma expansão dos computadores pessoais.

Segundo Diana, alguns estudiosos preferem acrescentar a "Quinta Geração de Computadores" com o aparecimento dos supercomputadores, utilizados pela Google, Facebook, NASA, IBM, etc. Nesse período é possível avaliar a evolução da tecnologia multimídia, da robótica e da internet.

Na década de 60, em plena guerra fria, nascia a ARPANET[8], a precursora da internet, que tinha como objetivo inicial a criação de uma rede que fosse indestrutível aos bombardeios e que interligasse pontos estratégicos para fins militares, ou seja, centros de pesquisa e tecnologia e serviços de informação nacional. A partir de 1990, o Departamento de Defesa dos Estados Unidos desmantelou a ARPANET e criou a NSFNET que se popularizou em todo o mundo, com a denominação da Internet, transformando-se num sistema mundial público de redes de computadores. A internet permitiu que qualquer pessoa ou computador, previamente autorizado, pudesse se conectar, e quando obtida a conexão, possibilitou a transferência de informação entre computadores (BASÍLIO, p.12, *apud* NOGUEIRA, 2016).

Atribui-se que a própria internet é fruto da engenharia militar. Um produto da guerra fria, entre Estados Unidos e a União Soviética, cuja função era articular centros de defesa em caso de um ataque soviético (AZEVEDO, 2001, p.01). Mas o avanço

[8] ARPANET foi desenvolvida pela Advanced Research Projects Agency – ARPA. A futura rede deveria abranger todas as localidades das instituições financiadas pela ARPA, interligando seus computadores com sistemas de tempo compartilhado, com o objetivo de reduzir os custos de transmissão, aumentar a confiabilidade e, potencialmente, ampliar os objetivos militares nas pesquisas em torno do assunto. (CARVALHO, p.12, *apud* NOGUEIRA, 2016).

tecnológico favoreceu também a aplicação da internet nos meios universitários e comerciais.

No entanto, a internet se tornou um ambiente favorável para a ação de pessoas mal-intencionadas, que tentam obter informações dos usuários para usos ilícitos, como invadir um computador para conseguir uma senha para um acesso indevido em uma conta bancária, conta de e-mail ou um determinado sistema. Também tem servido para arregimentar um verdadeiro exército de pessoas dispostas a provocar caos nos sistemas econômico, bancário, hospitalar, transporte, industrial, comunicação, entre outros.

Estados Unidos, China e Rússia já dispõem de uma divisão de combate cibernético em prol da defesa nacional. O governo americano tem empregado jovens ligados a essa nova realidade para buscar falhas e formas de minar os sistemas de defesa das potências adversárias, pois a guerra cibernética é considerada, neste início de século, a principal ameaça à segurança nacional. Segundo Rudzit (*apud* GUEDES, BRASIL e PAGANINE, 2012, p.38) os americanos reconhecem que as ações militares são cada vez mais dependentes do aparato tecnológico; para exemplificar o que pode ocorrer em um campo de batalha, ele explicou a seguinte situação:

> Quebrada essa estrutura de comando e controle baseada em tecnologia, para de funcionar a guerra moderna. Você está num tanque, numa tela, clicando o que outra unidade está vendo, o que um avião está vendo. Se você quebra isso, eles param e deixam de funcionar, como essa máquina de guerra que eles têm. Então, tecnologia passa a ser, hoje em dia algo fundamental (p.38) ".

Rudzit destaca que a maioria dos países estão empenhados em se preparar para esta modalidade de guerra, "organizações terroristas adorariam quebrar toda a rede de eletricidade da costa leste americana. Imagine o caos? E se for a rede bancária? ". Ataques de proporções incalculáveis podem ser realizados por qualquer indivíduo que detenha conhecimentos do mundo cibernético e uma única pessoa pode desencadear um ataque a partir de sua casa.

Essa tem sido também uma preocupação das forças armadas brasileiras, o general Aderico Mattioli (*apud* GUEDES, BRASIL e PAGANINE, 2012, p.38) tem o mesmo entendimento quanto ao risco de o país receber um ataque cibernético. Para ele, o fato de o Brasil ser dependente de diversos programas, aplicativos e sistemas de computadores de empresas multinacionais, muito desses utilizados nas redes corporativas e governamentais, põe a segurança nacional vulnerável, pois falta ao país um "simples programa antivírus genuinamente nacional".

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) tem coordenado uma série de ações voltadas para a elaboração da Proposta de Política Nacional de Segurança da Informação (PNSI) com o objetivo de estabelecer uma estrutura e modelo de governança para a integração e a coordenação nacional das atividades de segurança da informação, em um cenário de crescentes ataques cibernéticos e elevada interdependência das tecnologias da informação (GSI/PR, 2018). Os gráficos a seguir demonstram o total de incidentes de segurança da informação reportados ao CERT.br por ano de 1999 a 2017; os tipos de ataques realizados de janeiro a dezembro de 2017 e as origens desses ataques de janeiro a dezembro de 2017:

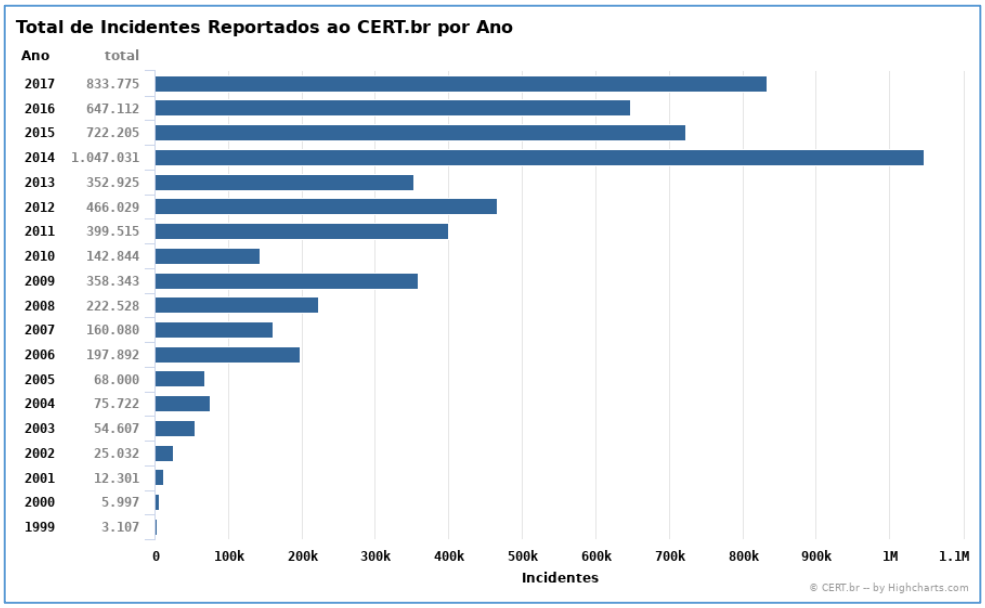

Figura 2.2.1 – Total de Incidentes Reportados ao CERT.br no Ano (CERT, 2018)

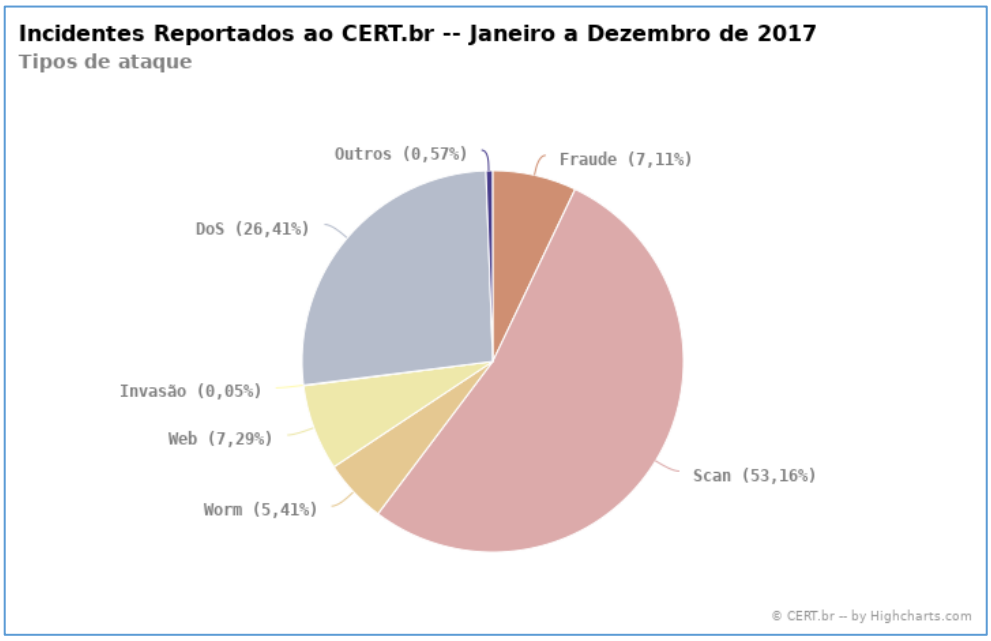

Figura 2.2.2 – Incidentes Reportados ao CERT.BR – janeiro a dezembro de 2017 (CERT, 2018)

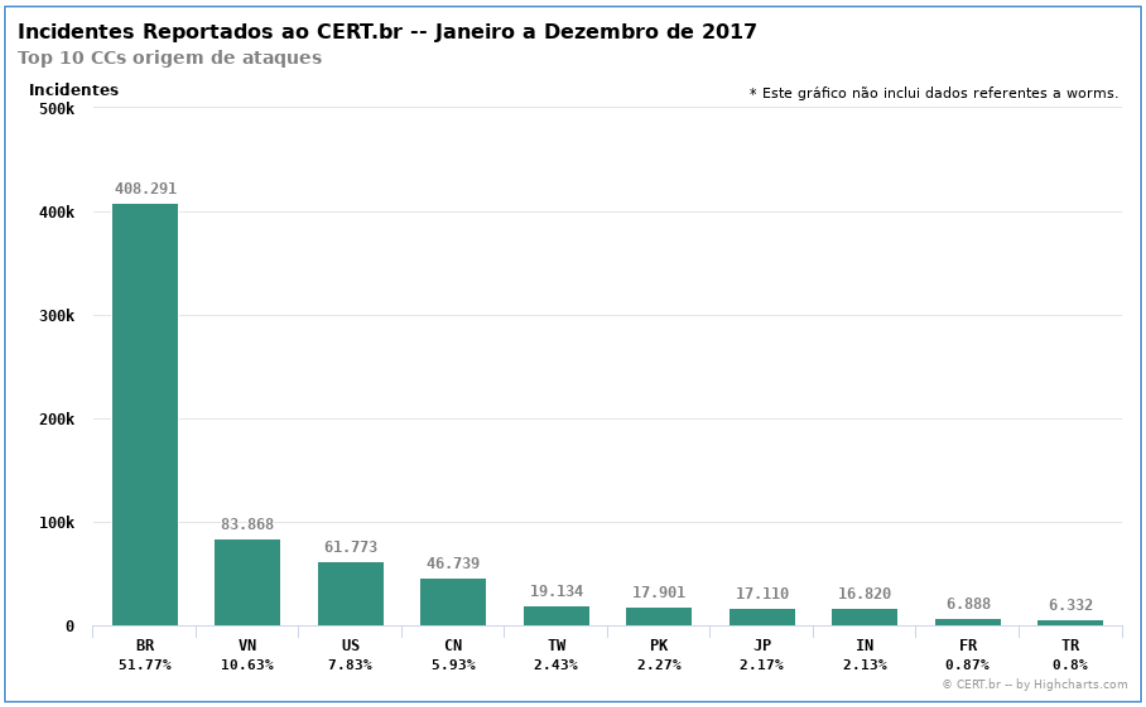

Figura 2.2.3 – Incidentes Reportados ao CERT.br – Janeiro a Dezembro de 2017 (CERT 2018)

Legenda dos países:

BR – Brasil; VN – Vietnã; US – Estados Unidos; CN - China; TW – Taiwan; PK – Paquistão; JP – Japão, IN – Índia, FR – França; TR - Turquia

O Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil é hoje responsável por tratar incidentes de segurança em computadores conectados à rede de dados em todo território nacional.

Atualmente o Brasil possui o seu próprio Centro de Defesa Cibernética, que segundo a doutrina militar brasileira (2014, p.13), o assunto é tratado como uma questão de soberania nacional, sendo que o país precisa estar preparado para "contrapor às ameaças externas, de modo compatível com sua própria dimensão e suas aspirações político-estratégicas no cenário internacional. "

> Na atual conjuntura mundial, caracterizada por incerteza, mutabilidade e volatilidade das ameaças potenciais, bem como pela presença de novos atores não estatais nos possíveis cenários de conflito, a sociedade brasileira, em particular a expressão militar do Poder Nacional, deverá estar permanentemente preparada, considerando os atuais e futuros contenciosos internacionais. Para tal, medidas deverão ser adotadas de forma a capacitá-la a responder oportuna e adequadamente, antecipando os possíveis cenários adversos à Defesa Nacional.

Existe ainda a preocupação em relação ao "aumento do risco de perpetração de ataques por Estados, organizações e até mesmo pequenos grupos, com as mais diversas motivações". Em razão desses fatos, a Defesa Cibernética tem trabalho em todos os escalões de comando por meio da proteção de ativos de informação, de forma a impedir que o oponente exerça a quebra de segurança da informação.

A Estratégia Nacional de Defesa (END) elaborada em dezembro de 2008 "estabeleceu prioridade em três setores estratégicos para a Defesa Nacional: Nuclear, Cibernético e Espacial". Conforme a Diretriz Ministerial nº 14, de 2009 do Ministério da Defesa, do dia 09 de novembro de 2009, estabeleceu ao Exército Brasileiro a responsabilidade pela coordenação e pela integração do Setor Cibernético. Em 20 de setembro de 2012, o Decreto Presidencial nº 7.809 incluiu na Estrutura Regimental do Comando do Exército, o Centro de Defesa Cibernética.

Neste contexto, observou-se que a mobilização do governo brasileiro para fomentar a sua defesa cibernética ocorreu no mesmo ano do conflito entre a Rússia e a Geórgia como se poderá verificar no capítulo seguinte.

3. ESTUDO DE CASO: RÚSSIA X GEÓRGIA

Este capítulo apresenta um breve contexto histórico em relação ao conflito bélico ocorrido entre as nações da Rússia e Geórgia, em agosto de 2008. Por último, trata da guerra cibernética a fim de demonstrar como ocorreu o ataque aos servidores de dados da Geórgia e como isso foi usado para uma posterior invasão do exército russo lá.

3.1. RÚSSIA E A GEÓRGIA

A Rússia é considerada o país mais extenso do planeta, possui 11 fusos horários, que vai do estreito de Bering, a leste, até o limite com a Estônia, a Oeste. No período da União Soviética chegou a ser aproximadamente três vezes o tamanho do Brasil (AGUIAR, 2002, p. 203). De acordo com o sítio da Embaixada da Federação da Rússia no Brasil, sua área total é de 17.125.178 quilômetros quadrados[9]. A Rússia faz fronteira com 18 países, sua população é de 146 milhões de pessoas. Moscou é a capital do país e a língua oficial é o russo. Mas a Rússia é considerada um estado multinacional, composta por representantes de 176 nações e nacionalidades, de diferentes religiões e que falam mais de cem idiomas.

Após a revolução comunista, formou-se a União Soviética, que tipificava uma federação de Estados soberanos, uma união voluntária, não-exploradora, "um modelo para uma mais ampla integração de outros países e fragmentos dos impérios europeus" (SUNY, 2008 p. 86). No entanto, o seu fim ocorreu em 1991 com o golpe que tinha o objetivo de tirar Mikhail Gorbachev do poder. Boris Yeltsin derrotou os golpistas e assumiu a posição de líder político soviético e assinou em conjunto com a Ucrânia e Bielorrússia o acordo de Minsk para dissolução da União Soviética e a criação da Comunidade dos Estados Independentes – CEI (XAVIER, 2010, pag. 10), conforme se pode verificar no mapa a seguir:

[9] No sítio da Embaixada da Federação da Rússia existe um erro ao mencionar a extensão territorial: "17.125.178 metros quadrados", mas em consulta em outras fontes, entende-se que são quilômetros quadrados.

Figura 3.1.1- a Rússia é o maior país do mundo. Fonte: Gazeta do Povo, 2011[10]

Um dos motivos da União Soviética ter perdido a guerra fria com os Estados Unidos ocorreu por causa do retrocesso tecnológico que ela enfrentou nos anos 80. Esse déficit no campo da investigação científica e tecnológica teve várias causas, uma delas se deu pela "fuga de cérebros", milhares de cientistas russos fugiram para países estrangeiros em busca de melhores condições de vida e trabalho. Outros motivos foram a degradação do nível de ensino do país, a corrupção, a burocracia, e principalmente a falta de investimento em pesquisa científica e renovação no parque tecnológico (MILHAZES, 2009).

> Constatada a situação de crise no início da década de 80, impõe-se explicar as razões da desaceleração da economia soviética. Em seu informe perante a sessão plenária do CC do PCUS de 11 de junho de 1985, Gorbatchev denunciou o que se seriam as principais mazelas da economia soviética: atraso tecnológico; desperdício crescente de matérias-primas e energia; baixa qualidade de muitos produtos industriais, que acarretava sua baixa competitividade no mercado mundial; baixo rendimento dos investimentos, excessivos e em grande parte efetuados em obras inacabadas e uma planificação desequilibrada e crescentemente desarticulada (MANDEL, 1989, p. 25, *apud* RODRIGUES, 2006, p.164).

Segundo Rodrigues (2006, p. 179) durante a década de 70 o atraso tecnológico da URSS não era significativo no domínio da pesquisa científica em relação aos países europeus, EUA e Japão, pois "os físicos e matemáticos soviéticos destacavam-se entre os melhores do mundo. Os livros de cálculo integral e diferencial russos, por exemplo, eram referências, sendo utilizados em cursos de ciências exatas em todo o mundo".

[10] https://www.gazetadopovo.com.br/mundo/paradoxo-russo-aqzgon438enc8m1berttejo7i/

Rodrigues (p. 181) defendeu uma tese contrária ao apresentado por Milhazes, que não foi a falta de nível cultural e de qualificação técnicas dos profissionais soviéticos e muito menos questões de falta de pesquisa e de desenvolvimento técnico e científico que levou à estagnação da evolução tecnológica. A sua tese se baseava na questão que o sistema soviético não conseguiu reproduzir a revolução tecnológica que mudava o mundo nos anos 80, "pois esta pressupunha um grau mínimo de flexibilidade, democracia e liberdade de informação, exatamente aquilo que o sistema negava aos cidadãos soviéticos. E neste aspecto, demonstrou-se menos flexível que as democracias capitalistas".

Após o fim da guerra fria, os russos trabalharam para se atualizar tecnologicamente, inclusive teriam atuado nos assuntos norte-americanos, como ocorrido nas eleições de 2016. Segundo Arraes (2017, p.3) "especula-se que Moscou teria conseguido acesso ao cadastro dos votantes, ao infiltrar-se em uma das empresas – terceirizadas – responsáveis pela organização do pleito". Para exemplificação, Arraes argumentou que uma forma de embaraçar o processo eleitoral havia envolvido o longo tempo para verificação da identidade dos eleitores em distritos tipicamente democratas, conforme pesquisas realizadas. Isso desmotivou o voto de cidadãos que se depararam com longas filas, pois nos EUA o voto não é obrigatório e a eleição não é feriado nacional. Arraes (2017, p.2) considerou a doutrina Gerasimov[11] como "alcunha destinada a caracterizar ações, ou melhores ingerências, algures pelo segmento da contrainformação através de meios recentes e sofisticados como o cibernético".

Já a Geórgia fica localizada na região da Europa Oriental e faz fronteira com a Rússia, Turquia, Armênia, Azerbaijão e o Mar Negro. Possui um território de 69.700 quilômetros quadrados. Atualmente, a população é de cerca de 3.718,20 milhões, segundo o censo de 2017, do Escritório de Estatística Nacional da Geórgia. A capital e principal cidade é Tbilisi.

Em 1918, a Geórgia se declarou independente com a Revolução Russa. De 1919-1920, a Ossétia do Sul combateu a Geórgia com apoio bolchevique. Em 1921, a Geórgia foi conquistada pelos comunistas. Somente em 1991, a Geórgia declarou independência e a União Soviética apoiou os separatistas da Ossétia do Sul. No ano seguinte, um cessar-

[11] Doutrina Gerasimov em referência ao oficial general chefe do Estado Maior da Rússia desde 2012 (ARRAES, 2017, p02).

fogo interrompeu a guerra civil, com Ossétia do Sul e também Abecásia mantendo regimes autônomos com a presença de forças russas autorizadas no acordo. Em 2004, Mikheil Saakashvili assumiu a presidência da Geórgia e buscou a reunificação do país e aproximação com União Europeia e OTAN.

No entanto, no mês de abril de 2008, a crise entre a Geórgia e a Rússia piorou, sendo que a Rússia estabeleceu laços com áreas pró-Moscou. Por fim, em agosto de 2018, a Geórgia atacou a Ossétia do Sul no dia 7; no dia seguinte, a Rússia invadiu a Geórgia.

As imagens a seguir demostram como eram os mapas do período de incorporação do Império russo das terras do Cáucaso, a independência da Geórgia e posteriormente a separação da Ossétia do Sul e Abecásia em 1992.

Figura 3.1.2 – Geórgia e Rússia têm relação conflituosa desde os tempos dos czares (GIELOW, 2018)

3.2. CONFLITO BÉLICO E A GUERRA CIBERNÉTICA

O conflito entre a Rússia e a Geórgia não apenas envolveu a região como a Ossétia do Sul, como também teve repercussão sobre a região da Abecásia. Tanto a Abecásia quanto a Ossétia do Sul governam-se como Estados independentes e buscam há anos obter o reconhecimento de sua soberania pelo governo georgiano e pela comunidade internacional, que as consideram parte da Geórgia (RANDIG, 2008).

Segundo Ramina (2010, p. 3693), a ofensiva russa no Cáucaso foi defendida por alguns como um retorno às políticas da antiga União Soviética, ou seja, o renascimento do poder econômico, político e militar da Rússia, que havia saído da experiência comunista aniquilada, constituindo uma nova realidade na região. Para Freire e Simão (2014, p. 92) a guerra na Geórgia no verão de 2008 teve como elemento central o fato da Rússia "se afirmar no espaço pós-soviético perante a ingerência crescente ocidental, e acima de tudo, perante um conjunto de políticas e ações liderados pelos EUA em particular", o que colocava em risco a segurança da Rússia. A exemplo do projeto do escudo de defesa antimíssil e a ampliação da aliança ao espaço dos países da CEI.

Quando Mikhail Saakashvili foi eleito presidente da Geórgia em 2004, os laços com os Estados Unidos foram fortalecidos e as intenções eram de se aproximar da OTAN que tinha como promessa a incorporação da Ossétia do Sul e Abecásia. Ocorreu que em 2008 a Rússia que na época o primeiro-ministro era Vladimir Putin estabeleceu relações formais com as duas regiões separatistas, integradas economicamente ao país apesar de serem consideradas pela ONU como parte da Geórgia" (GIELOW, 2018, p. A18). Em 8 de agosto de 2008, a Rússia atacou a Geórgia em resposta à tentativa desse país de reincorporar pela força, a região da Ossétia do Sul (MIELNICZUK, 2013).

> O que talvez não tenha sido previsto por Saakashvili foi a reação russa. No dia seguinte, ataques aéreos começaram e 70 mil homens mobilizados para um exercício militar no norte do Cáucaso entraram em ação com outros 9.000 soldados separatistas. Navios russos no mar Negro foram acionados e, ao fim do conflito, soldados de Moscou já ocupavam território georgiano fora das duas áreas separatistas. Os cerca de 25 mil homens de Saakashvili estavam perdidos (GIELOW, 2018, A18).

Para que a ofensiva russa ocorresse, houve uma preparação de invasão, sobretudo depois do reforço de tropas russas acima dos seus níveis habituais, de múltiplas violações do espaço aéreo georgiano por aviões russos, a derrubada de aparelhos georgianos de vigilância sem piloto e de um exercício militar em larga escala perto da fronteira (KAKACHIA, 2008). Cerca de 1.100 pessoas, sendo que 400 delas eram civis, morreram no conflito e aproximadamente 200 mil perderam seus lares (GIELOW, 2018, A18).

A matéria do G1, de 19/08/2008, noticiou o início do ataque russo contra a Geórgia - "Bombardeio virtual de hackers" - que começou no dia 20 de julho. Segundo especialistas, foi a 1ª vez que ação o ataque cibernético coincidiu com guerra real.

> Semanas antes de começarem a cair bombas reais na Geórgia, um pesquisador de segurança no subúrbio de Massachusetts, nos EUA, assistia a um ataque contra o país no ciberespaço (...).

> Outros especialistas em internet nos Estados Unidos dizem que os ataques contra a infraestrutura da rede da Geórgia tiveram início em 20 de julho, com barragens coordenadas de milhões de pedidos – conhecidos como ataques distribuídos de negação de serviço (ou DDoS, na sigla em Inglês) – que sobrecarregaram certos servidores georgianos. O governo da Geórgia culpou a Rússia pelos ataques, mas os russos negaram envolvimento.

Essa matéria relatou ainda que o ataque de negação de serviço no mês de julho de 2008 pode ter sido um ensaio para uma guerra cibernética assim que os disparos começaram entre Geórgia e Rússia. Korns e Kastenberg (2009, p.1) relataram que três semanas depois, no dia 8 de agosto, especialistas em segurança da informação observaram um segundo grande ataque de DDoS contra os sítios eletrônicos da Geórgia. Analistas verificaram que este ataque coincidiu com o movimento de tropas russas na Ossétia do Sul em resposta às operações militares realizadas no dia anterior pelas tropas georgianas na região. No dia 10 de agosto, os ataques de DDoS tornaram inoperante a maioria dos sítios governamentais da Geórgia. "Durante essa fase, os ataques distribuídos de negação de serviço foram particularmente levados a cabo por botnets[12]" (SHAKARIAN, 2011, p. 67).

De acordo com Handler (2012, p.224), o objetivo principal da campanha de ataque cibernético russo era dar suporte à invasão russa na Geórgia, tendo como alvo a infraestrutura principal. A escalada de ciberataques foi significativo: 54 sítios eletrônicos da Geórgia ficaram inoperantes. Os alvos eram todos voltados para produzir benefícios para as forças militares russas e incluíam atingir os setores da imprensa e as áreas de comunicação que a princípio em uma guerra convencional seriam os primeiros pontos a serem atingidos por mísseis ou bombas no início dos combates. Por meio da negação de acesso a imprensa e aos sítios governamentais, os ataques cibernéticos atingiram sítios

[12] Uma botnet é uma rede de computadores conectados à internet [chamados de "zumbis" ou "bots" (diminutivo de robot ou robô — N. do T.)] e infectados por um aplicativo conhecido como malware. O malware permite que o servidor de "comando e controle" envie comandos a esses *bots*. *Botnets* são comumente utilizadas para lançar mensagens eletrônicas de campanhas publicitárias (spam), mas também podem ser usadas para iniciar ataques de negação de serviço em larga escala. Tipicamente, o "sequestro" dos computadores zumbis ocorre da mesma maneira que as infecções com outros tipos de vírus (por exemplo, mensagens eletrônicas e páginas falsas, falsos endereços eletrônicos, documentos infectados). Para que não seja detectada, a comunicação do computador de comando e controle com os computadores zumbis pode ser conduzida por meio de canais aparentemente inocentes (como um canal normalmente utilizado para bate-papos on-line). Organizações criminosas, como a Russian Business Network (RBN), usam e alugam *botnets* para uma variedade de propósitos. As *botnets* usadas no violento ataque contra os sítios internet na Geórgia eram afiliadas a organizações criminosas russas, incluindo a RBN7 (SHAKARIAN, 2011, p. 67).

críticos importantes para a comunicação entre as tropas e a população georgiana, que não sabia ao certo o que estava sendo atacado tanto no espaço cibernético como em território. Situação que dificultou a coordenação efetiva de um contra-ataque da Geórgia.

De toda forma, os ataques cibernéticos limitaram a resposta efetiva das forças da Geórgia às operações cinéticas da Rússia. Além do mais, os ataques cibernéticos tiveram um impacto psicológico importante na população local, criando pânico e confusão (HANDLER, 2012, p.224). Para Mshvidobadze (*apud* Giles 2011, p. 46) a Rússia vislumbrou a capacidade cibernética como ferramenta de guerra da informação articulada com o sistema de inteligência, contra inteligência, *maskirovka*[13], desinformação, guerra eletrônica, desativação do sistema de comunicações, degradação de suporte de navegação, pressão psicológica e destruição da capacidade computacional do inimigo.

As táticas de guerra utilizadas por ambos os lados desencadearam uma variedade de "operações de informação" - em inglês, Information Operations (IO). Pela Rússia, utilizou-se de operações de rede de computadores - em inglês, Computer Network Operations (CNO) cujo objetivo era desativar os sítios da Geórgia. Nesse contexto, a estratégia russa e as operações táticas se destacavam ao lidar com vulnerabilidades de segurança da informação e uso de defesa de rede de computadores - Computer Network Defense (CND) (BARKER, FERMAINT, NEFF, 2013, p.3).

O mesmo entendimento é apresentado por Giles (p. 51) que identificou como "tropas de informação" (Information Troops) nas forças armadas russas para fins de operações de informação. Panarin (*apud* Giles) chamou de Forças Especiais de Informação (Information Special Forces) que deveriam "preparar operações efetivas sob condições potenciais de crise", cuja orientação era cobrir todos os aspectos das operações de informação, incluindo o CNO. "O objetivo é certamente, criar centros que envolveriam os chamados ataques de "*hacker*" em território inimigo" (p.51).

> O pessoal das Tropas de Informação deve ser composto por diplomatas, peritos, jornalistas, escritores, publicitários, tradutores, operadores, técnicos em comunicação, *web designers*, *hackers*, e outros... Para construir uma rede de contramedidas de informação, é necessário desenvolver um centro para determinar a criticidade e a importância da informação à respeito do inimigo, inclusive **como eliminá-los psicologicamente**, e como conduzir uma guerra eletrônica, uma guerra psicológica, um sistema de contrapropaganda e operações de rede que inclua treinamento de hacker (BBC MONITORING, *apud* Giles, p.52, tradução nossa).

[13] É o antigo sistema de camuflagem soviético (KEATING, 1981, p.4).

O envolvimento de CNO na guerra contra a Geórgia foi negada pelo governo russo, mas o chefe da Segurança Nacional da Geórgia, Eka Tkeshelashvili, afirmou em 2009 que "(...) existem diversas evidências que esses ataques foram diretamente organizados pelo governo da Rússia" (SHACHTMAN, 2009, 1, *apud* BARKER, FERMAINT, NEFF, 2013, p.4). Shatchman ainda destacou a questão da Geórgia ter sofrido ataques de rede de computadores (Computer Network Attacks – CNA) três semanas antes dos disparos dos primeiros tiros. Uma unidade de consequências cibernéticas dos Estados Unidos (U.S. Cyber Consequences Unit – USCCU) reportou os seguintes eventos:

> Quando os ataques cibernéticos começaram, não havia nenhum indicativo de qualquer fase de reconhecimento ou mapeamento, mas os pacotes de dados foram direcionados para desativar as websites sob ataques. Isso indica que o reconhecimento e as escritas de scripts de ataques tinham sido realizados com antecedência (USCCU, 2009, 3, *apud* BARKER, FERMAINT, NEFF, 2013, p.04, tradução nossa).

De acordo com Hollis[14] (*apud* HADDCIK, 2014, p.2), as unidades de inteligência russa fizeram o reconhecimento de sítios importantes e fizeram infiltração nas redes militares da Geórgia e nas redes governamentais em busca de dados úteis para a realização dos ataques. O governo russo também organizou milícias cibernéticas russas, hackers irregulares de fora do governo com o objetivo de dar apoio às operações táticas militares e governamentais. Foi um período que tanto o governo como as milícias cibernéticas atuaram para desestruturar o espaço cibernético georgiano.

Mesmo com todas essas informações disponíveis, não se pode comprovar ao certo o envolvimento da Rússia nos ataques cibernéticos à Geórgia, devido à dificuldade de se localizar com exatidão de quais redes de computadores partiram esses ataques. Por esse motivo, Moscou mantém a sua versão de negar qualquer envolvimento no "apagão" cibernético da Geórgia (BARKER, FERMAINT, NEFF, 2013, p.5).

Enquanto isso, a capacidade de defesa cibernética da Geórgia foi bastante limitada e realizada de forma dispersa; a barreira de proteção das redes de computadores não foi eficiente para deter os ataques. A primeira resposta da Geórgia ao grande volume de atividades em sua infraestrutura de internet foi estabelecer mecanismos de filtragem para bloqueio de qualquer endereço IP (*internet protocol*) russo que acessasse as redes georgianas. Hagen (2012, p.10) apresentou algumas considerações sobre a análise

[14] David Hollis, analista sênior de política do Gabinete da Subsecretaria de Defesa para a Inteligência e oficial da reserva do exército do Comando Cibernético Americano.

realizada pela unidade de consequências cibernéticas (*U.S. Cyber Consenquences Unit*) que menciona que a maioria dos ataques saíram de servidores de dados da Rússia e que os bloqueios realizados pela Geórgia foram facilmente contornados, pois os *hackers* utilizaram servidores de outros países para continuar a desestabilizar os sítios da Geórgia.

Evidenciou-se também que o governo da Geórgia contatou de imediato a Estônia na esperança conseguir apoio em relação a sua vasta experiência após os ataques cibernéticos sofrido no ano anterior, já que não havia nenhuma organização internacional que pudesse orientá-los. A única contramedida defensiva realmente eficaz que os georgianos alcançaram sucesso foi conseguir manter alguns canais de informação abertos ao público por meio da transferência de ativos de rede e hospedagem de sítios em servidores de outros países, como os Estados Unidos, Estônia e Polônia. Essas medidas muitas vezes foram realizadas por terceiros, como empresas privadas. O sítio da presidência da Geórgia foi transferido para os servidores da Google na Califórnia. O do Ministério da Defesa para uma empresa privada em Atlanta, o do Ministério das Relações Exteriores para servidores da Estônia e a Polônia autorizou a hospedagem dos sítios georgianos nos servidores do governo polonês (TIKK et al *apud* HAGEN, 2012, p.11).

Segundo Clarke e Knake (*apud* HAGEN, 2012, p.11) a empresa americana Tulip Systems ofereceu seus serviços à Geórgia com o objetivo de possibilitar o acesso aos sítios do país, mas sem aprovação do governo americano. Após o fim do conflito, a empresa relatou que também sofreu ataques cibernéticos em seus servidores de internet.

> A reação georgiana aos ataques russos consistiu, primeiramente, na filtragem de endereços IP russos. Contudo, os hackers russos se adaptaram rapidamente e usaram servidores não russos ou endereços IP falsificados. Os georgianos, então, transferiram muitos de seus sítios para servidores localizados fora do país (principalmente nos Estados Unidos). Não obstante, mesmo esses servidores no exterior permaneceram suscetíveis à exploração por inundação, devido ao grande volume de força bruta empregado no ataque russo (BUMGARNER E BORG *apud* SAKARIAN, 2011, p. 69).

Korns e Kastenberg (*apud* HAGEN, 2012, p.12) mencionaram que se na época do conflito se existisse uma legislação internacional que tratasse da soberania do espaço cibernético, o simples fato de usar servidores de dados de outros países poderia ter potencializado e ampliado a escalada do conflito. Os ataques em grande escala aos bens de um país geralmente exigem o envolvimento do governo. Essa realocação de ativos cibernéticos poderia ter envolvido os Estados Unidos, a Polônia ou a Estônia no conflito russo-georgiano, política ou militarmente. Questões como derrubar sítios de internet são

muitas vezes considerados crimes cibernéticos. Korns e Kastenberg alegaram que essas classificações deveriam ser reconsideradas caso fossem aplicados como ferramenta de guerra e não simplesmente como crime comum. O uso de ativos cibernéticos abriria novo precedente nessas operações e precisaria ser tratada no futuro por causa da sua capacidade de envolvimento de outros atores em um confronto, o que impactaria a neutralidade.

4. CONCLUSÃO

A pesquisa apresentada no trabalho quanto à guerra cibernética ser futuro desdobramento da guerra regular ou irregular, o estudo de caso demonstrou que ela ocorreu em ambos os desdobramentos. Em relação à hipótese, constatou-se ser factível que as transformações tecnológicas operadas na sociedade moderna afetaram a forma de fazer a guerra.

Especificamente, verificou-se que a Rússia iniciou semanas anteriores à invasão da Geórgia grande ataque cibernético e manteve esta tática de guerra irregular durante o processo de ocupação no território da Geórgia, com a finalidade de "isolar e silenciar" os georgianos. A população enfrentou uma derrota significativa, que se manifestou no âmbito psicológico e da informação, pois ficou incapacitada de transmitir ao mundo o que ocorria.

Mesmo tendo durado pouco, a guerra regular foi vencida pelas forças russas que utilizaram combates pesados, aéreos, navais e terrestres, para subjugar o poderio militar georgiano. Nesse caso, o combate bélico foi inevitável, com baixas para ambos os lados. Infere-se que o ataque cibernético servirá de ferramenta militar para qualquer conflito internacional e não se dará somente no âmbito militar, mas terá a participação do civil nacional, estrangeiro e empresarial, como se verificou neste estudo. Ou seja, civis que estejam envolvidos em uma causa ideológica ou simplesmente que estejam interessados em usar os seus conhecimentos como uma forma de lograr lucros. E também por empresas que estejam engajadas com a tecnologia da informação e de telecomunicações.

Muito embora Moscou negue a sua participação no ataque cibernético à Geórgia, conclui-se que a Rússia foi beneficiada pelos seus efeitos e essa é uma possibilidade factível de continuar acontecendo em conflitos futuros. O fato é que o *modus operandi* de planejamento e tática de guerra deverá ser ajustado quanto ao reconhecimento e vigilância cibernéticos, tendo como base a capacitação do inimigo na área cibernética.

A lição aprendida é que um país deve saber, a par da defesa convencional, proteger-se dos ataques cibernéticos; se for possível isso, saberá também valer-se do instrumento do atacar seu adversário com sucesso.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Francisco. **Estratégia o grande debate Sun Tzu e Clausewitz**. Esfera do Caos Editores, Lisboa, 2006.

ALMEIDA, Fábio Chang. **O historiador e as fontes digitais: uma visão acerca da internet como fonte primária para pesquisas históricas**. AEDOS, v. 3, n. 8, 2011. Disponível em < http://www.seer.ufrgs.br/aedos/article/view/16776 >. Acesso em: setembro de 2018.

ALMEIDA, Gisele Iecker. **Futuro e história: análise da temporalidade atual.** História da historiografia, n. 15, p. 51-69, 2014. Disponível em: < https://goo.gl/JApBtS > Acesso em: novembro de 2018.

ARRAES, Virgílio. **"Rússia: a aplicação incidental da doutrina Gerasimov"**. Mundorama – Revista de Divulgação Científica em Relações Internacionais. 2017. Disponível em: < http://www.mundorama.net/?p=23880 >. Acesso em: setembro de 2018.

_____. **"Rússia: embaraço ao poderio dos Estados Unidos"**. Mundorama – Revista de Divulgação Científica em Relações Internacionais, 2017. Disponível em: < http://www.mundorama.net/?p=23670 >. Acesso em: setembro de 2018.

AZEVEDO, Carlos. **Meios de Comunicação como armas de guerra.** 2001. Disponível em: < https://goo.gl/o8skKe > Acesso em: setembro de 2018.

BEAUFRE, A. **Introdução à Estratégia**. Trad. Araripe, Luiz de Alencar. Rio de Janeiro: Biblioteca do Exército, 1998.

BRASIL. MINISTÉRIO DA DEFESA. **Doutrina Militar de Defesa**. MD51-M-04. 2ª ed., 2007. Disponível em: < https://goo.gl/7tYGXh > Acesso em: abril de 2018.

_____. MINISTÉRIO DA DEFESA. **Doutrina Militar de Defesa Cibernética**. MD31-M-07. 1ª ed., 2014. Disponível em: < https://goo.gl/cHWJDg > Acesso em: agosto de 2018.

_____. GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA. **Objetivo do Plano Nacional de Segurança da Informação**.

Disponível em: < http://dsic.planalto.gov.br/pnsi/objetivo > Acesso em: maio de 2018.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Estatística de Incidentes Janeiro a Dezembro de 2017**. Disponível em: < https://www.cert.br/stats/incidentes/ > Acesso em: maio de 2018.

CLAUSEWITZ, Carl. **Da guerra**. WWF Martins Fontes, 2017.

COUTINHO, Luciano. **A terceira revolução industrial e tecnológica. As grandes tendências das mudanças.** Economia e sociedade, v. 1, n. 1, p. 69-87, 1992. Disponível em: < https://goo.gl/FGKCMq > Acesso em: novembro de 2018.

CREVELD, Martin V. **Ascensão e declínio do Estado**. Tradução Jussara Simões. São Paulo: Martins Fontes, 2004.

_____. **The transformation of War**. Ed. The Free Press, New York – NY, 1991.

COPELAND, B. Jack. **The Modern History of Computing**. Stanford Encyclopedia of Philosophy. Revisão 2006. Disponível em < https://plato.stanford.edu/entries/computing-history/ > Acesso em: maio de 2018.

COSTA, Cristiano R. A. da. **Evolução da Arte da Guerra – Das Gerações da guerra Moderna aos Conflitos Assimétricos. Parte 4 e 5 – A Quarta Geração da Guerra Moderna.** JRI – Jornal de Relações Internacionais, 2017. Disponível em < https://goo.gl/62ovEB >. Acesso em: outubro de 2018.

DIANA, Daniela. **História e Evolução dos computadores**. Toda Matéria, 2018. Disponível em < https://goo.gl/2sAZZR > Acesso em: maio de 2018.

DICIONARIOETIMOLOGICO.COM.BR. Dicionário Etimológico – Etimologia e Origem das Palavras. **Origem da palavra guerra**. Disponível em < https://www.dicionarioetimologico.com.br/guerra/ >. Acesso em: abril de 2018.

DUROSELLE, Jean-Baptiste. **Todo império perecerá.** Tradução de Ane Lize S. de S. Magalhães. Brasília. Ed. Universidade de Brasília: São Paulo. Imprensa Oficial do Estado, 2000. 484 p.

DUTRA, André Melo Carvalhais. **Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto.** IX Simpósio de Guerra Eletrônica, 2007. Disponível em < http://www.sige.ita.br/anais/IXSIGE/Artigos/GE_39.pdf >. Acesso em: outubro de 2018.

EMBAIXADA DA FEDERAÇÃO DA RÚSSIA NA REPÚLICA FEDERATIVA DO BRASIL. **Rússia – Informação Geral**. Disponível em < https://goo.gl/bxnYdR >. Acesso em: setembro de 2018.

FONSECA FILHO, Cléuzio. **História da computação: O Caminho do Pensamento e da Tecnologia**. EDIPUCRS, 2007. Disponível em < https://goo.gl/xWkekF > Acesso em: maio de 2018.

FREIRE, Maria Raquel; SIMÃO, Licínia. **A Rússia e o Cáucaso do Sul: das relações neocoloniais à realpolitik no" estrangeiro próximo"**, Imprensa da Universidade de Coimbra p. 85-112, 2014.

FRIEDMAN, George. **Os próximos 100 anos: uma previsão para o século XXI.** Tradução: Gabriel Zide Nero. Rio de Janeiro. Best Business, 2009.

GIELOW, Igor. **Guerra que fez de Putin vilão também consolidou seu poder – Cinco dias de conflito em 2008 com a Geórgia mudaram equilíbrio geopolítico.** Folha de São Paulo – Mundo A18, domingo, 12 de agosto de 2018.

GILES, Keir. **"Information Troops" – a Russian Cyber Command?"** Conflict Studies Research Centre, Oxford, UK. 3rd Internacional Conference on Cyber Conflict, Tallinn, Estonia, 2011. Disponível em: < https://goo.gl/fkWBSy >. Acesso em: agosto de 2018.

GUEDES, Sylvio; BRASIL, Thâmara; PAGANINE, Joseana. **Inimigos invisíveis: a guerra cibernética.** Revista Em Discussão. Senado Federal. Ano 3 - nº 10 – março de 2012. Disponível em: < https://goo.gl/1osQXa > Acesso em: maio de 2018.

HANDLER, Stephenie Gosnell. **"The new cyber face of battle: developing a legal approach to accommodate emerging trends in warfare."** Stanford Journal of International Law, Winter 2012, p. 209+. Disponível em: < https://goo.gl/hYfpBT >. Acesso em: agosto de 2018.

HADDICK, Robert. **This week at war: Lessons from cyberwar I – How Russia pioneered the use of cyberattacks as military tactic.** Foreignpolicy, 2011. Disponível em: < https://goo.gl/dD8hRK > . Acesso em: setembro de 2018.

HAGEN, Andreas. **The Russo-Georgian War (2008): The Role of the Cyber Attacks in the Conflict**. The Armed Forces Communications and Electronics Association, 2012. Disponível em: < https://goo.gl/wnba2U > Acesso em: setembro de 2018.

HOBBES, Thomas. **Leviatã ou matéria, forma e poder de um estado eclesiástico e civil.** Trad. João Paulo Monteiro; Maria Beatriz Nizza da Silva, 1999.

KAKACHIA, Kornely K. **A guerra dos cinco dias. Relações Internacionais** (R: I), n. 20, p. 33-43, 2008. Disponível em: < https://goo.gl/7YJXpD >. Acesso em: julho de 2018.

KEATING, Maj Kenneth C. **U.S Army Russian Institute – Student research report: Maskirovka – The Soviet System of Camouflage.** Garmisch, Germany, 1981. Disponível em: < https://goo.gl/Xfc2rE >. Acesso em: agosto de 2018.

KEEGAN, John. **Uma História da Guerra**. Tradução Pedro Maia Soares. São Paulo: Schwarcz Ltda, 1993.

KORNS, Stephen W.; KASTENBERG, Joshua E. **Georgia's cyber left hook**. ARMY WAR COLLEGE CARLISLE BARRACKS PA STRATEGIC STUDIES INSTITUTE, 2009. Disponível em: < https://goo.gl/SKKpVB > Acesso em: agosto de 2018.

LIND, William S. **Compreendendo a guerra de quarta geração**. Military Review, v. 85, n. 3, p. 12-17, 2005. Disponível em < https://goo.gl/y16ra9 >. Acesso em: abril de 2018.

MAGNOLI, Demétrio. Organizador. **História das guerras**. 3. São Paulo: Contexto, 2006.

MAQUIAVEL, Nicolau. **A Arte da Guerra**. Tradução e notas de Eugênio Vinci de Moraes. Porto Alegre – RS: L&PM, 2011.

MIELNICZUK, Fabiano. **O Conflito entre Rússia e Geórgia: uma revisão histórica.** Estudos internacionais: revista de relações internacionais da PUC Minas, v. 1, n. 2, p. 157-166, 2013. Disponível em: < https://goo.gl/KJFEVF >. Acesso em: julho de 2018.

MILHAZES, José. **Dirigentes russos reconhecem crise tecnológica no país.** 2009. Disponível em: < https://goo.gl/4JqHdm > Acesso em: setembro de 2018.

MORIMOTO, Carlos E. **O ENIAC – A História da Informática** (Parte 6: Sistemas embarcados e supercomputadores). Hardware.com.br, 2011. Disponível em: < https://goo.gl/trbamV > Acesso em: maio de 2018.

NOGUEIRA, Michel Gomes. **O uso do processo de e-Discovery como forma de aprimoramento da segurança da informação**. Dissertação de Mestrado. Publicação PPGENE.DM – 624/2016. ENE/FT/UnB, 2016. Disponível em: < https://goo.gl/2DwrbS >. Acesso em: abril de 2018.

RAMINA, Larissa Liz Odreski. **O Princípio da Autodeterminação dos Povos e seus Paradoxos:** A Aplicação na Guerra do Cáucaso de 2008. Anais do XIX encontro Nacional do CONPEDI, 2010. Disponível em: < https://goo.gl/b6mg97 >. Acesso em: julho de 2018.

RANDIG, Rodrigo Wiese. **Guerra na Ossétia do Sul: a Geórgia como foco de conflito entre a Rússia e o Ocidente.** Meridiano 47, v. 9, n. 97, p. 21, 2008. Disponível em: < https://goo.gl/8MQc9H >. Acesso em: julho de 2018.

RIBEIRO, Raimundo D. P. **Memória e contemporaneidade: as tecnologias da informação como construção histórica**. Disponível em < https://goo.gl/K5JQNc > Acesso em: outubro de 2018.

RODRIGUES, Robério Paulino. **O colapso da URSS: um estudo das causas**. Tese de Doutorado. Universidade de São Paulo, 2006. Disponível em: < https://goo.gl/9avGEc > Acesso: setembro de 2018.

SARAIVA, Márcio. **Um "exame de DNA" na carreira de dois grandes cientistas para descobrirmos o "pai" da nossa profissão. 2009.** Disponível em < https://goo.gl/G5JzS7 > Acesso em: maio de 2018.

SHAKARIAN, Paulo. **Análise da Campanha Cibernética da Rússia Contra a Geórgia**, **em 2008**. Kansas: Military Review, 2011. Disponível em: < shorturl.at/cGMY2 > Acesso em: outubro de 2018.

STORTI, Janaina Marques. **Enfrentando as novas ameaças: estrategia e politica internacional norte-americanas no pós-guerra fria**. Dissertação de Mestrado, UNICAMP, Campinas – SP, 2009. Disponível em: < https://goo.gl/s8wXPu > Acesso em: setembro de 2018.

SUN-TZU. **A Arte da Guerra: Por uma Estratégia Perfeita**. Tradução Heloísa Sarzana Pugliesi, Márcio Pugliesi – São Paulo: Madras, 2005.

SUNY, Ronald G. **Ascensão e queda da União Soviética: o império de nações**. Lua Nova, n. 75, São Paulo - SP, 2008. Disponível em: < http://www.scielo.br/pdf/ln/n75/05.pdf >. Acesso em: setembro de 2018.

TEIXEIRA, Ana Paula T. **Breve panorama de uma nova "guerra": os conflitos cibernéticos**. Café História, 2017. Disponível em: < https://bit.ly/2LZo0iT >. Acesso em: outubro de 2018.

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

XAVIER, Fernanda O. **Episódios da Guerra Fria: seu início, meio e fim**. Diálogo e Interação, vol. 4, 2010. Disponível em: < https://goo.gl/i2iMZA >. Acesso em: setembro de 2018.

WALTZ, Kenneth N. **O homem, o Estado e a Guerra.** Trad. Adail Ubirajara Sobral. Martins Fontes, São Paulo – SP, 2004.

WEBER, Max. **Economia e Sociedade - Fundamentos da sociologia compreensiva.** Trad. Regis Barbosa; Karen Elsabe Barbosa. Vol. 2. Brasília: UnB, 2004.