HOPLOS
VOL. 06 Nº 10/2022

Juliana Zaniboni de Assunção

Graduada em Relações Internacionais pela Universidade Federal Fluminense. Mestranda no Programa de Pós-Graduação em Estudos Estratégicos da Defesa e Segurança (PPGEST).

A CIBERGUERRA É GUERRA?

IS CYBERWAR A WAR?

RESUMO: Para Clausewitz (1989), a guerra é um ato de força que obriga nosso inimigo a fazer a nossa vontade. Uma outra definição, feita pelo mesmo autor, é que a guerra seria a continuação da política por outros meios. A teoria clausewitziana foi bastante usada para explicar diversos conflitos posteriores a ele, como o evento das Guerras Mundiais. Ter utilizado a obra para entender o fenômeno da guerra não significa dizer que a guerra permaneceu imutável, pelo contrário, ela passou por diversas mudanças, mas mesmo assim, elas estavam dentro de um contexto maior, onde a teoria clausewitziana conseguiu explicá-las. No entanto, será que a teoria de guerra feita por Clausewitz poderia também explicar novos fenômenos como a Ciberguerra? Apresentando os debates dos conceitos de ciberguerra, ciberespaço e ciberataque, analisando juntamente com os casos ocorridos no Irã, em 2010, e na Ucrânia, em 2015, pretende-se compreender se a ciberguerra pode se enquadrar também na teoria tradicional de guerra, como um fenômeno belicoso.
Palavras-chave: Ciberguerra; Ciberespaço; Guerra; Ciberataque.

ABSTRACT: For Clausewitz (1989) war is an act of force that forces our enemy to do our will. Another definition, made by the same author is that war would be the continuation of politics by other means. Clausewitzian theory was used extensively to explain several later conflicts, such as the World Wars event. Using his work to understand the phenomenon of war does not mean to say that the war remained unchangeable, on the contrary, it went through several changes, but even so, they were within a larger context, where the Clausewitzian theory managed to explain them. However, could Clausewitzian's war theory also explain new phenomena such as cyberwar? Presenting the debates of the concepts of cyberwar, cyberspace and cyberattack, analyzing together with the cases that occurred in Iran in 2010, and in Ukraine in 2015, it is intended to understand whether cyberwar can also fit into the traditional theory of war, as a bellicose phenomenon.
Keywords: Cyberwar; Cyberspace; War; Cyber Attack.

1 Introdução

Existe o debate no meio acadêmico refletindo o que é ciberguerra. Com as pesquisas realizadas até aqui ainda não há um consenso definitivo sobre o assunto. Além de não haver uma definição, ocorre ainda discussões calorosas sobre possíveis conceitos, sendo vista e tratada de diferentes maneiras por outros países também. Esses debates sobre a ciberguerra, normalmente, ganham mais amplitude quando conflitos aplicam táticas cibernéticas.

O artigo se divide nas seguintes seções:

Na primeira seção, são apresentadas algumas conceituações sobre a ciberguerra, com o intuito de compreender o debate sobre o termo. Na segunda seção, é apresentada uma teoria tradicional da guerra, desenvolvida por Clausewitz. É sabido que o autor em sua obra, Da Guerra, trata do fenômeno da natureza da guerra. Por essa razão, também é citado o autor Brustolin, que se baseia nas ideias de Clausewitz para dar uma definição mais determinante sobre o fenômeno.

Na terceira seção, são demonstradas as características próprias da ciberguerra, como o ciberespaço, o ciberataque e seus exemplos. Assim como na ciberguerra, existe um denso debate sobre o ciberespaço, que em 2016, foi reconhecido pela OTAN como um domínio operacional. Na subseção, é exposto sua definição e suas peculiaridades. Após isso, é apresentada a definição e as características dos ciberataques. No sentido de ilustrar os dois elementos anteriormente mencionados, são apresentados dois casos de ciberataques, um no Irã, em 2010, e o outro na Ucrânia, em 2015.

Na última seção, é apresentada a relação entre a ciberguerra e a guerra. Ou seja, as definições apresentadas são analisadas, juntamente com os exemplos mencionados, com o objetivo de compreender se a ciberguerra pode ser considerada guerra ou não.

A partir dessa estrutura, é possível estabelecer que o objetivo geral do trabalho seja evidenciar os debates disponíveis sobre o tema. Além de analisar se é possível enquadrar o fenômeno da ciberguerra na teoria tradicional de guerra Clausewitziana, observando os estudos de casos realizados no Irã, em 2010 e na Ucrânia, em 2015.

2 Definindo Ciberguerra

Existe um denso debate sobre a definição da ciberguerra que ainda não tem consenso entre os acadêmicos. Dessa forma, são analisadas algumas definições sobre o reconhecimento da ciberguerra com o intuito de ampliar a visão sobre o assunto.

Os autores John Arquilla e David Ronfeldt em 1993, com o texto Cyberwar is coming, já desenvolviam sobre a ciberguerra, no entanto, eles a tratavam como Guerra de Informação. Segundo os autores, a definição do conceito é:

> a ciberguerra refere-se à condução e preparação para conduzir operações militares de acordo com os princípios relacionados à informação. Refiro-me a perturbar, se não destruir, os sistemas de informação e comunicação, amplamente definidos para incluir até mesmo a cultura militar, em que um adversário depende para 'conhecer' a si mesmo: quem é, onde está, o que pode fazer quando, porquê da luta, quais ameaças combater primeiro, etc. Significa tentar saber tudo sobre um adversário, evitando que ele saiba muito sobre si mesmo (ARQUILLA & RONFELDT, 1993, p. 30, tradução nossa).

Os autores reconheciam a ciberguerra como assunto militar, para além do uso da tecnologia. Pois, para eles, a ciberguerra está ligada à informação.

> Para suas forças, a guerra não é mais uma função primordial de quem coloca mais capital, trabalho e tecnologia no campo de batalha, mas de quem tem as melhores informações sobre o campo de batalha. O que distingue os vitoriosos é a compreensão das informações – não apenas do ponto de vista mundano de saber encontrar o inimigo mantendo-o no escuro, mas também em termos doutrinários e organizacionais (ARQUILLA & RONFELDT, 1993, p. 23, tradução nossa).

Em verdade, eles afirmavam que 'a ciberguerra poderia ser para o século XXI, o que a Blitzkrieg foi para o século XX, em questão da inovação de guerra' (ARQUILLA & RONFELDT, 1993, p.31, tradução nossa). Essa afirmação significa que os autores acreditavam que a ciberguerra resultaria em uma transformação na natureza da guerra. Ou seja, a forma com que a guerra se apresenta iria mudar, assim como ocorreu com a inovação da Blitzkrieg, na Segunda Guerra Mundial.

Basicamente Arquilla e Ronfeldt (1993) preveem como a ciberguerra será e como ela poderá ser travada. Os autores chamam a atenção para novas tecnologias que poderão surgir, mudando a guerra, afirmando: "que as guerras futuras serão travadas principalmente por armas, robôs e computadores autônomos 'brilhantes'; esse homem será subordinado à máquina; e que o combate será extraordinariamente rápido e carregado de ataques isolados." (Ibid, 1993, p. 32, tradução nossa).

Devido às características únicas que a ciberguerra possui, os autores também chamaram atenção para a aplicação de novas doutrinas e forças necessárias pensando na derrota do inimigo. Os autores mencionam o ciberespaço, ambiente em que os ciberataques se iniciam, como uma dessas características, principalmente por não se parecer com outros domínios operacionais.

O texto apresentado é de 1993, é interessante notar que na época da publicação do texto, ainda não se tinha uma discussão densa, além de casos de ciberataques na época. Os exemplos dados pelos autores recorrem ao Império Mongol, assim como eventos da Segunda Guerra Mundial. Mesmo que os autores não tenham presenciado ciberataques, é interessante notar que a análise realizada se aproxima de certa maneira com autores atuais.

Segundo Singer e Friedman (2014), os elementos aplicados na guerra, como a busca do objetivo político e a presença da violência, se mantêm até mesmo no ciberespaço, ambiente onde os ataques se iniciam. Os autores afirmam que mesmo utilizando o ciberespaço, deve-se buscar o dano físico ou destruição do inimigo.

Os autores também chamam atenção para a dificuldade de definição da ciberguerra, pois nela não se sabe exatamente quando se inicia ou termina. Essa situação, no entanto, não foge ao escopo da guerra, visto que alguns conflitos não negociam seu fim formalmente, como a guerra das Coreias, que mesmo não se enfrentando mais ativamente, permanecem sem assinar acordo de paz.

Como mencionado anteriormente, a ciberguerra possui características próprias, o que pode dificultar a compreensão do fenômeno. No entanto, Singer e Friedman (2014) elencam elementos chave que estão presentes na guerra, sendo os ataques iniciados no ciberespaço ou em outros domínios operacionais.

Na definição da ciberguerra existe um debate constante, principalmente porque além da não concordância sobre o conceito final do fenômeno há alguns autores que discordam sobre sua existência. Rid (2011) é um exemplo deles que em seu artigo *Cyberwar will not take place*, afirma que a ciberguerra não é propriamente uma guerra, pois nos ciberataques analisados não existe o uso da violência, mais especificamente letalidade. Isso significa dizer que, até o momento analisado no artigo, ciberataques não provocaram mortes direta ou indiretamente. Rid (2011) baseando-se em Clausewitz, enxerga a violência como elemento essencial da guerra. Dessa forma, o autor não enxerga a ciberguerra como guerra.

Stone (2013), ao contrário de Rid (2011), analisa os conceitos de força e violência e afirma que a ciberguerra é um fenômeno possível. O autor justifica a afirmação abordando o sentido dos ciberataques, vendo estes como atos de guerra. Logo, a ‘condição’ estabelecida por Stone (2013) para a existência da ciberguerra seria a análise do ciberataque, ou seja, dependendo do dado empregado, o ciberataque seria visto como ato de guerra e logo se daria início à ciberguerra. Stone (2013, p. 107, tradução nossa) afirma que:

> atos de guerra envolvem a aplicação da força para produzir efeitos violentos. Esses

> efeitos violentos não precisam ter caráter letal: eles podem quebrar coisas, em vez de matar pessoas, e ainda se enquadram na rubrica de guerra. Além disso, a influência mediadora da tecnologia significa que pequenos atos de força – como tocar um teclado – podem resultar em grandes quantidades de violência, letal ou não.

Existem ainda alguns elementos importantes para que a definição da ciberguerra esteja completa, pois, não basta apenas definir um conceito, é necessário mencionar as características presentes nela. Os autores Alcântara e Silva (2018) analisam diversos conceitos da ciberguerra, produzidos por três esferas distintas: a acadêmica, estatal e empírica. As duas últimas categorias enfatizam a conceituação de alguns Estados, visando determinados interesses de Estado. Como a pretensão do artigo é definir a ciberguerra de uma maneira ampla e não de acordo com demandas estatais precisas, são mencionadas as características que tocam a esfera acadêmica.

Segundo Alcântara e Silva (2018, p. 139-140), a Guerra Cibernética possui as seguintes características:

> 1) a presença mandatória de Estados, 2) o uso de poderes assimétricos, 3) a existência de um elemento surpresa e 4) o uso de trapaça no decorrer do conflito, 5) implicações com envolvimento de IC e/ou sistemas de redes governamentais, 6) ações com motivação político – militar por detrás, 7) ações via ciberespaço, com invasão de redes alheias, 8) envolvimento de hard e soft power, traduzido aqui enquanto forças físicas e virtuais, e 9) o alcance de impactos multidimensional.

As características apresentadas pelos autores aplicadas às ações no ciberespaço podem demonstrar se o fenômeno faz parte ou não da ciberguerra. Tendo em mente a discussão da definição da ciberguerra, é necessário tentar comparar alguns conceitos e características apresentadas com uma teoria tradicional de guerra, buscando validar o fenômeno da ciberguerra como, de fato, guerra.

3 Clausewitz e a Guerra

Antes de mostrar a definição de guerra para Clausewitz, é importante ressaltar o momento em que o autor escreve. Lendo sua obra, fica evidente que Clausewitz cita diversos acontecimentos belicosos durante a história da humanidade e em suas análises leva em consideração os interesses dos Estados. Atualmente, quando se pensa em guerra, de modo geral e tradicional, remete-se à mente imagens das Grandes Guerras Mundiais. Entretanto, nem sempre houve essa ideia nítida de quais papéis os atores deveriam ter em uma guerra.

As guerras napoleônicas, contexto histórico em que Clausewitz desenvolveu seu livro *Da Guerra*, pode ser visto como um ponto importante para essa possível análise. Isso porque, quando se fala em guerra, o autor deixa claro a sua relação com a política. Para Clausewitz, “a

guerra não é um fenômeno independente, mas a continuação da política através de meios diferentes ” (1989, p. 6).

No evento mencionado, é possível observar algumas mudanças econômica-social-militar responsáveis por recentes elementos na guerra, como o estabelecimento do exército nacional. A ideia do exército nacional como instrumento de ação do Estado era algo novo na Europa, principalmente porque antes disso, os exércitos além de serem formados por milícias, eram um setor instável da sociedade (KEEGAN, 2006). Ou seja, a ação da força militar se baseava mais nos interesses próprios da milícia do que do Estado. Analisando a adaptação da guerra no período histórico mencionado e trazendo outros exemplos bélicos para a análise, Clausewitz avalia a natureza da guerra.

A obra de Clausewitz, originalmente escrita em alemão define-se por: “*der Kriege ist also ein Akt der Gewalt, um der Gegner zur Erfüllung unseres Willens zu zwingen*” (2018, p. 3). Enquanto que em inglês, tem-se: “ *war therefore is an act of violence intended to compel our opponent to fulfil our will*” (1982, p. 101). Por último em português a definição é: “a guerra é, portanto, um ato de força para obrigar o nosso inimigo a fazer a nossa vontade” (1989, p. 75).

A necessidade de comparação da mesma definição em idiomas distintos se dá pela palavra, originalmente em alemão, *Gewalt*. Segundo o dicionário Langenscheidt, ela pode significar: poder, força, violência e domínio (2009, p. 455). Na definição em inglês, utiliza-se a palavra violência, enquanto em português, força. Em um primeiro momento, é possível imaginar que todas essas palavras não tenham distinção muito relevante. Ou seja, para análise de conflitos todas elas seriam relacionadas. Apesar da similaridade, elas não possuem o mesmo significado, o que pode trazer alguma dificuldade de compreensão na natureza da guerra. Dessa forma, se faz necessário apresentar a devida distinção entre os conceitos poder, força, violência e domínio.

Segundo o dicionário do Bobbio, a palavra poder “[...] designa a capacidade ou a possibilidade de agir, de produzir efeitos” (2008, p. 943). A palavra força “[...] entende-se qualquer intervenção física voluntária de um homem ou grupo contra um outro homem ou grupo, objetivando destruir, ofender ou coartar.” (2008, p. 503). A palavra violência “[...] entende-se a intervenção física de um indivíduo ou grupo contra outro indivíduo ou grupo (ou também contra si mesmo)” (2008, p. 1291). Por último, a palavra domínio, segundo o dicionário Aurélio se refere a : “1. Autoridade, poder; 2. Posse” (2006, p. 328).

A análise da ciberguerra com a teoria tradicional de guerra desenvolvida por Clausewitz é melhor apresentada nas próximas seções, no entanto, se faz necessário apresentar os pontos

selecionados da teoria do autor que podem ser confundidos quando aplicados à ciberguerra. O que parece ser uma mera variação de traduções, na verdade, se torna um dos pontos chave na discussão sobre a ciberguerra. O uso das palavras poder e domínio, além de estarem relacionadas, não são tão frequentes quando relacionadas à ciberguerra. Dessa forma, são analisados os conceitos de força e violência. Mas afinal, a guerra é um ato de força ou violência?

Refletindo sobre a guerra em si e não apenas na ciberguerra, é possível analisar alguns exemplos históricos para esclarecer essa questão. É sabido que na Guerra Fria, houveram momentos mais e menos 'quentes' do conflito. Com a inovação bélicas das bombas atômicas, foi travada uma nova 'fase' da guerra. As potências principais do conflito, Estados Unidos da América (EUA) e União das Repúblicas Socialistas Soviéticas (URSS), diferentemente das guerras mundiais, não se enfrentaram diretamente. O que se observou foi a influência dessas potências sob outros Estados, fazendo com que eles entrassem em guerra por interesses estatais alheios.

No entanto, pode-se citar uma movimentação, durante a Guerra Fria, que poderia ser considerada um ato de guerra, que iniciaria a Terceira Guerra Mundial. Esse episódio é a Crise dos Mísseis, que ocorreu em 1962, devido a presença de mísseis balísticos dos Estados Unidos implantados na Itália e Turquia, enquanto a União Soviética colocava mísseis nucleares em Cuba. A descoberta dos mísseis soviéticos em Cuba fez com que crescesse a possibilidade de uma nova guerra mundial, utilizando armas atômicas. Durante esse período, o momento mais apreensivo foi o bloqueio militar que os Estados Unidos fizeram às embarcações soviéticas, para que se impedisse que novos mísseis chegassem a Cuba. A ação de impedir a locomoção dos navios soviéticos pode ser vista como um ato de força e não de violência. Durante treze dias, houve inúmeras negociações entre os presidentes russo Nikita Khrushchev e americano John F. Kennedy para que uma nova guerra não se iniciasse. Um acordo foi estabelecido entre as partes e a Terceira Guerra Mundial não aconteceu. Logo, pode-se entender que o conflito se iniciaria pelo ato de força produzido pelos Estados Unidos obrigando seu inimigo (União Soviética) a fazer a sua vontade, que seria o impedimento da instalação de armas nucleares em Cuba.

Como mencionado, Clausewitz analisa a natureza da guerra, no intuito de limitar o conceito de guerra, é interessante analisar uma definição mais característica, ainda levando em consideração os preceitos clausewitzianos. Segundo Brustolin (2019, p. 663), " guerra é um ato de força – de indivíduos que agem sob um comando de última instância em um espaço físico, contra indivíduos que agem sob um outro comando de última instância em um espaço físico –

para obrigar um comando à vontade do outro.” Com essa definição, é possível delimitar melhor a ideia de guerra, que posteriormente pode ser aplicada à ciberguerra.

4 Ciberataques no Ciberespaço

A seguir são mencionados alguns exemplos de ciberataques que possuíram motivações políticas para sua realização, podendo ser caracterizados como o início de uma ciberguerra. Antes de examinar os exemplos, é necessário definir os conceitos de ciberespaço e ciberataques, que estão intrinsecamente relacionados ao fenômenos da ciberguerra.

4.1 O Ciberespaço

Assim como o conceito da ciberguerra, o ciberespaço também gera diversos debates. Strate (2009, p. 393, tradução nossa) resume que: “o ciberespaço pode então ser definido como as diversas experiências do espaço associadas à computação e tecnologias relacionadas”. É interessante ressaltar que a Internet faz parte do ciberespaço, mas ela não a resume. Dessa forma, o ciberespaço se faz presente quando existem sistemas de redes, ligados à Internet ou não. O ciberespaço também não é puramente virtual. Libicki (2009) afirma que o ciberespaço possui três camadas, a física que seria a base, a sintática e no topo viria a semântica. Resumidamente, a camada física se refere aos dispositivos utilizados para que o sistema funcione; o nível sintático se trata da contenção de instruções que os designers e os usuários dão à máquina, além dos protocolos que fazem a máquina funcionar; o nível semântico lida com as informações que a máquina possui.

Libicki (2009) demonstra que o ciberespaço não é apenas virtual. Singer e Friedman possuem a mesma percepção e alegam que o ciberespaço, “compreende os computadores que armazenam dados mais os sistemas e infraestrutura que permitem o fluxo. Isso inclui a Internet de computadores em redes, intranets fechadas, tecnologias celulares, cabos de fibra óptica e comunicações.” (2018, p.13-14, tradução nossa). Singer e Fridman (2018) ainda afirmam que “o ciberespaço é definido tanto pelo domínio cognitivo quanto pelo físico ou digital.” (2018, p. 14, tradução nossa). Os autores possuem tal alegação, pois diferentemente de outros domínios operacionais, o ciberespaço foi algo fabricado pela humanidade.

A discussão sobre o ciberespaço é complexa e primordial para entender o fenômeno da ciberguerra, que ganhou mais um foco de discussão, quando em 2016, a OTAN reconheceu o ciberespaço como um domínio operacional. Ou seja, o ciberespaço era reconhecido como mais um ambiente em que era possível a realização de ações de cunho militar, além de terra, mar, ar

e espaço. Logo, é possível deduzir que o ciberespaço pode ser utilizado para fins militares, iniciando o ataque no ambiente virtual, podendo ter consequências diretas no mundo real.

4.2 O Ciberataque

Existem diversos tipos de ciberataques, alguns produzem mais e outros menos danos. Assim como o ciberespaço, o ciberataque também gera algumas discussões. Em relação ao conceito, Libicki (2009, p.23, tradução nossa) define ciberataque como "interrupção ou corrupção deliberada por um estado de um sistema de interesse de outro Estado. O antigo estado será referido como o atacante; o último estado será referido como o destino".

Em relação a forma como o ciberataque acontece, Singer e Friedman afirmam que:

> no ciberespaço, um ataque pode literalmente se mover na velocidade da luz, ilimitada por geografia e as fronteiras políticas. Ser desvinculado da física também significa que pode estar em vários lugares ao mesmo tempo, o que significa que o mesmo ataque pode atingir vários alvos ao mesmo tempo (2018, p. 69, tradução nossa).

É interessante notar a multiplicidade que o ciberataque apresenta, pois diferentes alvos podem ser atingidos de longas distâncias, produzindo danos aos países. Singer e Friedman (2018) também destacam que para um ciberataque causar algum dano físico, é necessário que o ataque seja iniciado no ambiente virtual. Ou seja, mesmo que os ciberataques tenham consequências no ambiente físico, ele foi iniciado no ciberespaço. A seguir são dados alguns exemplos de ciberataques, que produziram danos aos países-alvo.

4.3 O Caso do Irã

Em 2010, o Irã foi alvo de um ataque cibernético massivo em sua usina nuclear, que fez com que especialistas dessem uma estimativa entre cinco a dez anos[1] para que ela fosse restaurada completamente. O ataque em questão foi realizado por um dos vírus mais sofisticado que se tem notícia, o Stuxnet. O vírus além de danificar quase 1.000 centrífugas[2], foi responsável por espionar e também comprometer 60% das redes de computadores do setor

[1]CORREIO. Vírus que atrasou programa nuclear do Irã foi criado pelos EUA e por Israel. Disponível em < https://www.correio24horas.com.br/noticia/nid/virus-que-atrasou-programa-nuclear-do-ira-foi-criado-pelos-eua-e-por-israel/ > Acesso em: 05 de out. de 2021.

[2] KATZ, Yaakov. The Jerusalem Post. Stuxnet may have destroyed 1,000 centrifuges at Natanz. Disponível em < https://www.jpost.com/defense/stuxnet-may-have-destroyed-1000-centrifuges-at-natanz > Acesso em: 05 de out. de 2021.

industrial[3]. O ataque foi atribuído a Israel e Estados Unidos, devido à complexidade do vírus e também a interesses políticos na região. O contexto histórico para este ciberataque especificamente é intenso e longo, pois desde que o Irã afirmou que iria aumentar sua produção de energia nuclear, para fins energéticos, foram trazidos à prova algumas imagens que o país poderia estar produzindo armas nucleares, o que não seria interessante para os Estados Unidos e Israel. Logo, é possível identificar a motivação política por trás do ciberataque.

Além da complexidade tecnológica no vírus, é interessante notar que o Stuxnet possuía características coincidentemente ideais para atuar e corromper o sistema das centrífugas iranianas. Segundo Kushner (2013), o vírus funcionava em três fases:

> primeiro, ele teve como alvo máquinas e redes Microsoft Windows, repetidamente se replicando. Em seguida, procurou o software Siemes Step7, que também é baseado no Windows e usado para programar sistemas de controle industrial que operam equipamentos, como centrífugas. Finalmente, comprometeu os controladores lógicos programáveis. Os autores do vírus poderiam, portanto, espionar os sistemas industriais e até mesmo fazer com que as centrífugas de rotação rápida se separem, sem o conhecimento do humano dos operadores humanos da fábrica (p. 1, tradução nossa).

Após análise do vírus, analistas perceberam que se tratava de um item muito sofisticado para ter sido fabricado por algum grupo clandestino. É interessante notar que a responsabilidade foi posta entre Israel e Estados Unidos, pois eles possuem tecnologia avançada suficiente para produzir um vírus com essa eficácia. É importante lembrar que o Stuxnet não fez apenas um ataque e consequentemente causou danos. Segundo Kushner (2013), ao ser injetado o USB que possuía o vírus na rede de computadores responsáveis pela usina, o vírus ainda ficou um tempo na máquina analisando e espionando os computadores, enviando falsos feedbacks para que não soubessem que ele estava agindo. Na realidade, quando a máquina começa a dar sinais que pode estar infectada por algum vírus, já é tarde demais e não tem nada que se possa fazer a respeito.

4.4 O Caso da Ucrânia

Em 2015, uma cidade ucraniana chamada Kyivoblenergo foi atingida por diversos ciberataques, provocando a interrupção de energia por três horas, atingindo aproximadamente 225.000 de pessoas na área. O governo ucraniano declarou que o apagão foi de fato causado por ataques cibernéticos e que o governo russo era o responsável. Assim como aconteceu no Irã, a Rússia tinha motivações políticas para que tal ataque acontecesse, pois o país, desde 2014,

[3]DW. Deutsche Welle. Stuxnet infecta Irã. Disponível em < https://www.dw.com/pt-br/ir%C3%A3-confirma-ter-sido-alvo-de-ataque-cibern%C3%A9tico/a-6046851 > Acesso em: 05 de out. de 2021.

trava um conflito constante com a Ucrânia, devido às questões geopolíticas envolvendo a Crimeia.

Assim como no Irã, os agressores no caso da Ucrânia, também utilizaram medidas que se adequaram ao sistema operante. Em um relatório realizado pelo *Electricity Information Sharing and Analysis Center* (E-ISAC) em 2016, afirma-se que:

> os invasores demonstraram uma variedade de recursos, incluindo e-mails de spear phishing, variantes do malware BlackEnergy 3 e a manipulação de documentos do Microsoft Office que continham o malware para se estabelecer nas redes de Tecnologia da Informação (TI), das empresas de eletricidade. Eles demonstraram a capacidade de obter uma base e coletar credenciais e informações para obter acesso à rede ICS (Sistema de Controle Industrial). Além disso, os invasores mostraram experiência, não apenas em infraestrutura conectada à rede; como Fontes de Alimentação Ininterrupta (FAIs), mas também na operação dos ICSs por meio de sistema de controle supervisório; como a Interface Homem-Máquina (IHM) (2016, p. 7).

No caso da Ucrânia, uma série de ciberataques aconteceram, pois além da interrupção de energia causada pelos hackers, houve uma contínua ação no ciberespaço para que o restabelecimento da energia não fosse concluída (E-ISAC, 2016). Dessa forma, é possível identificar a ação contínua no ciberespaço com o intuito de atingir a rede elétrica ucraniana.

5 A Ciberguerra e a Guerra

Com os exemplos e as definições da guerra e da ciberguerra apresentados, é possível tentar estabelecer alguns paralelos entre os fenômenos. Relembrando o conceito estabelecido por Clausewitz, “a guerra é, portanto, um ato de força para obrigar o nosso inimigo a fazer a nossa vontade” (1989, p. 75). Nesse sentido, o conceito mais restrito apontado por Brustolin, afirma-se que: “guerra é um ato de força – de indivíduos que agem sob um comando de última instância em um espaço físico, contra indivíduos que agem sob um outro comando de última instância em um espaço físico – para obrigar um comando à vontade do outro” (2019, p.663).

Aplicando o conceito aos exemplos mencionados, é possível perceber que houve um ato de força, seja a interrupção de energia ucranianas ou do funcionamento das usinas iranianas. Esse ato foi feito por parte dos indivíduos que agem sob um outro comando de última instância, ou seja, existe a participação efetiva de Estados, que se comprova tanto pelos interesses políticos na ação, quanto pela sofisticação e conhecimento dos alvos selecionados. O comando realizado em um espaço físico, como foi citado o ciberespaço também possui sua camada física, no entanto, é possível afirmar que em última instância o dano deve ser físico, independente do domínio operacional que ele tenha se iniciado. O ato de força deve ser feito contra indivíduos

que agem sob um outro comando de última instância, ou seja, o Estado-alvo, em um espaço físico – para obrigar um comando à vontade do outro. Entende-se, portanto, que esse comando deve ser realizado para que a vontade do Estado-agressor seja cumprida. Dessa forma, é plausível aplicar o conceito de guerra ao fenômeno da ciberguerra.

Outro ponto importante da guerra, já mencionado em outras seções, é a ideia de violência e força. Além disso, o debate sobre a falta de violência e letalidade na ciberguerra. A variação da tradução faz com que não se reconheça a ciberguerra como de fato uma guerra. Analisando sobre a questão da letalidade, mais especificamente mortes na ciberguerra, é possível afirmar que até o presente momento o ciberespaço não foi o responsável por causar nenhuma morte. Porém, é interessante mencionar um caso ocorrido em 2021, nos Estados Unidos.

Em fevereiro no ano mencionado, ocorreu um ciberataque no sistema de distribuição de água da cidade de Tampa, na Flórida, com 407,104 habitantes[4]. O hacker que invadiu o sistema estava tentando aumentar em 100 vezes a proporção de hidróxido de sódio, soda cáustica, na mistura. Essa substância pode ser utilizada em tratamentos de água, no entanto, quando ingerida em grandes proporções, pode causar danos graves à saúde[5]. Felizmente ninguém foi ferido, pois um vigia que estava no local percebeu a movimentação do hacker e conseguiu desfazer a ação. Apesar da gravidade da situação, o hacker ainda não foi encontrado.

É fato que a ciberguerra não causou nenhuma morte, no entanto, não se sabe até quando essa afirmação continuará vigente. É interessante lembrar que o caso mencionado acima foi realizado por um hacker, ou seja, uma pessoa que invadiu o sistema, ou seja, até o momento não foi confirmada a participação de outros Estados. Isso mostra a periculosidade que o ciberespaço pode apresentar, onde uma pessoa realizando um ciberataque foi quase capaz de aumentar, para além do permitido, o nível de soda cáustica na água. Se faz necessário refletir sobre a tecnologia que os Estados possuem e até onde eles podem ir. Logo, é possível afirmar que a morte no ciberespaço seria mais uma questão de tempo ou de conveniência e não uma falta de possibilidade.

No intuito de desvalidar a ciberguerra, Ridd (2011), baseando-se em Clausewitz, também aponta que a guerra não é apenas um ato isolado. Logo, apenas um ataque,

[4]World Population Review. Tampa, Florida Population 2022. Disponível em <https://worldpopulationreview.com/us-cities/tampa-fl-population > Acesso em: 01 de fev. de 2022.
[5]GARRETT, Filipe. Techtudo. Hackers invadem computador e tentam envenar água de cidade. Disponível em <https://www.techtudo.com.br/noticias/2021/02/hackers-invadem-computador-e-tentam-envenenar-agua-de-cidade.ghtml > Acesso em: 01 de fev. de 2022.

independente do domínio operacional, não seria suficiente para iniciar uma guerra. Vale ressaltar no entanto que devido às características próprias do ciberespaço, os ciberataques ocorrem com demasiada frequência. Analisando somente os exemplos mencionados do Irã e da Ucrânia é possível perceber isso. No Irã, por exemplo, existem analistas que apontam que o vírus já estava em andamento, desde 2007[6]. Ou seja, os danos causados em 2010 possivelmente tiveram início muito antes das consequências aparentes, demonstrando que não foi apenas um ataque isolado. O mesmo pode ser afirmado no caso da Ucrânia, onde uma série de ataques foram realizados tanto para que houve o rompimento de energia, quanto para que não pudesse ser realizada a reconexão.

Logo, é possível perceber que a ciberguerra possui os elementos intrínsecos à guerra de fato. E com os exemplos cada vez mais frequente, se torna gradativamente mais dificultoso a negação dela.

6 Considerações Finais

As questões cibernéticas se tornam cada vez mais complexas, de acordo com conectividade progressivamente crescente. Por isso, o debate da ciberguerra se faz tão relevante. Buscando uma definição de ciberguerra, no intuito de compreender o alcance dela, foi apresentado diferentes versões sobre o fenômeno.

Foi apresentado também o conceito de guerra, baseando-se na natureza da guerra de Clausewitz (1989), Brustolin (2014) reforça os limites da guerra. Pois, o intuito do trabalho se apresenta não só no debate das ideias sobre a existência da ciberguerra, mas a aplicação dela a uma teoria tradicional de guerra.

Para entender o fenômeno da ciberguerra, é necessário compreender alguns elementos intrínsecos a ela, como o ciberespaço e o ciberataque. Dessa forma, são dados os conceitos de cada um, demonstrando algumas características relevantes na ciberguerra. Também são apresentados alguns casos de ciberataques, como os ocorridos no Irã em 2010 e na Ucrânia em 2015.

Após a apresentação de cada uma das partes, tanto da ciberguerra, quanto da guerra, pretendeu-se analisar os casos de ataques cibernéticos à luz da definição de guerra defendido por Brustolin (2014), baseando-se em Clausewitz (1989). Como foi apresentado, o ciberespaço

[6]FINKLE, Jim. REUTERS. Researchers say Stuxnet was deployed against Iran in 2007. Disponível em < https://www.reuters.com/article/us-cyberwar-stuxnet-idUSBRE91P0PP20130226> Acesso em: 01 de fev. de 2022.

possui seus atributos específicos. Acredita-se que por essa razão, a ciberguerra seja desvalida como um fenômeno bélico. Além disso, o uso do ciberespaço ainda é pouco demarcado, dessa maneira, pode haver uma dificuldade maior de reconhecimento de alguns ataques no ciberespaço, algo que provavelmente não aconteceria em outros domínios operacionais.

Algo que deve ser enfatizado é que o reconhecimento da ciberguerra não faz com que os outros tipos de guerra sejam esquecidos ou não utilizados. Pelo contrário, o intuito de validar o fenômeno se vê pela necessidade de perceber que o ciberespaço pode e está, de acordo com os exemplos demonstrados, sendo utilizado para ações militares, com o cunho político. Ou seja, pode-se declarar que a ciberguerra é apenas mais uma faceta da guerra. Isso deve estar bem claro, pois a afirmação de uma não anula, de forma alguma, os outros meios de fazer a guerra.

Entende-se que ainda há inúmeros aspectos que podem e devem ser debatidos em relação à cibernética. E que possivelmente como apresentado por Arquilla e Ronfeldt (1993), será necessário a criação de doutrinas para a ciberguerra, no entanto, deve-se reconhecer os indícios apresentados para que ela possa ser reconhecida como também um meio possível de realizar a guerra.

O que acredita-se que é relevante para a análise do fenômeno é manter-se atento às inovações que a cibernética apresenta e ser possível de identificar o que pode ou não ser considerado guerra.

Referências

ALCANTARA, Bruna Toso; CASTELLANO DA SILVA, Igor. Guerra Cibernética: Uma análise conceitual sobre o termo. In: Danielle Ayres; Ana Luiza Vedovato; Daniela Lunkes; Elany de Souza; Juliano Bravo. (Org.). *Política Internacional Contemporânea*. 1 ed. Rio de Janeiro: Autografia, 2018.

ARQUILLA, John & RONFELDT, David. *Cyberwar is coming!* Califórnia: RAND Corporation, 1993.

AURÉLIO, D*icionário da Língua Portuguesa*. 6º ed. Curitiba: POSITIVO, 2006.

BOBBIO, Noberto. *Dicionário de Política.* 11º ed. Brasília: UnB, 2008.

BRUSTOLIN, Vitelio. *Criteria for defining war, terrorism, and guerrilla warfare based on Clausewitz's concepts of the nature and essence of war.* v. 25, n.3, 2019. Disponível em < https://revista.egn.mar.mil.br/index.php/revistadaegn/article/view/881 > Acesso em 20 de nov. de 2021.

CLAUSEWITZ, Carl von. *Vom Kriege,* Munique: Anaconda Verlag, 2018.

CLAUSEWITZ, Carl von. *On war*. Nova Jersey: Princeton University Press, 1982.

CLAUSEWITZ, Carl von. *Da Guerra.* São Paulo:WMF Martins Fontes, 1989.

E-ISAC. TLP: White – *Analysis of the Cyber Attack on the Ukrainian Power Grid* – Defense Use Case, Ucrânia, 2016.

KEEGAN, John. *Uma história da guerra.* São Paulo: Companhia de bolso, 2006.

KUSHNER, David. *The Real Story of Stuxnet.* Fev/2013. Disponível em <https://spectrum.ieee.org/the-real-story-of-stuxnet > Acesso em 20 de out. de 2021.

LANGENSCHEIDT. D*icionário Euro-Wörterbuch Portugiesisch-Deutsch*. Berlin: Langenscheidt Pub Inc, 2009.

LIBICKI, Martin C. *Cyberdeterrence and cyberwar.* Califórnia: RAND Corporation, 2009.

RIDD, Thomas. Cyberwar will not take place. *Journal of Strategic Studies.* v.35, n.1, 2011. Disponível em < http://dx.doi.org/10.1080/01402390.2011.608939 > Acesso em 20 de out. de 2021.

SINGER, P.W. & FRIEDMAN, Allan. *Cybersecurity and Cyberwar – what everyone needs to know*. Oxford: Oxford University Press, 2014.

STONE, John. Cyberwar will take place! *Journal of Strategic Studies*. v36, n.1, p. 101-108, 2013. Disponível em < http://dx.doi.org/10.1080/01402390.2011.608939 > Acesso em 20 de out. de 2021.

STRATE, Lance. The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication.* v. 63, n. 3, 2019. Disponível em < http://dx.doi.org/10.1080/10570319909374648 > Acesso em: 20 de out. de 2021.

Recebido em 06 de dezembro de 2022.
Aceito para publicação em 15 de maio de 2022.