Clausewitz, a Ciberguerra e a Guerra Russo-Georgiana

Clausewitz, the Cyberwar and the Russian-Georgian War

DOI: 10.21530/ci.v15n3.2020.1065

Pedro Henrique Miranda Gomes[1]
Vágner Camilo Alves[2]

Resumo

Este artigo discute o conceito de "guerra cibernética" e outros afins, de modo a verificar e delimitar sua aplicabilidade técnica. A partir da revisão conceitual acerca do fenômeno da guerra, tal como se apresenta na obra de Clausewitz, são apontados elementos essenciais e generalizáveis a qualquer guerra. Posteriormente, as diferentes noções sobre "guerra cibernética" são esmiuçadas, buscando-se verificar até que ponto elas condizem com a teoria consolidada na área e se podem ser úteis para análise dos fenômenos bélicos contemporâneos. Em seguida, examina-se a Guerra Russo-Georgiana como estudo de caso para ilustrar a abrangência e os limites dos conceitos discutidos. Conclui-se que a ideia da "guerra cibernética" é, de fato, válida somente quando os instrumentos cibernéticos são empregados em assistência a operações convencionais de guerra, que envolvem destruição e aplicação de força cinética.

Palavras-Chave: Guerra Cibernética; Guerra Russo-Georgiana; Clausewitz.

1 Mestrando do Programa de Pós-Graduação em Estudos Estratégicos da Defesa e da Segurança (PPGEST/UFF), Rio de Janeiro, Brasil. (pedro_gomes@id.uff.br); ORCID: https://orcid.org/0000-0003-1881-3395.

2 Doutor em Ciência Política (IUPERJ, 2005), Professor Associado do INEST/UFF, Rio de Janeiro, Brasil. (vcamilo@id.uff.br); ORCID: https://orcid.org/0000-0002-4399-6835.

Artigo submetido em 12/04/2020 e aprovado em 29/07/2020.

Abstract

The present paper seeks to discuss the concept of "cyberwar" and others related to it so as to verify and to restrict its technical applicability. From a conceptual revision on the phenomenon of war as it appears in the work by Clausewitz, a number of essential and generalizable elements in any war are shown. Subsequently, different notions of "cyberwar" are scrutinized to verify how consistent they are with the consolidated theory in the field and whether they can be useful for the analysis of contemporary war phenomena. Then, the Russian-Georgian War is examined as a case study to to shed light on the breadth and limits of the concepts under discussion. It follows that the idea of "cyberwar" is, in fact, valid only when cyber instruments are employed as an aid to conventional military operations, which involve destruction and application of kinetic force.

Keywords: Cyberwar; Russian-Georgian War; Clausewitz.

Introdução

Assim como ocorre nas demais áreas do conhecimento, a comunidade epistêmica dos Estudos Estratégicos (EE) vê-se constantemente desafiada a adaptar-se à inexorável marcha do tempo, abarcando à teoria os novos fenômenos e problemáticas conceituais que a história lhe apresenta. Estando o léxico deste campo de estudo tradicionalmente concentrado em torno da guerra, verifica-se que os recentes e acelerados avanços tecnológicos o impactaram-no diretamente, tanto em seu aspecto operacional quanto social organizacional, resultando na revisão ou consolidação de conceitos tradicionais.

Não é de hoje que estrategistas veem seu objeto de estudo ser empregado discursivamente de forma metafórica, em expressões como "guerra comercial" ou a "guerra à pobreza" de Lyndon Johnson (Azevedo 2005). Contudo, o advento da tecnologia da informação se impôs de tal forma que se faz necessário separar o discurso em torno da ciberguerra da sua verificação concreta.

Considera-se que está em curso, hoje, uma RAM[3] liderada pelas tecnologias de informação e comunicação não oriundas de tecnologias especificamente militares, mas que combina a capacidade de monitoramento, comando e controle,

3 Revolução nos Assuntos Militares, ou RAM, pode ser definida como "uma grande mudança na natureza da guerra, resultante do emprego de novas tecnologias as quais, combinadas com as dramáticas mudanças na doutrina, nos conceitos operacional e organizacional militares, alteram fundamentalmente o caráter e a conduta das operações militares" (Longo 2007, 6).

computação e informação, com forças dotadas de armas precisas, em um "sistema de sistemas" (Longo 2007). Ao mesmo tempo, proliferam ataques cibernéticos liderados por grupos subnacionais, como nos casos do hacktivismo e ciber-crimes, ou capitaneados por Estados, como ciber-espionagem, sabotagem e outros. O objetivo central deste artigo será o de definir os conceitos que emergem com a tecnologia da informação e impactam na política internacional, de modo a delimitar o que pertence ao léxico dos EE.

Este esforço justifica-se pela gravidade das consequências práticas que têm as definições acadêmicas e institucionais para fenômenos ligados à estratégia. Conforme Sheldon (2013, 305, tradução nossa[4]), no que se refere ao ciberespaço, "o que é ou não incluído em qualquer definição poderá ter sérias implicações para a sua utilização estratégica". Isso porque a forma como as entidades políticas entendem os fenômenos estratégicos define quais situações são passíveis, por exemplo, de causarem uma guerra.

A metodologia aplicada consiste, primeiro, na revisão conceitual da definição de guerra e a subsequente análise dos conceitos-chave ligados ao tema guerra cibernética, utilizando-se bibliografia especializada. Este contraste permitirá delimitar de forma mais clara a amplitude prática do conceito de guerra cibernética, ao verificar em quais situações reais os elementos essenciais do fenômeno guerra encontram-se presentes em meio a um conflito cibernético.

De forma complementar, será realizado um estudo de caso da Guerra Russo-Georgiana, integrando os fenômenos aí observados aos conceitos desenvolvidos anteriormente, de forma a ilustrar a verdadeira abrangência da guerra cibernética. Nesse estudo, além de fontes ocidentais, em língua inglesa, espanhola e francesa, também são utilizadas fontes russas. O caso marca a ocorrência, pela primeira vez, de maior interface entre ações disruptivas no ciberespaço com manobras militares convencionais, o que o indica como exemplo por excelência de conflito cibernético dentro dos EE.

A Guerra Cibernética e os estudos estratégicos

A Guerra Clausewitziana

Maynard (2018), em texto apresentando diferentes abordagens em torno da guerra cibernética, aponta muito lucidamente que um elemento-chave para

4 Do original: what is not included in any definition may have serious implications for its strategic application

o entendimento da questão é a noção de violência. Para entendê-lo é preciso rever a concepção geralmente aceita de guerra no meio dos EE, elaborada por Clausewitz.

O autor prussiano define guerra como "um ato de violência destinado a forçar o adversário a submeter-se a nossa vontade" (Clausewitz 2014, 7). Mesmo Maynard (2018), que parte da tradução desta frase como "ato de força", aponta que, nesta concepção, este ato se dá sempre por meio de ações violentas. Aqui se encontra o cerne da discordância entre especialistas, variando a partir de definições mais amplas ou restritas de violência, ou força.

Uma visão mais ampla entende que "a violência pode se encontrar em quase qualquer situação coercitiva" (Limnéll *apud* Maynard, 2018, 470, *tradução nossa*[5]), enquanto um sentido mais estrito do termo importaria necessariamente na consecução de danos físicos ou morte. Os ataques contidos nesta última interpretação podem ser chamados de cinéticos (*kinetic*), termo que se liga à produção de danos materiais, tais como aqueles causados pela ação de um punho, uma espada ou uma bomba (Singer e Friedman 2014).

A última parece ser a interpretação mais adequada para "ato de violência", pois, do contrário, a noção de violência — ou de força — se confundiria com a de poder. Por sua vez, este é entendido como "toda probabilidade de impor a própria vontade numa relação social, mesmo contra resistências" (Weber 1999, v.1, 33), logo, incorporando elementos não materiais ou diretos de se fazer valer a própria vontade. Uma forma de diferenciá-la das noções de força ou violência é restringir tais noções ao seu aspecto não apenas coercitivo, mas também cinético, conforme definido acima.

Como resultado, para que uma ação coercitiva pudesse ser classificada como "guerra" seria necessário o elemento da destruição, do dano físico ou da morte, ou seja, um ataque cinético. Por fim, sendo a guerra, para Clausewitz, "continuação da política por outros meios" (Clausewitz 2014, 27), é-nos possível parafrasear, dentro do léxico dos EE, aquela que nos servirá de definição essencial deste fenômeno da seguinte forma: "a guerra é o embate violento entre agrupamentos humanos visando a consecução de um objetivo político".

O entendimento de violência a partir de um componente cinético facilita a posterior classificação de guerra, uma vez que a distinção pode ser feita tanto

5 Violence can be found in almost any coercive situation. Cabe destacar que, aqui, "situação coercitiva" é empregada em seu sentido amplo, não restrita apenas ao uso da força militar, mas outras ações, tais como roubo de dados e distúrbios a sistemas computacionais de outros governos (Maynard 2018).

em situações de conflitos tradicionais quanto contemporâneos. Os Estados (e outros agentes políticos) estão acostumados a um grande leque de ações que visam desestabilizar outro agente ou compeli-lo e que, independentemente disto, não configuram um ato de guerra. Muitas destas ações, já frequentes, podem ser simplesmente transpostas ao ambiente cibernético, sem modificar sua natureza, como a propaganda, espionagem e sabotagem, nas quais a ausência de um "ato de violência" torna pouco provável que se vá à guerra por causa deles.

Outro aspecto importante é a inerente reciprocidade da guerra. Nenhuma guerra pode ser pensada a partir de apenas um lado. Conforme explicitou Clausewitz (2014, 11): "a guerra não é a ação de uma força viva sobre uma massa inerte, mas, como a não resistência absoluta não seria guerra, ela é sempre a colisão de duas forças vivas". Este aspecto virá a ser particularmente relevante para debatermos a questão do anonimato, elemento intimamente ligado aos ataques cibernéticos.

Finalmente, antes de entrarmos em uma descrição mais profunda em torno do ciberespaço e da ciberguerra, é relevante frisar as consequências da junção da definição de guerra ao seu sentido inerentemente político. Clausewitz (2014) atrela à figura dos líderes políticos o elemento da razão em um contexto de guerra, no sentido da definição dos objetivos políticos que se buscam em meio ao ato de violência e a dimensão dos esforços que se está disposto a realizar para alcançá-los. Portanto, a guerra, cibernética ou não, é resultado da política e, como tal, no final do dia, é o líder político quem decide se uma ação levará à guerra ou não.

O Espaço Cibernético

Uma vez definidos os elementos essenciais ao fenômeno da guerra, resta-nos analisar os conflitos cibernéticos de modo a verificar se os mesmos elementos estão presentes. É conveniente partir do meio pelo qual os ataques ocorrem: o espaço cibernético (ou ciberespaço), que se diferencia da terra, do mar e do ar por se descolar, em um primeiro momento, do meio físico, da geografia e das fronteiras.

Singer e Friedman (2014, 13, *tradução nossa*[6]) definem o espaço cibernético, em sua essência, como "o domínio de redes de computadores (e os usuários

6 Do original: the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online.

por trás delas) no qual informação é guardada, compartilhada e comunicada *online*", ao que entendemos ser necessário adicionar, ainda, as estruturas físicas e o espectro eletromagnético que englobam esse domínio. Ações perpetradas pelo meio cibernético seguem lógicas próprias, e podem ocorrer em velocidades altíssimas e pulverizadas do ponto de vista espacial, mas há limites para esta liberdade, sobretudo ao incluirmos os usuários como elemento constituinte da definição.

Primeiramente, o espaço cibernético, por mais global que seja, não está fora do alcance dos Estados. Divisões podem ser criadas neste meio, da mesma forma que nações e países o foram no espaço material. Isto ocorre porque a comunicação em rede depende de infraestrutura física por onde os dados são transportados e armazenados. Essas infraestruturas, sejam os cabos submarinos que transmitem tais dados[7], sejam as entidades de administração dos nomes de domínio, são controladas por organizações privadas submetidas a leis de um país.

É neste aspecto, inerentemente geográfico, que a dimensão do alcance do Estado pode ser verificada. Os Estados, por exemplo, buscam controlar as portas de conexão entre seus países e a internet global, como faz Moscou ao aprovar lei de proteção da seção da internet global com conteúdo russo, a Runet (Iasakova 2019).

Da mesma forma que a infraestrutura, os usuários por trás dos computadores também respondem às leis dos países nos quais se encontram e onde praticam suas atividades. Assim, ataques cibernéticos e atividades ilícitas que ocorram dentro de um país podem ser considerados crimes e os responsáveis podem ser levados à justiça, enquanto os mesmos ocorridos fora têm que contar com previsões legais por parte do país de origem, bem como cooperação diplomática para alcançar os agentes delituosos.

Portanto, o ciberespaço não é, inteiramente, uma "terra de ninguém", um mais puro estado de natureza, uma vez que está, em alguma medida, submetido à ação e à regulação por parte dos Estados. Suas divisões, rotas, portas e fronteiras são, ao mesmo tempo, físicas e imaginárias, da mesma forma que uma fronteira imaginária divide o Brasil e o Uruguai, mas rodovias físicas ligam os dois países.

7 Pode-se ver os cabos conectando os países à rede global no *site* <https://www.submarinecablemap.com/>.

O Poder Cibernético e os Ciberataques

Uma vez delimitada a essência do ciberespaço, e entendendo-o como um meio de projeção de poder — tal como a terra, o mar, o ar e o espaço sideral — deve-se analisar as diferentes formas pelas quais este poder pode ser exercido. Similarmente ao que ocorre no debate em torno dos conflitos armados, no espaço cibernético a noção de "poder" é mais ampla do que a de "ato de violência", que é condição necessária para a verificação de uma guerra, de modo que se pode exercer poder sem necessariamente recorrer a um ato de violência.

Poder cibernético, portanto, transpondo o entendimento de poder para o meio cibernético, pode ser entendido, a partir da definição de Sheldon (2013, 306, *tradução nossa* [8]), como "a habilidade, em paz, crise ou guerra, de exercer influência pronta e sustentada no ciberespaço ou a partir dele". Em se tratando de uma proposta conceitual no âmbito dos Estudos Estratégicos, o autor adiciona, ainda, que "o poder cibernético é o processo de converter informação em efeito estratégico" (Sheldon 2013, 306, *tradução nossa* [9]), o que é apenas verdade em definições mais amplas do termo estratégia.

A literatura especializada majoritariamente entende os Estudos Estratégicos sob o prisma do Estado (Figueiredo 2010; Moreira 2010; Gray 1999, etc.). Contudo, a propagação do uso do ciberespaço para projeção de poder aponta para o fortalecimento de grupos não-estatais, de modo que indivíduos por trás de um computador podem causar mais dano do que células terroristas armadas (Kiras 2002).

Para além da definição de poder cibernético, há confusão acerca de uma das formas na qual ele se manifesta: os ataques cibernéticos. Sobretudo na mídia, o termo foi usado para uma miríade de fenômenos, desde roubo de dados até sabotagem de infraestrutura nuclear, ou ações coordenadas com engajamento no campo de batalha.

Para dirimir tal ambiguidade, um relatório do *National Research Counsil*, dos Estados Unidos, definiu ataques cibernéticos, ou ciberataques, como "ações deliberadas para alterar, interromper, enganar, deteriorar ou destruir sistemas ou redes de computadores ou a informação e/ou programas residindo

8 Do original: The ability in peace, crisis, and war to exert prompt and sustained influence in and from cyberspace.

9 Do original: Cyberpower is the process of converting information into strategic effect.

ou transitando nestes sistemas ou redes" (William et al. 2009, 1, tradução nossa[10]). Esta conceituação, ao delimitar mais adequadamente o que seriam ataques cibernéticos, ao mesmo tempo indica que eles podem ser desferidos em diversos âmbitos essencialmente diferentes entre si, incluindo o cibercrime, ciberespionagem, hacktivismo[11] ou ataques em contexto de guerra.

Ciberataques tornam-se mais danosos na medida em que, nas últimas décadas, evoluíram do âmbito da comunicação e do comércio virtual para atingir as chamadas infraestruturas críticas, abrangendo setores essenciais à civilização moderna, como o setor bancário, eleitoral, sistemas de transporte, de água, de energia e outros (Singer e Friedman 2014). Isso faz com que um ciberataque seja um golpe particularmente efetivo em um país como a Estônia, no qual o cotidiano está fortemente conectado com a rede (chegando mesmo a ter eleições online), como ficou claro nos ataques de 2007 ao país (Maynard 2018).

Estes ataques, por operarem no espaço cibernético e, portanto, desconectarem-se do espaço físico, podem acertar múltiplos alvos de uma só vez, de forma quase instantânea. Ao considerar-se a integração da infraestrutura crítica ao ciberespaço, resulta que ciberataques podem ter o resultado prático de dano de infraestrutura física, derivado de uma ação no meio virtual[12].

Há, ainda, duas propriedades, nesses ataques, particularmente importantes quando se considera seu uso político: as questões da atribuição e da previsibilidade dos danos. Ataques cibernéticos são bem difíceis de terem uma origem atribuída e, particularmente, difíceis de terem conexões políticas que derivem em objetivos políticos calculáveis. Ademais, devido à natureza global da conexão com a internet, é possível o espalhamento de uma determinada contaminação, o que não exclui eventuais danos à própria origem dos ataques, ao contrário do que acontece, em geral, quando se dispara um míssil em direção a um alvo distante, por exemplo.

Singer e Friedman (2014) indicam três tipos de ataque cibernético: (1) ataques de disponibilidade, que visam barrar o acesso a uma rede, ao sobrecarrega-la

10 Do original: deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks.

11 Atividade que visa a promover ou a resistir a mudanças sociais ou políticas utilizando-se de métodos cibernéticos de protesto, que são, de uma só vez, não violentos e questionáveis (Singer e Friedman 2014).

12 É o caso do software *Stuxnet*, que atacou o sistema operacional das centrífugas de enriquecimento de urânio iranianas e causou destruição — *física* — de seu maquinário, levando a uma queda de 20% no ritmo de trabalho do programa nuclear iraniano no espaço de 5 meses (Maynard 2018).

com o número de visitas[13] ou deixando-a *off-line*, para interromper os processos físicos e virtuais que dependem dela; (2) ataques de confidencialidade, que buscam entrar em redes de computador de modo a monitorar as atividades e extrair informações dos sistemas e usuários; e (3) ataques de integridade, que visam entrar em um sistema para alterar a informação contida — úteis para mudar a percepção dos alvos, ou para sabotagem. Todos os três tipos de ataques, em um contexto de crescente integração das tecnologias civis e militares a redes de computadores, podem causar graves danos materiais e virtuais a seus alvos.

A Guerra Cibernética

Mas, afinal de contas, quando ataques cibernéticos podem ser entendidos num contexto maior de guerra cibernética? Este termo é passível de ser empregado? Se sim, quando? Estas perguntas só podem ser respondidas pela transposição dos elementos considerados essenciais ao fenômeno da guerra, vistos anteriormente, para a realidade do ciberespaço como um novo meio de realização de conflitos.

O termo "guerra cibernética" vem sendo utilizado, sobretudo na mídia, majoritariamente de forma simbólica, para se referir a uma vasta coleção de fenômenos diferentes. Equipararam-se, então, cibervandalismo a mobilizações reais de um estado de guerra utilizando-se recursos cibernéticos.

Dentro da academia, as confusões se repetem devido a interpretações díspares em torno de conceitos tradicionais. Por um lado, Limnéll, devido à sua interpretação ampla da noção de violência, entende como ciberguerra, por exemplo, o roubo de informações governamentais (Limnéll e Rid 2014). Clarke menciona ainda que, para que uma ação configurasse uma ciberguerra, seria necessário que ela fosse perpetrada por Estados-nações contra congêneres (Clarke e Knake 2010). Alguns acreditam, inclusive, que até hoje não teria havido uma guerra cibernética.

Passo inicial para resolução desta questão reside em um aspecto linguístico que impacta os conceitos utilizados. É pertinente uma distinção clara entre guerra em sua essência (*war*) e em seu sentido operacional, levando-se em consideração os elementos táticos empregados (*warfare*). A ciberguerra deve ser pensada a partir desta última noção, uma vez que ela destaca que os ataques cibernéticos, quando integram operações de guerra, não são inovadores a ponto de mudar

13 A este processo se dá o nome de *Denial-of-Service* (DoS). Uma variação desses ataques, o *Distributed-Denial-of-Service* (DDoS) ocorre quando o tráfego que está atacando uma rede é originado em grande número de fontes geograficamente distribuídas, a partir de computadores "zumbis" (Lohachab e Karambir 2018).

fundamentalmente a natureza do conflito, mas são, sim, um instrumento para nele ser usado. O ciberespaço apenas abriu as portas para o uso de mais um meio para o conflito bélico, como fizeram as aeronaves ao levar a possibilidade de guerra ao ar.

O fenômeno da ciberguerra (*cyberwarfare*) sucedecom modificações meramente incrementais em relação ao de guerra, mais amplo. Isto porque os elementos essenciais de uma guerra permanecem inalterados: dela sempre derivam objetivos políticos e ela sempre sobrevém por meio de um ato de violência. Portanto, podemos definir guerra cibernética como "interferência eletrônica direta a alvos civis e militares estrangeiros com a intenção de causar dano" (Valuch et al. 2017, 66). Ressaltamos ainda, a noção de "dano" em seu sentido cinético.

Atualmente, o governo estadunidense parte do entendimento que, para que um ciberataque seja considerado um ato de força — ou seja, como violência —, é preciso que resulte em "morte, ferimentos ou destruição significativa" (Singer e Friedman 2014, 121, *tradução nossa*[14]). Isto não significa que seja o caso apenas de ataques que, em si, digamos, visem causar uma explosão, resultando em morte. Ataques cibernéticos podem ser usados como instrumento tático, acompanhando operações militares convencionais. Se ataques de DDoS interrompem as comunicações do adversário, causando problemas organizacionais, ao mesmo tempo em que uma batalha convencional ocorre, o ciberataque foi parte integrante do "ato de violência", funcionando de forma tática.

Singer e Friedman (2014) adicionam ainda, para a classificação de atos de violência, a objetividade e mensurabilidade, no sentido de que deve haver uma conexão direta e pretendida entre o ato e seu resultado. Assim sendo, um ato de ciberespionagem, por exemplo, pode resultar na perda de vidas humanas, mas a conexão entre um fato e outro não o qualifica como ato de guerra. Quando um país é atingido por um míssil, não é muito complicado descobrir a sua origem e compreender os objetivos políticos vinculados ao ataque. Mesmo em ataques terroristas, onde o ator estatal está ausente, em geral um agente político assume a autoria. O mesmo já não ocorre nos ataques cibernéticos.

As ferramentas utilizadas em tais ataques são desenhadas para garantir o anonimato do atacante. Em um DDoS, os rastros deixados podem provir de múltiplos computadores ao redor do mundo, de modo que, para se encontrar a fonte, é preciso trabalho forense meticuloso, raramente definitivo (Singer e

14 Death, injury or significant destruction.

Friedman 2014). Ainda, o poder sobre a atribuição está sempre sob o controle do atacante, que pode imitar, falsificar ou remover dados que a evidenciem, levando investigadores à direção contrária (Segal 2016).

Se o autor não pode ser identificado, mais do que apenas não saber os objetivos do atacante, o país atacado estará impossibilitado de retaliar. Como a guerra é a colisão de duas forças vivas, situações nas quais não se sabe quem contra-atacar não poderiam ser consideradas guerra. Por esta razão, a situação mais clara na qual ataques cibernéticos atingem todos os requisitos para serem configurados como guerra é quando eles ocorrem como apoio a operações militares convencionais, quando já se sabe quem está atacando.

Casos onde o conflito ocorreu inteiramente no meio cibernético — ou seja, ouve reciprocidade — a ausência de danos cinéticos impediu que os Estados se considerassem em guerra. Desta forma, considerar o ciberespaço como um domínio combatente por si só — desacompanhado da refrega no terreno, com armas cinéticas — é, na maioria dos casos, um equívoco (Júnior; Vilar-Lopes; Freitas 2017).

No já mencionado caso Stuxnet, por exemplo, houve efetivamente a consecução de dano cinético, com a infraestrutura nuclear iraniana sendo duramente impactada. Enquanto o contexto e algumas evidências apontavam para uma ação dos Estados Unidos e de Israel, elas não puderam figurar, para a liderança política iraniana, como cristalino ato de violência ao qual se poderia reagir com atos cinéticos mais diretos. A mesma reação não seria esperada no caso de um dano similar causado, por exemplo, por um míssil.

A decisão acerca do engajamento em uma guerra é sempre política, e depende da percepção e das informações à disposição das lideranças. Desta forma, os líderes iranianos, não encontrando evidências suficientemente sólidas para a atribuição do ataque, julgaram que a resposta a tais prováveis ações deviam cingir-se ao mesmo meio, respondendo com ataques cibernéticos contra o sistema financeiro americano e à ARAMCO saudita (Sanger 2018).

Desta forma, os conflitos cibernéticos poderão ter, em alguma medida, o poder de impactar doutrinas militares no que diz respeito à dissuasão. Tradicionalmente, esta se divide em dissuasão por negação, quando se reduz a confiança de um potencial atacante pela demonstração de que se tem o poder necessário para negar os frutos do ataque; e dissuasão por punição, que consiste em desestimular um inimigo a um ataque pelo preço da punição que virá em seguida (Freedman 2013).

Já no reino cibernético, a dissuasão passa a ser necessariamente baseada mais em negar benefícios aos atacantes do que em impor custos em uma retaliação, justamente devido à dificuldade de atribuição (Segal 2016). Protegido pelo anonimato, há um estímulo maior ao atacante. O foco, portanto, é desenvolver proteções e barreiras mais efetivas, bem como investir em inteligência, de modo a prevenir possíveis ataques, mesmo que isso, na prática, seja extremamente difícil.

A guerra cibernética, assim, parece gerar impactos profundos nos cálculos da guerra, embora mais de um ponto de vista tático do que estratégico. Como concluem Júnior, Lopes e Freitas (2017, 49):

> Como arma estratégica, por um lado, a guerra cibernética é incapaz de produzir coerção, em razão das características do ciberespaço e seus limites na produção de efeitos cinéticos. Ao permitir, na maioria das vezes, o anonimato de seus agressores, inviabiliza assim a dissuasão, seja por negação, seja por punição.

A "Guerra" Informacional

A globalização das informações acabou por acentuar a importância das narrativas dominantes no ambiente político. Ademais, há uma conexão direta entre ataques cibernéticos e o aspecto informacional, com um relatório técnico da comissão europeia chegando a mencionar que a "desinformação deve ser considerada uma ferramenta completamente integrada à guerra cibernética" (Flore et al. 2019, 7, *tradução nossa*[15]).

Definição de guerra informacional foi dada por Valuch et al como "controlar ou influenciar o humor da sociedade via engenharia social" (2017, 66, *tradução nossa*[16]). Ciberataques, ao controlar as narrativas disseminadas em torno de um evento, facilitam a obtenção e consolidação de objetivos políticos. No entanto, seria possível que uma abordagem informacional possua elementos essenciais de uma guerra?

Ataques cibernéticos podem ser desenhados para alcançar objetivos estratégicos ligados ao aspecto informacional, que dão suporte à obtenção de objetivos militares táticos em meio a operações convencionais, cinéticas. Contudo, similar

15 Do original: Disinformation should be considered a fully integrated cyber-warfare tool.

16 Controlling or influencing the mood in the society via social engineering.

ao exemplo a respeito da espionagem, ainda que um ataque cujo alvo seja a informação resulte de alguma forma em violência ou na obtenção de objetivos militares, este efeito não é direto o suficiente para que o ataque seja considerado um ato de violência. Conforme aponta o próprio autor da definição de guerra informacional, este termo tem sido usado, majoritariamente, como metáfora, assim como a própria guerra cibernética (Valuch et al 2017).

Um olhar técnico sobre a questão não deve conceber, portanto, a guerra informacional como um conceito autônomo, dispondo do *status*, per se, de guerra. Pelo contrário. Trata-se tão somente de mais um instrumento que visa auxiliar, indiretamente, na obtenção de objetivos políticos, por vezes *pari passu* com operações convencionais. Não chegam nem a ser uma novidade em si, uma vez que os ciberataques apenas permitiram um novo meio de difusão da tradicional propaganda[17].

A Guerra Russo-Georgiana

Antecedentes e Contexto

Após a dissolução da União Soviética, o governo russo valeu-se de "conflitos congelados" para manter uma força de tração sobre as antigas repúblicas soviéticas, evitando que elas abandonassem sua zona de influência. Isso se fez a partir do apoio a movimentos separatistas nesses países, frequentemente liderados por minorias russas (Mongrenier e Thom 2016).

Na Geórgia, essas minorias estavam localizadas no noroeste do país, na região chamada Abecásia, e no norte, na Ossétia do sul, povoada por cristãos russófonos não assimilados pelos georgianos, que se identificavam com seus pares da Ossétia do norte, localizada em território russo. Isso levou à organização, em 1992, de um referendo na área onde 98% foram favoráveis a anexação à Rússia. Uma série de crises se seguiu, nas quais o vizinho do norte participou como país mediador, mantendo tropas estacionadas em território georgiano (Yakemtchouk 2008).

Em 2003, os georgianos manifestaram-se através da "revolução das rosas", derrubando o presidente pró-russo Chevardnadze do poder, substituindo-o por

17 Sequer é novo o uso de propaganda em auxílio a operações convencionais no próprio campo de batalha. Exemplo disso são os panfletos em português jogados por tropas alemãs na Itália, que buscavam levar os soldados da Força Expedicionária Brasileira a desertar (Costa 2009).

Mikhaïl Saakashvili, que passou a adotar uma postura de aproximação com o ocidente e, em particular, com a OTAN (Yakemtchouk 2008). Destaque foi dado à construção do oleoduto BTC, que passaria pela Geórgia, mas que cortava território russo e transportava petróleo do Azerbaijão para a Europa.

Após criar tensões com seu vizinho pela nova postura e por ameaçar os objetivos geoenergéticos russos, Saakashvili envidou esforços, em 2008, no sentido de retomar efetivamente a Ossétia e integrá-la ao território georgiano após "provocação" russa em exercícios militares na fronteira entre a Ossétia do Sul e a Geórgia (Maynard 2018). Esse foi o estopim para a invasão russa do território georgiano, o que levou ao reconhecimento da independência dos territórios separatistas (Mongrenier e Thom, 2016). Este episódio destaca-se por ser considerado o primeiro caso de uso de ataques cibernéticos em apoio a operações militares tradicionais.

Os Ataques

Antes de caírem as bombas, uma primeira onda de ataques cibernéticos foi realizada nos dias 6 e 7 de agosto de 2008, encetadas por *botnets* e sistemas de comando-e-controle associados ao crime organizado russo (Blank 2017). Em seguida, iniciaram-se as operações convencionais, com Moscou enviando tropas adicionais a Ossétia do Sul e respondendo aos ataques de Saakashvili na região com bombardeios ao território georgiano. Somou-se a isto um bloqueio naval à Geórgia e o desembarque de fuzileiros navais na costa da Abecásia. Do ponto de vista das operações convencionais, as FFAA mecanizadas russas e as milícias ossetas derrotaram o exército georgiano, levemente armado, no único engajamento de larga escala da guerra, a batalha por Tskhinvali (Hollis 2011).

O grande marco desta guerra foram os ataques cibernéticos realizados *pari passu* com esta batalha. Na nova onda de ciberataques, foram feitas postagens em *sites* que continham ferramentas eletrônicas para a realização dos ataques e listas de alvos sugeridos. Eles consistiam em ataques de DDoS e desfiguração de *websites*, pelos quais grande número de *sites* do governo, da mídia e de instituições financeiras foram bloqueados (*denied*) ou desfigurados (Segal 2016).

Os alvos destes ataques isolaram o governo georgiano dos seus mais efetivos meios de comunicação, deixando-o incapaz de se comunicar tanto internamente quanto com o exterior. Mostrou-se, assim, que seu acesso à internet era extremamente vulnerável à interferência russa (Hollis 2011). Conforme as

tropas russas estabeleciam posições no país vizinho, a lista para ataques era ampliada para abranger agências governamentais, instituições financeiras, grupos de negócios, instituições de educação, mídia e, sobretudo, fóruns georgianos de *hackers*, com o objetivo de impedir respostas a altura aos ataques cibernéticos (Blank 2017).

Como resultado, o governo georgiano tinha dificuldade em formular uma resposta organizada à presença russa. Ele estava incerto sobre o que as tropas de Moscou poderiam vir a fazer e via a confusão se espalhar entre sua população, que não conseguia buscar informações com o governo. Com a derrubada das redes de mídia do país caucasiano, o Kremlin iniciou uma campanha de propaganda que permitiu saturar as redes de notícia com a versão russa dos eventos, às quais a população local teria acesso, uma vez que o canal russo em língua inglesa *Russia Today* estava cobrindo a situação na Geórgia desde o dia 3 de agosto (Priporov 2013). O ataque combinava, portanto, ataques DoS, sabotagem e ciberpropaganda (Vakhyu I Gede 2019).

Finalmente, chama atenção que os ciberataques não foram desenvolvidos por uma seção institucionalizada das FFAA russas, mas por grupos conhecidos como *hackers* patrióticos, recrutados pelas mídias sociais e que gravitavam ideologicamente em torno do governo (Singer e Friedman 2014)[18]. A disseminação das ferramentas para os ataques e a coordenação dos alvos eram feitas através dos fóruns "xaker.ru" e "stopgeorgia.ru", que seguiam uma hierarquia particular, na qual os líderes mais habilidosos forneciam as ferramentas, vulnerabilidades e alvos para a ação dos seguidores menos aptos (White 2018). Os ataques levaram a uma reação bem-sucedida de *hackers* georgianos, resultando em um conflito cibernético independente entre terceiros atores não-estatais, sob o pretexto das hostilidades oficialmente declaradas[19].

Não obstante, apesar do uso de terceiros nas operações, é possível observar uma coordenação rigorosa dessas ações com os objetivos estratégicos russos. Os ciberataques foram realizados de maneira limitada e contida, sem atacar infraestruturas críticas, mas demonstrando a capacidade de fazê-lo, sinalizando

18 Estes grupos, que convergem patrioticamente com os objetivos estratégicos do governo, operam também em benefício próprio, chegando a possuir ligações com o cibercrime. O que ocorre, portanto, é um acordo tácito, no qual é dada alguma liberdade para que estes indivíduos operem, em troca do seu serviço, quando este for requisitado pelo governo (Singer e Friedman 2014).

19 *Hackers* do lado georgiano reagiram interrompendo o acesso às mídias russas, o que era complementado pelo bloqueio, desta vez por parte do governo da Geórgia, da entrada em *sites* do domínio ".ru" e o bloqueio de acesso russo a *sites* georgianos (Priporov 2013).

para o governo da Geórgia que a escalada do conflito não era desejável. Houve, assim, verdadeira compulsão cibernética (Blank 2017).

Evento ilustrativo do objetivo russo diz respeito à infraestrutura energética georgiana, que se encontrava no epicentro das tensões geopolíticas entre os dois países, devido à construção do gasoduto BTC. Enquanto os ataques cibernéticos evitaram a infraestrutura energética do país, as forças armadas russas espelharam este movimento, efetuando ataques no entorno do oleoduto, sem de fato acertá-lo (Hollis 2011).

A Abordagem Russa para o Ciberespaço

Um elemento não desprezível na análise do conflito de 2008 é o fato de que os ataques às mídias e a campanha informacional em torno da versão russa dos acontecimentos não aparece, aqui, como mero detalhe da operação, nem são vistos como menos estratégicos por Moscou em relação à ruptura tática das comunicações no lado georgiano. Pelo contrário, a Rússia integra os mecanismos cibernético e informacional ao seu planejamento e sua capacidade de projeção de poder (Blank 2017).

O Kremlin, seguindo sua política externa desenvolvida nas últimas duas décadas, manifesta-se discursivamente como em meio a um confronto informacional contra o ocidente[20], o que é natural do ponto de vista do debate político, frequentemente metafórico. Contudo, o país passou a institucionalizar este entendimento ao mencionar, em sua doutrina de defesa, que os conflitos militares contemporâneos seriam caracterizados pelo "fortalecimento do papel do conflito informacional" (Rússia 2010, *tradução nossa*[21]).

Em artigo de 2013, o general russo Valeryi Gerasimov comenta que os conflitos estariam mudando de natureza, dando ênfase ao amplo uso de medidas "econômicas, informacionais e outras não-militares, implementadas com o uso do potencial de protesto da população" (Gerasimov 2013, *tradução nossa*[22]). Isto

20 Ainda no final de 2019, por exemplo, o presidente russo declarou, no colegiado estendido do ministério da defesa, que o país estaria preparado para garantir a justiça histórica em torno dos relatos sobre a 2ª Guerra Mundial, apontando para tentativas estrangeiras de manchar a história do país (Perviy Russkiy 2019). A medida mais notória da resposta do país eslavo foi, em tempos de paz, a promoção das redes de notícias Sputnik e RT, com a missão de difundir a versão russa dos eventos para o resto do mundo.

21 усиление роли информационного противоборства.

22 политических, экономических, информационных, гуманитарных и других невоенных мер, реализуемых с задействованием протестного потенциала населения.

ainda seria complementado por medidas militares secretas, incluindo o conflito informacional e ações das forças de operações especiais. Esta abordagem acerca dos conflitos no século XXI passou a ser chamada de doutrina Gerasimov, cuja aplicação já podia ser observada na Guerra Russo-Georgiana. Ela ficaria ainda mais patente durante o conflito no leste ucraniano[23].

Este é um aspecto particular da abordagem russa para as noções de conflito e paz. Diferentemente da dualidade existente no ocidente, a abordagem russa possui certas nuances. Contudo, contrariamente ao entendimento de Blank (2017), isto não permite que se fale em guerra informacional (*informational warfare*), mesmo na perspectiva russa. Em toda sua doutrina militar (Rússia 2010), não há associações entre o elemento informacional e a palavra guerra (война), preferindo-se o termo conflito (противоборство). A grande particularidade aqui é a manutenção e evolução deste conflito psicológico em períodos de guerra deflagrada, abordagem que deriva do passado soviético e que foi aperfeiçoada a partir das experiências das duas guerras na Chechênia[24] (Blank 2017; White 2018).

Partindo deste princípio, ataques cibernéticos são vistos como um elemento orgânico na doutrina de conflito informacional da Federação Russa, encarados de maneira mais ampla, como um mecanismo que permite o domínio do panorama de informações, para além dos efeitos em sistemas de comunicação adversários. Isso contrasta com a visão mais rígida e estreita da abordagem estadunidense para o ciberespaço (Segal 2016).

As Lições da Guerra

As principais lições a serem tiradas dos eventos ocorridos na rápida guerra de 2008 podem ser divididas em dois subgrupos, que exprimem bem os elementos academicamente relevantes a serem observados. De um lado, há os elementos particularmente novos ou extraordinários identificados em meio à guerra, com

23 Em sua campanha no leste ucraniano, a Rússia, ao combinar ataques cibernéticos e os *little green men* — exército não-oficial de soldados russos, utilizando uniformes verdes não-identificados — buscava não apenas consolidar seus objetivos materiais de domínio do território e impedir que o país, em meio a tensões centrífugas, tivesse viabilizada sua adesão à OTAN. Ela buscava também um objetivo psicológico, passando a mensagem de que a Ucrânia, enquanto país, só existiria se a Rússia permitisse (Sanger 2018).

24 A primeira guerra da Chechênia (1994-1996) teve custo físico e moral demasiadamente grandes, o que dificultou a obtenção dos objetivos estratégicos do Estado russo. Na segunda guerra da Chechênia (1999-2009), estes custos foram diminuídos pela campanha midiática russa, que a retratou como uma guerra anti-terrorista (Blank 2017).

destaque para a participação de grupos terceiros, não-estatais. De outro, existe o método e os princípios absolutamente ordinários e tradicionais do uso do ciberespaço, dialogando diretamente com doutrinas de conflito convencional já bem estabelecidas.

O primeiro ponto a ser destacado no uso de terceiros para a realização de ataques cibernéticos é a acrescida dificuldade na atribuição das ações, por remover ligações diretas com as autoridades responsáveis. Isso dificulta que seja montada, posteriormente, preparação adequada para o fenômeno, inclusive em termos jurídicos, uma vez que, até hoje, o Conselho Europeu e os Estados Unidos ainda entendem oficialmente os ataques de DDoS, ocorridos na Geórgia, como cibercrime.

Cohen (2017) indica que, atualmente, existe uma descentralização da propriedade da tecnologia de uso militar, que tende a derivar do setor civil e não o contrário, como era marcante em tempos idos. Neste processo, também os profissionais ligados à operação dessas tecnologias deixaram de estar associados diretamente ao governo, que passa a ter que competir com empresas do setor privado por tais profissionais.

Isto fica claro no estudo de caso feito. A procura por terceiros está, também, ligada ao fato de que ações efetivas no ciberespaço requerem um nível de criatividade e inovação que burocracias militares, marcadas pela disciplina, hierarquia e mentalidades orientadas por processos bem definidos, têm dificuldade em exercer com maestria (White 2018). A grande atribulação causada por esta captação indireta é a perda de unicidade e organicidade em meio à preparação dos ataques, em virtude da dificuldade de entendimento entre as comunidades técnica e não-técnica. Esta dificuldade é ainda reforçada por canais de comunicação debilitados pela própria natureza não-institucionalizada da relação entre forças armadas e terceiros.

Por outro lado, a campanha russa de 2008 demonstrou que o conflito cibernético permanece governado pelos mesmos princípios gerais que regem conflitos convencionais. As fases do ciclo operacional permaneceram inalteradas: salas de bate-papo foram utilizadas para o recrutamento e para o processo de mobilização de forças; foi feito trabalho de reconhecimento em busca de vulnerabilidades e alvos virtuais; ataques foram realizados contra comunidades *hackers* rivais como prevenção a contra-ataques; e a neutralização dos meios de informação do adversário foram feitas anteriormente ao ataque por meios físicos (White 2018).

Os ataques cibernéticos, apesar da operacionalização por terceiros, demonstraram alto grau de coordenação de objetivos táticos e estratégicos perseguidos na campanha mais ampla. Não se excederam ou transbordaram para as infraestruturas físicas, passando, então, a mensagem que deveria ser passada, no sentido de mostrar capacidade de materialização de dano e nada mais (Blank 2017).

Foi rompida a ideia de efeito instantâneo em toda atividade desenvolvida no ciberespaço. Tais ataques requerem um longo processo de localização de vulnerabilidades e, no conflito em questão, as ações contra os sistemas de informação começaram 20 dias antes do início do conflito (Sepetich 2016). Uma das ferramentas utilizadas para a desfiguração de *websites* havia sido desenvolvida há aproximadamente dois anos, especificamente para a campanha na Geórgia (White 2018).

Tais atividades preliminares no espaço cibernético podem criar assinaturas identificáveis, que podem ser monitoradas antecipadamente de modo a desarticular futuros ataques (Hollis 2011). Portanto, é recomendável o monitoramento de fóruns de *hackers* de modo a permitir, o mais cedo possível, a identificação de atividades suspeitas, que poderiam indicar eventual recrutamento e preparação para um ataque cibernético por parte de outro Estado.

Finalmente, fica o aprendizado de que, contrariamente ao que se acredita, no espaço cibernético, o terreno importa, e a geografia permanece decisiva. A dependência física da Geórgia para com a infraestrutura de rede russa, com quase metade das rotas da rede georgiana passando pelo vizinho, amplificou a efetividade dos ataques cibernéticos. A Geórgia não possuía, ainda, o próprio ponto de troca de tráfego (IXP), elemento que havia permitido que a Estônia, em meio a ataques no ano anterior, não perdesse a capacidade de comunicação interna (Segal 2016).

Conclusões

Após revisão bibliográfica, fica evidente que as ambiguidades e divergências existentes na área em torno do tema da guerra cibernética podem ser substancialmente pacificadas pela adoção do elemento da violência, em seu aspecto cinético, como orientador da classificação de um fenômeno como sendo guerra. O estudo de caso realizado foi particularmente útil para ilustrar tal entendimento,

uma vez que foi o primeiro evento claro no qual ataques cibernéticos foram realizados de maneira sincronizada com uma campanha convencional.

A guerra foi marcada simultaneamente e na mesma medida por suas novidades — com destaque ao uso de terceiros, recrutados a partir de vínculos indiretos com a autoridade responsável — e por suas continuidades em relação às guerras tradicionais. No que permaneceu inalterado, destaca-se a capacidade de controle dos terceiros no que diz respeito ao seu engajamento em torno dos objetivos táticos e estratégicos desejados.

Um ponto que segue para debate é a questão da relação do fenômeno com o Estado. O espaço cibernético parece estar sendo cada vez mais povoado por entidades não-estatais, por vezes transnacionais, que passam a ocupar espaços antes ocupados unicamente por burocratas. Isto faz com que guerras cibernéticas possam ser inteiramente praticadas à revelia do Estado? Pouco provável no curto prazo. Isto porque, ainda que isto possa mudar, o Estado ainda é o único ator político com capacidade de organização necessária à consecução de ataques cibernéticos em apoio a campanhas militares no domínio físico. Além, convém recordar dos aspectos físicos, territoriais e jurídicos controlados pelos Estados, conforme já mencionado acima.

Ainda assim, deve-se destacar que, tendo-se escolhido analisar um caso ocorrido há mais de uma década, o que em termos cibernéticos pode ser considerado um tempo distante, não foram vistas em profundidade atualizações das capacidades de tais ataques. A título de ilustração, basta imaginar os efeitos práticos gerados por eventual dispositivo como o *Stuxnet* se aplicado aos sistemas de lançamento de mísseis de uma potência nuclear. Contudo, em se dispondo a realizar, também, uma revisão conceitual, verificamos que as consequências da abordagem cinética para o conceito de guerra seguem sustentando-se em meio ao aprofundamento da tecnologia cibernética.

Referências

Azevedo, Cecília. 2005. Guerra À Pobreza: Eua, 1964. São Paulo, *Revista De História* 153, no.2.

Blank, Stephen. 2017. Cyber War And Information War À La Russe. In: Perkovich, George; Levite, Ariel E. *Understanding Ciber Conflict:* Fourteen Analogies. Georgetown: Georgetown University Press.

Clarke, Richard A.; Knake, Robert K.. 2010. *Cyber War: The Next Threat To National Security And What To Do About It*. Nova York: Harper-Collins Publishers.

Clausewitz, Carl Von. 2014. *Da Guerra*. São Paulo: Martins Fontes.

Cohen, Eliot. 2017. Technology And Warfare. In: Baylis, John Et Al. *Strategy In The Contemporary World: An Introduction To Strategic Studies (5th Edn)*. New York: Oxford University Press.

Costa, Marcos A. T.. *Força Expedicionária Brasileira*: Memórias De Um Conflito. 2009. Dissertação (Mestrado Em História, Cultura E Poder) — Pós-Graduação Em História, Universidade Federal De Juiz De Fora, Juiz De Fora.

Figueiredo, Eurico De Lima. 2010. "Os Estudos Estratégicos, A Defesa Nacional E A Segurança Internacional". In: Lessa, Renato (Organizador). *Horizontes Das Ciências Sociais, A Ciência Política*. Petrópolis, Vozes.

Flore, Massimo Et Al. 2019. *Understanding Citizens' Vulnerabilities To Disinformation And Data-Driven Propaganda*. Eur 29741 En, Publications Office Of The European Union, Luxemburgo.

Freedman, Lawrence. 2013. The Primacy Of Alliance: Deterrence And European Security. *Proliferation Papers*, no. 46.

Gerasimov, Valeryi. 26 fev. 2013. Ценность Науки В Предвидении [O Valor Da Ciência No Prognóstico]. *Voenno-Promyshlennyi Kurrier*. Disponível Em: < Https://Www. Vpk-News.Ru/Articles/14632 > . Acesso Em: 03 Jun. 2020.

Gray, Collin S.. 1999. *Modern Strategy*. Oxford: Oxford University Press.

Hollis, David. 2011. Ciberwar Case Study*:* Georgia 2008. *Small Wars Journal*. Disponível Em: < Https://Smallwarsjournal.Com/Blog/Journal/Docs-Temp/639-Hollis.Pdf > . Acesso Em: 11 De Dez. 2019.

Iasakova, Ekaterina. 01 mai. 2019. Владимир Путин Подписал Закон О Рунете [Vladimir Putin Assinou Lei Sobre A Runet]. *Rossiyskaia Gazeta*. Disponível Em: < Https://Rg.Ru/2019/05/01/Vladimir-Putin-Podpisal-Zakon-O-Runete.Html > . Acesso Em: 13 Jan. 2020.

Júnior, Augusto W. M. T.; Vilar-Lopes, Gills; Freitas, Marco T. D.. 2017. As Três Tendências Da Guerra Cibernética: Novo Domínio, Arma Combinada E Arma Estratégica. *Rev. Carta Inter.*, Belo Horizonte,12, no. 3.

Kiras, James D. 2002. Terrorism And Irregular Warfare. In: In: Baylis, John Et Al. *Strategy In The Contemporary World: An Introduction To Strategic Studies*. New York: Oxford University Press.

Limnéll, Jarno; Rid, Thomas. 2014. Is Cyberwar Real? Gauging The Threats. *Foreign Affairs*.

Lohachab, Ankur; Karambir, Bidhan. 2018. Critical Analysis Of Ddos — An Emerging Security Threat Over Iot Networks. *Journal Of Communications And Information Networks* 3 no. 3.

Longo, Waldimir Pirro. 2007. Tecnologia Militar: Conceituação, Importância E Cerceamento. *Tensões Mundiais*, Fortaleza 3, no. 5.

Maynard, Dalton. 2018. Considerações Sobre A Ciberguerra. In: Silva, Francisco Carlos Teixeira Da & Schurster, Karl (Org.). *Por Que A Guerra?* Rio De Janeiro: Civilização Brasileira.

Mongrenier, Jean-Sylvestre; Thom, Françoise. 2016. *Géopolitique De La Russie*. Paris: Presses Universitaires De France.

Moreira, William S. 2010. Estudos Estratégicos — Epistemologia, Crítica E Novas Abordagens. Trabalho Apresentado No Iv Encontro Nacional Da Associação Brasileira De Estudos De Defesa, Brasília2010.

Perviy Russkiy. 24 dez. 2019. *"Испоганить Память Не Дадим": Путин Ярко Показал, Что Готов К Информационной Войне С Западом Ради Исторической Справедливости* ["Não Permitiremos Que Manchem A Memória": Putin Vivamente Demonstrou Que Está Pronto Para A Guerra Informacional Com O Ocidente Pelo Bem Da Justiça Histórica]. Disponível Em: < Https://Tsargrad.Tv/News/Ispoganit-Pamjat-Ne-Dadim-Putin-Jarko-Pokazal-Chto-Gotov-K-Informacionnoj-Vojne-S-Zapadom-Radi-Istoricheskoj-Spravedlivosti_231940 > . Acesso Em: 18 Jan. 2020.

Priporov, E. S. 2013. Роль Традиционных И «Новых Сми» В Освещении Грузино-Южноосетинского Конфликта В Августе 2008 Года [O Papel De Meios De Informação De Massa Tradicionais E Novos Na Elucidação Do Conflito Entre Geórgia E Ossétia Do Sul Em Agosto De 2008]. *Vestnik Nizhegorodskovo Universiteta Im. Ni Lobatchevskovo*, 5, no. 1.

Rússia. Decreto Do Presidente Da Federação Russa, De 5 De Fevereiro De 2010. *Военная Доктрина Российской Федерации* [Doutrina Militar Da Federação Russa]. Disponível Em: < Http://Kremlin.Ru/Supplement/461 > . Acesso Em: 18 Jan. 2020.

Sanger, David E. 2018.. *The Perfect Weapon*: War Sabotage And Fear In The Cyber Age. New York: Crown.

Segal, Adam. 2016. *The Hacked World Order*. New York: Public Affairs.

Sepetich, Sergio E. 2016. Las Ciberoperaciones Aplicadas A Un Teatro De Operaciones — Estudio De Caso: Guerra Ruso Georgiana. Escuela Superior De Guerra Conjunta De Las Fuerzas Armadas. Disponível Em: < Http://Www.Cefadigital.Edu.Ar/Handle/1847939/900 > . Acesso Em: 5 Jun. 2020.

Sheldon, John B. 2013. The Rise Of Cyberpower. In: Baylis, John Et Al. *Strategy In The Contemporary World: An Introduction To Strategic Studies (4th Edn)*. New York: Oxford University Press.

Singer, P. W.; Friedman, Allan. 2014. *Cybersecurity And Cyberwar:* What Everyone Needs To Know. New York: Oxford University Press.

Vakhiu I Gede, B. K. 2019. Роль Методов Кибервойны Как Средства Противоборства В Современной Прокси-Войне [O Papel De Métodos De Guerra Cibernética Como Meio De Conflito Na Guerra Por Procuração Moderna]. Anais. Xv Conferência Científica Nacional De Estudantes, Aspirantes E Jovens Cientistas, Tomsk.

Valuch, Jozef Et Al. 2017. Cyber Attacks, Information Attacks, And Postmodern Warfare. *Baltic Journals Of Law & Politics*. 10, no. 1.

Weber, Max. 1999. *Economia E Sociedade*: Fundamentos Da Sociologia Compreensiva. Brasília: UnB. 2.

White, Sarah. 2018. *Understanding Cyberwarfare: Lessons From The Russo-Georgian War*. Modern War Institute.

William, A. Owens Et Al. 2009. *Technology, Policy, Law, And Ethics Regarding U.S. Acquisition And Use Of Cyberattack Capabilities*. Washington: National Academy Of Sciences.

Yakemtchouk, Romain. 2008. *La Politique Etrangère De La Russie.* Paris: L'harmattan.