REVISTA NEIBA
CADERNOS ARGENTINA-BRASIL

Volume 12, 2023, p. 01-18
DOI: 10.12957/neiba.2023.74696 | e74696 I ISSN: 2317-3459

"A GUERRA É UM CAMALEÃO": A CIBERGUERRA SOB A ÓTICA CLAUSEWITZIANA

"WAR IS A CHAMELEON": CYBERWAR FROM THE CLAUSEWITZIAN PERSPECTIVE

Juliana Zaniboni de Assunção[1]

[1]Universidade Federal Fluminense (PPGEST/UFF), Rio de Janeiro, RJ, Brasil. E-mail: julianazaniboni@id.uff.br ORCID: https://orcid.org/0000-0001-9695-6661

Recebido em: 11/04/2023 | Aceito em: 27/10/2023.

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 e ainda é bastante utilizada para explicar diversos conflitos tradicionais como as Guerras Mundiais e outros fenômenos não convencionais como terrorismo, guerra de guerrilha. Mesmo com a elasticidade da teoria, será que ela poderia ser aplicada à ciberguerra? Com o intuito de responder a essa questão, a metodologia utilizada foi qualitativa, baseada na revisão bibliográfica e no método de coleta e análise de dados denominado Análise de Conteúdo de Laurence Bardin (1977).

O resultado encontrado demonstrou os principais argumentos que defendem sua invalidação não são suficientes para desqualificá-la como um conflito. Diante desse resultado, concluí que a teoria de Clausewitz consegue justificar o fenômeno da ciberguerra.

Palavras-chave: Ciberguerra; Ciberespaço; Ciberataque.

ABSTRACT

For Clausewitz (1989), war is an act of ofrce that compels 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. The clausewitzian theory was and still is widely used to explain several traditional conflicts such as the World Wars and other unconventional phenomena such as terrorism and guerrilla warfare. Even with the elasticity of the theory, could it be applied to cyberwarfare? In order to answer this question, the methodoly used was qualitative, based on a bibliographical review and on the data collection and method analysis called Content Analysis by Laurence Bardin (1977).

The result found demonstrated that the main arguments that defend its invalidation are not enough to disqualify it as a conflict. Given this result, I concluded that Clausewitz's theory can justify the ohenomenon of cyberwar.

Keywords: Cyberwar; Cyberspace; Cyberattack.

1. INTRODUÇÃO

O debate apresentado neste artigo reflete sobre a ciberguerra e sua validação enquanto um conflito bélico. Na revisão da literatura, foram elencados quatro argumentos medulares que testam se a teoria de Clausewitz poderia justificar a ciberguerra, ou não. Os textos selecionados para esse recorte focam na corrente de autores que invalidam a ciberguerra, baseando-se em Clausewitz. São eles: Rid (2012), Canabarro e Borne (2013) e Valeriano e Maness (2015).

Dessa forma, o artigo está apresentado na seguinte divisão:

Na primeira seção, é apresentada um pouco da definição do ciberespaço, um elemento chave para entender a ciberguerra e que é constantemente mencionado no texto. A compreensão de sua existência, assim como complexidade, faz com que fenômenos cibernéticos deixem de ser tão abstratos. O ciberespaço, ou espaço cibernético, é o domínio operacional no qual os fenômenos cibernéticos se manifestam, sendo um exemplo deles, a ciberguerra. Ou seja, é o ambiente em que ela acontece, assim como a guerra naval ocorre no mar, a ciberguerra, no ciberespaço. Nesse elemento também foi identificado um extenso debate sobre suas definições, delimitações e aplicações. Como esse não é o foco da pesquisa, mas seu entendimento é fundamental para ela, o extrato exibido não tem o objetivo de mostrar todas as discussões sobre o tema, mas sim elucidar sobre suas distintas possibilidades.

A segunda seção se subdividiu na apresentação dos quatro argumentos encontrados que deslegitimam a ciberguerra, sendo eles:

1) A guerra nunca é um ato isolado;
2) Um ato de guerra precisa ser violento;
3) Um ato de guerra sempre é instrumental;
4) Natureza política da guerra;

Nas conclusões finais, são analisados todos os exemplos e argumentos apresentados nas seções anteriores, com o objetivo de compreender se a teoria da Guerra, de Clausewitz pode justificar fenômenos cibernéticos, como a ciberguerra.

2. O CIBERESPAÇO

A discussão do ciberespaço é primordial para o entendimento da ciberguerra. Afinal, sem ela, discussões sobre a ciberguerra podem se tornar um tanto quanto vagas e distorcidas. Como mencionado anteriormente, existe um debate denso sobre o tema, que inclusive abarca diversas áreas, indo desde a literatura até a academia, perpassando por empresas de tecnologia. Além dessa gama de possibilidades em diversas áreas, ainda é destacado que em 2016, a Organização do Tratado do Atlântico Norte (OTAN) classificou o ciberespaço como um domínio operacional de guerra[2], apesar de alguns países como Brasil e Estados Unidos, entre outros, assumirem essa definição anos antes. Devido a vasta configuração, o foco do tema se baseia em sua conceituação, além de suas características.

2.1 O CIBERESPAÇO NA ACADEMIA

Mesmo que o tema seja subdividido em diferentes áreas de estudo, ainda existem numerosas visões sobre o mesmo objeto. Assim, não se pode considerar a visão da academia sobre o ciberespaço como única, visto que dentro dela também não há consenso. Apesar disso, a discussão foi dividida em duas correntes: ambiente virtual e físico.

Basicamente, essa divisão possui o intuito de destacar que existem autores que consideram o ciberespaço somente como um ambiente majoritária ou prioritariamente virtual e outros que consideram também sua parte física.

2.1.1 PARTE VIRTUAL

Autores como Gartzke (2013) argumentam que o ciberespaço seria uma espécie de sinônimo da Internet. Ou seja, que seu funcionamento, assim como suas consequências estão atreladas ao ambiente virtual. Com esse pensamento, fenômenos cibernéticos poderiam ser vistos como um problema menos urgente, principalmente pela sua condição vinculada e restrita a Internet.

Outra contribuição que vai no mesmo sentido de exclusividade virtual do ciberespaço é afirmação que:

> O ciberespaço não é um lugar físico – ele desafia a medição em qualquer dimensão física ou continuum espaço-tempo. É um termo abreviado que se refere ao ambiente criado pela influência de redes cooperativas de computadores, sistemas de informação e

[2] SPUTNIK. Otan classifica ciberespaço como domínio operacional de guerra. Disponível em <https://sputniknewsbrasil.com.br/20160614/otan-ciberespaco-dominio-guerra-5084700.html > Acesso em: 23 mar. 2023.

> infraestruturas de telecomunicações comumente referidos como Internet e World Wide Web. A informação é a mercadoria valiosa do ciberespaço, mas nada existe realmente no ciberespaço. Quando se diz que algo está no ciberespaço, na verdade, está fisicamente residente em um computador ou sistema de informação, ou está em trânsito dentro de uma infraestrutura de telecomunicações. (Sharp, 1999, p. 15, *tradução da autora*)

2.1.2 PARTE FÍSICA

Diferentemente dos autores citados acima, existe a visão de que o ciberespaço, para além de sua parte virtual, também engloba uma parte física. Nesse sentido, é afirmado que:

> O ciberespaço é, antes de tudo, um ambiente de informação. É composto de dados digitalizados que são criados, armazenados e, mais importante, compartilhados. Isso significa que não é apenas um lugar físico e, portanto, desafia a medição em qualquer tipo de dimensão física. Mas o ciberespaço não é puramente virtual. Ele compreende os computadores que armazenam dados, além dos sistemas e infraestrutura que permitem que ele flua. Isso inclui a Internet de computadores em rede, intranets fechadas, tecnologias de celular, cabos de fibra ótica e comunicações baseadas em espaço. (Singer e Friedman, 2014, 13-14, *tradução e grifo da autora*).

Dessa forma, os autores afirmam que o ciberespaço é mais do que a Internet. Logo:

> O ciberespaço e a internet não são sinônimos: o primeiro é um domínio operacional eletrônico / eletromagnético, o segundo é a rede central do domínio operacional baseada em computadores." O primeiro existe sem o segundo, mas o segundo só existe porque o primeiro existe. Assim, o ciberespaço e a sua possibilidade como cenário e recurso de guerra é algo muito mais alargado, já a internet é uma ferramenta que pode ser utilizada para um conflito, mas que ainda não teve sua efetiva dimensionalidade bélica determinada, ou mesmo, efetivamente consensualizada entre o meio acadêmico e militar. (Ayres, Grassi, 2020, p. 106, *grifo da autora*)

Reforçando a existência do componente físico do ciberespaço, é afirmado que:

> O ciberespaço é um espaço de todas as redes de computadores do mundo e tudo que eles se conectam e controlam. Não é só a Internet. Sejamos claros sobre a diferença. A Internet é uma rede aberta de redes. De qualquer rede na Internet, você deve ser capaz de se comunicar com qualquer computador conectado a qualquer uma das redes da Internet. O ciberespaço inclui a Internet e muitas outras redes de computadores que não deveriam ser acessíveis a partir da Internet. Algumas dessas redes privadas se parecem com a Internet, mas eles são, pelo menos teoricamente, separados. Outras partes do ciberespaço são redes transacionais que fazem coisas como enviar dados sobre fluxos de dinheiro, negociações no mercado de ações e transações com cartão de crédito. Algumas redes são sistemas de controle que apenas permitem que as máquinas falem com outras máquinas, como painéis de controle conversando com bombas, elevadores e geradores. (Clarke & Knake, 2010, p. 63, *tradução da autora*)

Logo, com os extratos apresentados, a posição metodológica deste artigo é entender que o ciberespaço possui dimensões que perpassam tanto o ambiente virtual, quanto físico. Dessa forma, a Internet seria apenas um dos elementos que envolvem sua dinâmica, tendo que considerar fios, cabos, equipamentos e computadores.

Outro elemento de igual relevância para a ciberguerra que necessita de destaque é o ciberataque. É sabido que existem diversos tipos de ciberataques, alguns que 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 da autora*) 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 (2014, p. 69) 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" (*tradução da autora*).

Com a menção do ciberataque, é possível entender a dimensão do ciberespaço e porque ele deve ser considerado para além da Internet. Um exemplo disso seria o ciberataque ocorrido no Irã, em 2010, chamado Stuxnet. A questão principal desse ciberataque foi a forma como o vírus conseguiu forçar sua entrada nos computadores que operavam as centrífugas iranianas. O malware foi instalado através de um pendrive USB, ou seja, através de um equipamento e não através da Internet (Kushner, 2013).

2.1.3 AS CARACTERÍSTICAS DO CIBERESPAÇO

De forma geral e usando definições preliminares, o ciberespaço possui as seguintes características:

> (a) As infraestruturas físicas básicas, como computadores, dispositivos móveis, servidores e roteadores, que permitem a conexão entre tecnologia e redes de sistemas de comunicação;
> (b) Sistemas de computador e diversos softwares de suporte para garantir sua funcionalidade e conectividade;
> (c) Redes entre computadores distribuídos e as redes de redes;
> (d) Dados e informações residentes, bem como atividades relacionadas, como armazenamento, transmissão, troca, processamento e compartilhamento. (Ning, 2022, p.3, *tradução da autora*)

A partir do vislumbre dos debates que concernem ao ciberespaço, são analisados os argumentos com base na teoria de Clausewitz a fim de testar se é possível que sua obra justifique fenômenos como a ciberguerra.

3. OS ARGUMENTOS E A CIBERGUERRA

São demonstrados a seguir os quatro argumentos que deslegitimam a ciberguerra, baseando-se em Clausewitz.

3.1 A GUERRA NUNCA É UM ATO ISOLADO

Dois pontos que Canabarro e Borne (2013) apontam na teoria de Clausewitz é que a guerra, nunca é um ato isolado e não consiste em apenas um simples golpe. Isso significa dizer que um único ciberataque, no caso, não seria o suficente para iniciar uma guerra. De fato, um ataque não justifica a nomeclatura de guerra. No entanto, essa condição depende de qual ciberataque é analisado.

O exemplo utilizado para esse argumento é o ciberataque Stuxnet,ocorrido no Irã, em 2010. Através do relatório sobre as Ameaças Cibernéticas Iranianas (CISA), foi identificado uma atividade cibernética entre os seguintes países: Irã, vítima do vírus, Israel e Estados Unidos, ambos atribuídos como responsáveis pelo ataque. A seguir são exibidas duas tabelas com as atividades cibernéticas entre Irã-Estados Unidos e Irã-Israel.

Tabela 1- Atividade Cibernética entre Irã e Estados Unidos

Atividade Cibernética entre Irã e Estados Unidos		
Data	**Título**	**Descrição**
Final de 2011 até metade de 2013	DDoS direcionado ao Setor Financeiro dos Estados Unidos	Os ataques privavam os clientes de acessar suas contas e custou aos bancos milhões de dólares em remediação.
Abril de 2012	**Flame e Wiper**	**Sabotagem visando infraestruturas críticas**
Julho de 2012	**Madi**	**Ciberespionagem de infraestruturas críticas**
Agosto de 2012	**Shamoon**	**Destruia dados e impedia o computador de reiniciar**
Setembro de 2012	**Operação Ababil**	**DDos contra instituições financeiras americanas**
Fevereiro de 2014	Sands Las Vegas Corporation Hackeada	Atores de ameaças cibernéticas invadiram a Sands Las Vegas Corporation em Las Vegas, Nevada, e roubaram dados de clientes, incluindo dados de cartão de crédito, números de previdência social e números de carteira de motorista. O ataque também envolveu uma parte destrutiva, pois os sistemas dos computadores também foram apagados. Em setembro de 2015, o Diretor de Inteligência Nacional dos EUA identificou o governo iraniano como perpetrador do ataque.
2013 a 2017	Campanha de roubo cibernético em nome do Exército dos Guardiões da Revolução Islâmica (EGRV)	Os roubos tiveram como alvo dados acadêmicos e de propriedade intelectual, bem como credenciais de contas de e-mail.
2016- 2017	Shamoon 2	Foco nas empresas de energia de gás no Oriente Médio

Fonte: Relatório sobre as Ameaças Cibernéticas Iranianas (CISA) – *Formulação própria*.

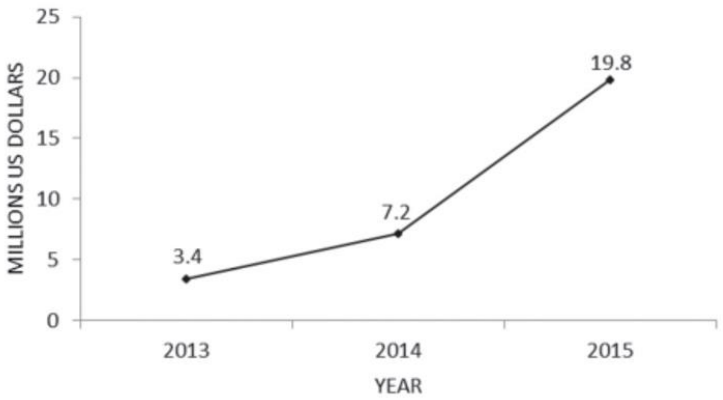
Tabela 2- Atividade Cibernética entre Irã e Israel

Atividade Cibernética entre Irã e Israel		
Data	**Título**	**Descrição**
2010	Stuxnet	Ataque nas centrífugas nucleares iranianas
2012 a 2015	Stars, Duqu, Wiper, Flame, outros	Destruição de dados, ciberespionagem
2020	Ciberataque a Infraestrutura de Água em Israel	Ciberataque com o objetivo de aumentar o nível de cloro no abastecimento de água para níveis consideravelmente altos.
Algumas semanas depois do ataque mencionado acima	Ciberataque no tráfego marítimo no porto de Shahid Rajaee, no Irã.	Interrupção nos sitemas de computador que regulam o tráfego marítimo. Ação durou 3 dias.
Setembro de 2012	Operação Ababil	DDos contra instituições financeiras americanas
2021	Mensagens Falsas no Irã	As mensagens espalhadas no Irã causaram caos nas estações de trem iranianas postando mensagens falsas sobre cancelamentos.
2021	Blecaute na instalação nuclear iraniana em Natanz	A ocasião causou explosões, sendo considerada pelo Irã como sabotagem, levando 9 meses para restaurar a produção em Natanz.
2022	Diversos ciberataques	Retirando do ar alguns sites governamentais de Israel

Fonte: Collin e Sadjadpour, 2018 – *Formulação própria*

É destacado também que essa regularidade só pode ser realizada, devido aos investimentos dos países em cibersegurança/ ciberdefesa. Através do gráfico abaixo, é notado que o Irã vem aumentando gradativamente seu empenho em aprimorar esta área.

Gráfico 1- Orçamento de Cibersegurança do Irã (2013-2015)



Fonte: Small Media, 2015.

Através das tabelas, foi identificado que o Stuxnet não foi o único ciberataque, mas que pelo contrário, existe uma certca recorrência de atividades cibernéticas entre os países envolvidos. Logo, esse exemplo demonstra que o ciberataque mencionado foi um de vários ataques dentro desta atividade cibernética entre os países. Dessa forma, nem todos os ciberataques podem ser

considerados de forma isolada, mas sim levando em consideração a frequência de ciberataques no ciberespaço e as disputas de poder de cada ator.

3.2 UM ATO DE GUERRA PRECISA SER VIOLENTO

A definição do conceito guerra cunhado por Clausewitz possui as seguintes definições, em três idiomas: no alemão (original), inglês e português. A necessidade dessa exposição se faz principalmente pela tradução da palavra Gewalt, como é demonstrada a seguir.

Em alemão: “Der Kriege ist also ein Akt der Gewalt, um der Gegner zur Erfüllung unseres Willens zu zwingen” (2010, p. 3).

Em inglês: “ War therefore is an act of violence intended to compel our opponent to fulfil our will” (1989, p. 101).

Em português: “A guerra é, portanto, um ato de força para obrigar o nosso inimigo a fazer a nossa vontade” (2014, p. 75).

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. Utilizando as traduções mais adequadas para o caso, tem-se: violência e força. Com isso posto, a guerra seria um ato de força ou violência?

Para entender essa diferenciação, é necessário dividir um ato de força e de violência.

Ato de força: Na Crise dos Mísseis de 1962, ocorreu o episódio do bloqueio militar americano, fazendo com que os navios soviéticos não conseguissem chegar até Cuba, com o objetivo de implantar mais mísseis balísticos. Ou seja, o bloqueio naval americano pode ser considerado um ato de força pelo qual obrigaram ao seu inimigo (União Soviética) a não fazer o que desejavam.

Ato de violência: Durante a Guerra dos 6 Dias, houve o episódio do bombardeio israelenses às forças aéreas egípcias e sírias, inviabilizando o ataque árabe contra Israel. Desde a criação do

Estado de Israel, o país estava cada vez mais se expandindo pelo Oriente Médio, chegando até o território egípcio. O combate foi visto como uma forma de suspender a expansão israelense, no entanto, não obteve o resultado esperado para os árabes. Ao realizar esse ato de violência, Israel impossibilitou o avanço aéreo sírio e egípcio sobre o país. Dessa forma, além do ataque não ter sido bem sucedido, Israel conseguiu o reconhecimento formal de seu território.

Ainda sobre o ato de violência, é possível desdobrá-lo em duas formas de análise: 1º destruir algo, como o caso da destruição da força aérea egípcia; 2º a letalidade, ou seja, levar alguém à morte. Quando Rid (2012), Canabarro e Borne (2013) e Valeriano e Maness (2015) falam sobre violência na guerra, eles se referem ao 2º ponto.

Realmente, até a data da escrita deste artigo nenhuma pessoa foi morta em decorrência de algum ciberataque. Entretanto, um exemplo para refletir sobre isso seria o ciberataque ocorrido em Tampa, Flórida, em fevereiro de 2021.

No ocorrido, um hacker conseguiu invadir o abastecimento de água da cidade e aumentou em 100 vezes o permitido de distribuição de hidróxido de sódio (soda cáustica). Por sorte, o segurança do local identificou que o mouse estava se movimento sozinho e acionou o alarme. Ainda não se sabe quem foi o responsável pelo caso, se ele pertencia a alguma organização ou qual era seu objetivo em realizar tal ação. No entanto, é entendido que esse ciberataque ocorreu através de um programa chamado TeamViewer. Esse software é capaz de operar e fazer manutenções de computadores remotamente. Suponha que existam dois computadores, um na Flórida e outro no Brasil. Uma pessoa possui arquivos que estão no computador da Flórida, mas ela está no Brasil e esqueceu de fazer o upload no drive. Do computador do Brasil, se ambos possuem instalados o software TeamViewer, através de um código que o software produz, essa pessoa consegue acesso ao seu outro computador e mexer em todos os arquivos como se ela estivesse no local.

No caso da rede de abastecimento de água, o código não foi dado ao invasor, mas sim hackeado (roubado), fazendo com que ele pudesse alterar qualquer parte que desejasse, inclusive

a taxa de soda cáustica na água. Felizmente, o ciberataque não foi bem sucedido, no entanto, caso fosse, milhares de pessoas poderiam ser impactadas com o ato.

3.3 UM ATO DE GUERRA SEMPRE É INSTRUMENTAL

Sobre esse argumento, Rid (2012) e Canabarro e Borne (2013) exploraram o conceito de guerra, de Clausewitz, mencionado na seção anterior. Ou seja, na guerra um oponente deve ser subjulgado pelo outro. Com isso, é possível perceber duas ideias presentes nesse argumento: linearidade da guerra e rendição. Isso significa dizer que os autores interpretaram a guerra como se ela sempre fosse um evento linear, ou seja, que tenha início, meio e fim e que um oponente sempre será subjulgado a outro.

Na questão do ciberespaço, ainda não é possível identificar o desligamento total de todas as redes e subjulgação total de um oponente sobre o outro. No entanto, historicamente também houve outros exemplos em que o caráter instrumental não foi seguido à risca. Essa afirmação se comprova com o fim da Guerra Fria (1950-1991).

Analisar a Guerra Fria por si só já seria algo complexo, visto sua modificação em relação aos conflitos convencionais até então travados como as Guerras Mundiais. Durante o episódio, houve momentos mais e menos 'quentes' do conflito. Com a inovação bélica das bombas atômicas, foi travada uma nova 'fase' da guerra. As potências principais do evento, Estados Unidos e União das Repúblicas Socialistas Soviéticas (URSS) não se enfrentavam mais 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, a ênfase está no seu fim.

O fim da Guerra Fria ocorreu não através de ocupação e subjulgação militar pelos Estados Unidos, mas sim devido às questões e disputas políticas e econômicas, que assolavam a União Soviética na época (Darraj, 2010). Dessa forma, o fim do conflito não envolveu a condição de rendição diretamente. Além disso, o próprio Clausewitz (1989, p.89) afirma que "a guerra é mais que um verdadeiro camaleão". Nesse sentido, ele afirma que:

> Na guerra o resultado nunca é definitivo. Por último, mesmo o resultado final de uma guerra nem sempre deve ser considerado final. O estado derrotado muitas vezes considera o resultado apenas como um mal transitório, para o qual um remédio ainda pode ser encontrado nas condições políticas em alguma data posterior. É óbvio que isso

> também pode afrouxar a tensão e reduzir o vigor do esforço. (Clausewitz, 1989, p. 80, *tradução da autora*)

Logo, o caráter instrumental não invalida a classificação de um fenômeno enquanto belicoso ou não. Pelo contrário, Clausewitz destaca a complexidade e irregularidade linear dos conflitos.

3.4 NATUREZA POLÍTICA

Rid (2012) argumenta que os ciberataques não estão ligados às questões políticas. A política é o elemento central da teria clausewiztiana. Assim, ela é definida como a "representação de todos os interesses da comunidade" (Clausewitz, 2014, p. 607). Nesse sentido, é possível fazer um paralelo com o primeiro argumento citado, onde se faz necessário analisar a atividade cibernética entre os atores envolvidos. Assim, os ciberataques podem estar atrelados às questões políticas da mesma maneira, analisando o ciberespaço como um novo ambiente para realizar ataques.

Assim como na seção 3.1, o exemplo mencionado é o Stuxnet. A relação política entre os atores envolvidos Irã-Israel-Estados Unidos não começou com o ciberataque mencionado. Pelo contrário, ela remonta muitos anos anteriores. No entanto, o que se deve focar na análise é o contexto em que os atores estão para que tal episódio acontecesse. Para isso, a conjuntura enfatizar a questão nuclear. Os Estados Unidos, Israel e Irã nem sempre tiveram uma relação estremecida. Na verdade, dependendo da conjuntura, uma aproximação entre eles já foi identificada. Como o cerne da questão se localiza através da questão nuclear, são destacados os pontos fulcrais para a mudança de posição.

3.5 QUESTÃO NUCLEAR

A história do Irã com seu programa nuclear começa na década de 1950, solicitado pelo Xá Mohammad Rezā Shāh Pahlavi, auxiliado pelos Estados Unidos, chamado programa Átomos para a Paz, tendo como parte do acordo a ajuda do país para construir um reator de pesquisa de água-leve na Universidade de Teerã, no Irã, sendo essa a primeira planta nuclear do país. O programa mencionado posteriormente originaria a Agência Internacional de Energia Atômica (AIEA), agência autônoma das Organização das Nações Unidas (ONU), desde 1957.

Após os Estados Unidos e a União Soviética desenvolverem bombas nucleares, outros países também começaram uma disputa para ter acesso a tal dispositivo. Foi então desenvolvido em

1960, o Tratado de Não-Proliferação de Armas Nucleares (TNP), para que outros países não tivessem acesso a armas nucleares, exceto os já detentores além de Grã-Bretanha, França e China.

Em 1968, o Irã assina o TNP e em 1974 é estabelecida a Organização Iraniana de Energia Atômica. Na época, o Irã era entendido como aliado norte-americano devido ao Xá Pahlavi. Em 1979 ocorreu a Revolução Iraniana, ascendendo ao poder o Ayatollah Ruhollah Khomeini. A partir da instabilidade política que se firmava no Irã, o contrato sobre o programa nuclear foi interrompido. Ele é retomado apenas na Guerra Irã-Iraque (1980-1988), pois havia a possibilidade do Iraque estar desenvolvendo armas nucleares (Broad, 2001), sendo uma ameaça direta para o Irã. Na conjuntura, o Irã se via isolado, tanto dos países árabes, quanto dos Estados Unidos. A disputa da balança de poder estava entre Irã e Iraque, sendo este temido por Israel, por acreditar ser sua próxima ameaça. Para Israel, além do isolamento político, não era descartado o conflito direto caso o Iraque se tornasse um hegemon na região. (Parsi, 2007)

O fim da Guerra Fria proporcionou um cenário mais vantajoso para Israel. Isso se devia ao fim da Guerra do Irã-Iraque, estando este flertando com os Estados Unidos e a ausência da ameaça da União Soviética. Essa conjuntura fez com que Israel visse a oportunidade de se aproximar mais dos países árabes, mudando seu posicionamento drasticamente, passando a enxergar o Irã como uma nova ameaça. Dessa forma, os países árabes e Israel deveriam se juntar contra a nova ameaça na balança de poder: Irã.

Apesar desse novo cálculo estratégico israelense, isso foi encarado com bastante ceticismo no Ocidente, principalmente porque Israel era aliado do Irã há poucos anos atrás. No entanto, essa relação vai se deteriorando cada vez mais. Principalmente porque com o fim da Guerra Fria, ou seja, sem a ameaça soviética, era necessário criar um novo inimigo que justificasse todo o aparato militar construído (Pecequilo, 2013).

A partir dos anos 2000, as relações Irã-Israel-Estados Unidos só pioraria, principalmente com a ascensão do neoconservadorismo americano e os atentados do 11/09, que reverberaram na Guerra ao Terror[3].

[3] Guerra ao Terror: campanha militar liderada pelos Estados Unidos da América em resposta aos atentados do 11 de setembro, com a finalidade de aniquilar o terrorismo. "O esforço politicamente correto de não vincular o Islã ao terrorismo foi atravessado por manifestações ambíguas e estigmatizantes nos discursos que definiram a chamada *guerra ao terror – war on terror* – lançada por Bush no seu discurso ao Congresso estadunidense – o Discurso do Estado da União – de 21 de setembro de 2001, no qual afirmou que os EUA entravam numa 'guerra longa, invisível e de conclusão indeterminada'. (Rodrigues, 2013, p. 207)

Esse contexto fez com que as relações entre os países fossem piorando, até que em 2002 em um discurso anual do presidente George W. Bush, o Irã foi adicionado à lista de países do Eixo do mal, juntamente com Iraque e Coreia do Norte. Sobre isso, o presidente afirma que:

> Estados como estes, e seus aliados terroristas, constituem um eixo do mal, armando-se para ameaçar a paz do mundo. Ao buscar armas de destruição em massa, esses regimes representam um perigo grave e crescente. Eles poderiam fornecer essas armas aos terroristas, dando-lhes os meios para igualar seu ódio. Eles podem atacar nossos aliados ou tentar chantagear os Estados Unidos. Em qualquer um desses casos, o preço da indiferença será catastrófico.
> Trabalharemos em estreita colaboração com nossa coalização para negar aos terroristas e seus patrocinadores estatais os materiais, a tecnologia e o conhecimento para fabricar e entregar armas de destruição em massa.
> Desenvolveremos e implantaremos defesas antimísseis eficazes para proteger os Estados Unidos e nossos aliados de um ataque súbito. (The Washington Post, 2002, *tradução da autora*)

A partir do contexto demonstrado, organizado em eixos, é entendido como a aproximação e distanciamento entre Irã-Israel-Estados Unidos ocorreu. Nas próximas subseções são apresentados o programa nuclear e de mísseis do Irã, a fim de entender o impacto político em suas agendas.

Coincidentemente, ou não, no mesmo ano em que o país entra para a lista dos países do Eixo do Mal, no dia 14 de agosto de 2002, o Conselho Nacional de Resistência ao Irã, oposição do governo, realiza uma coletiva de imprensa e declara que o Irã construiu instalações nucleares perto de Natanz e Arak (NCRI, 2022). Mesmo não possuindo provas suficientes para comprovar as alegações, esse episódio ajudou a fomentar as suspeitas de que o país estava desenvolvendo seu programa secreto de enriquecimento de urânio. A partir desse momento, o Irã é enxergado como um inimigo financiador de terrorismo e possível detentor de bombas atômicas. Até o dia que este artigo foi escrito, não existe nenhuma prova substancial que consiga comprovar isso.

Apesar das inúmeras tentativas de seguir com seu programa de energia nuclear, inclusive realizando parcerias com países como Rússia, França, Alemanha e Grã-Bretanha, devido a quebra de acordo, o Irã não conseguiu o apoio suficiente para isso. Vale destacar que o país continuou sendo duramente exonerado com diversas sanções.

Em fevereiro de 2010, o Irã anuncia que retomou seu processo de enriquecimento nuclear a 20% (Cunningham e Fahim, 2021), com capacidade de chegar a 80%. Em maio do mesmo ano, é assinado o Acordo Tripartite, entre Brasil, Turquia e Irã. Através desse acordo, era pretendido o

fim da crise nuclear que se perdurava por anos, entre o Irã e as potências globais envolvidas durante o processo. Apesar da iniciativa, França, Rússia e os Estados Unidos não o aceitaram. A partir de junho de 2010, uma nova série de severas sanções são aplicadas ao Irã e junto a esse contexto, é descoberto o vírus Stuxnet.

Com a descrição da sucessão dos fatos, foi percebido que foi crescente a suspeita e preocupação do Irã obter os materiais necessários para fabricar uma bomba nuclear. Porém, ter a bomba nuclear por si só não seria somente o problema, visto que seria preciso o equipamento apropriado para levá-la ao destino do ataque, caso o país realmente a tivesse.

4. CONSIDERAÇÕES FINAIS

O objetivo deste recorte era analisar os argumentos principais que deslegitimavam a ciberguerra através da teoria de Clausewitz. Realizando a revisão da literatura, chegou-se a quatro argumentos dentro desse modelo, cunhado pelos autores Rid (2012), Canabarro e Borne (2013) e Valeriano e Maness (2015). Os argumentos foram:

1) A guerra nunca é um ato isolado;

2) Um ato de guerra precisa ser violento;

3) Um ato de guerra sempre é instrumental;

4) Natureza política da guerra.

Durante o artigo, cada um desses argumentos foi analisado, mostrando os pontos presentes na ciberguerra e também em outros conflitos considerados convencionais. No primeiro ponto, foi observado que os ciberataques podem ter uma certa frequência, dependendo de determinadas circunstâncias. O ponto fulcral deste argumento é enfatizar que os ciberataques devem ser entendidos dentro de um contexto de disputas e que é capaz de ter linearidade também. Dessa forma, analisar os ciberataques de forma separada e longe dessa óptica pode gerar interpretações errôneas sobre o conflito.

No segundo ponto, foi exibida uma discussão sobre a tradução do conceito de guerra e debatida a presença de dois elementos intrínsecos à guerra: a violência e a força. Como foi

apresentada, delimitar a guerra a um elemento não faria sentido se fosse utilizada a abordagem de Clausewitz. Apesar disso, não houve o descarte total do elemento da violência dentro do fenômeno da ciberguerra.

No terceiro ponto, foi mostrada que a guerra nem sempre é linear e possui a ideia de rendição total ao inimigo. Não abordando somente a ciberguerra, como outros eventos históricos como o fim da Guerra Fria. O próprio Clausewitz entende que a guerra pode retornar e se dinamizar diante da conjunta dos atores envolvidos na disputa.

No quarto ponto, que também pode ser feito um link com o primeiro, é possível perceber que o ciberespaço não está alheio aos acontecimentos do mundo físico. Dessa forma, é reforçada a necessidade de análise em conjunto para melhor compreensão da gravidade, decorrência e justificava política que o ciberataque abarca.

Com os quatro pontos delimitados, se entende que a teoria de Clausewitz pode justificar o fenômeno da ciberguerra e os autores que apresentam tais argumentos não conseguem invalidá-la. No entanto, se destaca que nem todo o ciberataque pode ser considerado guerra e entendido dentro da lógica de disputa de determinados atores. Dito isso, entende-se que é necessário reconhecer a interdisciplinariedade e complexidade do fenômeno antes de analisá-lo. Dessa forma, entende-se que "a guerra, então, é apenas um verdadeiro camaleão, que modifica um pouco a sua natureza em cada caso concreto". (Clausewitz, 2014, p. 30)

REFERÊNCIAS BIBLIOGRÁFICAS

Ayres, D. e Grassi, J. (2020). "Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil". *Brasil: Revista Brasileira de Estudos de Defesa*. v. 7, p. 103-131.

Bardin, L. (1977). *Análise de Conteúdo*. França: Edições 70.

Broad, W. J. (2001). NY TIMES. Document Reveals 1987 Bomb Test by Iraq. Disponível em < https://www.nytimes.com/2001/04/29/world/document-reveals-1987-bomb-test-by-iraq.html > [Acesso em: 10 de dez. 2021].

Canabarro, D. R.; Borne, T.. (2013). *Reflections on the Fog of (Cyber)War*. SSRN Electronic Journal. Disponível em < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3155453 > [Acesso em: 06 de jun. 2021].

Anderson, C. e Sadjadpour, K. (2018). *Iran's cyber Threat: espionage, sabotage, and revenge.* Carnegie Endowment for International Peace.

CISA: Cybersecurity & Infrastructure Security Agency. (ano?) I*ran Cyber Threat Overview and Advisories*. Disponível em <https://www.cisa.gov/uscert/iran#iranian > [Acesso em: 26 de jun. 2022].

Clarke, R. A. e Knake, R. K. (2010). *Cyber war: The next threat to National Security and what to do about it*. New York: Eco Press.

Clausewitz, Carl von. (1989). *On war*. New Jersey: Princeton University Press.

Clausewitz, Carl von. (2010). *Vom Kriege*, Munique: Anaconda Verlag.

Clausewitz, Carl von. (2014). *Da Guerra*. São Paulo: WMF Martins Fontes.

Cunningham, Eric & Fahim, Kareem. (2021). *The Washington Post. Iran begins enriching uranium to 20 percent in new breach of nuclear deal*. Disponível em < https://www.washingtonpost.com/world/middle_east/iran-nuclear-uranium-enrichment/2021/01/04/588949be-4e76-11eb-a1f5-fdaf28cfca90_story.html > [Acesso em: 06 de jan. 2023].

Darraj, S.M. (2010).*The Collapse of Soviet Union*. New York: Chelsea House.

Gartzke, E. (2013). "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth". *International Security*, 38(2), p. 41–73.

Kushner, D.. (2013) "The real story of stuxnet". *IEEE Spectrum*, 50(3), p. 48–53, mar.

Langenscheidt. (2009). *Dicionário Euro-Wörterbuch Portugiesisch-Deutsch*. Berlin: Langenscheidt.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. California: Rand Corporation.

NCRI: (National Council of Resistance of Iran). (2022). Timeline of NCRI's Revelations to Prevent a Nuclear-armed Iran. Disponível em < https://www.ncr-iran.org/en/news/exclusive-report/timeline-of-ncris-revelations-to-prevent-a-nuclear-armed-iran/ > [Acesso em: 06 de jan. 2023].

Ning, H. (2022). *A Brief History of Cyberspace.* Florida: CRC Press.

Parsi, T. (2007). *Treacherous Alliance: The Secret Dealings of Israel, Iran, and the United States*. London: Yale University Press.

Pecequilo, C. S. (2013) *Os Estados Unidos e o século XXI*. Rio de Janeiro: Elsevier.

Rid, T. (2012). "Cyber War Will Not Take Place". *Journal of Strategic Studies*, 35(1), p. 5–32, fev.

Rodrigues, T. (2013). *Guerra e Terror*. In: Terrorismo de Estado. Belo Horizonte: Autêntica.

Sharp, W. G. (1999). *Cyberspace and the use of force*. Virginia: Aegis Research Corporation.

Singer, P. W. e Friedman, A. (2014). *Cybersecurity and cyberwar: what everyone needs to know*. New York: Oxford University Press.

Small Media (2015). Iranian Internet Infrastructure and Policy Report. Disponível em < http://smallmedia.org.uk/sites/default/files/u8/200215_InternetInfrastructure%20(1).pdf> Acesso em: 24 de mar. De 2023.

The Washignton Post. (2002)*Text of President Bush's 2002 State of the Union Adress*. Disponível em < https://www.washingtonpost.com/wp-srv/onpolitics/transcripts/sou012902.htm > [Acesso em: 05 de jan. 2022].

Valeriano, B. e Maness, R. C. (2015) *Cyber war versus cyber realities: cyber conflict in the international system*. New York: Oxford University Press.