ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO
ESCOLA MARECHAL CASTELLO BRANCO

AMANDA RODRIGUES BERNARDES

(IM)POSSIBILIDADES DA GUERRA CIBERNÉTICA:
ANÁLISE DO ATO DE GUERRA NAS AGRESSÕES CIBERNÉTICAS

Rio de Janeiro
2022

AMANDA RODRIGUES BERNARDES

(IM)POSSIBILIDADES DA GUERRA CIBERNÉTICA:
ANÁLISE DO ATO DE GUERRA NAS AGRESSÕES CIBERNÉTICAS

Texto apresentado como Dissertação de Mestrado do Programa de Pós-Graduação em Ciências Militares do Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, como requisito para a obtenção do título de Mestre em Ciências Militares

Orientador: Prof. Dr. Luiz Rogério Franco Goldoni

RIO DE JANEIRO

2022

B522i Bernardes, Amanda Rodrigues.

(Im)possibilidades da guerra cibernética: análise do ato de guerra nas agressões cibernéticas**.** / Amanda Rodrigues Bernardes. ─2022.
106 f.; 30 cm.

Orientação: Luiz Rogério Franco Goldoni**.**
Dissertação (Mestrado em Ciências Militares)─Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2022.
Bibliografia: f. 95-105.

1. GUERRA. 2. ESPAÇO CIBERNÉTICO 3. GUERRA CIBERNÉTICA. 4. ATO DE GUERRA. I. Título.

CDD 364.325

AMANDA RODRIGUES BERNARDES

"(IM)POSSIBILIDADES DA GUERRA CIBERNÉTICA

Dissertação apresentada à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Mestre em Ciências Militares.

Aprovada em 12 de abril de 2022.

BANCA EXAMINADORA

LUIZ ROGÉRIO FRANCO GOLDONI – Prof Dr – Presidente
Escola de Comando e Estado-Maior do Exército - ECEME

RUBENS DE SIQUEIRA DUARTE – Prof Dr – Membro
Escola de Comando e Estado-Maior do Exército - ECEME

Documento assinado digitalmente
Danielle Jacon Ayres Pinto
Data: 13/04/2022 16:39:52 -0300
CPF: 391.367.488-70
Verifique as assinaturas em https://verificador.iti.br

DANIELLE JACON AYRES PINTO – Profª Drª – Membro
Universidade Federal de Santa Catarina – UFSC

Ciente

AMANDA RODRIGUES BERNARDES – Postulante
Escola de Comando e Estado-Maior do Exército

Dedico o trabalho à minha mãe, Claudina, e ao meu marido, Leonardo.

AGRADECIMENTOS

A Deus e aos meus guias espirituais, por terem me ajudado a ultrapassar todos os obstáculos encontrados ao longo do curso.

À minha mãe, Claudina, e ao meu padrasto, Evaldo, que acreditaram em mim, me deram a esperança para seguir em frente apesar das dificuldades, a segurança e certeza de que não estou sozinha nesta caminhada.

Ao meu marido, Leonardo, que ao longo desses meses me deu não só força, mas apoio para vencer essa etapa da vida acadêmica. Obrigada, meu amor, por suportar as crises de estresse.

Ao professor Luiz Rogério Franco Goldoni, por ter sido meu orientador e ter desempenhado tal função com enorme dedicação e paciência. A construção dessa dissertação só foi possível ocorrer perante os seus inúmeros conselhos e correções.

À minha querida amiga Monique, que sempre esteve ao meu lado, pela amizade incondicional e pelo apoio demonstrado ao longo de todo período em que me dediquei a este trabalho.

À minha extraordinária banca de avaliação, composta pelo professor Dr. Rubens de Siqueira Duarte e pela professora Dra. Danielle Jacon Ayres Pinto, pelas correções e ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação profissional ao longo do curso.

À professora Dra. Mariana Carpes, pela atenção especial e pelas orientações no que se refere a parte metodológica da tese em questão.

À Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro-FAPERJ, pela bolsa de estudos e auxílio financeiro que possibilitou a dedicação integral ao programa de pós-graduação e a operacionalização do estudo.

Por fim, agradeço à Escola de Comando e Estado-Maior do Exército e ao corpo docente e técnico-administrativo do Instituto Meira Mattos, essenciais no meu processo de formação profissional, pela dedicação, e por tudo o que aprendi ao longo desses dois anos do curso.

"*The human spirit must prevail over technology*."

Albert Einstein, 1951

RESUMO

O objetivo geral da pesquisa é explorar o que caracterizaria uma agressão cibernética como "ato de guerra" e os elementos que até o momento impossibilitaram esta caracterização. A dissertação possui o seguinte problema de pesquisa: por que, até hoje, nenhuma agressão cibernética foi considerada um ato de guerra? Em 2012, Thomas Rid afirmou que a guerra cibernética nunca ocorrerá, pois em sua visão, um ataque cibernético poderá ser classificado apenas como um ato de subversão, espionagem ou sabotagem e não ato de guerra. Destarte, a dissertação tem como hipótese que os eventos cibernéticos não foram amplamente considerados atos de guerra por outras questões, que são: as imprecisões relacionadas à configuração dos elementos essenciais de materialidade e atribuição dos ataques, à legislação internacional e à vontade política. Sendo assim, é pretendido nesse trabalho compreender o conceito de guerra, ciberespaço e guerra cibernética; estudar as questões que dificultam atribuir o "ato de guerra" nos ataques cibernéticos; e como forma de averiguação da hipótese, serão investigados três casos de eventos cibernéticos que apesar de apresentarem indícios e elementos que poderiam caracterizá-los como "atos de guerra", não foram. A metodologia utilizada parte de uma abordagem qualitativa e consiste em uma pesquisa exploratória pelo método hipotético-dedutivo. São exploradas fontes primárias e secundárias, como artigos científicos, reportagens jornalísticas e documentos oficiais da ONU e da OTAN.

Palavras-chave: Guerra. Espaço Cibernético. Guerra Cibernética. Ato de Guerra.

ABSTRACT

The general objective of the research is to explore what characterizes a cyber attack as an “act of war” and the elements that have so far made this characterization impossible. The dissertation has the following research problem: why, until today, no cyber offense has been considered an act of war? In 2012, Thomas Rid never confirmed an attack in his vision, a cyber attack would just be a war like the version, espionage or sabotage and not war. Thus, the war as a hypothesis that the cybernetic concepts considered for other questions were not considered, which are: as implicit questions related to the essential elements of materiality, there is a presentation of the political elements and the international configuration of the attacks, the legislation and the international will. Therefore, it is intended in this work to understand the concept of cyber warfare and cyber warfare; study the issues that make it difficult to sign the “act of war” in cyber attacks; and as a way of verifying the hypothesis, cybernetic studies will be investigated which, despite presenting examples and elements that could be characterized as “acts of war”, were not. The methodology used starts from a qualitative approach and consists of a hypothetical-deductive research method. Primary sources and secondary documents are explored, such as scientific articles, journalistic and official reports from the UN and NATO.

Keywords: War. Cyber Space. Cyberwar. Act of War.

LISTA DE ABREVIATURAS E SIGLAS

AIEA – Agência Internacional de Energia Atômica

CCDCOE - Cooperative Cyber Defence Centre of Excellence

CENTCOM - The United States Central Command

DDoS - Distributed Denial of Service

FGV - Fundação Getulio Vargas

IP – Internet Protocol

ISIS - Islamic State of Iraq and Syria

IRGC - Islamic Revolutionary Guard Corps

NASA - National Aeronautics and Space Administration

ONGs - Organizações não Governamentais

ONU - Organização das Nações Unidas

OTAN - Organização do Tratado do Atlântico Norte

RBN - Russian Business Network

SCADA - Supervisory Control And Data Acquisition

USB - Universal Serial Bus

SUMÁRIO

1 INTRODUÇÃO.....11

2 BREVES DISCUSSÕES DA GUERRA.....19

2.1 O QUE É GUERRA.....19

2.2 ATO DE GUERRA: PARTICULARIDADES QUE O CONFIGURAM.....22

2.3 O CIBERESPAÇO E OS DESAFIOS DO NOVO DOMÍNIO.....26

2.4 GUERRA CIBERNÉTICA.....33

3 ELEMENTOS QUE DIFICULTAM CONSIDERAR OS EVENTOS CIBERNÉTICOS COMO ATOS DE GUERRA.....40

3.1 OS ATAQUES CIBERNÉTICOS APENAS COMO ATOS DE SUBVERSÃO, DE ESPIONAGEM E DE SABOTAGEM.....40

3.2 A IMPRECISÃO DE AUTORIA NOS CIBERATAQUES.....44

3.3 A MATERIALIDADE DOS ATAQUES CIBERNÉTICOS.....48

3.4 A CARÊNCIA DE DEFINIÇÃO LEGAL AOS CONFLITOS CIBERNÉTICOS.....51

3.5 A AUSÊNCIA DE VONTADE POLÍTICA EM CLASSIFICAR AS AGRESSÕES CIBERNÉTICAS COMO ATOS DE GUERRA.....56

4 ANÁLISE DE EVENTOS CIBERNÉTICOS.....61

4.1 CONFLITOS CIBERNÉTICOS EM QUE A RÚSSIA FOI ACUSADA INFORMALMENTE DE SER A AUTORA DO ATO.....61

4.1.1 Estônia – 2007.....62

4.1.2 Geórgia – 2008.....66

4.1.3 Ucrânia – 2014/2015.....70

4.2 O CASO STUXNET.....75

4.3 AGRESSÃO CIBERNÉTICA À INFRAESTRUTURA CRÍTICA DO IRÃ REALIZADA PELOS ESTAOS UNIDOS.....82

5 CONSIDERAÇÕES FINAIS.....87

REFERÊNCIAS.....95

1 INTRODUÇÃO

Divergências de definição acerca da guerra cibernética dificultam atribuir o ato de guerra em um ataque cibernético (FERNANDES, 2012, p. 55). Diante desse cenário, o presente trabalho parte do seguinte problema de pesquisa: por que, até hoje, nenhum ataque cibernético foi considerado um ato de guerra? De acordo com Rid (2012), um ataque cibernético poderá ser classificado apenas como um ato de subversão, de espionagem ou de sabotagem e não ato de guerra. Apesar do entendimento de Rid (2012), o presente trabalho parte da hipótese de que os eventos cibernéticos não foram amplamente considerados atos de guerra por conta das imprecisões relacionadas à configuração dos elementos essenciais de materialidade, atribuição dos ataques, à legislação internacional e à vontade política.

A dissertação tem como objetivo geral: explorar o que caracterizaria uma agressão cibernética como "ato de guerra" e os elementos que até o momento impossibilitaram esta caracterização. Para isso, serão abordados os seguintes objetivos específicos:

a- Entender e definir "Guerra cibernética";

b- Analisar os elementos que dificultam atribuir o "ato de guerra" nos ataques cibernéticos: atos de subversão, de espionagem e de sabotagem; ausência de definição legal; materialidade; imprecisão de autoria; e vontade política.

c- Investigar três casos de eventos cibernéticos que, apesar de apresentarem indícios e elementos que poderiam os caracterizar como "atos de guerra", não foram entendidos como tais: 1) os casos em que a Rússia foi acusada informalmente de ter desferido agressões cibernéticas contra os Estados da Estônia em 2007, Geórgia em 2008, e Ucrânia em 2014-2015; 2) o ataque cibernético contra a Usina Nuclear de Natanz, conhecido como Stuxnet, que ocorreu em 2009, mas só foi notado em 2010 (ZETTER, 2017); 3) a agressão cibernética à infraestrutura crítica do Irã realizado pelos Estados Unidos, na gestão do presidente Trump, em julho de 2019, que acarretou o desligamento dos computadores militares iranianos (WASHIGTON POST, 2019).

O ciberespaço é o novo campo de batalha dos conflitos contemporâneos (CLARKE; KNAKE, 2015) e os ataques cibernéticos aumentam a cada dia (INTERPOL, 2020; NYT, 2021). Só no primeiro trimestre de 2021, ocorreram mais de 3,4 bilhões de tentativas de ataques cibernéticos no Brasil (FORTINET, 2021). As agressões no ciberespaço são desferidas tanto por atores estatais quanto não estatais. Em maio de 2021,

o grupo russo DarkSide paralisou as atividades da norte-americana Colonial Pipeline. O incidente cibernético afetou 45% do abastecimento de combustível na costa leste dos Estados Unidos (BBC, 2021). Apesar da crescente ocorrência de operações cibernéticas no ciberespaço, até hoje, nenhuma foi considerada um ato de guerra.

Diante do crescimento dos ataques cibernéticos, da carência de pesquisadores e especialistas na área, é importante estudar os elementos que implicam a atribuição do ato de guerra nesses ciberataques e, dessa forma, contribuir para as áreas das Ciências Militares e da Segurança e Defesa Cibernética, campos que estão em constantes transformações.

Embora nenhum ataque cibernético tenha sido oficialmente considerado um ato de guerra por algum Estado, especialistas e cientistas da área de Segurança e Defesa Cibernética debatem a respeito da guerra cibernética e dos conceitos e definições acerca da temática (AYRES; GRASSI, 2020). No decorrer desta pesquisa, um levantamento na biblioteca digital da Fundação Getúlio Vargas-FGV[1] sobre as definições: "*cyber war*" e "*act of war*", encontrou 143 obras revisadas por pares. Observa-se a falta de consenso entre os especialistas.

Em 1989, Lind realizou considerações sobre as possibilidades de conflitos no ciberespaço; quatro anos mais tarde, John Arquilla e David Rofendelt escreveram acerca desse novo domínio operacional. Esses autores são considerados os pioneiros no assunto (KENKEL; LOBATO, 2015). Assim como Nye (2010; 2011), que analisou o ciberespaço sob um novo tipo de poder, o poder cibernético, agora existe mais um campo de soberania o qual as forças militares terão que assegurar aos seus países, fato que demanda novas estratégias e financiamentos. Outros especialistas em conflitos cibernéticos sob a perspectiva de guerra também terão suas obras estudadas nesta dissertação, como Libicki (2009), Cavelty (2010), Ventre (2011), Nielsen (2012), Singer e Friedman (2014), Fitton (2016), Wirtz (2017) e Mazarr (2015). Assim, será possível analisar as implicâncias em atribuir o ato de guerra nos ataques cibernéticos.

Diferentemente da guerra tradicional, na qual os beligerantes são formados pelas forças armadas dos Estados, na guerra cibernética nem sempre a autoria de um ataque cibernético será de um Estado ou ente armado regular. De acordo com Visacro (2009), a guerra irregular é "uma forma de beligerância que transcende os estreitos limites do campo militar, destaca-se a atuação de forças predominantemente nativas e faz-se

[1] Optou-se por esta biblioteca digital por ela oferecer acesso a bases e conteúdos não contemplados pelo Portal de Periódicos da CAPES.

referência à guerra de guerrilhas, à subversão, à sabotagem e ao terrorismo" (VISACRO, 2009, p. 265).

Além da natureza da guerra, outros elementos devem ser considerados na caracterização da guerra cibernética. Rid (2012) não acredita que a guerra cibernética acontecerá. O autor argumenta que os ataques cibernéticos podem ser caracterizados apenas como atos de subversão, de espionagem e de sabotagem, mas não como atos de guerra. Para justificar seu ponto de vista, Rid (2012) faz uma comparação dos ataques cibernéticos com o conceito de guerra tradicional descrito por Clausewitz (1984), ou seja, o ato de guerra deve ser subordinado à política, ter caráter instrumental e ser violento, o que para Rid (2012) enseja ocorrer letalidade. Em resposta ao artigo de Rid (2012), Stone (2013), também mediante interpretação dos conceitos de guerra de Clausewitz (1984), afirma que a guerra cibernética acontecerá, pois, um ato de violência não precisa ser letal para se configurar um ato de guerra. O debate entre os autores será expandido no decorrer do trabalho.

Para analisar um ciberataque como ato de guerra, não apenas as premissas de Rid (2012) e Stone (2013) devem ser consideradas, mas também outros quatro elementos, dentre eles a falta de definição legal da guerra cibernética pelas instituições de Segurança Internacional. Conforme descrevem Libicki (2009), Ayres e Grassi (2020), Dipert (2010) e Fernandes (2012), existe a necessidade das Nações Unidas e da OTAN regulamentarem as ações cibernéticas atentadas entre Estados ou por um Estado contra um ator não-estatal como possíveis atos de guerra. A ausência de regulamentação legal dificulta a compreensão sobre a forma na qual os Estados devem responder aos ataques cibernéticos e se esses devem ou podem ser classificados como atos de guerra.

A título de exemplo acerca da ausência de normas pelas instituições internacionais, Libicki (2009) apresenta hipóteses de ciberataques que poderiam se configurar atos de guerra, dentre elas um ataque cibernético a uma usina nuclear. Ainda que o caso especulado pelo autor tenha sido apenas um exemplo, em 2009, a Usina Nuclear de Natanz, no Irã, sofreu sucessivos ataques cibernéticos por meio de um vírus que causou a destruição do seu sistema de centrífugas e assim atrasou o programa nuclear do país por anos (ZETTER, 2017). O caso em questão foi descoberto apenas em 2010, ficou conhecido como Stuxnet, e não foi considerado um ato de guerra. Além da imprecisão de autoria, talvez tenha faltado respaldo na legislação internacional. Esse evento será analisado no capítulo três.

O segundo elemento de debate na questão “agressões cibernéticas” e “atos de guerra” é a materialidade. Para Teixeira Júnior, Vilar-Lopes e Freitas (2017) a materialidade de um evento cibernético pode causar a desestabilização no sistema de computadores dos inimigos ou gerar o vazamento de dados, mas não necessariamente ocasionar resultados similares a um conflito físico, o que pode dificultar a caracterização do ato de guerra no ciberataque. A materialização da guerra cibernética é um campo nebuloso (SINGER; FRIEDMAN, 2014), pois seus efeitos nem sempre são imediatos, não há “fumaça”, como acontece em um conflito bélico e nem há garantia de êxito, às vezes as consequências são silenciosas e tardam a aparecer.

O evento WannaCry[2], que ocorreu em 2017, quando cibercriminosos desenvolveram um software malicioso, um *ransomware*[3], que infectou mais de 230 mil computadores Windows em torno de 150 países, provocou diversas consequências, como a invasão do ciberespaço dos Estados, o bloqueio de arquivos importantes e prejuízo econômico para pessoas, empresas e órgãos públicos que tiveram seus sistemas corrompidos (NYT, 2017; REUTERS, 2017). Por mais que o ataque cibernético tenha causado danos, esses não ocorreram por meio de confrontos físicos e não houve consequências cinéticas, tampouco letalidade (pelo menos atribuídas diretamente ao ataque), como geralmente aconteceria em uma guerra tradicional.

No que se refere à imprecisão de autoria, Medeiros e Goldoni (2020) abordam que no ciberespaço há uma multiplicidade de atores difíceis de serem identificados, pois “considerando a natureza complexa do emaranhado de interconexões e camadas semânticas e sintáticas do ciberespaço, é difícil rastrear um determinado resultado de volta a uma ação causativa específica”[4] (MEDEIROS; GOLDONI, 2020, p.44, tradução própria). Para Dipert (2010) e Ayres e Grassi (2020), essa imprecisão na identificação do autor compromete atribuir o ato de guerra nas incursões cibernéticas. Esse ponto também é compartilhado pelo especialista em Segurança Computacional da ONU, Bruce Schneier, que afirmou: “infelizmente, quando você está sendo atacado no ciberespaço, as duas coisas que você geralmente não sabe são quem está atacando você e por quê. [...] Isso

[2] Na época foi especulado que o atentado foi efetuado por um grupo da Coreia do Norte, o Lazarus Group, o que não foi confirmado (NYT, 2017; REUTERS, 2017).

[3] *Ransomware* é um ataque digital que tem como objetivo danificar os sistemas internos de uma máquina virtual. Nessa ação, os dados armazenados em um computador são infectados e criptografados, e assim, impede que o usuário original tenha acesso aos seus dados. Para poder liberar os dados, normalmente os criminosos exigem um resgate, ou, em inglês, *ransom*.

[4] [Tradução própria]. No original, lê-se: “considering the complex nature of the tangle of interconnections and semantic and syntactic layers of cyberspace, it is difficult to trace a given outcome back to a specific causative action.”

torna a defesa e a política nacional de Defesa Cibernética difíceis" [5] (SHENEIER, 2013, p. 13, tradução própria).

Nos ataques cibernéticos contra a Estônia, em 2007, os sites do governo ficaram fora do ar durante horas e os serviços que dependiam do espaço cibernético foram interrompidos (NYT, 2007; DIPERT, 2010). Em vista do histórico[6] e de fortes indícios, os governantes da Estônia acusaram a Rússia de ser a mandante dos ataques, fato veemente negado por Moscou (DIPERT, 2010; LIBICKI, 2009). Ou seja, mesmo que o atentado tenha se originado na Rússia, não foi possível comprovar que o governo foi o responsável pelo conflito cibernético (NYT, 2007). O caso também envolveu a ausência de materialidade física, pois os sistemas "só" ficaram fora do ar, ou seja, não houve uma "explosão", agressão física ou morte; a falta de definição legal pelas instituições internacionais também limitou as respostas de Talin. O caso será explorado no capítulo três do trabalho.

A última característica a ser analisada é a ausência de vontade política em declarar um evento cibernético como ato de guerra. Para que haja um ato de guerra é necessário que o conflito seja subordinado à política (CLAUSEWITZ, 1984; MEI, 2018; SINGER; FRIEDMAN, 2014). Dessa forma, Singer e Friedman (2014) compreendem que caso um Estado declare guerra perante uma ação cibernética, assim será considerado. Libicki (2009) compartilha do mesmo pensamento de Singer e Friedman (2014): a decisão de declarar guerra é do líder político do Estado.

Os especialistas em guerra cibernética, como Ayres e Grassi (2020); Gomes e Alves (2020) acreditam que não há interesse dos Estados em normatizar e nem de declarar guerra no que diz respeito às agressões cibernéticas. A ausência de leis internacionais permite que os Estados ajam sem que de fato se tenha um conflito armado e sem serem punidos (AYRES; GRASSI, 2020; GOMES; ALVES, 2020). A declaração de guerra enseja uma série de consequências ao Estado causador, como prejuízos econômicos, rompimentos de acordos e tratados e a aplicação de medidas restritivas de direito pelas instituições de segurança internacional, como a ONU e a OTAN (DINSTEIN, 2003).

---

[5] [Tradução própria]. No original, lê-se: "Unfortunately, it is very difficult to identify attackers and their motivations in cyberspace. A result, nations are classifying all serious cyberattacks as cyberwar. This perturbs national policy and fuels a cyberwar arms race, resulting in more instability and less security for everyone. We need to dampen our cyberwar rhetoric, even as we adopt stronger law enforcement policies towards cybersecurity, and work to demilitarize cyberspace."

[6] Suposta resposta à retirada de uma estátua que homenageava os soldados russos de Tallinn para outra localidade, comunicação e códigos das ofensas escritos em russo.

Metodologia

A presente pesquisa visa compreender o que é uma agressão cibernética e quais são as implicâncias que dificultam caracterizá-la como um ato de guerra. O estudo será realizado por meio de uma revisão de textos acadêmicos sobre o novo campo de batalha que é o ciberespaço. Nesse sentido, o presente trabalho se situa, principalmente, no campo teórico. Eis que o trabalho seguirá a metodologia qualitativa e exploratória. A pesquisa qualitativa tenta compreender e interpretar um fenômeno (POLIT et al, 2004), que, nesse caso, será analisar e dispor de uma forma polida e organizada os motivos pelos quais os eventos cibernéticos não foram, até o momento, considerados atos de guerra. O método exploratório tem como base analisar assuntos com pouco ou nenhum estudo anterior a seu respeito (GERHARDT; SILVEIRA, 2009), assim como é o ciberespaço, um novo domínio operacional que está em constante transformação.

Além dos métodos citados acima, o trabalho será organizado no sistema hipotético-dedutivo, pois o campo geral a ser estudado, que são as agressões cibernéticas, constroem uma parte de um postulado, que, no caso da dissertação, é o ato de guerra inserido nos conflitos cibernéticos. De acordo com Quivy e Campenhoudt (2005, p. 150), esse formato de dedução gera "os indicadores para os quais será necessário buscar correspondentes no real".

Para testar o falseamento da hipótese nas considerações finais do trabalho, será analisado os elementos destacados na hipótese, que são a materialidade, a imprecisão de autoria, a falta de definição legal e a ausência de vontade política nos seguintes estudos de caso: os eventos cibernéticos em que a Rússia foi acusada informalmente de ter desferido agressões cibernéticas contra Estados - Estônia em 2007, Geórgia em 2008 e Ucrânia em 2014-2015; o ataque cibernético contra a Usina Nuclear de Natanz, o Stuxnet (2009-2010) (ZETTER, 2017); e a agressão cibernética à infraestrutura crítica do Irã, que foi realizado pelo governo Trump, em julho de 2019, e que teve como resultado o desligamento dos computadores militares iranianos (WASHIGTON POST, 2019). Desse modo, poderá ser verificado que essas quatro premissas são questões determinantes para não atribuir o ato de guerra na guerra cibernética.

Sendo assim, para compreender o ato de guerra nos conflitos cibernéticos, deverá ser analisado primeiro o que é a guerra cibernética. Nesse momento, será exposto o conceito de guerra, por Wright, Mei, Teixeira da Silva, Dinstein, Clausewitz e pelas normas internacionais da ONU e da OTAN. As normas da Organização das Nações

Unidas possuem caráter mundial e uma de suas finalidades é promover a cooperação internacional perante os conflitos internacionais (ONU, 1945). Já a Organização do Tratado do Atlântico Norte, apesar de possuir um sistema de defesa coletiva apenas entres seus membros, possui grande influência em decisões político-econômicas em nível mundial (OTAN, 1949; SINGER; FRIEDMAN, 2014, FITTON, 2016). Ao que se refere à guerra cibernética, a Aliança Militar foi a primeira instituição de segurança internacional a investigar um conflito cibernético no âmbito de guerra, que foi na Estônia (2007), além de ser a primeira organização internacional a considerar o espaço cibernético como um novo domínio operacional de guerra (OTAN, 2016; SINGER; FRIEDMAN, 2014, FITTON, 2016).

Em seguida, serão analisados os diversos conceitos do ciberespaço e quais são as camadas desse novo domínio operacional pelos seguintes autores: Nye, Libicki, Nielsen, Ventre, Singer e Friedman, Medeiros e Goldoni. Em conseguinte, será abordado o conceito da guerra cibernética, que será iniciado pelas previsões de Lind e pela definição de guerra irregular de Visacro, Dinstein e Heydte. A seguir, as obras dos autores contemporâneos, Arquilla, Rofendelt, Cavelty, Libicki, Ventre, Singer e Friedman encerrarão a discussão.

No segundo momento da pesquisa serão identificados e explorados os elementos que dificultam atribuir o ato de guerra nas agressões cibernéticas, estudo que se iniciará com o debate entre Thomas Rid e John Stone à luz da Teoria de Guerra de Clausewitz acerca dos conflitos cibernéticos. Em conseguinte, as obras de: Lobato, Kenkel, Grassi, Ayres, Libicki, Stevens, Gomes, Alves, Mazarr, Dipert, Medeiros, Olson, Fernandes, Nye, Banks, Blank, Singer, Friedman, Wirtz, Fitton, Tabansky, Buchanan e Zetter far-se-ão parte do escopo. Ao final, como será necessário compreender as definições legais da guerra cibernética, fontes primárias, como as leis, normas e tratados internacionais, serão explorados. Como forma de averiguação das dificuldades apontadas no segundo capítulo para atribuir o ato de guerra nos ataques cibernéticos, serão realizadas três análises de casos concretos, pois "um único estudo não pode abordar todos os aspectos interessantes de um evento histórico"[7]. (GEORGE et al, 2005, p. 95, tradução própria).

Portanto, a pesquisa será composta por três capítulos. No primeiro será abordado o conceito das agressões cibernéticas; essa lente teórica a respeito das agressões cibernéticas será utilizada para analisar os demais capítulos. O segundo capítulo

[7] [Tradução própria]. No original, lê-se: A single study cannot address all the interesting aspects of a historical event.

investigará os elementos que dificultam a atribuição do ato de guerra nos ataques cibernéticos elencados na hipótese. No terceiro capítulo realizar-se-á as análises dos casos citados de ataques cibernéticos. Por fim, as considerações finais encerram a dissertação.

2 BREVES DISCUSSÕES DA GUERRA

O presente capítulo tem como objetivo compreender o ato de guerra nas agressões cibernéticas. A guerra cibernética é uma zona cinzenta (CLARKE; KNAKE, 2015). Não há definição acerca do ato de guerra nas incursões cibernéticas, o que gera uma preocupação dos Estados perante suas seguranças internas e externas (AYRES; GRASSI, 2020; FITTON, 2016). Antes de abordar a temática específica, que é a guerra cibernética, será explorado o conceito de guerra, do ato de guerra e do ciberespaço. Assim o leitor irá compreender o que é um ato de guerra e as características desse novo domínio operacional, considerado o campo de batalha do século XXI (CLARKE; KNAKE, 2015).

2.1 O QUE É GUERRA

As definições de guerra são abrangentes. A atemporal Teoria de Guerra de Clausewitz (1780-1831) pode ser utilizada, inclusive, no que se refere à guerra cibernética (AYRES; GRASSI, 2020; RID, 2012; STONE, 2013). Conforme Clausewitz (1984), a guerra é um duelo entre Estados, "um verdadeiro instrumento político, a continuação do conflito político, levado adiante com outros meios"[8] (CLAUSEWITZ, 1984, p. 91, tradução própria). Sua teoria segue duas vertentes de guerra: a Limitada – que tem objetivos restringidos, seu nível de violência e hostilidade são palpáveis, ou seja, não chega a desenvolver uma interação extrema entre os beligerantes; e a Absoluta – que causa a destruição por completo, gera o aniquilamento total do oponente e atinge a sua verdadeira perfeição quando não há limites ao uso da violência (CLAUSEWITZ, 1984). De todo modo, as duas vertentes contêm violência, mas a sua proporcionalidade se distingue. Para o estrategista militar, a guerra é um confronto em grande escala e o objetivo de cada parte consiste em compelir a obediência do oponente por meio de um ato de força.

[8][Tradução própria]. No original, lê-se: "a real political instrument, the continuation of political conflict, carried out by other means".

O ato de força para Clausewitz (1984) possui três tendências. A primeira é a violência: uma agressão de guerra tem que ser violenta, ter rancor, hostilidade e o anseio de que o inimigo seja morto. A segunda tendência é o acaso, ou seja, no combate o soldado tem que trabalhar com a imprevisibilidade. Por fim, a terceira premissa é de que a guerra sempre é instrumental, é o elemento de subordinação, o propósito da guerra. Em um conflito entre Estados, a guerra está subordinada ao governo e à política. As três tendências são sequencialmente conectadas com o Povo, o Exército e o Governo (CLAUSEWITZ, 1984).

Ao observar o conceito de guerra de Clausewitz fica evidente a ênfase que o autor dá a existência da violência nos combates; há que se considerar que o termo "violência" possui variações em sua definição. De acordo com Galtung (1969), existem três formas de violência: (1) a direta, que é todo e qualquer ato que tenha como objetivo causar dano a alguém ou alguma coisa; (2) a estrutural, que é um tipo de violência indireta em que não há apenas um ator identificável que cause essa forma de violência, éuma forma de violência em que alguma estrutura social ou instituição social pode prejudicar as pessoas, impedindo-as de atender as suas necessidades básicas. Não há um único agente responsável concreto que possa ser responsabilizado pelas consequências, mesmo que o resultado gere mortes ou sofrimento físico e psicológico; (3) a cultural, que é considerada mais sutil, indireta e duradoura através do tempo. Essa violência se embasa em diferenças culturais, étnicas e de gênero e pode se manifestar por intermédio da arte, religião, ideologia, linguagens e ciência.

Ao analisar os conceitos de violência, entende-se que para Clausewitz (1984), nas batalhas a violência aplicada é a direta. No entanto, a violência estrutural e a cultural também podem estar presentes em uma guerra. Não há uma classificação de violência estabelecida pelas instituições de segurança internacional, a violência é a ausência de paz, isso é, caso um intentado ameace a paz mundial ou a soberania de um Estado, poderá ser considerado violento o bastante para ser um ato de guerra (GALTUNG, 1969, ONU, 1945; SINGER; FRIEDMAN, 2014).

Outros autores também pontuam em suas definições de guerra o uso de violência como essencial. Mei (2018) define a guerra pelo mesmo aspecto de Clausewitz; a guerra "é um confronto violento entre grupos politicamente organizados" (MEI, 2018, p. 542). Além disso, Mei (2018) argumenta a respeito do fator social para que haja guerra. O autor salienta que, apesar dos confrontos envolverem as forças militares e as normas jurídicas,

a guerra abarca a vida em sociedade, é uma atividade humana, ou seja, é um fenômeno social.

Assim como Mei, Wright (1988) retrata a violência como característica imprescindível nas batalhas. Ele classificou a guerra como "um contato violento de entidades distintas, mas semelhantes" (WRIGHT, 1988 p. 3). Essa definição é ampla e, de acordo com o autor, foi utilizada como forma de discussão entre juristas, diplomatas e militares. Assim como Clausewitz e Mei, Wright (1988) define a guerra a partir da criação dos Estados. Dentro dessa abrangente acepção acerca dos conflitos, o autor elenca quatro formas de apresentação da guerra: a) por atividades militares; b) pela alta tensão entre os beligerantes; c) pela presença de direito de exceção no Estado; e d) pela ocorrência de integração política intensa presente internamente no país. O autor conclui que "a guerra pode ser considerada como um conflito simultâneo de forças armadas, sentimentos populares, reivindicações jurídicas e culturais que chegam a extremos de intensificação em cada aspecto" (WRIGHT, 1988, p. 14).

Dinstein (2003) conceitua duas formas de confronto, a técnica e a material. Na forma técnica, o combate "começa com uma declaração de guerra e termina com um tratado de paz ou alguma outra etapa formal indicando que a guerra acabou"[9] (DINSTEIN, 2003, p. 9, tradução própria) e, na forma material, a guerra "(...) se desenvolve independente de quaisquer etapas formais. Sua ocorrência depende apenas do surgimento de hostilidades entre as partes, mesmo na ausência de uma declaração de guerra"[10] (DINSTEIN, 2003, p. 9, tradução própria).

Diferente do posicionamento de Mei e Wright, Dinstein (2003) aponta que nem sempre haverá um ato físico em uma guerra. Para elucidar o seu ponto de vista, Dinstein (2003) exemplifica o caso em que a Alemanha, tanto na Primeira quanto na Segunda Guerra Mundial, não trocou um "tiro" sequer com vários Estados Aliados, especialmente os países da América Latina e, ainda assim, a guerra se estabeleceu, pois o país alemão havia declarado formalmente guerra – sentido técnico – aos Estados. Nesse ato de formalidade não houve confronto direto, porém, os Estados entraram na configuração de "Estado de Guerra". No sentido material, a guerra inicia-se perante os atos de violência, nessa forma, as ações se sobressaem a frente das declarações. Diante dessas duas

[9] [Tradução própria]. No original, lê-se: "it starts with a declaration of war and ends with a peace treaty or some other formal stage indicating that the war is over".
[10] [Tradução própria]. No original, lê-se: "(...) develops independently of any formal stages. Its occurrence depends only on the emergence of hostilities between the parties, even in the absence of a declaration of war".

possibilidades de combate, Dinstein (2003) determina que a guerra é "uma interação hostil entre dois ou mais Estados, seja em um sentido técnico ou material"[11] (DINSTEIN, 2003, p. 14, tradução própria).

Além da violência, uma outra questão se apresenta nos combates desde o fim da Guerra Fria (1947-1991). É a participação crescente de atores não estatais nas batalhas (SILVA, 2018; VISACRO, 2009). Nesse sentido, Teixeira da Silva (2018, p. 609) entende que diferentes configurações de guerra apresentar-se-ão, sendo elas, de ordem midiática, cibernética e econômica, como forma de "desestabilizar, mudar ou mesmo constituir governos em outros Estados-nações, paralisando e inibindo as caracterizações clássicas de guerra emanadas do direito internacional".

Teixeira da Silva (2018) determina quatro aspectos de conflito: a) o primeiro ocorre entre Estados, por meios militares ou outros; b) o segundo acontece entre um ator não estatal e um Estado, por meios ofensivos letais, tendo então um caráter interestatal; c) o terceiro é realizado na configuração interestatal, aqui vale destacar que poderá haver intervenção de terceiros estrangeiros; d) e, por último, realizar-se-á uma agressão entre atores não estatais que adotam meios ofensivos letais e são apoiados, de forma direta ou indireta, por Estados. O autor esclarece que essas particularidades ensejam um estado permanente de guerra.

Desse modo, compreende-se a guerra como um fenômeno social, pois envolve as generalidades das relações humanas, sejam elas pelo viés político, jurídico, cultural, econômico e/ou étnico. Esse fenômeno social é permeado por um confronto violento entre Estados e/ou atores não estatais. A guerra pode eclodir por uma declaração formal ou pela ocorrência de hostilidades, de atividades militares ou de ataques violentos de uma forma geral. Por demais, determina-se que, caso haja uma intimidação ou um ato de agressão violento desferido por um Estado ou por um ator não estatal que ameace/ataque um Estado, poderá se configurar uma guerra.

2.2 ATO DE GUERRA: PARTICULARIDADES QUE O CONFIGURAM

Conforme Wright (1988), quando as guerras cessam, há uma movimentação mundial que enseja a paz. Essa ação geralmente ocorre por meio de tratados, de acordos e de normas que buscam o equilíbrio de poder entre os Estados. De acordo com Fuller

[11] [Tradução própria]. No original, lê-se: "war is a hostile [violent] interaction between two or more states, whether in a technical or material sense."

(1966) e Carneiro (2006), o primeiro evento que discutiu e normatizou os confrontos adveio após a Guerra dos 30 anos (1648). No fim da guerra, centenas de negociadores da Europa se reuniram, em 1648, na Alemanha, e selaram um acordo de paz, conhecido como a Paz de Vestfália (FULLER, 1966; CARNEIRO, 2006).

A partir desse acordo, surgiu a Teoria de Guerra Justa de Hugo Grotius[12] (FULLER, 1966). De acordo com a teoria, os atos de guerra só poderiam ocorrer dentro de três parâmetros: o primeiro, em caso de defesa contra um ataque ou ameaça de ataque; o segundo, para reaver algo, ou seja, uma reparação; e, por último, para punir um ato injusto (GROTIUS, 2005). Essas três premissas são justificativas que ainda vigoram no Direito Internacional (DRAPER, 1995).

Conforme Fuller (1966), independente dessas condições, os conflitos continuaram a eclodir, sendo eles justos ou injustos. Uma série de situações transformaram o conceito de ato de guerra. Por exemplo, na Revolução Francesa (1789-1799) o ato de guerra passou a ser declarado, ou seja, caso houvesse um impasse político entre os Estados, um declarava guerra ao outro, até que fosse proposto uma negociação de paz de comum acordo (MEI, 2018). De acordo com Mei (2018, p. 546), "o conflito bélico inicia[va]-se com a declaração de guerra e encerra[va]-se com o tratado de paz".

De acordo com Dinstein (2003), a normatização do ato de guerra na forma técnica adveio da Convenção de Haia, em 1907, pelo qual foi decidido que o ato de guerra passaria a ser "um anúncio unilateral e formal, emitido pela autoridade constitucionalmente competente de um Estado, estabelecendo a hora exata em que a guerra começa com um inimigo (ou inimigos) designado"[13] (DINSTEIN, 2003, p. 29, tradução própria). O ato de declarar guerra no sentido técnico configura ao Estado a situação de "Estado de Guerra"; essa nomenclatura enseja automaticamente a interferência de leis aos beligerantes em confronto, como por exemplo, a imposição de normas de neutralidade e de criminalidade (DINSTEIN, 2003).

Um outro movimento que transformou o ato de guerra foi a Revolução Industrial (1760) (WRIGHT, 1988; KEEGAN, 2006). Wright (1988) informa que surgiram diversos avanços tecnológicos, como armas mais letais, veículos que facilitavam o transporte de

[12] Hugo Grotius (1583-1645)foi um jurista holandês considerado um dos fundadores do Direito Internacional. Era considerado também diplomata, poeta, dramaturgo e historiador. É o autor da obra "O Direito da Guerra e Paz" e desenvolveu a doutrina da guerra justa, já estabelecida por St. Agostinho.

[13] [Tradução própria]. No original, lê-se: "a unilateral and formal announcement, issued by the constitutionally competent authority of a State, establishing the exact time when war begins with a designated enemy (or enemies)".

soldados e suprimentos nas batalhas, novos meios de comunicação, como o telégrafo (1835), dentre outras inovações (WRIGHT, 1988). Esses avanços tecnológicos fizeram com que as mortes nas batalhas aumentassem progressivamente, já que as armas se tornaram mais letais (GOLDONI, 2011). A mortandade nas guerras que a sucederam foi crescente: Guerra da Secessão (1861-1865) – 600 mil mortos; Primeira Guerra Mundial (1914-1918) – 10 milhões de mortos; e Segunda Guerra Mundial (1939-1945) – 50 milhões de mortos (FULLER, 1966; KEEGAN, 2006; HART, 2009; WRIGHT, 1988).

Wright (1988) argumenta que, em uma tentativa de frear o uso desmedido da tecnologia nas batalhas e assim diminuir as mortes, os Estados vencedores da Primeira Guerra Mundial criaram a Liga das Nações (1920). Foi uma maneira encontrada pelos Estados de limitar o uso das armas de guerra e para que os países resolvessem suas diferenças por meio de um processo de arbitragem ou de uma solução judiciária (FULLER, 1966). Apesar de boas perspectivas, o estabelecido pela Liga logo foi derrubado pela eclosão da Segunda Guerra Mundial, em 1939 (FULLER, 1966).

A Segunda Guerra Mundial também transformou os conflitos. Além dos domínios operacionais de guerra já reconhecidos, o marítimo e o terrestre, surgiram o aéreo e o sideral (esse último, a partir da Guerra Fria – 1947-1991) (FULLER, 1966; KEEGAN, 2006; HART, 2009; WRIGHT, 1988). Aqui vale destacar que foi a última vez que houve a declaração formal de guerra contra um Estado, que ocorreu em dezembro de 1941, quando os Estados Unidos declararam guerra contra o Japão (1939-1945) (DINSTEIN, 2003; KEEGAN, 2006; SINGER; FRIEDMAN, 2014). No entanto, apesar de não ter havido mais declaração de guerra formal, as guerras não deixaram de ocorrer (DINSTEIN, 2003; WRIGHT, 1988).

Os confrontos que ocorreram desde então foram manifestados por meio de hostilidades – sentido material - ou pela referência do termo “conflito armado internacional” (DINSTEIN, 2003; SINGER; FRIEDMAN, 2014). Nessa performance os Estados conseguem se desviar das normas da Convenção de Haia, ou seja, evitam entrar em um “Estado de Guerra” para que não ‘sofram’ imposições normativas e nem tenham suas ações internas e externas restringidas (DINSTEIN, 2003).

Com o fim da Segunda Guerra Mundial em 1945, os governos das grandes potências[14] da época decidiram criar a Organização das Nações Unidas (ONU) (1945) e

[14] Países signatários da ONU: URSS, Reino Unido, Estados Unidos e China. Hoje as Nações Unidas são compostas por 193 Estados-membros.

a Organização do Tratado do Atlântico do Norte – OTAN (1949) (FULLER, 1966; KEEGAN, 2006; HART, 2009; WRIGHT, 1988). Conforme Keegan (2006, p. 489), a ONU "reafirmou o Pacto da Liga, acrescentando ao mecanismo de arbitragens e sanções da Liga um conjunto de provisões que permitissem à ONU usar força militar contra um transgressor". Por sua vez, a OTAN surgiu com a premissa de que os Estados-membros do tratado reafirmariam sua fé nos intuitos e princípios da Carta das Nações Unidas e desejariam viver em paz (OTAN, 1949).

Com o desígnio de preservar a paz e a Segurança Internacional, o Conselho de Segurança da ONU é o responsável por determinar "a existência de qualquer ameaça à paz, ruptura da paz ou ato de agressão, e fazer recomendações ou decidir que medidas devem ser tomadas" (Art. 40 da ONU, 1945). Seguindo a mesma linha postulada pelas Nações Unidas, que tem como objetivo perpetuar a paz, a OTAN determina que um ataque armado contra o território de algum país participante da Aliança poderá ser visto como um ato de guerra (OTAN, 1949).

Ao analisar as normas da ONU, é possível observar que não há especificidades a respeito do ato de guerra, não há uma delimitação de violência para que um ato de agressão se configure como guerra. Não há referência de classificações da guerra, como por exemplo, a guerra limitada e total de Clausewitz, ou a guerra em sentido material e técnico de Dinstein. Para a instituição, qualquer ameaça ou emprego da força armada que ocorra aos Estados e à Segurança Internacional, após ser analisada pelo seu Conselho de Segurança, poderá ser considerado um ato de guerra (ONU, 1945). Já para a OTAN (1949), há uma delimitação dos atos de agressão, pois eles se darão apenas contra os Estados participantes da aliança.

Outro ponto acerca das normas da ONU deve ser destacado: a sua criação ocorreu em 1945, a instituição estabeleceu os atos de guerra entre Estados, entretanto, "a partir da década de 1990 (...) o Estado não mais monopoliza o campo de batalha, porque surgem novos atores não estatais" (SILVA, D., 2020, p. 40). Os atores não estatais só foram reconhecidos pela ONU como possíveis agressores de guerra após o atentado terrorista às Torres Gêmeas, em 11 de setembro de 2001, orquestrado por uma organização terrorista, a Al-Qaeda. A ONU, diante de muitas divergências, permitiu a inclusão de

---

Países signatários da OTAN: Bélgica, Canadá, Dinamarca, Estados Unidos, França, Islândia, Itália, Luxemburgo, Noruega, Portugal e Reino Unido. Hoje 28 membros fazem parte da sua composição.

atores não estatais no seu escopo legislativo (VISACRO, 2009; SILVA, C., 2003; SILVA, T., 2018; SILVA, D., 2020).

Sendo assim, é possível concluir que, apesar dos tratados, dos acordos, das leis e das normas internacionais que promovem a paz, as agressões não deixarão de existir e suas manifestações surgirão nas mais variadas formas. Por exemplo, por meio de declarações formais de guerra, como cita Dinstein (2003), ou pelas atividades militares, como salienta Wright (1988) ou pela realização de atos violentos. Os atos de guerra ocorrerão por atores estatais e não estatais. Assim, constata-se que agressões que intervenham no equilíbrio de poder, na manutenção da paz e na soberania de um Estado, bem como interfira na Segurança Internacional, podem ser considerados atos de guerra (ONU, 2021; OTAN, 1949; DINSTEIN, 2003).

2.3 O CIBERESPAÇO E OS DESAFIOS DO NOVO DOMÍNIO

Neste tópico da dissertação serão expostas algumas explicações de fontes acadêmicas sobre as características que compõe o ciberespaço, como sua estrutura, seu espaço geográfico e os atores que atuam em seu espectro. Assim poderá ser compreendido como ocorrem as agressões cibernéticas nesse novo domínio operacional de guerra do século XXI (CLARKE; KNAKE, 2015).

Para Nye (2010) o ciberespaço é um domínio operacional criado pelo homem e mais volátil do que os outros domínios - terrestre, marítimo, aéreo e o espaço sideral – pois permite a ampliação da capacidade de transmissão de informação, referenciado pelo autor como a "revolução de informação". De acordo com Nye (2010), o espaço cibernético possui duas camadas nas quais ocorrem diversas atividades manuseadas por variados tipos de atores cibernéticos. A primeira camada, a física, "segue as leis econômicas de recursos rivais e crescentes custos marginais"[15] (NYE, 2010, p. 3, tradução própria), já a segunda camada, a virtual, "possui características das redes econômicas de crescentes retornos de escala e práticas políticas que fazem o controle jurisdicional difícil"[16] (NYE, 2010, p. 3, tradução própria).

Aqui vale uma ressalva aos elementos que compõe o ciberespaço, pois apesar de toda sua estrutura física e virtual, esse espectro eletromagnético é operado por atores

[15] [Tradução própria]. No original, lê-se: "follows the economic laws of rival resources and rising marginal costs".
[16] [Tradução própria]. No original, lê-se: "has characteristics of economic networks of increasing returns to scale and political practices that make jurisdictional control difficult".

(SINGER; FRIEDMAN, 2014). Os atores cibernéticos são os agentes da ação no ciberespaço, ou seja, são usuários que interagem no ambiente virtual com outros atores e podem modificar as características internas do espectro eletromagnético e externas (SILVA, J.,2014). Esse ator pode ser qualquer pessoa que tenha acesso a uma rede de conexão, como um civil, um *hacker*, um criminoso, um militar, o governo ou ainda grupos ativistas e políticos, até mesmo de agentes públicos e privados, "todos eles realizam interações dentro do espaço cibernético utilizando serviços, trocando informações, comunicando-se, movimentando a economia, desenvolvendo serviços/facilidades, cometendo crimes e fazendo a guerra" (SILVA, J.,2014, p. 201).

Conforme a tecnologia avança, os atores cibernéticos se multiplicam, pois há um "aumento do acesso, da humanidade, às facilidades da computação (SILVA, J.,2014 p.202). Por esse aspecto, Nye (2010) atribui ao ciberespaço a condição de "poder cibernético". O autor define que o Poder Cibernético é "um conjunto de recursos que se relacionam à criação, ao controle e à comunicação de informações eletrônicas e baseadas em computador – infraestrutura, redes, softwares, habilidades humanas"[17] (NYE, 2010, p. 123, tradução própria), não apenas isso, "mas também intranets, tecnologias de telefonia celular e comunicações via satélite"[18] (NYE, 2010, p. 123, tradução própria). O poder cibernético abarca dois aspectos de poder: o *hard power* (poder duro), que é a realização de atividades tangíveis, como por exemplo, uma agressão cibernética que resulte consequências físicas; e o *soft power* (poder brando), que é a execução de ações cibernéticas intangíveis, como por exemplo, a transmissão de informações manipuladas.

Nye (2011) salienta, ainda, que há uma difusão de poder quando se refere ao Poder Cibernético, já que há uma descentralização em relação ao Estado, pois o custo para atuar no ciberespaço é relativamente baixo, o instrumento de guerra nesse caso não é uma arma militar de acesso exclusivo das forças armadas de um Estado, "qualquer" pessoa pode acessar um computador e ser um usuário no ciberespaço, desde o Estado até mesmo um adolescente. Sendo assim, um computador, um celular ou um outro aparelho digital pode se tornar uma arma de combate. Isso propicia um fluxo alto de variados usuários - atores estatais e não estatais - e implica o controle que o Estado tem sobre as ações cibernéticas. O autor conclui que a difusão de poder que rodeia o espaço cibernético o torna uma arena

[17] [Tradução própria]. No original, lê-se: "A set of resources that relate to the creation, control and communication of electronic and computer-based information - infrastructure, networks, software, human skills".
[18] [Tradução própria]. No original, lê-se: "but also intranets, cell phone technologies and satellite communications".

de guerra onde ocorrem diferentes níveis de eventos cibernéticos, os quais nem sempre serão identificados pelo Estado, desde um ato de desinformação até mesmo um ataque cibernético à uma infraestrutura crítica de um Estado (NYE, 2011).

Libicki (2009) conceitua o ciberespaço como um ambiente similar, em alguns aspectos, aos outros domínios operacionais, como o mar e a terra, já que é um ambiente propício a conflitos e demais interações realizadas pelos atores que o compõe, entretanto, diferente dos outros campos, que surgiram de forma orgânica, o espaço cibernético foi criado pelo homem e, por esse quesito, deve ser analisado por uma lente própria. O autor define o ciberespaço como "um meio virtual, muito menos tangível do que o solo, a água, o ar ou mesmo o espaço"[19] (LIBICKI, 2009, p. 12, tradução própria). Contudo, assim como Nye, Libicki (2009) argumenta que as ações cibernéticas podem resultar em consequências tangíveis, como ocorre nos demais domínios operacionais.

Libicki (2009) define o espaço cibernético pela sua estruturação. O autor o dispõe por camadas nas quais uma se sobrepõe à outra: primeiro a física, depois a sintática e, por último, a semântica. A camada física é composta por toda a estrutura palpável que constitui o ciberespaço, como os computadores, fios, cabos submarinos e satélites, é a composição da rede de computadores que permite a existência do espaço cibernético. O nível sintático é a operabilidade da rede de computadores, ou seja, são as instruções que deverão ser seguidas pelos usuários para que haja interação das máquinas digitais, por exemplo, a formatação de documentos, o endereçamento, o roteamento, o banco de dados, dentre outros. A última camada, a semântica, é formada pela composição das informações que identificam os computadores. O autor destaca que, nessa camada, é possível corromper os componentes de identificação e essa objeção de autoria é um dos elementos que dificulta classificar um ataque cibernético como um ato de guerra, ponto que será expandido no capítulo dois.

O ciberespaço para Ventre (2011) tampouco é simplesmente uma rede digital; para o autor, os elementos físicos também fazem parte do espaço cibernético, como os satélites, os computadores, os drones e os sistemas industriais que são informatizados. E, assim como Libicki, Ventre (2011) percebe esse novo campo operacional em três camadas. A primeira é a camada inferior, configurada por uma infraestrutura material de

[19] [Tradução própria]. No original, lê-se: "a virtual medium, much less tangible than soil, water, air or even space".

hardware[20] e redes. A segunda é a intermediária, composta por *softwares*[21] e aplicativos operacionais das redes. E a terceira esfera é a superior, definida pelo autor como cognitiva, nesse ambiente há uma interação informacional entre os usuários do espectro eletromagnético, por meio de sites de notícias e das redes sociais.

Ventre (2011), assim como Nye e Libicki, realça a possibilidade de o ciberespaço ser disposto como um campo de batalha e classifica quais agressões cibernéticas o intercorrem. Na camada material, há a ocorrência de ataques cibernéticos contra os sistemas físicos, como os cabos de comunicação ou contra os satélites; e contra as infraestruturas críticas, como os sistemas de energia, água e transporte dos Estados. Na camada intermediária, pode ser realizado operações de espionagem, de vazamento de dados e de ataques de negação de serviço (DDoS)[22]; e na camada cognitiva, são praticadas ações informacionais, nesse ambiente diversos atores podem manipular informações, inserir ofensas, difundir calúnias e ensejar discussões (VENTRE, 2011).

Ventre (2011) enfatiza o uso do ciberespaço como um campo de batalha. O autor dispôs algumas possibilidades de conflitos cibernéticos, como os discursos de ódio executados pelo Talibã[23] nas mídias sociais; ou os ataques cibernéticos exercidos por atores estatais e não estatais que às vezes destroem as infraestruturas críticas dos Estados, como o caso do Stuxnet (2009-2010) e do Oleoduto Colonial Pipeline (2021), que serão expostos no decorrer do trabalho. Os pontos elaborados por Ventre (2011) vão de encontro à exposição de Nye (2010; 2011), de que o espaço cibernético possui condição de poder cibernético (VENTRE, 2011; NYE, 2010; 2011; ZETTER, 2017).

Por seu turno, Nielsen (2012) ordena o ciberespaço em sete funções:

1- Como também colocado por Nye, Libicki e Ventre, a primeira característica apontada pela autora é a origem do ciberespaço, que ocorreu pela construção do homem, portanto, não é orgânica. Já a funcionalidade do espaço cibernético é a de acessibilidade, de disponibilidade, de interoperabilidade, de inovação e de expansibilidade. Ao mesmo tempo que essas características possuem um

[20] Hardware: é a parte física do computador, ou seja, peças e equipamentos que fazem o computador funcionar. O termo também se refere ao conjunto de equipamentos acoplados em produtos que necessitam de gerenciamento computacional.
[21] Software: é um conjunto de instruções que devem ser seguidas e executadas por um mecanismo, seja ele um computador ou um aparato eletromecânico. É o termo genérico usado para descrever programas, apps, scripts, macros e instruções de código, de modo a ditar o que uma máquina deve fazer.
[22] DDos – Ataque de negação de serviço: é uma tentativa de tornar os recursos de um sistema indisponíveis para os usuários do espaço cibernético.
[23] Grupo Talibã: O Talibã é considerado um grupo radical da corrente sunita e defende uma teocracia de cunho islâmico.

viés positivo, já que possibilitam facilitar a vida em sociedade de uma maneira abrangente, também permitem vulnerabilidades e riscos de segurança na mesma proporção;

2- O segundo elemento é o dinamismo. A estruturação que se sucede no espaço cibernético permite a manipulação e a alteração no comportamento do sistema, seja por um mecanismo humano, por um vírus malicioso ou por uma inteligência artificial;
3- O terceiro ponto é a velocidade. A propagação de uma atividade no ciberespaço é instantânea, talvez a percepção nem tanto, mas a ocorrência é quase que imediata;
4- A quarta característica do espaço cibernético, é a ausência de fronteiras. A autora destaca que existem algumas ponderações nessa afirmação, pois existem países que fazem o controle de suas redes digitais, como a China, que censura o livre exercício de seus usuários sobre diversos aspectos, como seus meios de comunicação, suas atividades profissionais, dentre outros. Mas ainda assim, "a geografia é relativamente menos significativa do que em outros domínios da interação humana, como terra, mar e ar"[24] (NIELSEN, 2012, p. 338, tradução própria);
5- A quinta premissa é a fragilidade no acesso ao ciberespaço. Qualquer pessoa pode ter acesso nesse campo operacional, é um ambiente de poucas barreiras;
6- A sexta característica é o aumento exponencial de usuários. Com a facilidade de acesso ao espaço cibernético, há um crescimento ininterrupto de atores, o que torna a operabilidade cibernética um tanto complexa, pois aumentam também as situações de riscos e ameaças sofisticadas aos desfrutadores;
7- A última categoria apontada por Nielsen é a variedade comportamental que o ciberespaço permite. A autora apresenta alguns exemplos, como: a troca de informação entre os usuários, as atividades comerciais e profissionais que ocorrem, as interações interestatais "onde os países buscam promover seus interesses nacionais na competição e conflito com outros Estados que buscam os seus"[25] (NIELSEN, 2012, p. 339, tradução própria).

[24] [Tradução própria]. No original, lê-se: "geography is relatively less significant than in other domains of human interaction, such as land, sea and air".
[25] [Tradução própria]. No original, lê-se: "where countries seek to advance their national interests in competition and conflict with other states that pursue their".

Diferente de Nye, que fundamenta o ciberespaço como um poder cibernético, e de Libicki e Ventre, que o definem pela sua estrutura, Nielsen (2012) o conceitua por essas sete funcionalidades. A autora, assim como Nye, enfatiza a facilidade de acesso de variados atores ao espaço cibernético e a interoperabilidade, características facilitadoras. Esses elementos permitem a realização de diversas atividades pelos atores cibernéticos, por exemplo, a realização de serviços econômicos, educacionais e informativos. Entretanto, a interoperabilidade também propicia vulnerabilidades, como as ameaças e os ataques cibernéticos.

Outra característica destacada por Nielsen (2012) diz respeito à condição geográfica do espaço cibernético. A autora relativiza a existência de fronteiras no ciberespaço, ela explica que os Estados têm controle de acesso de suas redes de conexão, mas a geografia desse ambiente é menos significativa do que nos outros domínios, como o terrestre, o marítimo e o aéreo, pois como havia dito Libicki, no ciberespaço pode haver manipulação e alteração na camada semântica e isso pode dificultar a detectar a origem das ações cibernéticas (LIBICKI, 2009; NIELSEN, 2012).

Singer e Friedman (2014, p. 23, tradução própria) definem que o "ciberespaço é a esfera das redes de computadores (e usuários por trás delas) na qual a informação é armazenada, compartilhada e comunicada *online*"[26]. A estrutura é composta por duas camadas, uma física, que são os computadores, os cabos de fibras óticas, os celulares e os aparelhos que possuem inteligência artificial e se conectam entre si; e uma camada virtual, concebida pelo banco de dados e pelos sistemas de informação que são compartilhados e armazenados pelos usuários.

Assim como Nielsen e Libicki, Singer e Friedman (2014) ressaltam que as características singulares do ciberespaço podem favorecer a manipulação e distorção da identificação das ações cibernéticas, operadas pelos atores cibernéticos. Entretanto, os autores destacam que as atividades cibernéticas identificáveis estão "sujeitas a noções nossas tais como soberania, nacionalidade e propriedade"[27] (SINGER; FRIEDMAN, 2014, p. 23, tradução própria), ou seja, por mais que haja descentralização do Estado no ciberespaço (NYE, 2010; 2011), quando há o reconhecimento da origem geográfica e do ator cibernético da intercorrência cibernética, as sanções locais e internacionais podem

[26] [Tradução própria]. No original, lê-se: "cyberspace is the realm of computer networks (and the users behind them) in which information is stored, shared and communicated online".
[27] [Tradução própria]. No original, lê-se: "subject to our notions such as sovereignty, nationality and property".

ser aplicadas aos responsáveis, sejam eles atores estatais e não estatais (SINGER; FRIEDMAN, 2014).

Singer e Friedman (2014) acrescentam, por fim, que o ciberespaço está em constante evolução, que não abrange apenas os meios de comunicação e informação, mas também as infraestruturas críticas dos Estados, como suas instituições financeiras, sistemas de saúde, de transporte, de água e de energia e se torna cada vez mais um lugar de risco e perigo, pois com a facilidade de acesso cada vez maior de atores cibernéticos, torna-se um verdadeiro campo de guerra (SINGER; FRIEDMAN, 2014).

Medeiros e Goldoni (2020) seguem a mesma linha que os autores acima no que se refere à artificialidade do ciberespaço perante os outros domínios operacionais. Os autores salientam a dissociação parcial do espaço físico, pois mesmo que o espaço cibernético apresente-se no espectro eletromagnético, é também composto por estruturas físicas e se conecta "por um fluxo de dados binários sendo enviados de um dispositivo para outro"[28] (MEDEIROS; GOLDONI, 2020, p. 37, tradução própria).

Conforme Medeiros e Goldoni (2020), há três aspectos desafiantes que moldam o ciberespaço, a desterritorialidade, a multiplicidade de atores e a incerteza. Diferente de Nielsen (2012), que relativiza a existência de fronteiras no ciberespaço, e de Singer e Friedman (2014), que acreditam haver fronteiras no espaço cibernético, Medeiros e Goldoni (2020) explicam que a imaterialidade do ciberespaço rompe com os conceitos tradicionais do território físico delimitado por fronteiras, ou seja, os fluxos virtuais são ilimitados. Os autores relatam que o ciberespaço possui alcance global e, assim, há uma multiplicidade de atores que operam em seu ambiente. Esse domínio operacional permite variadas atividades, desde serviços profissionais até mesmo ações militares, ou ainda, atos de espionagem de um Estado contra outro. Os autores finalizam a definição do espaço cibernético pela sua última característica, que é a imprecisão de autoria. Medeiros e Goldoni (2020), assim como Libicki, Nielsen e Singer e Friedman, salientam que a falta de precisão de autoria dificulta imputar qualquer tipo de sanção, como aconteceu no caso da Estônia (2007). Por fim, os autores declaram que o ciberespaço está em constante evolução e por isso essas características são passíveis de flutuações.

No que diz respeito ao ato de guerra no ciberespaço, é possível afirmar que o ciberespaço é um poder cibernético (NYE, 2010; 2011). Pois existe a possibilidade de as intercorrências cibernéticas realizadas no espaço cibernético causarem impactos nos

[28] [Tradução própria]. No original, lê-se: "by a stream of binary data being sent from one device to another".

outros domínios operacionais, e por esse fator a guerra se configurar (NYE, 2010; 2011). Entretanto, diferente dos outros domínios operacionais, no ciberespaço nem sempre será possível atribuir o ato de guerra nas operações cibernéticas, seja pela distorção de identidade do autor da agressão cibernética, ou pela precária materialidade do ato, ou pela ausência de normas internacionais, ou pela ausência de vontade política. Todas essas implicâncias serão abordadas no próximo capítulo.

Posto isso, para esse trabalho, o ciberespaço deve ser compreendido como um novo domínio operacional de guerra, composto por três camadas, a física, a virtual e a humana. A estrutura física é composta pelos computadores, celulares, satélites, infraestruturas críticas, dentre outros. O elemento virtual é integrado pelos *softwares*, como os bancos de dados, sistemas operacionais *online*, rede de computadores e as plataformas digitais. Por fim, a humana, essa camada corresponde aos atores cibernéticos que podem operar no espaço cibernético para diversas finalidades, como por exemplo, produzir atividades profissionais ou utilizar como um meio de comunicação, inclusive realizar operações cibernéticas ofensivas, tais como os crimes cibernéticos e até mesmo agressões cibernéticas que podem destruir infraestruturas críticas.

2.4 GUERRA CIBERNÉTICA

Em 1989, Lind (1989, p. 24, tradução própria) fez uma previsão sobre uma possível interferência do ciberespaço nos combates internacionais: "a crescente dependência dessa tecnologia [espaço cibernético] pode abrir a porta para novas fragilidades, como a vulnerabilidade de um vírus de computador"[29]. O autor acrescentou que as vulnerabilidades não ocorreriam apenas por um vírus de computador, mas também em forma de desinformação, já que a partir do ciberespaço, os meios de comunicação iriam se expandir, desse modo, "os noticiários televisivos podem tornar-se uma arma operacional" [30] (LIND, 1989, p. 24, tradução própria).

Não houve ainda um ataque cibernético que tenha sido considerado um ato de guerra, entretanto, como previu Lind (1989), as operações realizadas no ciberespaço, como os ataques cibernéticos, aumentam a cada dia e, assim, geram preocupações entre os especialistas em Segurança e Defesa Cibernética e nos governantes dos Estados no que se refere à Segurança Internacional (AYRES, GRASSI; 2020; FORTINET, 2021). Nesse

[29] [Tradução própria]. No original, lê-se: "the growing dependence on this technology can open the door to new vulnerabilities, such as vulnerability to computer viroses".
[30] [Tradução própria]. No original, lê-se: "television news can become an operational weapon".

sentido, esta seção tem como objetivo compreender o que é a guerra cibernética e quais suas características principais.

Arquilla e Ronfeldt (1993) foram os precursores ao explicarem as agressões cibernéticas como elementos de guerra (KENKEL; LOBATO, 2015). Os autores elaboraram sua pesquisa acerca dos conflitos cibernéticos em 1993, até então, haviam apenas previsões sobre conflitos cibernéticos em caráter de guerra; o primeiro caso ocorreu em 2007, na Estônia (KENKEL; LOBATO, 2015). Arquilla e Ronfeldt (1993) definiram as agressões cibernéticas em duas categorias: a) a guerra cibernética; e a b) guerra em redes, essa última sendo conceituada como uma forma de "conflito relacionado à informação em um grande nível entre nações ou sociedades; que significa tentar interromper, danificar ou modificar o que uma população-alvo 'sabe' ou pensa que sabe sobre si mesma e o mundo ao seu redor"[31] (ARQUILLA; RONFELDT, 1993, p. 28, tradução própria). Os autores compreendiam o ciberespaço como um meio de comunicação, que poderia ser manipulado, tanto pelo Estado, como por atores não estatais, com o objetivo de subverter a opinião pública por meio de propaganda política e campanhas psicológicas que influenciam as pessoas. Seria a guerra de informação. Para os autores os governos também poderiam participar indiretamente das operações cibernéticas permeadas pelos atores não estatais (ARQUILLA; RONFELDT, 1993).

Diferentemente da guerra em redes, a guerra cibernética implicaria não apenas os sistemas operacionais de tecnologia, mas também na organização e na doutrina militar, ou seja, seria uma nova forma de guerra (ARQUILLA; RONFELDT, 1993). Sendo assim, Arquilla e Ronfeldet (1993) definiram que a ciberguerra "significa(ria) perturbar, senão destruir, os sistemas de informação e comunicação, amplamente definidos para incluir até a cultura militar[32] (ARQUILLA; RONFELDT, 1993, p. 30, tradução própria). Os autores destacam que as ações cibernéticas poderiam, ainda, "cegar eletronicamente, bloquear, enganar, sobrecarregar e invadir os circuitos de informação e comunicação de um adversário"[33] (ARQUILLA; RONFELDT, 1993, p. 30, tradução própria). Para os autores, a guerra no ciberespaço seria utilizada para corromper os sistemas de informação e comunicação militares dos inimigos.

---

[31] [Tradução própria]. No original, lê-se: "information-related conflict at a large level between nations or societies. It means trying to interrupt, damage or modify what a target population 'knows' or thinks they know about themselves and the world around them".

[32] [Tradução própria]. No original, lê-se: "it means disturbing, if not destroying, information and communication systems, broadly defined to include even the military culture".

[33] [Tradução própria]. No original, lê-se: "electronically blinding, blocking, deceiving, overloading and invading an adversary's information and communication circuits".

De acordo com Arquilla e Ronfeldet (1993), a guerra cibernética atingiria numerosas características da guerra convencional, como a possibilidade de ser travada na forma ofensiva e defensiva, bem como de ser exercitada nos níveis estratégicos e táticos. Mas no quesito geográfico, os autores distinguiram a ciberguerra de um confronto convencional, pois "a guerra cibernética depende menos do terreno geográfico"[34] (ARQUILLA; RONFELDT, 1993, p. 30, tradução própria); e por esse motivo, perpetuar operações cibernéticas seria até mais vantajoso do que travar uma batalha bélica. Os autores encerraram a pesquisa definindo a guerra cibernética como um fenômeno informacional.

Contrário ao conceito de Arquilla e Ronfeldet, que classificaram a ciberguerra como um fenômeno de informação, Libicki (2009) a define como um possível campo de batalha, não por um aspecto informacional, mas pelo aspecto já apresentado por Nye, que é do poder cibernético, ou seja, um domínio operacional de guerra que pode causar destruição não apenas dos meios de comunicação dependentes do ciberespaço, mas também das infraestruturas físicas, assim como ocorre nos conflitos convencionais.

Libicki (2009) separa a guerra cibernética em duas vertentes. A primeira vertente é a estratégica, que condiz, à princípio, em uma "campanha de ataques cibernéticos lançados por uma entidade contra um Estado e sua população, mas não exclusivamente para afetar o comportamento do Estado-alvo"[35] (LIBICKI, 2009, p. 117, tradução própria). O autor não acredita totalmente na eficácia desse comportamento, para ele, os efeitos coercitivos que os ciberataques podem gerar são especulativos. O autor aponta que as consequências dos ataques cibernéticos da guerra estratégica são mais brandas do que os resultados de uma coerção estratégica convencional. Já a segunda premissa é a operacionalidade, essa sim o autor equipara aos combates tradicionais. Libicki (2009, p. 139, tradução própria) a entende como a ocorrência de "ciberataques em tempos de guerra contra alvos militares e civis relacionados ao esforço de guerra"[36], ou seja, as agressões cibernéticas podem ser um intensificador de força realizado pelas forças militares em um conflito convencional, é um meio instrumental para um combate.

No período em que Libicki desenvolveu sua pesquisa em relação ao ciberespaço e aos conflitos cibernéticos, aconteciam os primeiros casos de ataques cibernéticos contra

[34] [Tradução própria]. No original, lê-se: "cyber warfare relies less on geographic terrain".
[35] [Tradução própria]. No original, lê-se: "campaign of cyber attacks launched by an entity against a State and its population, but not exclusively to affect the behavior of the target State".
[36] [Tradução própria]. No original, lê-se: "wartime cyber attacks against military and civilian targets related to the war effort".

os serviços sensíveis de alguns Estados, como o caso da Estônia (2007) e da Geórgia (2008), que serão analisados no capítulo três. Esses eventos proporcionaram novos debates sobre a guerra cibernética (KENKEL; LOBATO, 2015). Isto é, as previsões a respeito das vulnerabilidades permeadas no ciberespaço e dos conflitos cibernéticos, como bem discorreu Lind, em 1989, expandiram-se conforme a tecnologia evoluía (CLARKE; KNAKE, 2015).

O termo "guerra cibernética" passou então a ser referido "a qualquer tipo de conflito no ciberespaço com dimensão internacional"[37] (CAVELTY, 2010, p. 1, tradução própria), como de ciber-vandalismo e de ciber-terrorismo (CAVELTY, 2010). Houve uma generalização da palavra, qualquer forma de ataque cibernético passou a se denominar como ciberguerra. Nesse sentido, para definir a guerra cibernética, Cavelty (2010) classificou os ataques cibernéticos em cinco níveis divergentes:

1. Ciber-Vandalismo: é uma violação de integridade, ou seja, são usuários que depredam sites e alteram seus conteúdos. Nesse nível a intenção do autor é considerada uma "travessura";
2. Crime de Internet: é uma ação criminosa, como por exemplo, um ato de fraude de identidade ou roubo de dados financeiros. As ações desse tipo são comuns no sistema corporativo;
3. Ciber-Espionagem: é um conflito de interesse político. É a realização de operações cibernéticas, por atores estatais e não estatais, que consistem em apropriar informações sensíveis de forma ilícita;
4. Ciber-Terrorismo: é um ataque cibernético realizado por atores não estatais contra redes de computadores, sites e banco de dados, empreendidas com o intuito de intimidar um Estado e o seu povo ou para obrigar algum tipo de comportamento, nesse nível o "alcance potencial do dano é considerado muito alto"[38] (CAVELTY, 2010, p. 1, tradução própria);
5. Guerra Cibernética: é o ensejo de hostilidades de alto índice no espaço cibernético, como por exemplo, ataques que causam letalidade e destruição de infraestruturas críticas.

[37] [Tradução própria]. No original, lê-se: "to any type of conflict in cyberspace with an international dimension".
[38] [Tradução própria]. No original, lê-se: "potential range of damage is considered too high".

Assim como Cavelty (2010), Ventre (2011) analisa que a guerra cibernética é a realização de ataques cibernéticos que têm como finalidade ameaçar a economia de um Estado, bem como desestabilizar a sua Segurança e a sua Defesa. Para Ventre (2011), as ações cibernéticas podem afetar o equilibro de poder dos Estados, como também "suas capacidades, sua liberdade de ação, sua eficiência e poder"[39] (VENTRE, 2011, p. 33, tradução própria). Desse modo, o autor explica que o aumento de casos de ataques cibernéticos às infraestruturas deve provocar cada vez mais a criação de normas de Segurança Cibernética e Defesa Cibernética dos Estados (VENTRE, 2011). Por fim, Ventre (2011) salienta que, além das normas internas, as forças militares dos Estados devem se preparar para as hostilidades presentes no ciberespaço e então desenvolver suas técnicas de ataque e defesa nesse novo domínio operacional de guerra.

Para compreender a guerra cibernética, Rid (2012) resgata o conceito de guerra de Clausewitz, de que as agressões devem ser efetuadas por um ato de força, que resulte em violência e seja subordinado à política. De acordo com Rid (2012), a guerra cibernética não preenche adequadamente estes três elementos, especificamente a necessidade de violência, que o autor entende necessariamente como violência física cometida sobre seres humanos. O autor admite que poderá chegar o momento em que um ciberataque ocasione consequências além do espectro eletromagnético que possam gerar letalidade, mas o articulista propôs que isso seria "ficção científica" (RID, 2012). Assim, Rid (2012) conclui que uma agressão cibernética jamais poderá ser considerada um ato de guerra e o seu objetivo será, no máximo, subverter, espionar ou sabotar (RID, 2012; BERNARDES; ÀVILA, 2021).

Em resposta a Rid (2013), o seu colega de departamento, Stone (2013), adota uma visão mais ampla de guerra. Stone (2013) se utiliza dos bombardeios estratégicos da Segunda Guerra Mundial para expandir seu persuasivo ponto de vista. Conforme o autor, nesse confronto – o Bombardeio de Schweinfurt, em 1943 – o objetivo dos ataques era destruir as infraestruturas críticas que reforçavam a defesa da Alemanha; a violência – letalidade - nesse caso, seria um "efeito colateral" do objetivo principal (STONE, 2013; BERNARDES; ÀVILA, 2021). Assim, Stone (2013) refuta a ideia de Rid (2012) e evidencia que não há ligação entre a violência e a letalidade.

Stone (2013), por fim, interpreta o pensamento de Clausewitz no que se refere à subordinação da guerra à política. Ao analisar os casos de ataques cibernéticos, como o

[39] [Tradução própria]. No original, lê-se: "sus capacidades, su libertad de acción, su eficiencia y potencia".

caso da Estônia (2007) e do Stuxnet (2009-2010), o autor conclui que o elemento primordial para o ensejo do ato de guerra em um evento cibernético seria a relação política e não a violência. Desse modo, o autor encerra seu ponto de vista afirmando que a guerra cibernética poderá, sim, ocorrer (STONE, 2013; BERNARDES; ÀVILA, 2021).

Na mesma linha da Teoria de Guerra de Clausewitz, Singer e Friedman (2014) compreendem que um ataque cibernético poderá ser um ato de guerra se possuir ensejo político e ser um ato violento. Os autores definem a guerra cibernética como a realização de uma ação cibernética que resulte em ameaça à segurança dos Estados e até mesmo na destruição de suas infraestruturas críticas. Singer e Friedman (2014) destacam, assim como Cavelty (2010), que a definição de guerra cibernética se configura em diversos tipos de ações, como um ato criminoso ou um ato de vandalismo. Mas os autores salientam que o conceito de guerra cibernética só será entendido como uma guerra real quando, de fato, uma agressão cibernética ameaçar ou atacar a segurança de um Estado. Singer e Friedman (2014) findam seus debates acrescentando que a guerra cibernética está em constante transformação e sua definição está apenas no começo, mais critérios serão desenvolvidos no decorrer da evolução dos conflitos cibernéticos.

Estudos mais recentes sugerem que a guerra cibernética, por não possuir definições concretas, talvez se insira no conceito de *Grey Zone Conflict* (WIRTZ, 2017 LIBICKI, 2012; FITTON, 2016). O *Grey Zone Conflict* ou a chamada zona cinzenta "é definida como a região entre a paz e a guerra, que ainda não é totalmente compreendida"[40]. Em outras palavras, é a realização de conflitos de baixa intensidade, consideradas abaixo da guerra, como a execução de operações militares com a aparência de "não guerra" (WIRTZ; 2017; FITTON, 2016). Wirtz (2017) pontua que os conflitos da zona cinzenta possuem características nebulosas, ou seja, é uma ameaça não convencional, assim como o é a guerra cibernética.

Nesse sentido, vale lembrar uma parte do conceito de guerra de Dinstein (2003). Conforme visto, o autor informa que quando um Estado entra em "estado de guerra" ou realiza operações militares convencionais, as normas das instituições de segurança internacional entram no escopo (DINSTEIN, 2003). Sendo assim, Fitton (2016) argumenta que para escapar desse enquadramento de "estado de guerra" e, por conseguinte, das possíveis sanções normativas, os Estados optam cada vez mais em realizar operações militares não convencionais, de zona cinzenta, como a guerra

[40] [Tradução própria]. No original, lê-se: "the gray zone is defined as the region between peace and war, which is not yet fully understood".

cibernética, para intentar contra outros Estados (FITTON, 2016; EUA, 2017; REUTERS, 2019).

No que tange às normas internacionais, tanto a ONU como a OTAN reconhecem a existência das agressões cibernéticas, entretanto, não há definições claras sobre suas classificações (AYRES; GRASSI, 2020). Em 2016, a OTAN reconheceu o espaço cibernético como um campo operacional de guerra e afirmou que as normas do Direito Internacional se expandiam ao ciberespaço (OTAN, 2016). No ano de 2021, a OTAN declarou que as "ameaças cibernéticas à segurança da Aliança estão se tornando mais frequentes, complexas, destrutivas e coercitivas"[41] (OTAN, 2021, tradução própria). Por fim, a Aliança Militar reforçou que a instituição está ativa frente às ameaças cibernéticas por meio de operações, missões, treinamento e exercícios que fortalecem a resiliência de todos os integrantes da aliança, além da parceria com a União Europeia, para que haja assistência, mitigação e recuperação das infraestruturas que venham sofrer ataques cibernéticos (OTAN, 2021).

Nas definições aqui suscitadas, é possível analisar a diversidade do conceito de guerra cibernética. Apesar da ciberguerra possuir similaridades com a guerra tradicional, a sua natureza de guerra se assemelha com a guerra irregular (VISACRO, 2009; DIENSTEIN, 2003). A guerra irregular é um fenômeno único e singular (HEYDTE, 1990), que não possui padrões rígidos, ela se molda aos "ambientes políticos, sociais e militares diferenciados" (VISACRO, 2009, p. 264). E diferentemente da guerra convencional, que os duelos acontecem entre os Estados, na guerra irregular os beligerantes são formados também por atores não estatais (VISACRO, 2009; DINSTEIN, 2003).

Portanto, neste trabalho, a guerra cibernética é definida pela ocorrência de ações cibernéticas, realizados por atores estatais e não estatais, que causam impactos destrutivos aos Estados, acerca de sua soberania e de seus serviços essenciais; possui natureza de guerra irregular; sua arena de conflito ocorre por intermédio do ciberespaço e mesmo que os danos das ações cibernéticas impactem os outros espectros, existem algumas complexidades que abarcam esse novo campo de batalha, que é a carência de definição legal, a relativa materialidade, a imprecisão de autoria e a ausência de vontade política, que serão expandidos no próximo capítulo.

[41] [tradução própria]. No original, lê-se: "Cyber threats to Alliance security are becoming more frequent, complex, destructive and coercive" (…) "will continue to adapt to the evolving scenario of cyber threats".

3 ELEMENTOS QUE DIFICULTAM CONSIDERAR OS EVENTOS CIBERNÉTICOS COMO ATOS DE GUERRA

Como visto anteriormente, não há um consenso entre os especialistas em Segurança e Defesa Cibernética sobre configurar os ciberataques em atos de guerra. Em 2012, Rid suscitou uma questão acerca da guerra cibernética, o autor classificou as agressões cibernéticas como atos de subversão, espionagem e sabotagem e por isso não seriam atos de guerra e provavelmente nunca serão. Em resposta, seu colega de trabalho, Stone (2013), afirmou que, sim, os conflitos cibernéticos poderão ocorrer futuramente como uma guerra real.

O presente capítulo pretende demonstrar que não são "só" as questões debatidas por Rid (2012) e Stone (2013) que dificultam a classificação dos eventos cibernéticos como atos de guerra, mas um leque de elementos: a imprecisão de autoria; a relativa materialidade dos ciberataques; a falta de definição legal pelas instituições de Segurança Internacional; e talvez o fator essencial, a ausência de vontade política em declarar uma guerra cibernética como ato de guerra.

3.1 ATAQUES CIBERNÉTICOS COMO ATOS DE SUBVERSÃO, DE ESPIONAGEM E DE SABOTAGEM

Conforme citado no capítulo anterior, Rid (2012) adota a Teoria de Guerra de Clausewitz para conceituar o que é guerra, ou seja, para uma agressão ser um ato se guerra, precisa ser violento, ser instrumental e ser subordinado à política. O autor afirma que uma agressão cibernética jamais atenderá ao mesmo tempo esses três critérios, portanto, nunca poderá ser classificada como um ato de guerra. Rid (2012) argumenta que um ciberataque possuirá no máximo o objetivo de sabotar, espionar e subverter. Antes de expandir o debate de Rid (2012), é preciso compreender o conceito dessas três ações.

A ação de sabotar apareceu no final do século XIX, na França, e era originalmente utilizada para se referir às disputas trabalhistas que ocorriam na época (POUGET, 1910). Como forma de protesto, os trabalhadores industriais destruíam as máquinas para atrasar a produção, ou até mesmo provocavam pequenos incêndios (POUGET, 1910). A prática de sabotagem aumentou muito na Primeira e na Segunda Guerra Mundial, as tropas britânicas desenvolveram dois manuais que estimulavam as pessoas a sabotarem os inimigos - o *Partisan Leader's Handbook* (1939) e o *Simple Sabotage Field Manual* (1944) – nesses manuais é possível encontrar instruções de diversas formas de sabotagem,

como cortar as comunicações de supostos inimigos ou de como danificar suas estradas ferroviárias (ASSIS, 2017). Portanto, entende-se que sabotar é o ato de atrapalhar o oponente de alguma maneira (ASSIS, 2017).

Já a prática de espionar é anterior ao ato de sabotar. As primeiras ações de espionagem registradas foram elaboradas por Sun Tzu, no seu livro de estratégias da guerra – A Arte da Guerra (500 a.C.) – o estrategista militar salientava a importância de coletar e transportar informações dos inimigos de guerra (ASSIS, 2017). Conforme Horn (2003), a espionagem consiste na realização de operações secretas precedidas por espiões treinados, que se destinam a enganar o inimigo e, assim, descobrir informações sensíveis. Desse modo, a espionagem pode ser definida pelo intuito de conhecer o inimigo, por meio de infiltração, técnicas operacionais ou até mesmo de ataques cibernéticos com o ensejo político, econômico ou militar (HORN, 2003; WOLOSYN, 2013).

Por último, o ato de subverter. A origem da palavra subversão deriva do latim "subversus", que significa derrubar e destruir; sendo assim, o ato de subverter significa revoltar-se contra a ordem econômica, militar e política vigentes em um Estado (GARCIA, 2007). O objetivo de um ato subversivo é derrubar um governo e a sua manifestação pode ocorrer de forma aberta e declarada ou de uma maneira oculta e prolongada. Alguns exemplos de ações subversivas se dão por propagandas enganosas; ou incitações de greves; ou até mesmo de movimentos que boicotam um governo (FERREIRA, 1986; GARCIA, 2007).

Dando continuidade ao debate de Rid (2012), o autor esclarece que dificilmente os ataques cibernéticos irão causar letalidade, portanto, não teria como considerá-los violentos. O autor afirma que a guerra precisa ser instrumental, ter um começo, um meio e um fim. Desse modo, Rid (2012) declara que um único evento cibernético não poderia ser classificado como um ato de guerra. Em sua visão, uma única ação cibernética não poderia ameaçar a soberania de um Estado. Por fim, o autor conclui que poucos ciberataques seriam subordinados à política e caso fossem não passariam de atos de sabotagem, espionagem e subversão.

Para expandir o seu ponto de vista sobre a sabotagem nas agressões cibernéticas, Rid (2012) pontua que um ataque cibernético sabotador não é precedido por violência. O autor argumenta que um ato de sabotagem cibernético não tem capacidade de causar letalidade, pois o alvo aqui não são as vidas humanas, mas as infraestruturas críticas dos Estados. Rid (2012) aponta que um ato de sabotagem no advento do ciberespaço pode até ser instrumental, mas ainda assim não configuraria guerra. Como forma de exemplo, Rid

(2012, p. 17, tradução própria) aborda o caso do Stuxnet (2009-2010): “o Stuxnet foi de longe o ataque cibernético mais sofisticado conhecido até hoje”[42]; o autor presumi que o caso do Stuxnet foi uma operação militar realizada “apenas” para sabotar o programa de enriquecimento de urânio na Usina Nuclear de Natanz, no Irã e não possuiu características de guerra, pois, em sua perspectiva, apesar de ser um ato subordinado à política, não houve violência.

Conforme Rid (2012), as operações cibernéticas que têm como finalidade espionar ocorrem com maior frequência do que os atos de subversão e sabotagem, pois o nível de complexidade para a sua operabilidade é baixo. Para Rid (2012) o intuito das agressões cibernéticas de espionagem é angariar informações para serem utilizadas como instrumento político. Portanto, em sua visão, o ato em si não é instrumental, apenas o seu resultado e por isso o ensejo de guerra nesses casos deveria ser afastado (RID, 2012).

Um evento cibernético que teve como objetivo espionar e pode servir de exemplo é o episódio do *Titan Rain* (2003) (THE GUARDIAN, 2007). Na época, sucessivos ataques cibernéticos foram disparados contra o espaço cibernético dos Estados Unidos (THE GUARDIAN, 2007). Quando os investigadores foram verificar as peculiaridades da incursão, constataram que o intento foi originário da China e teve como objetivo coletar informações sensíveis do governo dos Estados Unidos, como diversos documentos da NASA[43] e relatórios sigilosos das forças armadas norte-americanas (RID, 2012; THE GUARDIAN, 2007).

Em sua última análise, Rid (2012) elucida o que seria um ciberataque de subversão. De acordo com o autor, as agressões cibernéticas subversivas geralmente são realizadas por meio de declarações revoltosas contra uma ordem estabelecida nos sites de comunicação ou nas redes sociais, como o Twitter e o Facebook. Para Rid (2012) as ações subversivas possuem baixa materialidade, ou seja, não ocasionam explosões ou bombardeios; a intenção desses atos é causar desordem interna em um governo. Para exemplificar o entendimento de Rid (2012) é possível verificar o ensejo subversivo nos ataques cibernéticos praticados pelo grupo de ativistas Anonymous, o grupo é formado por diversos *hackers* e geralmente promovem ataques cibernéticos contra uma ordem

[42] [Tradução própria]. No original, lê-se: “Stuxnet was by far the most sophisticated known cyber attack to date”.

[43] NASA - é a sigla em inglês para National Aeronautics and Space Administration, que significa Administração Nacional da Aeronáutica e Espaço. A Agência Espacial norte-americana foi fundada em 1958 e é responsável pelo desenvolvimento de tecnologias e explorações espaciais.

política, como as incursões cibernéticas que realizaram no contexto da guerra entre a Rússia e a Ucrânia (NYT, 2022).

Em fevereiro de 2022, uma série de ciberataques desfiguraram os sites de comunicação da Rússia, onde foram exibidas mensagens pedindo o fim da guerra na Ucrânia, o Anonymous assumiu a autoria do ato cibernético subversivo (NYT, 2022). Rid (2012) encerra sua análise dos conflitos cibernéticos reafirmando que "o mundo nunca experimentou um ato de guerra cibernético, que teria que ser violento, instrumental e - o mais importante - atribuído politicamente; e nenhum ataque registrado atende a todos esses critérios"[44] (RID, 2012, p.29, tradução própria).

Ao analisar os entendimentos de Rid (2012) sobre os conflitos cibernéticos é possível identificar um argumento insistente de que os ataques cibernéticos não são e nem serão violentos o bastante para serem classificados como guerra, que no conceito do autor significa haver letalidade. Entretanto, a relação que Rid (2012) faz entre a violência e a letalidade é equivocada (STONE, 2013; DINSTEIN, 2003). Como bem colocou Stone (2013) em resposta às convicções de Rid (2012), um ato de guerra não necessita envolver uma violência letal para ser ato de guerra; e não é porque houve um ato de sabotagem, um ato de espionagem ou um ato de subversão que não foi um ato de guerra (STONE, 2013; DINSTEIN, 2003).

Como visto previamente no primeiro capítulo, para evidenciar o seu ponto de vista sobre atos de sabotagem, violência e atos de guerra, Stone (2013) cita um evento de guerra – o Bombardeio de Schweinfurt (1943) – na época, a Força Aérea dos Estados Unidos realizou uma operação de ataque às indústrias alemãs, na Bavária, que produziam rolamento de esferas. O autor analisa que o objetivo do ataque era sabotar as indústrias e assim prejudicar a produção de materiais de guerra para o exército alemão, entretanto, houve baixas como resultado das agressões, no primeiro ataque 203 pessoas foram mortas e no segundo 276 pessoas morreram (STONE, 2013).

Nessa situação exposta, Stone (2013) esclarece que os "atos de guerra podem envolver a aplicação da força para produzir efeitos violentos; esses efeitos violentos não precisam ser de caráter letal: eles podem quebrar as coisas, em vez de matar pessoas, e ainda caem sob a rubrica da guerra"[45] (STONE, 2013, p. 107, tradução própria). Assim,

[44] [Tradução própria]. No original, lê-se: "the world never experienced an act of cyberwar, which would have to be violent, instrumental, and – most importantly – politically attributed".
[45] [Tradução própria]. No original, lê-se: "Acts of war involve the application of force in order to produce violent effects. These violent effects need not be lethal in character: they can break things, rather than kill people, and still fall under the rubric of war".

Stone (2013) conclui seu posicionamento contrário de Rid (2012) e afirma que em uma guerra futura os ataques cibernéticos poderão sim constituir atos de guerra, pois os avanços tecnológicos já permitem uma maior letalidade ou destruição por um esforço menor, desse modo, um "simples" ataque cibernético poderá resultar em grandes quantidades de violência, letais ou não (STONE, 2013).

Importa salientar, que o conceito de guerra cibernética ainda está em construção e como bem citou Clausewitz (1984, p. 92, tradução própria), "a guerra é um verdadeiro camaleão, que modifica um pouco a sua natureza em cada caso concreto"[46]. Isso significa que a guerra muda, se transforma e a capacidade de uma guerra real no espaço cibernético não pode ser descartada, inclusive como forma de precaução dos institutos de Segurança e Defesa dos Estados (STONE, 2013; SINGER; FRIEDMAN, 2014).

O embate entre Rid e Stone se faz necessário aos estudos de guerra cibernética como atos de guerra. No entanto, conforme será visto a seguir, não são "somente" os elementos de subversão, de sabotagem e de espionagem que dificultam ou impedem a atribuição do ato de guerra nas agressões cibernéticas, mas sim a imprecisão de autoria, a baixa materialidade que os ciberataques normalmente têm como resultado, a falta de definição legal que causa insegurança jurídica e a ausência de vontade política dos líderes dos Estados (AYRES; GRASSI, 2020; DIPERT, 2010; SINGER; FRIEDMAN, 2014).

3.2 A IMPRECISÃO DE AUTORIA NOS CIBERATAQUES

De acordo com o que foi explorado no capítulo 1, é possível afirmar que as próprias características do ciberespaço permitem que haja manipulação e decodificação em seu sistema e isso dificulta a identificação dos atores cibernéticos (DIPERT, 2010; SINGER; FRIEDMAN, 2014). Desse modo, Dipert (2010) destaca que a falta de garantia em identificar os atores cibernéticos de uma agressão cibernética implica em classificá-la como um ato de guerra. O autor afirma que os ataques cibernéticos podem ser executados de qualquer parte do mundo, pois o custo é baixo e muitas vezes não é necessária uma estratégia complexa para atuar no ciberespaço de forma maliciosa, como por exemplo, desenvolver um vírus e espalhar para várias redes de conexão. O autor afirma que a identificação do ator cibernético é muitas vezes uma adivinhação (DIPERT, 2010).

[46] [Tradução própria]. No original, lê-se: "War is more than a mere chameleon that slightly adapts its characteristics to the given case".

Na mesma linha de raciocínio que Dipert (2010), Libicki (2009, p. 43, tradução própria) pontua que: “os computadores não deixam evidências físicas distintas para trás; os ciberataques podem vir de qualquer lugar”[47]. O autor esclarece que, ao se tratar do ciberespaço, há diversos cenários que dificultam na identificação do ator cibernético, pois o usuário pode usar uma rede de conexão pública; ou sequestrar uma rede e fazer o uso dela para desferir ciberataques; ou desenvolver um vírus que maquia a origem da ação cibernética; ou ainda utilizar um *bot*[48] que apaga o endereço de rede. Portanto, não há um rastro totalmente confiável sobre a origem das ações cibernéticas (LIBICKI, 2009; DIPERT, 2010).

Libicki (2009) salienta que essa incerteza gera insegurança em como responder um ataque cibernético, “a atribuição é tão incerta que as chances de qualquer resposta seriam bastantes baixas”[49] (LIBICKI, 2009, p. 43, tradução própria). Por exemplo, caso seja rebatido à pessoa errada, pode criar um inimigo, e esse é um dos motivos pelo qual tantos casos de conflitos cibernéticos não tenham tido punição, pela falta de precisão sobre quem aplicou o ciberataque (LIBICKI, 2009; DIPERT, 2010).

É possível observar que mesmo nas ações cibernéticas em que os atores cibernéticos são identificados, algumas situações podem dificultar esse reconhecimento, pois os perpetradores dos ataques podem trabalhar ou serem patrocinados por um Estado ou por uma empresa privada ou por um grupo mafioso, ou seja, não há exatidão de quem seja o mandante do ato (DIPERT, 2010). Por exemplo, em 2021, a empresa Microsoft, nos Estados Unidos, sofreu vários ataques cibernéticos, seu sistema de e-mail foi invadido e teve como consequência diversos dados vazados (BBC, 2021). Nesse caso, os Estados Unidos e alguns países da Europa acusaram a China de ser a executora dos ciberataques (BBC, 2021). A acusação foi negada pelo governo chinês (BBC, 2021). Mesmo que a origem das agressões cibernéticas tenha sido identificada como sendo na China, não há como afirmar que o executor ou o mandante do ato foi o Estado, os cidadãos ou mesmo grupos ativistas.

Singer e Friedman (2014) seguem o mesmo pensamento que Dipert (2010) e Libicki (2009), os autores compreendem que o problema de atribuição nos eventos

---

[47] [Tradução própria]. No original, lê-se: “computers do not leave distinct physical evidence behind; attacks can come from anywhere”.

[48] Bot: é um programa de software que executa tarefas automatizadas, repetitivas e pré-definidas. Os bots normalmente imitam ou substituem o comportamento do usuário humano. Por serem automatizados, operam muito mais rápido do que os usuários humanos.

[49] [Tradução própria]. No original, lê-se: “Attribution may be so uncertain that the odds that any one cyberattack could evoke a response would be fairly low”.

cibernéticos é o elemento mais difícil de ser solucionado. Singer e Friedman (2014) argumentam que existem muitas formas de mascarar a identificação de um ataque cibernético: "muitas formas de *malware*[50] assumem o controle do computador da vítima e formam um *bot* que conecta computadores não relacionados, e capacita o controlador a influenciar suas capacidades de computação e comunicações"[51] (SINGER; FRIEDMAN, 2014, p. 87, tradução própria). Os autores entendem que o ciberespaço é diferente dos outros domínios operacionais e a manipulação de suas configurações atrapalha especificar de onde partiram os ciberataques (SINGER; FRIEDMAN, 2014). Portanto, pode-se compreender que a imprecisão de autoria cria uma espécie de incentivo aos Estados a realizarem operações cibernéticas ofensivas, por meio de atores cibernéticos patrióticos, sem correrem o risco de serem punidos, é o Estado agindo por meio do seu próprio povo.

Para exemplificar a questão de o Estado estar vinculado às agressões cibernéticas, Singer e Friedman (2014) explicam que países que controlam totalmente seu ciberespaço e possuem uma política unipartidária, como a China e a Rússia, tendem a controlar e a incitar o seu povo a realizar operações cibernéticas ofensivas contra outros Estados. Perante esse cenário, quando há fortes indícios de que um ataque cibernético foi sediado na China ou na Rússia, presume-se que o governo seja o mandante do ato (SINGER; FRIEDMAN, 2014).

Olson (2012) também entende que os Estados podem controlar grupos de *hackers* para atacar o sistema de conexão de outros Estados e não serem responsabilizados pelo ato. Em uma tentativa de alertar os Estados Unidos nessa perspectiva, o autor declarou que:

> O valor da utilização de "fantoches" na guerra cibernética é que eles complicam ainda mais a possibilidade de atribuir responsabilidade. uma potência pode identificar e mapear vulnerabilidades e, em seguida, coordenar ataques usando intermediários. Mapeamentos passados de vulnerabilidades de rede e infraestrutura não foram tratados como um ato de guerra. assim, contanto que a potência hostil utilize "fantoches", haverá poucas medidas diretas que os EUA poderão tomar, ainda que se conheça a fonte de informações que possibilita os ataques (OLSON, 2012, p. 77).

Essa questão apontada por Olson (2012) é um cenário comum e crescente no que tange os conflitos cibernéticos (CLARKE; KNAKE, 2015; DIPERT, 2010). Todavia, é

[50] Malware é a abreviação de "software malicioso" (em inglês, *malicious software*) e se refere a um tipo de programa de computador desenvolvido para infectar o computador de um usuário legítimo e prejudicá-lo de diversas formas.

[51] [Tradução própria]. No original, lê-se: "many forms of malware take control of the victim's computer and form a bot that connects unrelated computers, and empowers the controller to influence their computing and communications capabilities".

preciso salientar que nem sempre a autoria das agressões cibernéticas será imprecisa (STEVENS, 2018). Stevens (2018) expõe que os ataques cibernéticos de baixa complexidade, como as incursões cibernéticas "de negação de serviço"[52], conhecidos também como os *DDos*, podem ser desenvolvidos por atores não estatais, ou até mesmo por *hackers* patrocinados e vinculados por um Estado; nesse caso, encontrar a origem pode até ser simples, mas nem sempre o ator cibernético malicioso será identificado. Contundo, Stevens (2018) destaca que nas operações cibernéticas de alta complexidade, que resultam em destruições de infraestruturas críticas, como o Stuxnet (2009-2010), só poderiam ser elaboradas por grandes potências, como os Estados Unidos, Israel, Rússia e China, isto é, apenas um Estado com alto poder econômico e tecnológico teria capacidade para produzir determinadas agressões cibernéticas (STEVENS, 2018).

Na mesma linha de Stevens (2018), Rid e Buchanan (2015) revelam que existem análises específicas de investigação que ajudam a identificar a origem de um ataque cibernético, essas averiguações devem incluir: "as explorações específicas que foram usadas, o mecanismo de carga útil, a infraestrutura de comando e controle, os dados direcionados, a análise de engenharia reversa e os dados brutos das redes afetadas" [53] (RID, BUCHANAN, 2015, p.11, tradução própria). Mas os autores lembram que esse aparato não é uma tarefa simples, para chegar na identificação da ação cibernética é preciso montar uma espécie de quebra-cabeça, ou seja, é necessário juntar muitas peças para chegar à origem do ciberataque; dependendo do caso, a investigação se torna extensiva, de custo elevado e inviável. O processo é multifacetado e requer liderança, treinamento e diligência (RID; BUCHANAN, 2015).

A questão de atribuição de autoria nos conflitos cibernéticos é um problema complexo, pois não tem como um ataque cibernético ser um ato de guerra se o autor da agressão não for identificado (ONU, 2013; DIPERT, 2010; RID; BUCHANAN, 2015). A própria ONU já declarou que sem o reconhecimento do autor de uma agressão cibernética não há como declarar que foi um ato de guerra (ONU, 2013). E ainda que um país poderoso como os Estados Unidos possa determinar a origem de um ciberataque, é provável que só esse fator não seja suficiente para atribuir o ato de guerra; conforme será

[52]Ataque cibernético de negação de serviço: é uma ação maliciosa que tem como efeito tornar os recursos de um sistema indisponíveis para os seus usuários.
[53] [Tradução própria]. No original, lê-se: "specific exploits that were used, the payload engine, the command infrastructure and targeted data, the reverse engineering analysis, and the raw data of the control networks".

apresentado logo mais, além da atribuição é necessário haver interesse político (RID; BUCHANAN, 2015).

3.3 A MATERIALIDADE DOS ATAQUES CIBERNÉTICOS

A outra característica que dificulta classificar os ciberataques como atos de guerra é o tipo de materialidade que essas agressões resultam (RID, 2012). Diferente dos ataques bélicos, onde há visivelmente "fumaça", ou seja, uma explosão ou bombardeios e até mesmo mortes, nos ataques cibernéticos nem sempre há esse tipo de materialidade (RID, 2012). Em alguns eventos cibernéticos o resultado demora anos para aparecer, como foi o caso do Stuxnet (2009-2010), que ficou oculto durante um ano (ZETTER, 2017) e será analisado no capítulo 3.

Singer e Friedman (2014) esclarecem que nem sempre é possível rastrear o início de um ataque cibernético, pois suas ações no espectro eletromagnético podem ser manipuladas e criptografadas, o que ocasiona a imprecisão de autoria. Os autores explicam que as configurações do ciberespaço permitem que diversos ataques cibernéticos ocorram na obscuridade e destacam que geralmente os resultados dessas incursões são de baixa materialidade, como por exemplo o derrubamento de um site que realiza operações bancárias, ou a interrupção de um portal online que oferece serviços públicos. E no que se refere aos atos de guerra, espera-se que o intentado cause alta materialidade, como grandes explosões e bombardeios que destruam as infraestruturas críticas de um país, como seus aeroportos e suas bases militares (SINGER; FRIEDMAN, 2014).

Assim como Singer e Friedman (2014), Banks (2013) destaca que os efeitos nocivos de um ataque cibernético costumam ocorrer em períodos distintos ao longo do tempo e nem sempre são perceptíveis, pois o dano não é imediato. O autor entende que a invasão de um sistema de rede de conexão pode ser gerenciada por diversos atores cibernéticos que estão sediados em lugares divergentes. Dessa forma, é possível considerar que a baixa materialidade e até a manifestação tardia de um ataque cibernético implica diretamente em caracterizá-los como atos de guerra.

Singer e Friedman (2014) esclarecem que um conflito cibernético deve ter natureza estratégica para ser considerado um ato de guerra, isto é, a agressão cibernética deve ter a finalidade de "atrapalhar a capacidade de outro país de implementar decisões

oficiais, defender-se ou prover serviços para seus cidadãos”[54] (SINGER; FRIEDMAN, 2014, p. 85, tradução própria). Em outras palavras, um ataque cibernético para ter caráter de guerra deve intentar contra alvos que deixam seu oponente fragilizado e vulnerável caso sejam destruídos, como por exemplo as infraestruturas críticas de um Estado.

Singer e Friedman (2014) apontam duas diferenças entre a guerra no espaço cibernético e nos conflitos tradicionais. Na primeira situação, os autores fazem um paralelo com as transformações de guerra que ocorreram com o surgimento dos aviões e consequentemente das agressões que suscitaram no espaço aéreo. Singer e Friedman (2014) explicam que os combates terrestres da Segunda Guerra Mundial causaram uma enorme carnificina, no entanto, com o desenvolvimento dos aviões, a violência das agressões se multiplicou, o espaço aéreo permitiu mais uma via de ataque. Os autores acreditam que na esfera cibernética os atos não terão o mesmo nível de poder destruidor que o espaço aéreo teve. Conforme pontuam, “as agressões cibernéticas terão menos impacto destrutivo a longo prazo”[55] (SINGER: FRIEDMAN, 2014, p. 152, tradução própria). É provável que não ocorra uma guerra cibernética equiparável à Segunda Guerra Mundial, contudo, com as infraestruturas críticas dependendo cada vez mais do espaço cibernético, não se pode excluir a possibilidade de uma guerra altamente destruidora e letal (CLARKE; KNAKE, 2015).

A segunda diferença é a imprevisibilidade que configura os ataques cibernéticos (SINGER; FRIEDMAN, 2014). De acordo com Singer e Friedman (2014), uma arma de guerra tradicional, como uma bomba, tem seus efeitos conhecidos, já no espectro eletromagnético não há exatidão, um vírus de computador não pode ser projetado de forma exata, ou seja, depois que o vírus é instalado em uma rede de conexão, seus efeitos são inesperados. Singer e Friedman (2014) citaram como exemplo uma operação cibernética que ocorreu na Guerra do Iraque (2003-2011). Na ocasião, os oficiais do exército dos Estados Unidos desenvolveram uma operação cibernética ofensiva com o objetivo de destruir uma rede de conexão inimiga, já que o sistema de rede era utilizado para treinar homens bombas (SINGER; FRIEDMAN, 2014). Infelizmente a operação não teve o resultado esperado, o conflito cibernético destruiu 300 redes de conexão que não eram alvos da missão militar e atingiu de forma prejudicial o ciberespaço de diversos países no Oriente Médio e na Europa (SINGER; FRIEDMAN, 2014). Em uma guerra

[54] [Tradução própria]. No original, lê-se: “disrupt another country's ability to implement official decisions, defend itself or provide services to its citizens”.
[55] [Tradução própria]. No original, lê-se: “will have less destructive impact in the long term”.

convencional normalmente as operações militares atacam seus alvos de forma certeira, por mais que haja elementos surpresas, o resultado da incursão já é esperado (CLAUSEWITZ, 1984)

Ao analisar os argumentos de Singer, Friedman (2014) e Banks (2013) é possível observar que as particularidades das agressões cibernéticas atrapalham caracterizá-las como atos de guerra, pois nem sempre o resultado será imediato e o dano dificilmente causará grandes consequências, como a destruição de infraestruturas críticas ou mesmo mortes (SINGER; FRIEDMAN, 2014; BANKS, 2013; RID, 2012). A maioria dos ciberataques possui baixa materialidade, que possivelmente seriam classificados como crimes cibernéticos e não atos de guerra (SINGER; FRIEDMAN, 2014; BANKS, 2013).

Apesar disso, alguns autores já fizeram previsões sobre as consequências que os conflitos cibernéticos podem gerar. Clarke e Knake (2015) salientam que a guerra cibernética como ato de guerra é uma questão de tempo. Para os autores, muitos serviços essenciais são operados progressivamente de forma remota e isso uma hora vai provocar grandes destruições, como o descarrilamento de trens, apagões de energia, até explosões e aterramentos de aviões.

Tabansky (2011) defende que o espaço cibernético possui função com alto potencial de destruição. O autor declara que os ataques cibernéticos podem produzir consequências materiais que resultem em destruições físicas e permanentes dos alvos. Tabansky (2011) classificou algumas possibilidades de destruições materiais iguais a de Clarke e Knake (2015), como a interrupção de sistemas de comunicação, de sistemas bancários, de sistemas de abastecimento de transporte, de sistemas de eletricidade, dentre outras.

O risco é real, alguns conflitos cibernéticos já causaram consequências materiais, como o ataque cibernético que atingiu um dos maiores oleodutos de combustível dos Estados Unidos (NYT, 2021). Em maio de 2021, o oleoduto Colonial Pipeline sofreu uma agressão cibernética, suas redes de computadores corporativas foram atingidas por um *ransomware*, o que levou à interrupção de suas atividades operacionais e prejudicou o abastecimento da Costa do Golfo até o porto de Nova York e os principais aeroportos do estado (NYT, 2021). Os investigadores declararam que a agressão cibernética afetou diretamente os sistemas de controle industrial que regulam o fluxo de petróleo, ou seja, ocasionou um dano físico à uma infraestrutura crítica (NYT, 2021).

O evento cibernético foi assumido pelo grupo russo de *hackers*, o Darkside, que pediu um resgate de 75 bitcoins, o valor equivalente a US$ 5 milhões para que o sistema

de produção da empresa tivesse suas operações restabelecidas (NYT, 2021). O valor foi pago pela Colonial Pipeline e logo suas atividades foram restauradas (NYT, 2021). Nesse caso, pode ser analisado que houve um detrimento material e um prejuízo econômico. Todavia, alguns elementos devem ser destacados, como a imprecisão de autoria, pois não teve como precisar quem eram os atores cibernéticos do Darkside; os investigadores não conseguiram descobrir se os executores agiram de forma autônoma ou se foram patrocinados pela Rússia ou por algum grupo de ativistas ou até mesmo por um grupo de terroristas. Uma outra característica das consequências do ataque cibernético foi a materialidade, isto é, embora o ato tenha causado dano físico, não resultou em uma grande explosão ou em bombardeios, e nem mesmo houve mortes (SINGER; FRIEDMAN, 2014).

Portanto, pode ser constatado que sim, conflitos cibernéticos podem acarretar consequências desastrosas (materialidade), como por exemplo a destruição de infraestruturas críticas e até mesmo em letalidade. Todavia, enquanto um ataque cibernético não possuir materialidade que ameace a Segurança e Defesa de um Estado, não interfira na manutenção da paz mundial, não seja violento, não tenha a sua autoria confirmada e não tenha propósito político, dificilmente será considerado um ato de guerra.

3.4 A CARÊNCIA DE DEFINIÇÃO LEGAL AOS CONFLITOS CIBERNÉTICOS

Não há leis específicas no Direito Internacional sobre a guerra cibernética (FERNANDES, 2012; AYRES; GRASSI, 2020). Dessa forma, não há como punir os atores cibernéticos maliciosos, o cenário enseja insegurança jurídica (FERNANDES, 2012). A primeira vez que um conflito cibernético foi levado às instituições de segurança internacional, nesse caso a OTAN, para ser classificado como ato de guerra, foi em 2007, na Estônia (LOBATO; KENKEL, 2015). Nessa época, o ciberespaço do país estoniano acabara de sofrer múltiplos ataques cibernéticos de negação o que "resultou em uma série de 'robôs' que capturaram mais de um milhão de computadores em 75 países"[56] (SINGER; FRIEDMAN, 2014, p. 141, tradução própria).

Após o ocorrido, a Estônia acusou a Rússia de ser a executora dos ciberataques e declarou que a incursão cibernética teria sido um ato de guerra (BLANK, 2017). A partir

[56] [Tradução própria]. No original, lê-se: "resulted in a series of bonets that captured over a million computers in 75 countries".

desse contexto, o governo estoniano invocou o artigo 5º do Tratado da OTAN[57] (OTAN, 1949). Por conseguinte, a Aliança Militar enviou à Estônia alguns investigadores para avaliar a situação (BLANK, 2017). E, por fim, a OTAN concluiu que o evento cibernético não seria ato de guerra (BLANK, 2017). Na visão da instituição, o país sofreu "apenas" consequências no espectro eletromagnético estoniano, não houve mortos ou feridos e nem infraestruturas críticas foram bombardeadas ou destruídas (SINGER; FRIEDMAN, 2014; BLANK, 2017).

O evento cibernético da Estônia inaugurou as discussões de líderes políticos e especialistas em guerra cibernética sobre uma guerra real no ciberespaço (SINGER; FRIEDMAN, 2014). Singer e Friedman (2014) explicam que o evento cibernético na Estônia "mostra o que vai e o que vem que toma lugar entre leis antigas e tecnologias novas, em especial quando chega-se à questão de o que se constitui um ato de guerra na esfera cibernética"[58] (SINGER; FRIEDMAN, 2014, p. 142, tradução própria). Isto significa que as leis internacionais que, atualmente, regem acerca da guerra estão defasadas. Conforme visto no capítulo um, as últimas normas de guerra foram constituídas em 1945 e 1949, quando o espaço cibernético não existia, as circunstâncias eram diferentes, o tipo de guerra era outro (SINGER; FRIEDMAN, 2014).

Singer e Friedman (2014) afirmam que os conflitos evoluíram desde a criação das normas internacionais, é provável que as leis estejam defasadas aos conflitos do século XXI. Os autores explicam que esse cenário interfere na classificação dos ataques cibernéticos entre atores estatais e não estatais, pois não há um respaldo legislativo que baseia os conflitos cibernéticos. As normas da OTAN e da ONU sofreram poucas modificações desde que foram criadas e nenhuma dessas alterações se refere à guerra cibernética (SINGER; FRIEDAMAN, 2014).

Conforme Singer e Friedman (2014), após o caso da Estônia (2007), alguns professores decidiram desenvolver o Manual de Tallin[59] para analisar se as leis estabelecidas pelas instituições de Segurança e Defesa Internacional abraçariam os ataques cibernéticos. No entanto, não houve e não há um consenso entre os Estados sobre

[57] O artigo 5º do Tratado do Atlântico Norte requer que os Estados-membros auxiliem qualquer membro que esteja sujeito a um ataque armado. É um princípio de Defesa Coletiva.
[58] [Tradução própria]. No original, lê-se: "shows what comes and goes that takes place between old laws and new technologies, especially when it comes to the question of what constitutes an act of war in the cyber sphere".
[59] Manual de Tallinn: É um conjunto de normas e regras, não vinculativo, que versa sobre a aplicabilidade da lei internacional na resolução de ciber-conflitos.

o Manual de Tallin, algumas nações não se mostraram entusiasmadas (SINGER; FRIEDMAN, 2014). O manual não tem validade legal (SINGER; FRIEDMAN, 2014).

Em uma tentativa de compreender os eventos cibernéticos como atos de guerra ou não, Singer e Friedman (2014) analisaram por analogia as leis internacionais dos conflitos armados. A primeira questão apresentada foi observar os resultados que as agressões cibernéticas poderiam gerar, por exemplo, se uma incursão cibernética causar destruição e morte, é possível que se configure em um ato de guerra (SINGER; FRIEDMAN, 2014). Já o segundo elemento a ser suscitado seria examinar se o ataque cibernético possui objetividade e mensurabilidade, ou seja, "deve existir uma ligação direta e pretendida entre causa e efeito"[60] (SINGER; FRIEDMAN, 2014, p. 144, tradução própria). Os autores apontam que esse último fator é fundamental para diferenciar atos de guerra de atos de espionagem, de sabotagem e subversão.

Tal como Singer e Friedman (2014), Banks (2013) argumenta que as normas internacionais estão ultrapassadas aos conflitos não convencionais do século XXI; e mesmo que o uso desse novo domínio operacional, que é o ciberespaço, esteja em crescente movimentação e evolução, ainda não há leis que definam a guerra cibernética. Banks (2013) destaca que é importante às instituições de segurança internacional se posicionarem de forma consensual a respeito dos conflitos cibernéticos, pois assim o mundo estaria mais seguro, não só ao que pode se tornar atos de guerra, mas aos atos de terrorismo também.

No mesmo raciocínio de Singer e Friedman (2014), Banks (2013) acredita que para analisar um evento cibernético como um ato de guerra é preciso observar quais foram as consequências da ação cibernética. Banks (2013) crê que os ciberataques serão ancorados pela ONU e pela OTAN quando "um ataque cibernético causar destruição física e/ou baixas em um nível significativo"[61] (BANKS, 2013, p. 162, tradução própria). Todavia, o autor declara que usar as normas da ONU e da OTAN por analogia aos conflitos cibernéticos enseja alguns desafios, como o problema de atribuição e o ato de força. Banks (2013) compreende que há um longo caminho normativo para a guerra cibernética.

[60] [Tradução própria]. No original, lê-se: "there must be a direct and intended link between cause and effect".
[61] [Tradução própria]. No original, lê-se: "a cyber attack causes physical de- struction and/or casualties at a significant level, a cyber intrusion may con- stitute an "armed attack"".

Ayres e Grassi (2020) concordam com Banks (2013) e Singer e Friedman (2014) no que diz respeito à ausência de leis internacionais acerca dos eventos cibernéticos. As autoras compreendem ser difícil escrever normas e tratados de Segurança Internacional sobre a guerra cibernética pois o ciberespaço possui características peculiares que interferem na criação legislativa. Por exemplo, no espectro eletromagnético não há certeza de autoria; o ato de força no ciberespaço não é físico; dificilmente é possível precisar o início de uma ação cibernética; não existe demarcação geográfica do espaço cibernético, dentre outras (SINGER; FRIEDMAN, 2014; LIBICKI, 2009). Todas essas nuances são relevantes para o desenvolvimento de leis internacionais (AYRES; GRASSI, 2020; BANKS, 2013).

Apesar disso, Ayres e Grassi (2020) ressaltam que muitos Estados desenvolveram suas próprias normas no que concerne à guerra cibernética. Os Estados Unidos foi um dos primeiros países a desenvolver leis de Segurança e Defesa Cibernética (SINGER; FRIEDMAN, 2014). Em 2011, o governo dos Estados Unidos criou suas Estratégias de Defesa Cibernética e em 2017 atualizou as leis, o presidente Tump informou em uma coletiva de imprensa que a partir de 2018 o país norte-americano iria realizar de forma progressiva operações cibernéticas ofensivas (EUA, 2011; EUA, 2017).

No Brasil, em 2008, foi criada a Estratégia Nacional de Defesa, desde então, normas de Segurança e Defesa Cibernética passaram a ser desenvolvidas (BRASIL, 2008). O conflito cibernético é validado pela doutrina brasileira, conforme consta na Doutrina Militar de Defesa Cibernética (2014, p. 19), a guerra cibernética "corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de comando e controle do adversário".

No que tange à atribuição do ato de guerra nas intercorrências cibernéticas, não existem normas brasileiras (BRASIL, 1988). A declaração de guerra no Brasil é normatizada pelo artigo 84 da Constituição Federal, e não faz referência aos conflitos cibernéticos (BRASIL, 1988). A lei informa que apenas o presidente do país poderá declarar guerra, e só transcorrerá mediante a autorização do Congresso Nacional (BRASIL, 1988). Outros Estados também possuem suas próprias normas de Segurança e Defesa Cibernética, como a Inglaterra, a Argentina e a Rússia.

Apesar das normas individuais dos países, Fernandes (2012) entende que a definição legal pelas instituições internacionais em relação à ciberguerra é necessária, pois é só por meio dessa base legal internacional que será possível determinar onde um ataque cibernético se encontra e se possui elementos imprescindíveis para ser um ato de

guerra. O autor compreende que a normatização dos conflitos cibernéticos trará não apenas segurança jurídica, mas será um fator decisório no âmbito político, pois a classificação das ações cibernéticas pelas instituições de Segurança Internacional contribuirá em como os Estados devem prosseguir caso sejam atacados ciberneticamente.

Nesse sentido, Dipert (2010) levanta algumas observações sobre a moralidade da guerra cibernética. O autor ilustra que sem uma definição legal algumas questões são suscitadas, como bem descreveu:

> 1. Um ataque cibernético é moralmente justificado em resposta a um ataque convencional inimigo?
> 2. Um ataque cibernético é moralmente justificado em resposta a um ataque cibernético inimigo?
> 3. Um ataque convencional é moralmente justificado por um ataque cibernético inimigo?
> 4. Um ataque cibernético é moralmente justificado nos casos em que o inimigo não lançou um ataque cibernético nem um ataque convencional? (Como um tipo de sanção das Nações Unidas, preventivamente, ou preventivamente por algum outro motivo.)
> 5. Uma vez iniciada uma guerra (cibernética ou convencional), que tipos de ciberataques são moralmente justificados? (DIPERT, 2010, p. 392, tradução própria)[62]

Em referência às perguntas 1 e 2, Dipert (2010) compreende que desferir um ataque cibernético como forma de retaliação em uma situação de conflito convencional ou não convencional pode ser justificado moralmente, principalmente no que concerne à pergunta 1, pois um ataque convencional geralmente tem a "aparência" mais violenta do que um ciberataque. Desta maneira, o autor explica que seria compreensível respondê-la com incursões cibernéticas. Contudo, Dipert (2010) argumenta que outros fatores precisam ser levados em consideração, como por exemplo a proporcionalidade do intento e a probabilidade de eficácia.

Nas questões 3 e 4, Dipert (2010) acredita que são casos mais difíceis de responder. No caso 3, o autor explica que existem algumas ponderações que precisam ser debatidas, como a questão da proporcionalidade, já que escolher um ataque convencional como resposta talvez seja uma opção desmedida em relação aos ataques cibernéticos; a segunda incerteza seria em decorrência da imprecisão de autoria que configura os eventos

[62] [Tradução própria]. No original, lê-se: "1. Is a cyberattack ever morally justified in response to an enemy conventional attack?
2. Is a cyberattack ever morally justified in response to an enemy cyberattack?
3. Is a conventional attack ever morally justified by an enemy cyberattack?
4. Is a cyberattack ever morally justified in cases where the enemy has launched neither a cyber- nor a conventional attack? (With United Nations sanction, preemptively, preventively, or for some other reason.)
5. Once a war (cyber- or conventional) has begun what kinds of cyberattacks are morally justified?".

cibernéticos. Na pergunta 4, Dipert (2010) argumenta que lançar um ataque cibernético preventivo poderia ser perigoso, visto que não há tanto esclarecimento sobre o assunto, no entanto, caso a incursão cibernética não cause destruições e nem mortes, talvez seja justificada a sua utilização de forma preventiva.

Na última pergunta, a 5, Dipert (2010) argumenta que uma nação que sofreu ataques cibernéticos poderia retaliar da mesma forma, isto é, desferir ataques cibernéticos. O autor analisa que nesse enredo, a agressão seria justificada pelas normas internacionais; ou ainda, por exemplo, uma nação que sofreu um ataque convencional poderia retaliar por meio de ciberataques, esse quadro hipotético também seria justificável. Apesar disso, Dipert (2010) faz uma ressalva para essa última indagação. O autor elucida que critérios de proporcionalidade e de probabilidade de sucesso também devem ser apreciados nessa situação. Todos esses panoramas poderiam ser respondidos com precisão caso houvesse um posicionamento legal das instituições de segurança internacional (DIPERT; 2010; AYRES; GRASSI, 2020; FERNANDES, 2012).

Contudo, Ayres e Grassi (2020) supõem que a ausência de normas internacionais parece ser proposital, pois assim os "Estados poderão utilizar-se desse meio para atingir seus objetivos no espaço interacional" (AYRES; GRASSI, 2020, p. 116). As autoras acrescentam que a falta de normas acerca das agressões cibernéticas no advento do espaço cibernético favorece o crescimento de ataques cibernéticos realizados por Estados mais tecnológicos e desenvolvidos.

À face do exposto, pode ser compreendido duas frentes, 1) sem o amparo legal das instituições internacionais, não há como classificar os conflitos cibernéticos; 2) mesmo que essa situação gere insegurança jurídica, talvez não tenha interesse das instituições de Segurança Internacional em legislar a respeito do ciberespaço, não apenas em considerar os ataques cibernéticos como atos de guerra, mas também aos atos cibernéticos de espionagem, sabotagem etc. Perante esse contexto, é possível concluir que o desenvolvimento de normas no tocante das ações cibernéticas seja iniciado apenas quando ocorrer uma agressão cibernética que resulte em grandes destruições e até mesmo em letalidade.

3.5 A AUSÊNCIA DE VONTADE POLÍTICA EM CLASSIFICAR AS AGRESSÕES CIBERNÉTICAS COMO ATOS DE GUERRA

Antes de iniciar o debate em relação ao interesse político nas agressões cibernéticas, é preciso lembrar o conceito de guerra explicado no primeiro capítulo. Foi analisado que um conflito precisa ser subordinado à política para ser classificado como um ato de guerra. Desse modo, compreende-se que caso haja vontade política de um líder de Estado declarar guerra perante uma agressão cibernética, assim ocorrerá (SINGER; FRIEDMAN, 2014; GOMES; ALVES, 2020). Embora a imprecisão de autoria, a baixa materialidade e a ausência de definição legal impliquem a atribuição do ato de guerra nos ciberataques, talvez seja a falta de vontade política o principal fator que leve os eventos cibernéticos não serem considerados atos de guerra.

De acordo com Libicki (2009), existem três possibilidades para uma agressão cibernética ser considerada um ato de guerra: a universal, a multilateral e a unilateral. A primeira característica, a universal, ocorreria quando houvesse a aceitação mundial dos Estados em caracterizar os eventos cibernéticos como possíveis atos de guerra. Não "só" dos Estados, mas também da ONU, pois é uma instituição de segurança internacional, a sua influência é mundial. Na segunda performance, a multilateral, as agressões cibernéticas seriam reconhecidas como atos de guerra quando um grupo relevante de Estados assim declarasse, por exemplo a OTAN. Por último, na forma unilateral, caso um ataque cibernético possuísse determinados elementos, como a identificação do ator cibernético, traços de violência que resultassem em destruição de infraestruturas críticas ou em letalidade, ou seja, ameaçasse a paz e a soberania de uma nação, poderiam então ser um ato de guerra. Nesse último caso, qualquer Estado poderia declarar unilateralmente que sofreu ou desferiu um ato de guerra cibernético, bastaria existir vontade política (LIBICKI, 2009).

Como forma de exemplo da possibilidade multilateral, Libicki (2009) cita o caso da Estônia (2007), visto no capítulo dois. O autor argumenta que na ocasião o país estoniano acusou a Rússia de ser a autora dos embates cibernéticos e declarou que o país russo havia cometido um ato de guerra. Por fazer parte da Aliança Militar, a Estônia invocou o princípio da defesa coletiva e solicitou que a OTAN declarasse guerra contra a Rússia (NYT, 2007; SINGER; FRIEDMAN, 2014). No entanto, a OTAN não quis declarar guerra, não teve vontade política (NYT, 2007; SINGER; FRIEDMAN, 2014). Nesse contexto, caso a "OTAN tivesse declarado que o ataque foi acionável, poderia ter servido como um aviso para os Estados"[63] (LIBICKI, 2009, p. 179, tradução própria).

[63] [Tradução própria]. No original, lê-se: "Had NATO declared that the attack was actionable, it might have served as a warning to potential attacking states".

Quer dizer, se porventura o episódio fosse considerado um ato de guerra pela OTAN, a situação ensejaria um precedente para os Estados declararem guerra (LIBICKI, 2009). O autor conclui que um ataque cibernético será considerado um ato de guerra caso haja vontade política, isto é, se um Estado assim declarar.

Apesar disso, Mazarr (2015) e Wirtz (2017) argumentam que desde o fim da Guerra Fria (1947-1989) o interesse político dos Estados em entrar em guerra se transformou. Os autores explicam que após a tensão geopolítica entre os Estados Unidos e a União Soviética e seus respectivos aliados, os Estados se tornaram cada vez mais interdependentes economicamente (WIRTZ, 2017; MAZARR, 2015). Nesse sentido, quando há um conflito armado em ação, a tendência é que os impactos da guerra atinjam todos os Estados (WIRTZ, 2017; MAZARR, 2015). Logo, Wirtz (2017) e Mazarr (2015) pontuam que é preferível o Estado se manter em uma zona de conflito abaixo da guerra, a zona cinzenta, para se obter algum acordo político do que declarar guerra.

Por exemplo, no ano de 2022, a Rússia entrou em guerra contra a Ucrânia, e no decorrer desse conflito já é possível observar uma série de efeitos colaterais (NYT, 2022). Como forma de punição, diversos países impuseram sanções à Rússia, como os Estados Unidos que restringiram à compra de petróleo, de diamante e de vodca russos (NYT, 2022). Esses embargos prejudicam não só a economia da Rússia, mas de diversos países (NYT, 2022). Em resposta, a Rússia cortou a distribuição de gás à Europa, isso fez o preço do gás no continente europeu disparar (THE GUARDIAN, 2022). A guerra não impacta "apenas" a economia mundial, nesse caso, há o repentino fluxo migratório de refugiados da Ucrânia que afeta os países vizinhos, já que mais de 2,5 milhões de pessoas deixaram o território ucraniano; além das mortes que acontecem diariamente, mais de 500 civis ucranianos foram mortos e milhares de militares também morreram[64] (NYT, 2022).

Mazarr (2015) explica que em razão dessas peculiaridades negativas da guerra, o que se tem visto no século XXI é um aumento progressivo de conflitos não convencionais, como a realização de operações cibernéticas militares. Como não existem normas internacionais que definem a guerra cibernética, os líderes dos Estados se utilizam dessa performance alternativa para atacar os seus inimigos (MAZARR, 2015; WIRTZ, 2017). Como bem citou Clausewitz (1984), o objetivo de uma agressão é fazer com que o inimigo exerça a "sua" vontade. Desse modo, caso um Estado consiga atingir a sua finalidade por meio de um conflito cibernético e não precise declarar guerra, é provável

[64] Não há um número certo e nem confiável no que se refere às mortes dos combatentes russos e ucranianos (NYT, 2022).

que a opção escolhida seja a de iniciar uma operação cibernética ofensiva, e assim se abster dos efeitos colaterais de uma guerra convencional (MAZARR, 2015; WIRTZ, 2017).

Contudo, não é porque até o momento nenhum conflito cibernético foi considerado um ato de guerra, que nunca será. Singer e Friedman (2014) acreditam que se um líder político, juntamente com seu governo, tiver vontade política de declarar guerra perante uma agressão cibernética, o evento não convencional será caracterizado um ato de guerra. Os autores citaram Clausewitz para defender o argumento: "a guerra não é um fenômeno independente, mas sim a continuação da política por meios diferentes"[65] (CLAUSEWITZ, 1984, p. 6, tradução própria). Em outras palavras, como toda guerra advém de um conflito político, onde cada oponente tenta impor a sua vontade, caso um Estado compreenda que um ataque cibernético é um ato de guerra, poderá assim ser considerado (LIBICKI, 2009; SINGER; FRIEDMAN, 2014).

No entanto, importa salientar que não é qualquer vontade política que caracterizaria um conflito cibernético como um ato de guerra. É preciso levar a assimetria de poder entre os Estados em consideração quando se refere ao interesse político na guerra cibernética (WALTZ, 2002; ARON, 2002; NYE, 2010). Nem todo país tem ou terá domínio do poder cibernético, apenas grandes potências, como os Estados Unidos e o Reino Unido, que possuem grandes tecnologias para expressar suas vontades políticas no que tange às agressões cibernéticas (WALTZ, 2002; ARON, 2002; NYE, 2010). À vista disso, não basta existir vontade política em declarar guerra, é preciso que o Estado possua capacidades de projetar o poder militar, o poder econômico e no caso da guerra cibernética, o poder cibernético (WALTZ, 2002; ARON, 2002; NYE, 2010; SINGER; FRIEDMAN, 2014). Portanto, o Estado deve ser capaz de empreender operações cibernéticas ofensivas no ciberespaço e impor-se pela força sobre quaisquer adversários.

Desse modo, ao analisar os posicionamentos aqui citados, entende-se que a falta de interesse político talvez seja o elemento primordial para que as agressões cibernéticas não sejam consideradas atos de guerra. Conforme Gomes e Alves (2020, p. 236) explicam, "no final do dia, é o líder político quem decide se uma ação levará à guerra ou não". Isso significa que quem irá decidir ir à guerra perante um ataque cibernético que tenha causado danos em infraestruturas críticas ou até mesmo mortes é o Estado que, por

[65] [Tradução própria]. No original, lê-se: "war is not an independent phenomenon, but the continuation of politics by different means".

meio de seus avanços tecnológicos, consegue demonstrar domínio cibernético (poder cibernético) contra seus inimigos.

4 ANÁLISE DE EVENTOS CIBERNÉTICOS

No capítulo dois expandiu-se o problema de pesquisa da dissertação, que era compreender por que, até hoje, nenhum ataque cibernético foi considerado um ato de guerra. Para ilustrar a abrangência e as complexidades das premissas que dificultam atribuir o ato de guerra nos conflitos cibernéticos, que são: a imprecisão de autoria, a falta de definição legal, a baixa materialidade e a falta de interesse político serão analisadas neste capítulo alguns eventos cibernéticos.

As agressões cibernéticas que serão explicadas neste capítulo são: os casos em que a Rússia foi acusada informalmente de ter desferido agressões cibernéticas contra Estados - Estônia em 2007, Geórgia em 2008, e Ucrânia em 2014-2015; o ataque cibernético contra a Usina Nuclear de Natanz, conhecido como Stuxnet (2009-2010); a agressão cibernética à infraestrutura crítica do Irã realizado pelos Estados Unidos, na gestão do presidente Trump, em julho de 2019 (WASHIGTON POST, 2019; YAHOO NEWS, 2019).

Posto isto, antes de estudar os ataques cibernéticos, é preciso lembrar algumas definições apresentadas no capítulo 1. Primeiro, uma guerra sempre será subordinada à política (CLAUSEWITZ, 1984; MEI, 2018). Segundo ponto, o ato de guerra é uma agressão que independe de uma declaração formal e pode ser realizada por atores estatais ou não estatais. Por fim, um ataque será um ato de guerra quando seus resultados causarem impactos à soberania de um Estado e à Segurança Internacional e, portanto, afetar a manutenção da paz mundial (DINSTEIN, 2003; ONU, 1945; OTAN, 1949; MEI, 2018).

4.1 CONFLITOS CIBERNÉTICOS EM QUE A RÚSSIA FOI ACUSADA INFORMALMENTE DE SER A AUTORA DO ATO

De acordo com Gomes e Alves (2020, p.244), “após a dissolução da União Soviética [1991], o governo russo valeu-se dos ‘conflitos congelados’ para manter uma força de tração sobre as antigas repúblicas soviéticas, evitando que elas abandonassem sua zona de influência”. Isto é, o governo russo passou a apoiar os grupos minoritários russos que residem nos países vizinhos, como a Estônia, a Geórgia e a Ucrânia, para realizarem movimentos separatistas (GOMES; ALVES, 2020).

Os episódios de tensão política entre a Rússia e a Estônia (2007), a Geórgia (2008) e a Ucrânia (2014-2015) foram precedidos por uma série de confrontos, como por exemplo, invasão territorial, propagação de desinformação, conflitos armados e ataques cibernéticos (GOMES; ALVES, 2020; BLANK, 2017). Conforme será analisado a seguir, em relação aos conflitos cibernéticos, apesar das evidências encontradas acerca da vinculação da Rússia nas incursões cibernéticas, o governo russo negou qualquer tipo de participação nos atos (SEGAL, 2016).

4.1.1 Estônia – 2007

Em 27 de abril de 2007, o governo estoniano decidiu mover a estátua de bronze de um soldado soviético que ficava no centro da cidade de Tallinn, a capital da Estônia, para um cemitério militar (BLANK, 2017). A estátua representava e homenageava os soldados soviéticos-russos que participaram da libertação da Estônia da Alemanha nazista na Segunda Guerra Mundial (THE GUARDIAN, 2007; LIBICKI, 2009; SINGER; FRIEDMAN, 2014).

A retirada da estátua foi vista pela Rússia como uma afronta, além da simbologia vinculada à imagem, o caso ocorreu às vésperas do dia em que a Rússia celebraria a vitória contra a política fascista da Alemanha nazista (DAFLON, 2020). A Rússia declarou que o ato foi um desrespeito com os cidadãos russos residentes na Estônia (DAFLON, 2020). De acordo com Daflon (2020, p. 13), "a remoção da estátua ocorreu em 27 de abril de 2007, e desencadeou uma série de protestos de etnia russa na Estônia, resultando na prisão de aproximadamente 1.300 pessoas e algumas mortes".

Subsequente às manifestações, iniciou-se uma sequência de ataques cibernéticos contra o espaço cibernético da Estônia (LIBICKI, 2009; BLANK, 2017). Eram ciberataques de *DDos*, isto é, um "ataque de negação" que impede a distribuição de serviço, é um tipo de agressão cibernética que bloqueia e interrompe a funcionalidade de uma rede ou de um site (THE GUARDIAN, 2007; NYT, 2007; BLANK, 2017). Esses atentados cibernéticos paralisaram a infraestrutura de tecnologia e comunicação da Estônia, causaram a obstrução de diversos sites governamentais, desestabilizaram as operações do maior banco do país e afetaram os portais dos principais jornais do país (THE GUARDIAN, 2007; NYT, 2007; BLANK, 2017).

Os conflitos cibernéticos duraram três semanas (NYT, 2007). Nas primeiras agressões, uma avalanche de mensagens foi direcionada ao servidor de e-mails do parlamento que, de imediato, parou de funcionar (THE GUARDIAN, 2007; NYT, 2007; BLANK, 2017). Em outro momento, os *hackers* invadiram o portal do Partido Reformista da Estônia e publicaram uma mensagem falsa, se passando pelo primeiro-ministro da época, Andrus Ansip (BLANK, 2017). O conteúdo da carta era um suposto pedido de desculpas à Rússia por ordenar a retirada da estátua (THE GUARDIAN, 2007; NYT, 2007; BLANK, 2017).

Nesse momento, Hillar Aarelaid, diretor da Equipe de Resposta a Emergências de Computadores da Estônia, reuniu especialistas em segurança cibernética de diversos setores de atuação na Estônia e solicitou ajuda de vários contatos de outros países, como Filândia, Alemanha e Eslovênia, com o objetivo de rastrear e bloquear os endereços de internet suspeitos e então cessar o tráfego de computadores que estavam atentando contra a Estônia (NYT, 2007; THE GUARDIAN, 2007).

Aarelaid e os especialistas se depararam não só com ataques de *DDos*, mas com ataques de recusa de serviço por difusão, que consistia em bombardear os sites da Estônia com dados que obstruíam os servidores do país, os seus roteadores e as chaves de codificação (NYT, 2007). Isto causou o congestionamento no tráfego das redes; os serviços que dependiam do ciberespaço foram paralisados (NYT, 2007; THE GUARDIAN, 2007). Além dessas duas técnicas, os *hackers* infiltraram no espectro eletromagnético estoniano vários *softwares*[66] conhecidos como *bots*, essas incursões se apossaram dos computadores, como soldados involuntários ou "zumbis" e tiraram o controle da Estônia sobre seus próprios servidores (NYT, 2007; THE GUARDIAN, 2007).

Mas o pior estava por vir, no dia 9 de maio de 2007: no Dia da Vitória, data em que a Rússia comemora a derrota da Alemanha nazista pela União Soviética, uma enxurrada de ciberataques invadiu o espaço cibernético da Estônia e no dia 10 de maio de 2007, o banco Hansabank foi obrigado a fechar o acesso de suas operações, pois só assim conseguiria conter a incursão (NYT, 2007; THE GUARDIAN, 2007). A ação de defesa do banco conseguiu impedir o acesso de mais de 300 endereços de internet suspeitos,

[66] Software: é uma sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas. Também pode ser definido como os programas que comandam o funcionamento de um computador.

todavia, com a paralisação das atividades bancárias, a instituição teve um prejuízo econômico de quase US$ 1 milhão de dólares (NYT, 2007; THE GUARDIAN, 2007).

No final do dia 10 de maio de 2007, a defesa da Estônia conseguiu frear as invasões. Essa performance só foi alcançada com a mesma atitude defensiva operada na instituição bancária, que consistiu em bloquear o acesso de fora do país aos serviços online estonianos (NYT, 2007; THE GUARDIAN, 2007). Esse movimento ocasionou desastrosas consequências, por exemplo: executivos estonianos que operavam fora do país não conseguiram acessar seus e-mails por mais de quatro dias e vários negócios foram afetados (NYT, 2007; THE GUARDIAN, 2007).

Os ciberataques ocorreram até o dia 18 de maio de 2007 (NYT, 2007; THE GUARDIAN, 2007). Os investigadores não puderam afirmar a autoria do ato, no entanto, foram encontrados em algumas redes sociais de bate-papo, mensagens em russo que continham instruções de como atacar ciberneticamente o espectro eletromagnético estoniano (NYT, 2007; THE GUARDIAN, 2007). Na época, o ministro da Defesa da Estônia, Aaviksoo, declarou que "no momento, não somos capazes de provar ligações diretas com o Estado [Rússia]"[67] (NYT, 2007, tradução própria), e por fim afirmou que "tudo o que podemos dizer é que um servidor no escritório do nosso presidente recebeu uma consulta de um endereço de IP[68] na administração russa. É um fato que temos em nossos registros de dados"[69] (NYT, 2007, tradução própria). Um representante do governo russo, Dmitri Peskov, negou qualquer envolvimento do Estado nos ataques cibernéticos; a Rússia não se dispôs a ajudar nas investigações (NYT, 2007; THE GUARDIAN, 2007). O caso da Estônia se tornou o primeiro conflito cibernético notório (SINGER; FRIEDMAN, 2014).

Conforme citado anteriormente, após o ocorrido, o ministro do Exterior da Estônia invocou o artigo 5º do Tratado da Aliança Militar, isto é, acusou que o ataque seria um ato de guerra praticado pela Rússia e requereu a ajuda da OTAN, com o argumento de que a segurança nacional e a soberania estoniana estavam em perigo (SINGER; FRIEDMAN, 2014). A OTAN enviou especialistas em segurança cibernética à Estônia para verificar os danos que os ciberataques causaram e concluíram que não se enquadravam em um ato de guerra e nem confirmaram que as ações cibernéticas foram

[67] [Tradução própria]. No original, lê-se: "at the moment, we are not able to prove direct links to the state".
[68] IP – Internet Protocol, que significa, endereço do protocolo de internet. Um endereço IP identifica uma rede ou dispositivo na internet.
[69] [Tradução própria]. No original, lê-se: "all we can say is that a server in our president's office received a query for an IP address in the Russian administration. It's a fact that we have in our logs".

orquestradas pela Rússia (LIBICKI, 2009; SINGER; FRIEDMAN, 2014). Apesar dos indícios da Rússia estar vinculada ao evento, ninguém foi punido (SINGER; FRIEDMAN, 2014; LIBICKI, 2009). O conflito cibernético levou a OTAN a criar o Centro de Excelência para a Cooperação em Ciberdefesa (2008) em Tallinn (SINGER; FRIEDMAN, 2014). A CCDCOE tem como missão: "apoiar nossos países membros e a OTAN com experiência interdisciplinar única no campo de pesquisa, treinamento e exercícios de defesa cibernética cobrindo as áreas de foco de tecnologia, estratégia, operações e direito"[70] (CCDCOE, 2022, tradução própria).

Ao examinar o incidente explorado acima, pode ser constatado que os especialistas em segurança e defesa não sabiam como proceder (BLANK, 2017). De acordo com Fitton (2016, p. 115-116, tradução própria), "as questões que envolvem a atribuição de operações cibernéticas e a negação projetada por parte dos adversários restringem drasticamente a capacidade da OTAN de responder as operações cibernéticas"[71]. Há um crescente números de adversários da OTAN que operam de forma ofensiva no ciberespaço, todavia, confirmar o inimigo ainda é um desafio para a Aliança Militar (FITTON, 2016). Por fim, conclui-se que sem a identificação dos atores cibernéticos, a OTAN não pôde atribuir o ato de guerra nos ciberataques à Estônia.

Além da incerteza de autoria, a falta de definição legal gerou insegurança jurídica para a OTAN classificar o conflito cibernético (SINGER; FRIEDMAN, 2014; BLANK, 2017). Era a primeira vez na história que ocorria um ataque cibernético naquelas proporções, os especialistas da OTAN não conseguiram de imediato afirmar que o evento cibernético seria um ato de guerra ou não, a OTAN enviou investigadores especializados em segurança cibernética para avaliar os ciberataques e apenas em outubro de 2008, ou seja, um ano após o embate cibernético, chegaram à conclusão de que os atos cibernéticos não seriam considerados atos de guerra (NYT, 2008). Isso mostra que a falta de definição legal dificultou a classificação do atentado cibernético contra a Estônia; gerou insegurança jurídica.

No quesito da materialidade, observa-se que a intercorrência cibernética na Estônia não ocasionou bombardeios, mortes ou destruições de estrutura físicas, como de aeroportos e de hidrelétricas, que é o que geralmente ocorre em uma guerra (SINGER;

---

[70] [Tradução própria]. No original, lê-se: "support our member countries and NATO with unique interdisciplinary expertise in the field of cyber defense research, training and exercises covering the focus areas of technology, strategy, operations and law."

[71] [Tradução própria]. No original, lê-se: "which involvement of complex issues and operations operations like cyber a part of complex issues and operations operations cyber".

FRIEDMAN, 2014). A materialidade dos ataques cibernéticos à Estônia foi caracterizada pela destruição de sites e interrupções de alguns serviços, como as operações bancárias que dependiam do espectro eletromagnético para funcionar (NYT, 2007). Nessa questão, a OTAN verificou que não havia materialidade o bastante para classificar a agressão cibernética como ato de guerra (LIBICKI, 2009; SINGER; FRIEDMAN, 2014).

No entanto, alguns especialistas como Singer e Friedman (2014) e Blank (2017) consideram que a OTAN não quis enfrentar uma guerra com a Rússia e por esse fundamento, não teve vontade política dos líderes da Aliança Militar em declarar guerra contra o governo russo. Apenas em 2016 a OTAN passou a considerar o espaço cibernético como um domínio operacional de guerra, ou seja, quase nove anos depois da agressão cibernética na Estônia (OTAN, 2016; SINGER; FRIEDMAN, 2014; BLANK, 2017). Nesse contexto, verifica-se que, naquele momento, faltou interesse político da OTAN em declarar guerra contra a Rússia.

4.1.2 Geórgia – 2008

A Guerra Russo-Georgiana (2008) originou-se a partir de um conflito que ocorreu entre a Geórgia e a Ossétia do Sul, nos anos de 1991 e 1992 (YAKEMTCHOUK, 2008). Nesse combate, um pouco mais da metade da Ossétia do Sul ficou sob o controle da Rússia; já a outra parte seguiu sendo controlada pela Geórgia (YAKEMTCHOUK, 2008). Após o fim desse evento, a Rússia se manteve presente na Geórgia e não retirou totalmente suas tropas da região; essa decisão ensejou sucessivos embates entre a Rússia e a Geórgia (YAKEMTCHOUK, 2008).

A Revolução das Rosas (2003) foi um desses episódios conflituosos. Na ocasião, os georgianos reivindicaram a saída do presidente Eduard Shevardnadze da Geórgia, pois o líder político simpatizava com os pensamentos separatistas pró-russos (YAKEMTCHOUK, 2008; MAYNARD, 2018). Com a derrubada de Shevardnadze, as eleições foram antecipadas, e assim, em janeiro de 2004, Mikheil Saakashvili se tornou o novo presidente da Géorgia e logo adotou uma postura de proximidade com a OTAN (YAKEMTCHOUK, 2008; MAYNARD, 2018). Saakashvili também autorizou a construção do oleoduto Bacu-Tiblíssi-Ceyhan-BTC; a infraestrutura crítica passaria pela Geórgia para transportar petróleo do Azerbaijão para a Europa, todavia, uma parte do oleoduto cortaria o território da Rússia (YAKEMTCHOUK, 2008; MAYNARD, 2018).

Essas iniciativas intensificaram as tensões existentes entre a Geórgia e a Rússia (MONGRENIER; THOM, 2016). Em 2008, a Rússia iniciou algumas operações militares na fronteira da Ossétia do Sul e na Geórgia (MONGRENIER; THOM, 2016). No dia 7 de agosto de 2008, Saakashvili ordenou que as forças armadas georginas retomassem a Ossétia do Sul (MONGRENIER; THOM, 2016). Esse movimento ordenado por Saakashvili foi o estopim para que as forças armadas da Rússia invadissem a Geórgia no dia 8 de agosto de 2008 (MONGRENIER; THOM, 2016).

Conforme Gomes e Alves (2020, p. 232) relatam, o combate Russo-Georgiano "foi considerado o primeiro caso de uso de ataques cibernéticos em apoio a operações militares tradicionais". Em 20 de julho de 2008, oito semanas antes da Rússia entrar no território da Geórgia, uma onda de ataques cibernéticos invadiu o ciberespaço georgiano (NYT, 2008; GOMES; ALVES, 2020). As primeiras agressões cibernéticas desferidas eram de negação, *DDos,* e tiveram como alvo o site do presidente Saakashvili. Os *hackers* escreveram no site a frase "win+love+in+Russia", que significa "conquistar o amor da Rússia", e derrubaram o portal por 24 horas (NYT, 2008). Os pesquisadores de Shadowserver, um grupo voluntário que rastreia atividades maliciosas da rede, alegaram que o servidor de comando que agrediu o site do presidente georgiano estava sediado nos Estados Unidos e ficou online semanas antes de começar o ataque (NYT, 2008).

A maioria dos alvos dos *hackers* eram sites jornalísticos (NYT, 2008; BLANK, 2017; GOMES; ALVES, 2020). Em 5 de agosto de 2008, os portais dos jornais OSInform News Agency e OSRadio sofreram ciberataques (NYT, 2008). Os conteúdos dos sites foram trocados pelo conteúdo da Alania TV, uma empresa de televisão apoiada pelo Estado da Geórgia que tem como público a Ossétia do Sul (NYT, 2008). Os responsáveis pela estação de televisão negaram qualquer participação no ataque cibernético às agências rivais (NYT, 2008).

Entre 8 e 11 de agosto, uma série de ataques cibernéticos de *DDos* intentaram contra o espectro eletromagnético da Geórgia e novas desfigurações foram iniciadas (NYT, 2008; SEGAL, 2016):

a- Em 9 de agosto de 2008, os *hackers* redirecionaram o tráfego de internet da Geórgia para os servidores com bases na Rússia e na Turquia; nesse mesmo dia, alguns especialistas em segurança cibernética da Alemanha conseguiram restabelecer o tráfego georgiano; entretanto, em poucas horas, diversos atores cibernéticos maliciosos o desviaram para os servidores sediados em Moscou (SEGAL, 2016; NYT, 2008);

b- No dia 10 de agosto de 2008, o site da agência de notícias RIA Novosti foi alvo de ciberataques e ficou desativado por várias horas (THE TELEGRAPH, 2008).

c- Em 11 de agosto de 2008, novamente, o site do presidente georgiano foi desfigurado; os *hackers* colocaram imagens o comparando com Adolf Hitler (DANCHO, 2008).

Após esses ciberataques, ainda no dia 11 de agosto de 2008, a Geórgia acusou a Rússia de travar uma guerra cibernética em sites do governo georgiano simultaneamente a uma ofensiva militar terrestre (NYT, 2008). O Ministério das Relações Exteriores da Geórgia emitiu o seguinte comunicado: "uma campanha de guerra cibernética da Rússia está prejudicando seriamente muitos sites georgianos, incluindo o do Ministério das Relações Exteriores"[72] (NYT, 2008, tradução própria). A acusação foi negada pela Rússia (NYT, 2008).

Segal (2016) salienta que, na época, foram encontrados vários fóruns como o StopGeorgia.ru, que forneciam as instruções sobre como congestionar os principais sites georgianos. Conforme pontuam Gomes e Alves (2020, p. 246): “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”. Assim que a Geórgia conseguiu bloquear o acesso dos servidores da Rússia ao seu espectro eletromagnético, os donos dos fóruns disponibilizaram novas instruções aos atores cibernéticos sobre os procedimentos que deveriam fazer para contornar os bloqueios e continuarem a proceder novos ataques cibernéticos à Geórgia (SEGAL, 2016; GOMES; ALVES, 2020). O cessar fogo terrestre entre os Estados se deu em 14 de agosto de 2008, mas os principais servidores da Geórgia continuaram inativos por algum tempo, isso dificultou a comunicação com o país (SEGAL, 2016; BLANK, 2017). De acordo com Blank (2017), a Geórgia ficou isolada e impedida de coordenar sua resposta _às agressões, bem como de informar ao mundo o seu lado no conflito.

Logo após o cessar fogo, Don Jackson, diretor de inteligência de ameaças da SecureWorks, declarou que “os invasores estão usando as mesmas ferramentas e os mesmos comandos pelo Russian Business Network-RBN e, em alguns casos, os ataques

[72] [Tradução própria]. No original, lê-se: “A Russian cyberwarfare campaign is seriously harming many Georgian websites, including the Ministry of Foreign Affairs”.

estão sendo lançados de computadores que eles controlam"[73] (NYT, 2008, tradução própria). O RBN é um grupo russo de *hackers* que está associado a diversas atividades cibernéticas criminosas, entretanto, não houve como confirmar qualquer relação entre o governo russo e o grupo (NYT, 2008). A Rússia não assumiu a autoria dos ataques cibernéticos; os comunicados emitidos pelo governo até confirmaram que atores patrióticos poderiam estar vinculados aos ataques como forma de protesto, todavia afirmaram que o estado russo não era o mandante (SINGER; FRIEDMAN, 2014; SEGAL, 2016).

Diferentemente do caso da Estônia (2007), onde o combate ocorreu apenas no espaço cibernético, o conflito na Geórgia destacou-se por ser classificado como o primeiro episódio em que houve o uso de ataques cibernéticos em apoio às operações militares convencionais (GOMES; ALVES, 2020). Enquanto as forças armadas da Rússia invadiam o território georgiano, o ciberespaço da Geórgia sofria consecutivos ciberataques aos seus principais sites de comunicação (BLANK, 2017).

No que se refere à imprecisão de autoria, examina-se que nesse caso o uso de terceiros nas agressões cibernéticas gerou uma difusão de poder (NYE, 2010; GOMES; ALVES, 2020). Embora a Rússia tenha negado ser a mandante dos ataques cibernéticos, especialistas em segurança cibernética, como os membros do Greylogic, os membros da Unidade de Consequências Cibernéticas dos Estados Unidos (US-CCU) e Stephen Blank, membro sênior do Conselho de Política Externa Americana, afirmaram que o apoio do governo russo aos *hackers* foi imprescindível no conflito cibernético (BLANK, 2017; NYT, 2008). Contudo, esse fator de disseminação de poder dificultou mais ainda verificar a identificação dos atores cibernéticos que estavam vinculados aos ciberataques, pois não houve como provar e nem afirmar que existia uma relação entre o governo russo e os grupos de *hackers* que intentaram contra o espectro eletromagnético da Geórgia (GOMES; ALVES, 2020; BLANK, 2017). Com a autoria imprecisa, não foi possível classificar os ciberataques como sendo atos de guerra ou não.

Como visto anteriormente, não há definição legal em âmbito internacional no que tange aos conflitos cibernéticos, apenas a OTAN considera o ciberespaço um domínio operacional de guerra (OTAN, 2016). Ao que se refere ao episódio na Geórgia, o Conselho dos Estados Unidos e da Europa compreenderam que os ataques de negação que o país sofreu, os *DDos*, não poderiam ser considerados atos de guerra, mas sim crimes

[73] [Tradução própria]. No original, lê-se: "attackers are using the same tools and commands over Russian Business Network-RBN and in some cases attacks are being launched from computers they control".

cibernéticos (GOMES; ALVES, 2020; BLANK, 2017). Isto é, caso os *hackers* fossem identificados, a ação cibernética seria criminosa e não um ato de guerra.

Pode-se concluir que os ataques cibernéticos sofridos pela Geórgia tiveram baixa materialidade, pois não acarretaram letalidade e nem em destruição de infraestruturas críticas essenciais georgianas. De acordo com a explicação de Gomes e Alves (2020, p. 246), "os ciberataques foram realizados de maneira limitada e contida, sem atacar infraestruturas críticas, mas demonstrando a capacidade de fazê-lo, sinalizando para o governo da Geórgia que a escalada do conflito não era desejada". Por fim, analisa-se que pelo aspecto da materialidade, os ataques cibernéticos também não seriam classificados como atos de guerra.

Os alvos dos ataques cibernéticos da Geórgia tinham caráter informacional (SEGAL, 2016). Na época, o ciberespaço da Geórgia dependia das redes de conexão da Rússia; o país georgiano não possuía sua própria rede de tráfego, isto é, quando os agressores cibernéticos intentaram contra o espaço cibernético da Geórgia, o país perdeu sua capacidade de comunicação interna e externa (SEGAL, 2016). A incursão cibernética isolou a Geórgia e isso demonstrou as vulnerabilidades do país à interferência da Rússia (SEGAL, 2016; HOLLIS, 2011). Conforme destacado, a Geórgia acusou a Rússia de ser a responsável pelos ataques cibernéticos (BLANK, 2017; HOLLIS, 2011; SEGAL, 2016). No entanto, em nenhum momento o governo georgiano declarou que os ciberataques eram atos de guerra (BLANK, 2017; HOLLIS, 2011; SEGAL, 2016). Desse modo, compreende-se que não teve interesse político da Geórgia em atribuir o ato de guerra na intercorrência cibernética.

4.1.3 Ucrânia – 2014-2015

Os conflitos entre a Ucrânia e a Rússia se sucedem desde o fim da União Soviética até os dias atuais (MAURER, 2015). Um desses episódios iniciou-se em 21 de novembro de 2013, quando o presidente da Ucrânia, Viktor Yanukovych se recusou a assinar um acordo de associação comercial com a União Europeia (MAURER, 2015). Na mesma noite, o povo da Ucrânia protagonizou diversos protestos contra o líder político, o movimento ficou conhecido como "Euromaidan" e teve como finalidade destituir Yanukovych do poder (MAURER, 2015). Por fim, em fevereiro de 2014, Yanukovych foi deposto do cargo presidencial, e então, novas manifestações de ativistas pró-russos e

antirrevolução se propagaram na região majoritariamente russófona da Crimeia (MAURER, 2015).

Desse modo, no dia 27 de fevereiro de 2014, a Rússia iniciou as agressões terrestres contra a Ucrânia na região da Crimeia (MAURER, 2015; WEEDON, 2015). Diversos ataques cinéticos foram disparados, as forças armadas da Rússia invadiram a Crimeia e se apossaram dos aeroportos internacionais da cidade de Simferopol e de Sevastopol e atentaram contra as infraestruturas críticas de comunicação ucranianas; os soldados russos avariaram os cabos de fibra óptica do sistema operacional da empresa de telecomunicação, a Ukrtelecom, e interromperam os serviços de suas redes de comunicação, isso impossibilitou o acesso dos usuários cibernéticos da Crimeia ao seu próprio ciberespaço (MAURER, 2015; WEEDON, 2015).

Em março de 2014, múltiplos ataques cibernéticos intentaram contra o ciberespaço da Ucrânia (NYT, 2014; SEGAL, 2016). O primeiro alvo foi o portal principal do governo da Ucrânia, a sua rede caiu e ficou fora do ar por mais de 72 horas; depois os *hackers* invadiram as redes de conexão dos celulares dos parlamentares ucranianos e todas as suas funcionalidades foram bloqueadas; outros ataques cibernéticos de *DDos* intentaram contra os portais do Conselho Nacional de Segurança e Defesa da Ucrânia; e outros ciberataques atingiram a agência de notícias estatal ucraniana, a Ukrinform; até o site da OTAN foi invadido, o grupo russo CyberBerkut atacou o portal da Aliança Militar e o interrompeu (NYT, 2014; SEGAL, 2016).

De acordo com Segal (2016), alguns atores cibernéticos da Ucrânia revidaram os ataques cibernéticos vindos da Rússia e retaliaram ciberneticamente os sites russos, como o do banco central e do Ministério das Relações Exteriores da Rússia. Nesse período iniciou-se uma guerra cibernética entre os dois países, o auge dos ataques ocorreu quando uma avalanche de quarenta e dois ataques de *DDos,* coordenados pelo grupo russo CyberBerkutt, atingiram os sites do governo ucraniano durante a votação da secessão da Ucrânia (SEGAL, 2016). Esse embate desequilibrou a Ucrânia no decorrer de 2014, que sofreu um encolhimento de até 8% por cento em sua economia (WEEDON, 2015).

Apesar dos indícios de a Rússia ter patrocinado os grupos de *hackers* a atacarem o ciberespaço da Ucrânia e da Crimeia, não houve nenhuma confirmação (WEEDON, 2015; SEGAL, 2016). Os conflitos cibernéticos na região não cessaram e, em 2015, a principal infraestrutura crítica de distribuição de energia da Ucrânia sofreria um ataque cibernético que comprometeria a distribuição de energia por 6 horas e afetaria mais de 200 mil ucranianos (WHITEHEAD et al., 2016).

No dia 23 de dezembro de 2015, às 15h30, os disjuntores das hidrelétricas *Kyiv*, *Prykarpattia* e *Chernivtsi* começaram a abrir e fechar remotamente, sem que houvesse qualquer intervenção por parte dos operadores que ali atuavam (WHITEHEAD et al., 2016). Nesse momento as três hidrelétricas estavam sofrendo sucessivos ciberataques em seus sistemas de comando e controle (WHITEHEAD et al., 2016). Os funcionários conseguiram restabelecer a energia de forma manual, eles tiveram que desligar o sistema remoto das subestações e controlar manualmente os seus sistemas de potência (WHITEHEAD et al., 2016).

Para atrapalhar os funcionários das hidrelétricas que tentavam restabelecer e distribuição de energia, os atores cibernéticos maliciosos "lançaram um ataque de negação de serviço baseado em telefonia, usando sistemas automáticos para sobrecarregar os serviços" (WHITEHEAD et al., 2016, p. 1). Esse ataque de sabotagem interferiu na comunicação dos operadores das subestações, que teve como resultado o atraso em recuperar a funcionalidade dos disjuntores (WHITEHEAD et al., 2016).

De acordo com Whitehead et al. (2016), que analisaram os relatórios elaborados pelo ICS-CERT "Industrial Control Systems Cyber Emergency Response Team" do Departamento de Segurança Interna dos Estados Unidos e pela E-ISAC ("Electricity Information Sharing and Analysis Center"), do departamento de tecnologia e informação do governo da Ucrânia, a agressão cibernética à infraestrutura crítica de rede de energia da Ucrânia foi direcionada a seis subestações de distribuição de energia, no entanto, atingiu apenas três, a *Kyiv*, a *Prykarpattia* e a *Chernivtsi*.

Whitehead et al. (2016) apontaram sete etapas do evento cibernético:

A) Primeiro houve uma invasão cibernética via e-mail, o "spear phishing"[74], e quando os usuários clicaram no documento enviado, automaticamente instalou-se um *malware* nas redes dos computadores das hidrelétricas;
B) Depois, o *malware* inserido estabeleceu uma porta de entrada para os hackers à rede corporativa;
C) Em seguida, os atores cibernéticos maliciosos se infiltraram nos sistemas de redes e logo acessaram as credenciais e contas dos operadores corporativos;

[74] Spear Phishing: É um golpe proveniente de e-mail ou comunicação eletrônica, direcionado a um indivíduo, organização ou empresa específicos. Embora tenha a intenção de roubar dados para fins mal-intencionados, os criminosos virtuais também podem tentar instalar um *malware* no computador do usuário.

D) Com a posse das credenciais, os usuários desenvolveram um canal criptografado de uma rede paralela e estabeleceram o controle das subseções de energia;
E) Assim, os agentes maliciosos passaram a ter o controle do sistema SCADA das hidrelétricas e então as configuraram propositalmente de forma incorreta;
F) No dia efetivo do ataque, dia 23 de dezembro de 2015, os *hackers* interromperam a distribuição de energia por meio das redes SCADA e então, desregularam os disjuntores;
G) Por fim, os *hackers* lançaram ataques de *DDos* aos serviços de telefonia, e então, conforme citado, retardaram a recuperação da distribuição de energia.

O episódio entrou para a história como o primeiro ataque cibernético bem-sucedido contra uma rede elétrica no mundo (NYT, 2016; ALJAZEERA, 2016; WHITEHEAD et al., 2016). Na época, a Rússia foi acusada pela Ucrânia de ser a mandante do ato, mas o governo russo negou, declarou que cidadãos russos e simpatizantes com a causa poderiam estar vinculados aos ataques, mas o governo não havia patrocinado e nem incentivado ninguém, nada foi confirmado (NYT, 2016; ALJAZEERA, 2016; WHITEHEAD et al., 2016).

Os conflitos políticos entre a Ucrânia e a Rússia ainda prevalecem. Em fevereiro de 2022 a Rússia invadiu a Ucrânia e iniciou uma guerra bélica (NYT, 2022; ALJAZEERA, 2022). Enquanto o território ucraniano é tomado pelas forças armadas russas, o seu ciberespaço sofre sucessivos ataques cibernéticos de desfiguração em suas instituições, como nos portais dos principais bancos, no site de suas forças armadas e nos sites dos ministérios da Educação, da Ciência, das Relações Exteriores e da Segurança e Defesa (NYT, 2022; ALJAZEERA, 2022). O governo da Ucrânia afirma que a Rússia é a responsável pelos ciberataques, pois quer desestabilizar internamente o país (THE GUARDIAN, 2022; NYT, 2022; ALJAZEERA, 2022). Além do governo ucraniano, as instituições como a OTAN e a União Europeia declararam que existem indícios o suficiente para constatar que a Rússia é a autora das agressões cibernéticas, algo que é veemente negado pelo governo russo (NYT, 2022; ALJAZEERA, 2022).

Quando se compara as primeiras incursões cibernéticas à Ucrânia, no ano de 2014, com o evento cibernético da Geórgia (2008), é possível perceber algumas semelhanças. Por exemplo, assim que a Rússia invadiu o território da Crimeia, diversos ataques cibernéticos de negação intentaram contra os sites do governo da Ucrânia, contra os aparelhos telefônicos dos parlamentares ucranianos e contra os meios de comunicação,

exatamente como aconteceu na Geórgia (2008) (NYT, 2014; SEGAL, 2016). Enquanto ocorria um conflito bélico entre os países, iniciou-se uma guerra cibernética em paralelo (NYT, 2014; SEGAL, 2016).

As agressões cibernéticas eram desferidas por atores não estatais, como o grupo russo CyberBerkut, mas não houve identificação dos autores que compunham o grupo (NYT, 2014; SEGAL, 2016). Na época, o governo da Ucrânia chegou a acusar a Rússia de ser a patrocinadora dos ciberataques; a Rússia explicou que alguns cidadãos russos poderiam até estar vinculados aos eventos cibernéticos (SEGAL, 2016). Todavia, o governo russo afirmou que não havia patrocinado e nem era o mandante das agressões cibernéticas (SEGAL, 2016). Posto isso, analisa-se que pela questão da autoria, a possibilidade de atribuir o ato de guerra não caberia no caso.

No elemento de materialidade, o evento cibernético não causou explosões, nem mortes e nem destruição de infraestruturas críticas (NYT, 2014). Os danos foram brandos comparados a um ataque cinético, "somente" os sites que ficaram fora do ar (NYT, 2014; SEGAL, 2016). Ao analisar as consequências sofridas pela Ucrânia é possível constatar que apesar do embate ser subordinado à política, não foi violento e nem instrumental, a intenção dos ataques teve como objetivo causar desordem interna, isto é, não teve características de um ato de guerra (NYT, 2014; CLAUSEWITZ, 1984; RID, 2012).

Na questão da definição legal e da vontade política, é a mesma situação do caso da Geórgia, os ataques cibernéticos não possuíram alta materialidade, assim como decorre em uma guerra (BLANK, 2017; NYT, 2014). Nesse contexto, as ações cibernéticas seriam consideradas como crimes cibernéticos e não atos de guerra. Conforme visto, o governo da Ucrânia acusou a Rússia de ser a autora dos ciberataques. Contudo, o governo ucraniano não teve vontade política de acusar o governo russo de cometer um ato de guerra em seu espaço cibernético, mas sim de querer desestabilizar internamente a Ucrânia enquanto invadia a Crimeia (NYT, 2014; SEGAL, 2016).

Já no ataque cibernético de 2015, que teve como alvo as hidrelétricas da Ucrânia, a materialidade da incursão cibernética foi alta, mesmo que não tenha sucedido em baixas ou explosões, uma infraestrutura crítica foi atingida e sabotada, assim como pode acontecer em uma guerra tradicional (STONE, 2013; SEGAL, 2016). A Ucrânia teve sua energia elétrica interrompida por mais de 6 horas, mais de 200.000 mil pessoas ficaram sem energia (THE GUARDIAN, 2016). Novamente a Ucrânia acusou a Rússia de ser a mandante do ato, mas a autoria não foi confirmada pelos investigadores e o governo russo negou ter qualquer ligação com o evento cibernético (THE GUARDIAN, 2016). Assim

como no caso da Estônia e da Geórgia, sem identificação e reconhecimento dos atores cibernéticos, a atribuição do ato de guerra no evento não seria exequível.

Destarte, sem normas internacionais que definam a guerra cibernética, afastou-se a possibilidade de classificar a agressão cibernética contra as hidrelétricas de energia da Ucrânia como atos de guerra e, ainda que o ato intentado tenha sido violento e instrumental, não houve como comprovar a subordinação à política, pois a Rússia não confirmou ter orquestrado os ciberataques. Por fim, não houve nenhuma acusação da OTAN, da ONU ou até mesmo vontade política da Ucrânia em acusar a Rússia de ameaçar a sua soberania e, portanto, ter cometido um ato de guerra.

O caso ainda pode ser observado como um ato de sabotagem, assim como Rid (2012) alega que são a maioria dos ataques cibernéticos, mas ao analisar o evento cibernético, compreende-se que não foi a "sabotagem" que impediu a atribuição do ato de guerra, mas a ausência de definição legal, a imprecisão de autoria e substancialmente a falta de interesse político do governo da Ucrânia ou das instituições de segurança internacional em declarar guerra (LIBICKI, 2009; SINGER; FRIEDMAN, 2014).

4.2 O CASO STUXNET

O caso do Stuxnet surpreendeu o mundo, foi o primeiro caso de uma agressão cibernética a uma Usina Nuclear (ZETTER, 2017; RID, 2012; LIBICKI, 2009). O planejamento do vírus iniciou-se em 2007, as primeiras intercorrências começaram em 2009 e a sua percepção desenrolou-se apenas em 2010 (ZETTER, 2017; RID, 2012; LIBICKI, 2009). Em junho de 2010, na Bielorrússia, uma empresa de segurança cibernética, a VirusBlokAda, recebeu uma máquina de um cliente do Irã que continha um problema, o computador parava de funcionar e logo reiniciava sozinho; não saia desse ciclo (ZETTER, 2017). Após algumas semanas de investigação, os engenheiros de computação Sergey Ulasen e Oleg Kupreev observaram um "movimento" suspeito nos arquivos da máquina iraniana (ZETTER, 2017). Os engenheiros identificaram um vírus muito peculiar, era um código que conseguia se ocultar e ficar invisível a qualquer antivírus (ZETTER, 2017). O vírus se propagava de máquina para máquina, era um "*exploit*[75] que atacava uma função fundamental para o sistema operacional Windows e assim colocava milhões de computadores em risco de infecção" (ZETTER, 2017).

[75]Exploit: São programas ou códigos projetados para abusar de vulnerabilidades de software ou hardware e causar efeitos indesejados pelos desenvolvedores ou fabricantes.

A maioria dos *malwares* são inseridos na internet por meio de um e-mail contaminado (ZETTER, 2017). No entanto, o vírus detectado por Ulasen e Kupreev foi disseminado através de um *pen drive*[76] (ZETTER, 2017). Os técnicos bielorrussos identificaram que o *exploit* agia sorrateiramente dentro das máquinas, um antivírus não seria capaz de detectar e nem de combater o vírus malicioso, na época nenhum sistema operacional da Microsoft estava habilitado para enfrentar esse *exploit* (ZETTER, 2017).

Os engenheiros de computação bielorrussos tentaram entrar em contato com a Microsoft para reportar à empresa que haviam descoberto um vírus malicioso que estava contaminando diversas máquinas pelo mundo e isso podia gerar grandes prejuízos (ZETTER, 2017). Como a Microsoft não respondeu as chamadas, Ulasen e Kupreev, em 12 de julho de 2010, divulgaram no site da empresa a descoberta do vírus e como era a sua estrutura e o seu comportamento (ZETTER, 2017).

A notícia deixou a indústria de computação em alerta, a Microsoft tomou conhecimento e emitiu um comunicado aos seus clientes sobre o perigo do vírus, que passou a se chamar "Stuxnet" (ZETTER, 2017). O Stuxnet foi estruturado em três partes: primeiro ele injetava uma carga em um sistema e depois executava a máquina atingida de forma remota; posteriormente, o *worm* se reproduzia automaticamente e várias cópias do vírus eram propagadas aos computadores ou máquinas industriais que operavam no sistema SCADA[77]; por fim, o Stuxnet possuía um componente de *rookit*, isto é, uma característica que permitia o vírus se esconder e, assim, evitava a sua detecção (ZETTER, 2017).

Após a divulgação do vírus pelos bielorrussos, especialistas do mundo inteiro começaram a investigar o Stuxnet (ZETTER, 2017). Ao rastrear os "passos" do vírus, descobriram que ele já existia desde 2009, ou seja, o *worm* ficou escondido mais de um ano até ser exposto (ZETTER, 2017). Ainda em julho de 2010, Frank Boldewin, um pesquisador da Alemanha, encontrou referências da empresa Siemens no Stuxnet e divulgou seu próprio prognóstico no mesmo fórum em que os bielorrussos noticiaram o *worm* (ZETTER, 2017). Essa descoberta levantou a suspeita de que os atacantes estariam interessados especificamente em máquinas industriais que operavam pelo sistema

[76]Pen Drive: é um dispositivo de armazenamento de dados que inclui memória flash e possui uma interface USB integrada, permitindo uma conexão a uma porta USB de um computador ou outro equipamento com uma entrada USB, como um computador.
[77]SCADA: é a sigla em inglês para Supervisory Control And Data Acquisition, que na tradução para o português significa Sistema de Supervisão e Aquisição de Dados. O SCADA é um sistema que usa um software para monitorar, supervisionar e controlar as variáveis e os dispositivos de um processo.

SCADA da Siemens (ZETTER, 2017). Isso fez com que as empresas de computadores, como a Microsoft ficassem mais tranquilas, já que o Stuxnet parecia ter como alvo apenas os softwares da Siemens instalados (ZETTER, 2017).

Em agosto de 2010, os especialistas em segurança cibernética Eric Chien e Liam O'Murchu, dos Estados Unidos, e Nicolas Falliere, engenheiro de software francês, iniciaram uma busca sobre a origem do Stuxnet e qual seria o objetivo do *hacker* por detrás do *worm* (ZETTER, 2017). Em novembro de 2010, os pesquisadores descobriram que o *worm* possuía características muito específicas, analisaram que as propriedades do Stuxnet buscavam um sistema industrial remoto que tivesse até 186 conversores instalados, todos eles operando acima de 800 Hz, o seu funcionamento efetivo incluía uma carga de *malware* especializada em atingir apenas sistemas de controle de supervisão e aquisição de dados (SCADA) da Siemens que são configurados para controlar e monitorar processos industriais específicos (ZETTER, 2017). De forma imediata os pesquisadores buscaram a origem desses conversores nucleares e puderam constatar que apenas os Estados Unidos tinham permissão para efetuar a sua exportação, logo deduziram que o alvo do Stuxnet era a Usina Nuclear de Natanz, no Irã, pois o país se encontrava em conflito com os Estados Unidos justamente pelo programa nuclear que realizavam na infraestrutura (ZETTER, 2017).

Nesse mesmo período, Ralph Langner, um ex-psicólogo que administrava uma empresa de segurança de computadores em Hamburgo, também decidiu investigar mais a fundo o Stuxnet (NYT, 2011; ZETTER, 2017). O empresário solicitou aos seus cinco funcionários que realizassem diversos testes operacionais com o código malicioso no sistema SCADA da Siemens e analisassem os seus efeitos (NYT, 2011; ZETTER, 2017). Langner constatou que o *worm* só entrava em ação quando detectava a presença de uma configuração única de controladores que pareciam existir apenas em uma planta de centrifugação (NYT, 2011; ZETTER, 2017). O empresário afirmou que "os atacantes tomaram muito cuidado para garantir que apenas seus alvos designados fossem atingidos"[78] (NYT, 2011, tradução própria). Nessa atividade pôde ser constatado que uma parcela do código estava sendo projetada para enviar comandos para 984 máquinas ligadas entre si (NYT, 2011; ZETTER, 2017). No final de 2009, meses antes do Stuxnet aparecer, quando os inspetores internacionais da Agência Internacional de Energia Atômica – AIEA - visitaram Natanz, descobriram que os iranianos haviam retirado de

[78] [Tradução própria]. No original, lê-se: "the attackers took great care to ensure that only their designated targets were hit".

serviço um total de exatamente 984 máquinas que estavam funcionando no verão anterior, ou seja, o mesmo número descoberto pelos funcionários de Langner (NYT, 2011; ZETTER, 2017). Langner compartilhou o resultado do seu teste com outros pesquisadores (ZETTER, 2017).

Em 12 de novembro de 2010, a Symantec, empresa de segurança cibernética, coletou as informações de Langner, juntou com o relatório dos pesquisadores Eric Chien, Liam O'Murchu e Nicolas Falliere e então emitiu uma publicação a respeito do Stuxnet em seu portal (ZETTER, 2017). No artigo, os pesquisadores explicaram como o Stuxnet funcionava, e que, nesse caso, o propósito do vírus seria destruir as centrífugas de enriquecimento de urânio da Usina Nuclear de Natanz que funcionava pelo sistema SCADA da Siemens, no Irã (ZETTER, 2017). Após quatro dias da publicação, os técnicos em Natanz paralisaram todas as centrífugas e depois de seis dias corridos, no dia 22 de novembro, todas as atividades na Usina de Natanz foram interrompidas (ZETTER, 2017). Nem os Estados Unidos e nem o Irã se manifestaram acerca do artigo apresentado (ZETTER, 2017).

Uma sucessão de eventos começou a acontecer. Em 29 de novembro de 2010, o presidente iraniano Mahmoud Ahmadinejad declarou, pela primeira vez, que um vírus de computador havia causado problemas com o controlador que manuseava as centrífugas nas instalações de Natanz: "conseguiram criar problemas para um número limitado de nossas centrífugas com o software que instalaram em peças eletrônicas"[79] (REUTERS, 2010, tradução própria). Nesse mesmo dia, dois carros bomba explodiriam contra os carros de dois cientistas nucleares iranianos perto da Universidade Shahid Beheshti, em Teerã (REUTERS, 2010). O físico quântico Majid Shahriari foi morto e Fereydoon Abbasi, funcionário do Ministério da Defesa, ficou gravemente ferido (REUTERS, 2010). Os dois trabalhavam em contato direto com a Usina Nuclear de Natanz (REUTERS, 2010). Não houve confirmação da autoria, apenas um artigo na revista Wired especulou que o governo iraniano teria relação direta com os assassinatos (WIRED, 2010; REUTERS, 2010).

Em janeiro de 2011, os jornalistas do New York Times, William J. Broad, John Markoff e David E. Sanger, apresentaram um prognóstico detalhado sobre a origem e o propósito do Stuxnet (NYT, 2011; ZETTER, 2017). Na época, os jornalistas declararam que o Stuxnet foi uma operação militar realizada entre o governo dos Estados Unidos e

[79] [Tradução própria]. No original, lê-se: "managed to create problems for a limited number of our centrifuges with the software they installed on electronic parts".

Israel para atrasar a produção de enriquecimento de urânio na Usina Nuclear de Natanz, *"*as pistas mais recentes e mais fortes sugerem que o vírus foi projetado como um projeto americano-israelense para sabotar o programa iraniano"[80] (NYT, 2011, tradução própria).

Na reportagem foi exposto a realização de algumas operações militares em Dimona, Israel, que produziram centrífugas nucleares praticamente idênticas às do Irã, como a Usina Nuclear de Natanz (NYT, 2011). Os jornalistas declararam que o governo de Israel testou a eficácia do *worm* de computador, o Stuxnet, nas centrífugas nucleares reproduzidas e tiveram como resultado o retardamento na produção de urânio, assim como ocorreu no Irã (NYT, 2011). Os jornalistas não informaram a fonte da informação, alegaram apenas que eram especialistas militares e de inteligência familiarizados com as operações que aconteciam em Dimona (NYT, 2011).

As autoridades dos Estados Unidos e de Israel se recusaram a comentar a reportagem (NYT, 2011; ZETTER, 2017). Na ocasião, apenas o estrategista-chefe do presidente Obama para combater armas de destruição em massa, Gary Samore emitiu o seguinte comentário no que se refere ao Stuxnet: "fico feliz em saber que eles estão tendo problemas com suas centrífugas [Irã], e os EUA e seus aliados estão fazendo tudo o que podem para complicar mais"[81] (NYT, 2011, tradução própria).

Os jornalistas do New York Times descobriram que em julho de 2008, a Siemens e um laboratório de computador em Idaho realizaram algumas operações cibernéticas que visavam buscar vulnerabilidades em sistemas de controle, assim como é o sistema SCADA (NYT, 2011). No entanto, quando o jornal indagou o laboratório sobre o evento cibernético, recebeu como resposta que as missões tinham caráter sigiloso e não seriam comentadas pelo Laboratório Nacional de Idaho (NYT, 2011).

Em dezembro do mesmo ano, o Institute for Science and International Security (ISIS)[82] declarou que o Stuxnet seria uma explicação plausível aos danos aparentes nas centrífugas da Usina de Natanz. Segundo o relatório emitido, o *worm* pode ter destruído até 1.000 centrífugas em algum momento entre novembro de 2009 e final de janeiro de 2010 e isso seria o suficiente para retardar o progresso de enriquecimento de urânio do

[80] [Tradução própria]. No original, lê-se: "the latest and strongest clues suggest the virus was designed as an American-Israeli project to sabotage the Iranian program".
[81] [Tradução própria]. No original, lê-se: "glad to hear that they are having problems with their centrifugal machines [Iran], and the US and its allies are doing everything they can to complicate matters further".
[82] Institute for Science and Internacional Security – ISIS: é instituição não governamental sem fins lucrativos fundada em 1993 pelo ex-inspetor nuclear da Agência Internacional de Energia Atômica (AIEA) das Nações Unidas, David Albright, que tem como objetivo informar o público sobre "questões científicas e políticas que afetam a segurança internacional".

Irã (ISIS, 2010). Segue um trecho da publicação sobre a atuação do Stuxnet nas centrífugas:

> O *worm* funcionou primeiro fazendo com que uma centrífuga iraniana IR-1 infectada aumentasse sua velocidade operacional normal de 1.064 hertz para 1.410 hertz por 15 minutos antes de retornar à sua frequência normal. Vinte e sete dias depois, o *worm* voltou à ação, diminuindo a velocidade das centrífugas infectadas para algumas centenas de hertz por 50 minutos completos. As tensões das velocidades excessivas, então mais lentas, fizeram com que os tubos centrífugos de alumínio se expandissem, muitas vezes forçando partes das centrífugas a entrar em contato suficiente umas com as outras para destruir a máquina (ISIS, 2010, tradução própria)[83].

Não houve confirmação da Usina Nuclear de Natanz, no entanto, as câmeras da Agência Internacional de Energia Atômica (AIEA) instaladas na usina registraram o súbito desmantelamento e remoção de aproximadamente 900 a 1.000 centrífugas durante o tempo em que o Stuxnet estava ativo na usina (WASHINGTON POST, 2011). Conforme consta no relatório da AIEA, os operadores iranianos da infraestrutura crítica substituíram rapidamente as centrífugas, a agência relatou que o enriquecimento de urânio provavelmente foi interrompido brevemente (ISIS, 2010; IAEA, 2011; WASHINGTON POST, 2011).

As evidências apresentadas pela ISIS e pela AIEA não incitaram os Estados envolvidos a declararem uma nota sobre o assunto. Todavia, em junho de 2012, o jornal New York Times vazou uma conversa do então Presidente Barack Obama, ocorrida em 2010, em que o líder político ordenava que as Forças Armadas norte-americanas deferissem sucessivos ataques cibernéticos, por meio de *worms,* às infraestruturas críticas do Irã, segue o trecho: "[Obama] secretamente ordenou ataques cada vez mais sofisticados aos sistemas de computadores que administram as principais instalações de enriquecimento nuclear do Irã" [84] (NYT, 2012, tradução própria).

Novamente, não houve declarações do governo dos Estados Unidos sobre a reportagem ou sobre o Stuxnet (ZETTER, 2017). Após o Stuxnet (2009-2010), tanto os Estados Unidos quanto Israel começaram a fortalecer suas estratégias de Segurança e Defesa Cibernética (SINGER; FRIEDMAN, 2014; ZETTER, 2017). Já as negociações

---

[83] [Tradução própria]. No original, lê-se: "The worm first worked by causing an infected Iranian IR-1 centrifuge to increase from its normal operating speed of 1064 hertz to 1410 hertz for 15 minutes before returning to its normal frequency. Twenty-seven days later, the worm was back in action, slowing the infected centrifuges to a few hundred hertz for a full 50 minutes. Stresses from the then slower excessive speeds caused the aluminum centrifuge tubes to expand, often forcing parts of the centrifuges into enough contact with each other to destroy the machine."

[84] [Tradução própria]. No original, lê-se: "President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program".

no que concerne ao programa nuclear iraniano continuam (NYT, 2022). Em 2021, os Estados Unidos e Israel ameaçaram atacar o Irã caso o país não interrompesse a construção de uma arma nuclear (NYT, 2021). Todavia, em 2022, as negociações correm por uma via mais diplomática e sem ameaças futuras de um conflito armado (NYT, 2022).

Ao analisar o Stuxnet, conclui-se que o vírus foi desenvolvido para danificar especificamente as instalações nucleares iranianas de Natanz (ZETTER, 2017; RID, 2012). O evento cibernético é considerado um dos ciberataques mais bem sucedidos que já ocorreram (RID, 2012). Conforme destacou Langner (2011), o *worm* Stuxnet só poderia ser criado a partir de grandes investimentos, isto é, apenas um Estado com alto poder tecnológico poderia estar vinculado à operação cibernética. (LANGNER, 2011; RID; BUCHANAN, 2015).

Igualmente aos outros casos aqui explorados, não houve confirmação de autoria no caso do Stuxnet (2017). Como dito anteriormente, as investigações levaram a crer que os Estados Unidos e Israel foram os patrocinadores dos ataques cibernéticos que suspenderam e atrasaram o programa nuclear do Irã (NYT, 2010; ZETTER, 2017; RID, 2012). Nem os Estados Unidos e Israel assumiram a culpa da ação cibernética, a autoria ficou imprecisa, portanto, o ato de guerra não poderia ser atribuído.

No que corresponde à materialidade, explorou-se que o Stuxnet teve um lapso temporal de quase três anos, o vírus deve ter sido planejado no final de 2007 e foi executado entre 2009 e 2010, isto é, o vírus causou destruição das centrífugas ao longo de um ano sem ser notado (RID, 2012; ZETTER, 2017). O Stuxnet penetrou nas centrífugas de enriquecimento de urânio e agiu “silenciosamente”, não houve explosões e nem baixas, no entanto, atingiu uma infraestrutura crítica de um Estado e provocou a destruição de até 1000 máquinas, conforme consta no relatório da AIEA (2011) (ISIS, 2010; IAEA, 2011; WASHINGTON POST, 2011). Nenhuma instituição de segurança internacional comentou a materialidade do Stuxnet como ato de guerra (SINGER; FRIEDMAN, 2014).

Conforme analisado nos casos anteriores, não há definição legal acerca dos conflitos cibernéticos (AYRES; GRASSI, 2020). A ONU (2013) tem um posicionamento de que a imprecisão de autoria dificulta punir os atores cibernéticos, já a OTAN (2016) compreende que uma guerra cibernética pode se tornar uma guerra real. Entretanto, aqui vale destacar que no período em que o Stuxnet foi evidenciado, em 2010, a Aliança Militar ainda não considerava o ciberespaço como um domínio operacional de guerra (ONU, 2012; OTAN, 2016). Mesmo o Stuxnet sendo considerado uma excelente

campanha de sabotagem contra o governo do Irã, não havia e ainda não há normas internacionais acerca de operações cibernéticas ofensivas no ciberespaço (SINGER; FRIEDMAN, 2014). A ausência de leis internacionais no que tange às agressões cibernéticas causa insegurança jurídica aos Estados (AYRES; GRASSI, 2020). Na época, o ministro iraniano de indústria e minas, Mahmud Liaii, classificou o ciberataque do Stuxnet da seguinte forma: "uma guerra eletrônica foi deflagrada contra o Irã" [85] (ANEJA, 2010, tradução própria). Embora o governo iraniano tenha emitido esse comunicado, não acusou os Estados Unidos, nem Israel ou outro país de ter cometido um ato de guerra, em outras palavras, não houve vontade política em declarar guerra.

Segundo Rid (2012), o Stuxnet foi uma operação cibernética de sabotagem extremamente sofisticada. O autor explicou que o vírus tinha finalidade específica, que era sabotar o programa de enriquecimento de urânio da usina nuclear de Natanz. Ao explorar a análise de Rid (2012) no capítulo 2, verificou-se que o autor classificou a agressão cibernética "apenas" como um ato de sabotagem e só por essa questão o autor concluiu que o Stuxnet não seria um ato de guerra. Na visão de Rid (2012), a operação cibernética só poderia ser desenvolvida por grandes potências, todavia, o autor não entrou no mérito da imprecisão de autoria, nem do interesse político e nem em explorar se a destruição (materialidade) das centrífugas da usina nuclear de Natanz poderia ser caracterizada como uma ameaça ou não à soberania do Irã.

Conforme analisado nesse trabalho, foi possível perceber que o ensejo de sabotagem não exclui necessariamente o ato de guerra (STONE, 2013). Ao levantar os elementos necessários para classificar o caso do Stuxnet como um ato de guerra, constatou-se que não foi a ação ser intitulada como sabotagem que o excluiu de ser um ato de guerra, mas sim a imprecisão de autoria, a falta de definição legal e a ausência de interesse político. A materialidade foi relevante, pois houve a destruição das centrífugas da Usina de Natanz; isso poderia ser enxergado como uma ameaça de soberania. Desse modo, entende-se que provavelmente a ausência dos outros elementos tenha implicado em considerar a operação cibernética como um ato de guerra.

4.3 AGRESSÃO CIBERNÉTICA À INFRAESTRUTURA CRÍTICA DO IRÃ REALIZADA PELOS ESTADOS UNIDOS – 2019

[85] [Tradução própria]. No original, lê-se: "an electronics war was unleashed against Iran".

Em 2015, o Irã selou um acordo nuclear com a China, os Estados Unidos, a Rússia, a Alemanha, o Reino Unido, a União Europeia e a França (BBC, 2015). Nesse acordo, o país iraniano concordou em eliminar até 98% de suas reservas de urânio e reduzir em até dois-terços os números de centrifugadores de gás em um período de até treze anos (BBC, 2015). Contudo, insatisfeitos com o pacto, em 08 de maio de 2018, os Estados Unidos retiraram-se do Plano de Ação do Conjunto Global. Donald Trump afirmou que o objetivo do acordo não foi atingido e por isso retiraria os Estados Unidos do pacto (NYT, 2018; ALJAZEERA, 2018; THE GUARDIAN, 2018).

De acordo com Trump, o Irã não interrompeu de vez o seu programa nuclear, apenas o camuflou (EUA, 2018). O Presidente alegou que Israel possuía provas de que os iranianos continuavam suas buscas por armas nucleares (EUA, 2018). Trump salientou que as inspeções internacionais no Irã não tinham capacidades para detectar os locais essenciais no território iraniano, como as suas instalações militares, e, por isso, a tranquilidade e paz mundial estariam ameaçadas (EUA, 2018).

A decisão dos Estados Unidos ensejou alguns episódios conflituosos. No começo de junho de 2019, dois navios petroleiros foram atacados no Golfo de Omã, um pertencia ao Japão, o "Kokuka Courageous", o outro era o "Front Altair", pertencente a uma empresa norueguesa; todos os tripulantes foram resgatados com vida (THE GUARDIAN, 2019). Logo após a agressão, sem demonstrar provas, o secretário de Estado dos Estados Unidos, Mike Pompeo, acusou o Irã de ser o mandante do ato e declarou em uma coletiva de imprensa na sede do Departamento de Defesa que: "é a avaliação do governo dos Estados Unidos que a República Islâmica do Irã é responsável pelos ataques que ocorreram no Golfo de Omã hoje"[86] (THE GUARDIAN, 2019, tradução própria). Pompeo justificou sua acusação ao comparar a intercorrência com outros episódios protagonizados pelo Irã que possuíam características semelhantes (THE GUARDIAN, 2019). O Irã negou a sua participação na ação (THE GUARDIAN, 2019).

Horas depois da acusação, o Comando Central das Forças Armadas dos EUA (CENTCOM) divulgou um vídeo que mostrava um barco com os membros da Guarda Revolucionária iraniana próximo ao casco de um dos navios atacados (CENTCOM, 2019). No vídeo é possível ver a sigla em inglês IRGC, que significa "Corpo de Guardiões da Revolução Islâmica" (CENTCOM, 2019). O Irã rejeitou as acusações sobre o atentado no Estreito de Ormuz e o porta voz do ministério das Relações Exteriores iraniano apenas

[86] [Tradução própria]. No original, lê-se: "it is the assessment of the United States government that the Islamic Republic of Iran is responsible for the attacks that took place in the Gulf of Oman today".

declarou: “estamos encarregados de manter a segurança no Estreito e resgatamos a tripulação dos petroleiros atacados no menor tempo possível (...) as acusações do secretário de Estado Pompeo ao Irã são alarmantes” [87] (REUTERS, 2019, tradução própria).

Uma semana depois desse incidente no Estreito de Ormuz, no dia 20 de junho, o Irã declarou que os Guardiões da Revolução do Irã haviam derrubado um *drone*, também no Estreito de Ormuz, do tipo RQ-4 Global Hawk, procedente ao Estados Unidos (IRNA, 2019; ALJAZEERA, 2019). O porta-voz do Ministério do Exterior do Irã, Abbas Mousavi informou que os Estados Unidos violaram o espaço aéreo do país e por isso o destruíram (IRNA, 2019; ALJAZEERA, 2019).

No mesmo dia os militares norte-americanos confirmaram o episódio, mas explicaram que o *drone* estava no espaço aéreo internacional quando foi atacado e não sob o território iraniano (BBC, 2019; CNN, 2019). O representante da Marinha dos Estados Unidos no Pentágono, Bill Urban, reafirmou a postura dos militares e informou que o ataque do Irã foi um ato injustificado (REUTERS, 2019). O presidente Trump redigiu em sua página no Twitter[88] que o Irã “cometeu um erro muito grande"[89] (THE GUARDIAN, 2019, tradução própria) e que “este país [Estados Unidos] não aceitará isso"[90] (THE GUARDIAN, 2019, tradução própria).

No dia 21 de junho de 2019, Trump informou em seu Twitter que havia cancelado um ataque cinético ao Irã: “estávamos armados e carregados para retaliar ontem à noite em 3 pontos turísticos diferentes quando perguntei quantos morreriam. 150 pessoas, senhor, foi a resposta de um general. 10 minutos antes do ataque eu parei”[91] (THE GUARDIAN, 2019, tradução própria); o presidente ainda afirmou que a agressão não seria “proporcional a derrubar um *drone* não tripulado; não tenho pressa”[92] (THE GUARDIAN, 2019, tradução própria).

---

[87] [Tradução própria]. No original, lê-se: “We are in charge of maintaining security in the Strait and rescuing the crew of the attacked tankers in the shortest possible time (...) Secretary of State Pompeo's accusations against Iran are alarming”.

[88] Twitter: Em 2020 o Twitter suspendeu a conta de Donald Trump de forma permanente (TWITTER, 2020). O Twitter declarou que as manifestações de Trump incitavam a violência, por isso desativaram a conta. Destarte, as declarações de Trump no Twitter citadas no presente trabalho terão como referências os meios de comunicação, como o The Guardian, The Washington Post, Al Jazeera, Yahoo! News e The New York Times.

[89] [Tradução própria]. No original, lê-se: “made a very big mistake”.

[90] [Tradução própria]. No original, lê-se: “this country [United States] will not accept this”.

[91] [Tradução própria]. No original, lê-se: “we were armed and loaded to retaliate last night at 3 different tourist spots when I asked how many would die. 150 people, sir, was a general's reply. 10 minutes before the attack I stopped”.

[92] [Tradução própria]. No original, lê-se: “not proportionate to shooting down an unmanned drone”.

Após as declarações de Trump no Twitter, os jornais The Washington Post (2019) e o Yahoo! News (2019) relataram que os Estados Unidos, como forma de retaliação às agressões intentadas pelo Irã, já haviam desferido uma série de ataques cibernéticos contra as infraestruturas críticas militares iranianas. O Yahoo! News relatou que na noite do dia 20 de junho de 2019 "o Comando Cibernético dos EUA lançou um ataque digital contra um grupo de espionagem iraniano que apoiou os ataques de minas contra navios comerciais na semana passada"[93] (YAHOO! NEWS, 2019, tradução própria). De acordo com o Yahoo! News (2019), a informação foi confirmada por dois ex-funcionários de inteligência do Comando Cibernético dos Estados Unidos; a instituição não quis comentar o atentado. A representante do Pentágono, Heather Babb, disse ao Yahoo! News que "por uma questão de política e de segurança operacional, não discutiam operações, inteligência ou planejamento no ciberespaço"[94] (YAHOO! NEWS, 2019, tradução própria).

No dia 22 de junho de 2019, o The Washington Post informou que Trump autorizou os ciberataques contra o grupo de espiões e contra o sistema de comando e controle do Irã. O jornal explicou que a agressão cibernética havia destruído o sistema de computador iraniano usado para controlar os lançamentos de foguetes e mísseis. Não houve declarações diretas sobre o caso e um novo acordo sobre o programa nuclear do Irã ainda segue em negociação com os Estados Unidos (THE WASHIGTON POST, 2019; NYT, 2022).

Desde que Trump assinou o novo plano de Estratégia Cibernética dos Estados Unidos, em 2017, o país norte-americano segue uma tendência crescente em realizar operações cibernéticas ofensivas no espaço cibernético como forma de retaliação (NYT, 2019). Conforme disse James Lewis à Reuters (2019), especialista cibernético do Centro de Estudos Estratégicos Internacionais, sediado em Washigton: "você consegue fazer estragos sem matar pessoas ou explodir coisas; isso acrescenta uma opção ao pacote que não tínhamos antes, e nossa disposição de usá-la é importante"[95] (REUTERS, 2019, tradução própria), isto é, os ataques cibernéticos são vistos como uma opção menos desafiadora que um conflito bélico.

[93] [Tradução própria]. No original, lê-se: "US Cyber Command launched a digital attack against an Iranian spy group that supported mine attacks on commercial ships last week".
[94] [Tradução própria]. No original, lê-se: "as a matter of policy and operational security, we do not discuss operations, intelligence or planning in cyberspace".
[95] [Tradução própria]. No original, lê-se: "you can do damage without killing people or blowing things up; this adds an option to the package that we didn't have before, and our willingness to use it matters".

Dessa forma, após explorar o evento cibernético, é possível afirmar que a autoria dos ciberataques contra o sistema de comando e controle do Irã permaneceu imprecisa. Embora todos os vestígios apontassem os Estados Unidos como o autor dos ataques cibernéticos contra as infraestruturas críticas do Irã, bem como as declarações de Trump no Twitter e a exposição do conflito cibernético no The Washington Post (2019) e no Yahoo! News (2019), ninguém do governo norte-americano atestou o ato, a autoria não foi confirmada (NYT, 2019).

Assim como o ataque cibernético contra as hidrelétricas da Ucrânia (2015) e o caso do Stuxnet (2009-2010), os ciberataques supostamente realizados pelo Comando Cibernético dos Estados Unidos destruíram o sistema de comando e controle iraniano, especificamente os sistemas de lançamento de mísseis e controle aéreo (THE WASHINGTON POST, 2019; YAHOO! NEWS, 2019). O embate ocasionou uma materialidade relevante, visto que incapacitou a infraestrutura crítica do Irã, mas não resultou em letalidade e nem em explosões (NYT, 2019).

Tal como os outros casos citados no presente trabalho, o conflito cibernético contra as infraestruturas do Irã não teve amparo de normas internacionais; nem a ONU e nem a OTAN comentaram o fato (NYT, 2019; THE GUARDIAN, 2019). Nesse caso, o intentado cibernético teve apoio apenas das leis internas dos Estados Unidos, que segue uma política de estratégia ofensiva no ciberespaço e tem como finalidade proteger e assegurar suas próprias infraestruturas críticas (EUA, 2017).

Logo após o evento cibernético, os parlamentares legislativos do Irã se reuniram e pronunciaram a frase “morte aos Estados Unidos” como forma de protesto à retaliação (REUTERS, 2019). Entretanto, não expressaram vontade política em declarar a ação como um ato de guerra (REUTERS, 2019). A escolha dos Estados Unidos em retaliar o Irã com ataques cibernéticos em vez de ataques cinéticos demonstra que não houve vontade política de Trump em cometer um ato de guerra, pelo contrário, foi uma operação cibernética militar bem planejada e estruturada para não eclodir em um conflito armado (REUTERS, 2019).

5 CONSIDERAÇÕES FINAIS

O presente trabalho parte de um cenário em que o espaço cibernético está cada vez mais inserido na vida do homem. Conforme a tecnologia avança, as atividades diárias e as infraestruturas críticas se tornam progressivamente dependentes desse novo domínio operacional que é o ciberespaço. No entanto, o emprego do espectro eletromagnético atinge também outras esferas, que são os confrontos de zona cinzenta, conhecido como conflitos de baixa intensidade que se encontram entre a paz e a guerra (FITTON, 2016; MAZARR, 2015; WIRTZ, 2017).

As incertezas que abarcam a guerra cibernética permitem que haja um aumento exponencial dos ataques cibernéticos. As agressões cibernéticas podem "somente" derrubar uma página na internet, como também ocasionar a destruição de infraestruturas críticas, como geralmente ocorre em uma guerra tradicional. Nesse contexto de zona cinzenta, a Segurança e Defesa dos Estados encontram-se ameaçadas. Eis que, como forma de contribuição à área de Segurança e Defesa Cibernética, a dissertação buscou compreender o que caracterizaria uma agressão cibernética como "ato de guerra" e os elementos que até o momento impossibilitaram esta caracterização.

Destaca-se que o intuito de analisar os elementos que dificultam atribuir o ato de guerra nos ataques cibernéticos partiu do debate sobre a guerra cibernética entre Thomas Rid e John Stone. As ponderações suscitadas por Rid (2012) levam a crer que os conflitos cibernéticos não passarão de ações de sabotagem, de espionagem e de subversão e por essas três características nunca poderão ser configurados como atos de guerra. Em resposta, Stone (2013) entende que uma incursão cibernética pode possuir como intenção sabotar, espionar e subverter e ainda ser considerada um ato de guerra. Logo, o trabalho tem o seguinte problema de pesquisa: por que, até hoje, nenhum ataque cibernético foi considerado um ato de guerra? Tem-se como hipótese que os eventos cibernéticos não foram amplamente considerados atos de guerra por conta das imprecisões relacionadas à configuração dos elementos essenciais de materialidade e atribuição dos ataques, à legislação internacional e à vontade política.

À vista disso, a pesquisa foi dividida em três capítulos. No primeiro capítulo foi construída uma base conceitual para ser utilizada em toda dissertação. Foram exploradas diversas conceituações de guerra, atos de guerra, espaço cibernético e guerra cibernética. A exploração da definição de guerra iniciou-se pela Teoria de Guerra de Clausewitz (1984); o conceito desenvolvido pelo estrategista militar, no século XIX, é utilizado até

os dias atuais para analisar os conflitos armados. Clausewitz (1984) compreende que toda guerra é violenta, imprevisível e subordinada à política.

A seguir, o conceito de guerra de outros autores foi levado em questão (WRIGHT, 1988; MEI, 2018; DINSTEIN, 2003; SILVA, 2018; VISACRO, 2009). Existem alguns pontos de divergência entre os autores, como por exemplo a guerra ser declarada de forma técnica ou material; a proporcionalidade "adequada" de violência que um conflito armado precisa incitar para ser declarado como ato de guerra; e a ocorrência de atos de guerra por atores não estatais. No entanto, os autores concordam em um ponto: a guerra sempre será subordinada à política.

Para o trabalho, foi definido que a guerra é um fenômeno social, subordinado à política, que será permeado por um confronto violento entre Estados e/ou atores não estatais. A ocorrência da guerra poderá ser precedida por uma declaração formal ou pela ocorrência de hostilidades, de atividades militares ou de ataques violentos de uma forma geral. Por fim, determina-se que, caso haja uma intimidação ou um ato de agressão violento desferido por um Estado ou por um ator não estatal que ameace/ataque um Estado, poderá se configurar uma guerra.

Em seguida, buscou-se elucidar as particularidades que conceituam o ato de guerra (GROTIUS, 2005; WRIGHT, 1988; DINSTEIN, 2003; FULLER, 1966; KEEGAN, 2006; GOLDONI, 2011; HART, 2009; MEI, 2018; SINGER; FRIEDMAN, 2014; ONU, 1945; OTAN, 1949). Nessa seção, constatou-se que os conflitos gerados por atores estatais ou não estatais, que causam o desequilibro de poder entre os Estados; interfiram na manutenção da paz e na soberania de um Estado; e por fim, ameaçam a Segurança Internacional, poderão ser classificados como atos de guerra.

Como a intenção da pesquisa enseja o debate acerca dos conflitos cibernéticos como atos guerra, foi imprescindível analisar diversos conceitos no que tange o ciberespaço (NYE, 2010, 2011; SINGER; FRIEDMAN, 2014; LIBICKI, 2009; VENTRE, 2011; NIELSEN, 2012; MEDEIROS; GOLDONI, 2020). Optou-se por definir o conceito de forma a adequá-lo ao trabalho. Logo, o espaço cibernético é entendido como um novo domínio operacional de guerra, composto por estruturas físicas e virtuais que são manipulados pelos atores cibernéticos, sendo os componentes físicos os computadores, celulares, satélites, infraestruturas críticas, dentre outros,e os componentes virtuais os *softwares*, como os bancos de dados, sistemas operacionais online, rede de computadores e as plataformas digitais. Essas características interagem entre si pela ação do ator cibernético, que o utiliza para inúmeras finalidades, como por exemplo a

realização de uma atividade profissional e para perpetrar conflitos que podem ensejar até mesmo uma guerra.

No final do primeiro capítulo foram estudadas uma série de entendimentos no que concerne à guerra cibernética (LIND, 1989; ARQUILLA; RONFELDT, 1993; LOBATO; KENKEL, 2015; AYRES; GRASSI, 2020; LIBICKI, 2009; CLARKE; KNAKE, 2015; CAVELTY, 2010; VENTRE, 2011; RID, 2012; STONE, 2013; WIRTZ, 2077; FITTON, 2016; EUA, 2017; ONU, 2012; OTAN, 2016). Foi possível observar que o conceito possui significados extremamente distintos entre si. Nessa seção é destacado que a ciberguerra é um novo tipo de confronto, passiva de transformações futuras.

Até o momento, os eventos cibernéticos se enquadram em uma agressão não convencional. Isto é, se encontram em uma zona cinzenta, o *Gray Zone Conflict*, o termo é utilizado para denotar "confrontos na extremidade inferior do espectro de conflito em que a guerra ainda não está em andamento, mas a coerção militar está ocorrendo para alterar o *status quo*"[96] (WIRTZ, 2017, p. 106, tradução própria). Especula-se que Estados, como os Estados Unidos, realizam operações militares cibernéticas ofensivas, nesse entendimento de zona cinzenta, como forma de abster-se de uma guerra, mas existem vertentes alterando o *status quo*. Espera-se que, em futuros trabalhos, a análise seja aprofundada para compreender a relação entre os conceitos de guerra e ciberguerra com o conceito de *Gray Zone Conflict*. Por fim, o primeiro capítulo encerra-se com a definição de guerra cibernética, que é compreendida como a ocorrência de incursões cibernéticas realizadas por atores estatais e não estatais que causam impactos destrutivos aos Estados acerca de sua soberania e de seus serviços essenciais; possui natureza de guerra irregular; e sua arena de conflito ocorre por intermédio do ciberespaço.

O segundo capítulo buscou responder o problema de pesquisa e, por conseguinte, analisar a hipótese suscitada na introdução. Nesse sentido, foram averiguados os elementos que dificultam classificar os confrontos cibernéticos como atos de guerra. O capítulo partiu do debate entre Rid (2012) e Stone (2013). Na seção foi possível demonstrar que as ações de sabotagem, de espionagem e de subversão não afastam a atribuição do ato de guerra em um conflito. Por outro viés, Rid (2012) explica que perante a Teoria de Guerra de Clausewitz, uma agressão de guerra precisa ser violenta e ter como resultado a letalidade. Por essa questão, o autor afirma que um ataque cibernético não proporciona a violência necessária para ser classificado como um ato de guerra, pois não

[96][Tradução própria]. No original, lê-se: "confrontations at the low end of the conflict spectrum in which war is not yet underway, but military coercion is occurring to alter the status quo".

ocasiona mortes. Todavia, ao analisar o conceito de guerra, explorou-se que não há nexo entre a letalidade e a violência, e nem sempre um ato de guerra causará mortes (DINSTEIN, 2003; STONE, 2013).

Após a análise de Rid (2012) e Stone (2013) no que diz respeito à guerra cibernética, buscou-se explorar o que de fato dificulta atribuir o ato de guerra nos ciberataques. Nesse sentido, foram elaborados estudos em relação à imprecisão de autoria, à materialidade, à ausência de definição legal e à falta de interesse político no que tange aos ataques cibernéticos.

Quando se explorou a questão de imprecisão de autoria nos ciberataques, foi destacado que existem tecnologias avançadas que conseguem precisar a agressão, contudo, o recurso é complexo e de custo elevado, poucos países dispõe desse ensejo. No mais, encontrou-se uma série de configurações que dificultam confirmar a identidade do ator cibernético. O primeiro ponto que atrapalha a precisão de autoria são as próprias características do espaço cibernético. O novo campo operacional de guerra, que é o ciberespaço, permite que haja distorções e manipulações em seu sistema quanto ao endereço de conexão do agente malicioso.

A segunda premissa é a incerteza, pois ainda que a origem da incursão cibernética seja constatada, descobrir quem de fato foi o executor ou patrocinador da ação cibernética, na maioria das vezes, não será possível. Por exemplo, foi visto no trabalho que em incursões cibernéticas sediadas na China ou na Rússia, geralmente o Estado está vinculado ao ataque cibernético, mas não tem como garantir essa presunção. Sendo assim, conclui-se que sem a identificação da autoria nos eventos cibernéticos, não há como punir ou responsabilizar o ator cibernético malicioso.

Na segunda particularidade do problema de pesquisa, que é a materialidade da guerra cibernética, foi observado que na maioria dos ciberataques, a materialidade é baixa e se situa na esfera virtual. A título de exemplo, tem-se os ataques de negação, os *DDos*, que têm como resultado o bloqueio de um site ou até mesmo a sua exclusão. Posto isso, conclui-se que poucas agressões cibernéticas teriam de fato o poder de destruir infraestruturas críticas, pois em apenas alguns casos excepcionais tiveram tal resultado, como por exemplo no caso do Stuxnet (2009-2010). Isso demonstra que a operacionalização de uma incursão cibernética violenta é árdua e cara. Sendo assim, ao relacionar a materialidade dos ataques cibernéticos com o conceito de guerra no primeiro capítulo, constata-se que, no cenário de guerra cibernética, nem todo Estado ou ator não estatal conseguirá ameaçar a Segurança e a Defesa de uma nação.

No quesito da ausência de normas a respeito da guerra cibernética, verificou-se que não há uma lei internacional que considere a possibilidade de os ataques cibernéticos serem classificados como guerra; a ONU (2013) tem como posicionamento que a imprecisão de autoria não permite atribuir o ato de guerra nos eventos cibernéticos. A OTAN (2016) até considera a possibilidade de uma guerra real por meio do espectro eletromagnético, no entanto, assim como a ONU, a Aliança Militar também não desenvolveu normas sobre os intentos cibernéticos.

Após analisar a opinião de diversos especialistas em Segurança e Defesa Cibernética (AYRES; GRASSI, 2020; SINGER; FRIEDMAN, 2014; BLANK, 2017; BANKS, 2013; DIPERT, 2010), observou-se que a falta de definição legal causa insegurança jurídica. O que se tem atualmente é uma série de dúvidas, por exemplo: como retaliar um ataque cibernético? Ou, seria justificável responder um ataque cibernético com um ataque convencional? O que se deduz desse ambiente de incertezas é que talvez não haja interesse das instituições de Segurança Internacional em legislar a respeito do ciberespaço, não apenas em considerar os ataques cibernéticos como atos de guerra, mas também aos atos cibernéticos de espionagem, sabotagem etc. O trabalho verificou que fortuitamente é preferível que se tenha liberdade de ação, o que não seria permitido caso houvesse leis que regulamentassem os ciberataques.

O último elemento analisado, foi a ausência de vontade política em atribuir o ato de guerra nas intercorrências cibernéticas. Notou-se que essa premissa é primordial, pois o propósito político sempre está à frente da guerra; um confronto só existe porque houve uma divergência política entre Estados ou entre um Estado e atores não estatais. Conforme analisado no primeiro capítulo, a guerra se transformou no decorrer do tempo, mas sempre seguiu subordinado à política. Contudo, foi destacado que não é qualquer tipo de manifestação política que irá "conseguir" caracterizar os ataques cibernéticos como atos de guerra, a assimetria de poder entre os Estados deve ser levada em consideração nessa premissa, pois nem todo Estado tem ou terá capacidade de projetar o poder cibernético.

O trabalho explorou que após a Guerra Fria (1947-1989) o mundo se tornou mais globalizado[97], em outras palavras, a subsistência dos Estados depende em muitas frentes

[97]A globalização e a interdependência: é preciso destacar que o assunto gera diversas divergências entre os especialistas de Relações Internacionais. O presente trabalho não tem como finalidade se aprofundar no

um do outro (WIRTZ, 2017). Por conseguinte, entende-se que, de uma forma geral, não há vontade política em declarar guerra, as consequências de um conflito armado atingem o mundo todo. Parece ser mais vantajoso para os Estados se utilizarem da guerra cibernética, que se encontra em uma zona cinzenta, para intentar contra outros Estados ou atores não estatais, do que iniciar uma guerra convencional (MAZARR, 2015; WIRTZ, 2017). Portanto, compreende-se que, enquanto um líder estatal ou a ONU e a OTAN não tiverem interesse político de imputar o ato de guerra nos eventos cibernéticos, eles não serão considerados atos de guerra.

Para elucidar as ponderações levantadas no capítulo dois, no último capítulo foram analisados três casos de eventos cibernéticos: os casos em que a Rússia foi acusada informalmente de ter desferido agressões cibernéticas contra Estados - Estônia em 2007, Geórgia em 2008, e Ucrânia em 2014-2015; o ataque cibernético contra a Usina Nuclear de Natanz, conhecido como Stuxnet (2009-2010); e a agressão cibernética à infraestrutura crítica do Irã realizada pelos Estados Unidos, na gestão Trump, em julho de 2019 (WASHIGTON POST, 2019; YAHOO NEWS, 2019).

Nas análises elaboradas, apurou-se que em todos os casos a autoria das agressões cibernéticas não foram confirmadas, por mais que houvesse indícios de um Estado estar vinculado à ação, nenhum ator cibernético malicioso foi reconhecido. No que se refere à definição legal, nenhuma incursão cibernética citada teve respaldo normativo. Não existem normas internacionais acerca da guerra cibernética. Conforme foi explorado, a ONU não considerada a possibilidade de um evento cibernético ser classificado como ato de guerra, já a OTAN passou a considerar o ciberespaço como domínio operacional de guerra apenas em 2016.

Na esfera da materialidade, algumas agressões cibernéticas estudadas tiveram classificação baixa, dentre elas estão: a Estônia (2007); a Geórgia (2008); e na primeira fase dos ciberataques na Ucrânia (2014). Nessas situações não houve letalidade e nem abatimentos “físicos”, isto é, destruição de hidrelétricas, aeroportos, sistemas de comando e controle. As intercorrências cibernéticas que resultaram em materialidade alta foram: no Stuxnet (2009-2010); na segunda fase dos ataques cibernéticos na Ucrânia (2015); e no ciberataque de retaliação dos Estados Unidos contra o Irã (2019). A dissertação

assunto. Sendo assim, para maior compreensão, orienta-se que sejam analisados os posicionamentos sobre globalização e interdependência de Keohane e Nye (1988); Held e McGrew (2001) e Strange (1994).

concluiu que nesses últimos casos seria possível que o ato de guerra fosse atribuído, porque teve destruição de infraestruturas críticas. Sendo assim, as ações cibernéticas poderiam ser vistas como uma forma de ameaça à soberania dos Estados atacados, no entanto, os outros elementos não se fizeram presentes.

Por fim, foi analisado se houve vontade política em classificar esses ataques cibernéticos como atos de guerra, e verificou-se que apenas no caso da Estônia (2007) existiu algum indício de interesse político. O governo estoniano acusou a Rússia de ter cometido um ato de guerra e invocou o artigo 5º da OTAN. No entanto, a OTAN não quis declarar guerra contra a Rússia, após investigar os fatos, concluiu que a materialidade dos ataques cibernéticos foi de baixo risco e justificou que não havia como confirmar a autoria dos ciberataques. Por fim, a Aliança Militar não teve interesse político. Nos demais casos também não houve vontade política em declarar guerra, nem do Estado que foi acusado de cometer a agressão cibernética e nem da nação que sofreu a incursão.

Análise da Hipótese

Hipótese: os eventos cibernéticos não foram amplamente considerados atos de guerra por conta das imprecisões relacionadas à configuração dos elementos essenciais de materialidade e atribuição dos ataques, à legislação internacional e à vontade política.

Em virtude dos fatos mencionados, entende-se que a hipótese foi comprovada. É possível inferir, a partir dos estudos de caso, que a precisão de autoria dos ataques cibernéticos, a materialidade dos intentos, o respaldo normativo acerca da guerra cibernética e à vontade política são premissas essenciais para atribuir o ato de guerra nas agressões cibernéticas. A ausência de um desses elementos prejudica considerar as incursões cibernéticas como atos de guerra, principalmente a falta de interesse político.

Nesse sentido, caso um ataque cibernético tenha a sua autoria confirmada; possua relevante materialidade, como a destruição ou explosão de infraestruturas críticas e letalidade; esteja ancorado pelas normas internacionais de Segurança e Defesa; e possua vontade política, poderá ser classificado como um ato de guerra. Todavia, vale destacar que, apesar da guerra sempre ser subordinada à política, portanto, o elemento "vontade política" ser essencial para declarar guerra perante um evento cibernético, explorou-se que é necessário avaliar qual é a capacidade que um Estado tem em projetar o poder cibernético. Isto é, deve ser levado em consideração a posição que esse Estado tem no cenário internacional. Não é simplesmente ter vontade política em declarar guerra, mas também de conseguir projetar seus domínios militares, econômicos e tecnológicos.

É reconhecido que as definições no que tange à guerra cibernética encontram-se em uma constante transformação. A pesquisa debateu algumas lacunas que existem a respeito dos conflitos cibernéticos, que foram os quatro elementos apresentados na hipótese: a imprecisão de autoria, a materialidade, a ausência de definição legal e a falta de interesse político. Diante do que foi analisado no presente trabalho é possível afirmar que há um longo caminho a ser construído. Pode ser observado que talvez não haja vontade política dos Estados poderosos, como os Estados Unidos, e até mesmo das instituições de segurança internacional, como a ONU e a OTAN, em definir ou classificar os eventos cibernéticos, pois essa delimitação implicaria na liberdade de ação dessas organizações, é possível que seja preferível manter a guerra cibernética em uma zona cinzenta. Esse é um debate que será construído em um futuro trabalho de doutorado.

Desse modo, compreende-se que todas essas quatro premissas apresentadas no decorrer do trabalho causam vulnerabilidades à Segurança e Defesa dos Estados, principalmente daqueles que não possuem tecnologias tão avançadas. Por seu turno, espera-se que a presente pesquisa possa contribuir para os futuros trabalhos acerca da guerra cibernética, bem como colaborar com as áreas de Ciências Militares e da Segurança e Defesa Cibernética.

REFERÊNCIAS

ARQUILLA, John; RONFELDT, David. **Cyberwar Is Coming!** In: _____ (Org.). In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica: RAND, 1993.

ASSIS, Raquel Lima de. **Inteligência, sabotagem, resistência: história comparada dos serviços de espionagem norte-americano e britânico na Segunda Guerra Mundial (1939-1945**), 2017. Programa de Pós-Graduação em História Comparada da Universidade Federal do Rio de Janeiro. Disponível em <https://bit.ly/34kqmYo>. Acesso em 03 de jan. de 2022.

ARON, Raymond. **Paz e Guerra entre as nações**. Trad. Port. Brasília e São Paulo: IPRI, UNB, Imprensa Oficial, 2002.

AYRES, Danielle; GRASSI, Jéssica. **Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil**. Rev. Bras. Est. Def. v. 7, n. 2, p. 103-131, 2020.

ALJAZEERA. **US 'launched cyberattacks on Iran weapons' after drone downing, 2019**. Disponível em <https://www.aljazeera.com/news/2019/6/23/us-launched-cyberattacks-on-iran-weapons-after-drone-downing >. Acesso em 19 de jul. de 2021.

ALJAZEERA. **Ukraine says evidence suggests Russia behind cyberattack**, 2022. Disponível em <https://www.aljazeera.com/news/2022/1/16/ukraine-claims-russia-behind-cyberattack-in-hybrid-war>. Acesso em 25 de jan. de 2022.

ALJAZEERA. **Iran's Revolutionary Guard shoots down US drone**. 2019. Disponivel em <https://www.aljazeera.com/news/2019/6/20/irans-revolutionary-guard-shoots-down-us-drone>. Acesso em 02 fev. 2022.

ALJAZEERA. **Donald Trump declares US withdrawal from Iran nuclear deal,** 2018. Disponível em < https://www.aljazeera.com/news/2018/5/8/donald-trump-declares-us-withdrawal-from-iran-nuclear-deal>. Acesso em 22 fev. 2022.

ALJAZEERA. **Us democrats blame Russia for cyber attacks**, 2016. Disponível em <https://www.aljazeera.com/news/2016/8/11/us-democrats-blame-russia-for-cyber-attacks>. Acesso em 10 mar. 2022.

ALJAZEERA. **Ukraine says evidence suggests Russia behind cyberattack,** 2022. Disponível em <https://www.aljazeera.com/news/2022/1/16/ukraine-claims-russia-behind-cyberattack-in-hybrid-war>. Acesso em 24 de fev. 2022.

ANEJA, A. **Under cyber-attack, says Iran.** The Hindu, 2010. Disponível em www.thehindu.com/news/international/Under-cyber- attacks-says-Iran/article16048668.ece. Acesso em 19 jun. 2021.

BANKS, William. **The Role Of Counterterrorism Law in Shaping ad Bellum Norms for Cyber Warfare,** 2013. International Law Studies. US Naval War College. Disponível em < https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1028&context=ils **>.** Acesso em 26 de jan. de 2022.

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

BBC News. **Massive ransomware infection hits computers in 99 countries.** 2017. Disponível em <https://www.bbc.com/news/technology-39901382>. Acesso em 23 de mar. 2021.

BBC News. **Microsoft accuses China over email cyber-attacks**, 2021. Disponível em < https://www.bbc.com/news/business-56261516 >. Acesso em 04 fev. 2022.

BBC NEWS. **Iran nuclear talks: 'Historic' agreement struck,** 2015. Disponível em < https://www.bbc.com/news/world-middle-east-33518524 >. Acesso em 22 fev. 2022.

BERNARDES, Amanda Rodrigues e ÀVILA, Karen Ludmila Barreto de. **O ato de guerra e o ataque cibernético: o caso STUCNET na visão de Clausewitz.** Observatório da Praia Vermelha. ECEME: Rio de Janeiro, 2021.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética – MD 31- M 07**. 18 de novembro de 2014. Disponível em <https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf > Acesso em 03 mar. 2022.

BRASIL. **Constituição da República Federativa do Brasil**. Presidência da República – Casa Civil. 1988. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm> Acesso em 25 fev. 2022.

CAVELTY, Myriam Dunn. **Cyber-Security.** The Routledge Handbook of New Security Studies Routledge. 2010.

CARNEIRO, Henrique. **Guerra dos Trinta Anos**. In: MAGNOLI, Demétrio (org.) História das Guerras. São Paulo: Contexto, 2006.

CENTCOM. **Unexploded Limpet Mine Removed from M/T Kokuka Courageous in the Gulf of Oman, 2019**. Disponível em <https://bit.ly/3Ig7GYf>. Acesso em 23 fev. 2022.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber War: The Next Threat to National Security and What To Do About It**. Nova York: Ecco, 2015.

CLAUSEWITZ, C. von; HOWARD, M.; PARET, P. (Eds.). ***On War***. Princeton: Princeton University Press, 1984.

CLAUSEWITZ, C. von. **Da guerra**. Tradução de Maria Teresa Ramos. 3. ed. São Paulo: Martins Fonte, 2010.

CCDCOE. **The NATO Cooperative Cyber Defence Centre of Excellence, 2021.** Disponível em <https://ccdcoe.org/about-us/>. Acesso em 05 de maio de 2021.

CNN. **Study warns of cyberwarfare during military conflicts**, 2009. Disponível em <https://edition.cnn.com/2009/US/08/17/cyber.warfare/index.html?iref=nextin. Acesso em 06 fev. 2022.

DINSTEIN, Y. **War, Aggression and Self-Defence.** Editora Cambridge University Press, 2003.

DAFLON, Cap QMB Marlon Anderson Santiago. **Modelos de Dominação do Espaço Cibernético: As abordagens brasileira e russa à guerra cibernética**. Escola de Aperfeiçoamento de Oficiais. 2020. Disponível em <https://bdex.eb.mil.br/jspui/bitstream/123456789/8557/1/AC%20-%20Daflon.pdf >. Acesso em 19 de jan. de 2022.

DANCHO, Danchev. **Coordinated Russia vs Georgia cyber attack in progress,** 2008. Disponível em <https://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670>. Acesso em 02 jan. 2022.

DIPERT, R. R. **The Ethics of Cyberwarfare**. Journal of Military Ethics, v. 9, n. 4, p. 384-410, 2010.

DRAPER, G. I. A. D. **Grotius' Place in the Development of Legal Ideas about War**. In: BULL, Hedley; KINGSBURY, Benedict; ROBERTS, Adam. *Hugo Grotius and International Relations*. Oxford: Claredon Press, 1995.

EUA. **National Cyber Strategy**, 2017. Disponível em <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>. Acesso em 02 mar. 2022.

EUA. **Remarks by President Biden at the Office of the Director of National Intelligence**, 2021. Disponível em < https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/27/remarks-by-president-biden-at-the-office-of-the-director-of-national-intelligence/ >. Acesso em 26 de jan. de 2022.

EUA. **President Donald J. Trump is Ending United States Participation in an Unacceptable Iran Deal**, 2018. Disponível em <https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-ending-united-states-participation-unacceptable-iran-deal/>. Acesso em 23 fev. 2022.

FERNANDES, J. P. T. **A ciberguerra como nova dimensão dos conflitos do século XXI**. Relações Internacionais, p. 53-69, mar. 2012.

FERREIRA, A. B. H. **Novo Dicionário da Língua Portuguesa.** 2ª edição. Rio de Janeiro. Nova Fronteira. 1986. p. 1 623.

FITTON, Oliver. **Cyber operations and gray zones_ Challenges for NATO.** Connections, v. 15, n. 2, p. 109-119, 2016.

FULLER, J. F. C. **A conduta da guerra de 1789 aos nossos dias**. Rio de Janeiro, Editora Bibliex, 1966.

FORTINET. **Brasil começa o ano com mais de 3,2 bilhões de tentativas de ciberataques**, **2021**. Disponível em < https://bit.ly/3BHeFY6 >. Acesso em 20 jun. 2021.

GALTUNG, Johan. **Violence, Peace and peace research**. International Peace Research Institute. Journal of Peace Research, Vol. 6, No. 3, 1969, pp. 167-191. Disponível em <https://www.jstor.org/stable/422690>. Acesso em 28 set. de 2021.

GARCIA, Francisco Proença. **Descrição do fenómeno subversivo na actualidade. A estratégia da Contra-subversão.** 2007. Contributos Nacionais, In Moreira, Adriano & Ramalho, Pinto (Coord), *Estratégia*, Vol XVII, Instituto Português da Conjuntura Estratégica, Lisboa, ISSN 1645-9083, pp. 113-182.

GEORGE, Alexander L. et al. **Case studies and theory development in the social sciences**. Mit Press, 2005.

GERHARDT, Tatiana E.; SILVEIRA, Denise T. **Métodos de pesquisa**. Coordenado pela Universidade Aberta do Brasil – UAB/UFRGS e pelo Curso de Graduação Tecnológica – Planejamento e Gestão para o Desenvolvimento Rural da SEAD/UFRGS. Porto Alegre: Editora da UFRGS, 2009.

GOLDONI, Luiz Rogério Franco. **Indústria de Defesa no Brasil entre as duas Guerras Mundiais /**. Luiz Rogério Franco Goldoni, Niterói: UFF, 2011.

GOMES, Michel. **Estudo de caso sobre o conflito cibernético entre a Rússia e a Geórgia**, 2018. Universidade de Brasília – Departamento de História, 2018. Disponível em https://bdm.unb.br/bitstream/10483/22858/1/2018_MichelGomesNogueira_tcc.pdf>. Acesso em 04 fev. 2022.

GOMES, Pedro H. M.; ALVES, Vágner Camilo. **Clausewitz, a Ciberguerra e a Guerra Russo-Georgiana**. Rev. Carta Inter., Belo Horizonte, v. 15, n. 3, 2020, p. 232-254, 2020.

GONÇALVES, Ricardo. **A primeira guerra cibernética: os ataques cibernéticos contra a Estônia,** em 2007, à luz da teoria dos cinco anéis do Coronel John Warden, 2018. Escola de Guerra Naval. Disponível em <https://www.marinha.mil.br/egn/sites/www.marinha.mil.br.egn/files/CEMOS%20023%20MONO%20CC%20RICARDO%20PENEDO.pdf>. Acesso em 12 jan. 2022.

GROTIUS, H. **O direito da guerra e da paz.** v.I. Trad. Ciro Mioranza. Ijuí: Editora Unijui, 2005.

HART, Liddel B. H**. As Grandes Histórias da Guerra.** Editora Ibrasa, São Paulo. 6 Edição, 2009.

HEYDTE, von der Friedrich August Freiherr, **A guerra irregular moderna em políticas de defesa e como fenômeno militar,** Rio de Janeiro, Bibliex, 1990.

HELD, D. e MCGREW, A. **Prós e Contras da Globalização**. Rio de Janeiro: Jorge Zahar Ed., 2001.

HOBSBAWM, Eric J. ERIC J. **A Era das Revoluções**. Europa 1789-1848. Tradução de. Maria Tereza Lopes Teixeira. Marcos Penchel. 10. Edição 10, 2012.

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 dez. 2021.

HORN, Eva. **Knowing the Enemy: The Epistemology of Secret Intelligence**. 2003. Translation from the German by Sara Ogger. Published in Grey Room 11, May 2003.

IAEA. **Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions in the Islamic Republic of Iran**, 2011. Disponível em <https://www.iaea.org/sites/default/files/gov2011-7.pdf>. Acesso em 04 mar. 2022.

INTERPOL. **Interpol report shows alarming rate of cyberattacks during COVID-19. 2020.** Disponível em **<** https://bit.ly/2SyG9gp**>.** Acesso em 23 de mar. 2021.

IRNA. **Iran shoots down US spy drone.** 2019. Disponível em <https://en.irna.ir/news/83362061/Iran-shoots-down-US-spy-drone>. Acesso em 12 fev 2022.

ISIS. **Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment**, 2010. Disponível em < https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/>. Acesso em: 23 fev 2022.

KEEGAN, J. **Uma história da Guerra.** São Paulo: Companhia de Bolso, 2006.

KEOHANE, R. e NYE, J. **Power and Interdependence: World Politics in Transition**. Boston: Little, Brown, 1988.

LANGNER, Ralph. **A declaration of bankruptcy for US critical infrastructure protection. The Last Line of Cyber Defense**, 3 June. 2011. Disponível em <https://www.langner.com/2011/06/a-declaration-of-bankruptcy-for-us-critical-infrastructure-protection/>. Acesso em 10 mar. 2022.

LEVY, Pierre. **O que é virtual?** Editora 34, São Paulo, 1999.

LIND, William. S. **The Changing Face of War: Into the Fourth Generation**. Marine Corps Gazette, 1989.

LIBICKI, Martin C. **Cyberdeterrence and Cyber War**. Santa Monica: RAND, 2009.

LOBATO, L. C.; KENKEL, K. M. **Discourses of cyberspace securitization in Brazil and in the United States**. Revista Brasileira de Política Internacional, v. 58, n. 2, p. 23-43, 2015.

MAURER, T. **Cyber Proxies and the Crisis in Ukraine**. In: Geers, K (ed.). Cyber War in Perspective: Russian Aggression Against Ukraine. p.79-86NATO CCDCOEPublications. Tallinn 2015.

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

MAZARR, Michael J. **Mastering the gray zone_ understanding a changing era of conflict.** US Army War College Carlisle, 2015.

MEI, E. **Dicionário de Segurança e Defesa**. Héctor Luis Saint-Pierre (ORG.), Mariana Gisela Vitteli (ORG.). Editora UNESP, 2018.

MEDEIROS, B. P.; GOLDONI, L. R. F. **The Fundamental Conceptual Trinity of Cyberspace. Contexto Internacional,** Vol. 42, N° 1, Jan/Apr, 2020.

MONGRENIER, Jean-Sylvestre; THOM, Françoise. **Gèopolitique de La Russie**. Paris: Presses Universitaires De France. 2016.

NEW YORK TIMES. **Animated Map of How Tens of Thousands of Computers Were Infected With Ransomware,** 2017. Disponível em <https://nyti.ms/2Q3bmre>. Acesso 23 de mar. 2021.

NEW YORK TIMES. **Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government,** 2014. Disponível em <https://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html>. Acesso em 12 fev. 2022.

NEW YORK TIMES. **Israeli Test on Worm Called Crucial in Iran Nuclear Delay,** 2011. Disponível em https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html. Acesso em 06 mar. 2022.

NEW YORK TIMES. **Trump Abandons Iran Nuclear Deal He Long Scorned,** 2018. Disponivel em < https://www.nytimes.com/2018/05/08/world/middleeast/trump-iran-nuclear-deal.html>. Acesso em 22 fev. 2022.

NEW YORK TIMES. **Russia cyber hack Trump,** 2019. Disponível em https://nyti.ms/2RCPrYo. Acesso em 23 de mar. 2021.

NEW YORK TIMES. **In Estonia, what may be the first war in cyberspace,** 2007. Disponível em <https://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html >. Acesso em 24 fev. 2022.

NEW YORK TIMES. **Russia Appears to Carry Out Hack Through System Used by U.S. Aid Agenc, 2021**. Disponível em <https://www.nytimes.com/2021/05/28/us/politics/russia-hack-usaid.html >. Acesso em 22 jul. 2021.

NEW YORK TIMES. **Before the Gunfire, Cyberattacks**, 2008. Disponível em <https://www.nytimes.com/2008/08/13/technology/13cyber.html>. Acesso em 14 fev. 2022.

NEW YORK TIMES. **F.B.I. Identifies Group Behind Pipeline Hack, 2021.** Disponível em < https://www.nytimes.com/2021/05/10/us/politics/pipeline-hack-darkside.html >. Acesso em 19 jul. 2021.

NEW YORK TIMES. **Animated Map of How Tens of Thousands of Computers Were Infected With Ransomware, 2017**. Disponível em < https://nyti.ms/3BaGSFe>. Acesso em 12 set. 2021.

NEW YORK TIMES. **Russia-Ukraine War.** 2022. Disponível em https://www.nytimes.com/news-event/ukraine-russia. Acesso em 15 de mar. 2022.

NEW YORK TIMES. **Utilities Cautioned About Potential for a Cyberattack, 2016.** Disponível em <https://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html>. Acesso em 23 de fev. 2022.

NEW YORK TIMES. **In the Trenches of Ukraine's Forever War**, 2022. Disponível em <https://www.nytimes.com/2022/01/16/magazine/ukraine-war.html. Acessado em 25 de jan de 2022.

NEW YORK TIMES. **Obama Ordered wave of cyberattacks against Iran**, 2012. Disponível em < https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html >. Acesso em 18 maio 2021.

NEW YORK TIMES. **U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say,** 2019. Disponível em <https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html>. Acesso em 23 jan 2022.

NIELSEN, Suzanne C. **Pursuing security in cyberspace: Strategic and organizational challenges**. **Orbis,** v. 56, n. 3, p. 336-356, 2012.

NUNES, Luiz Artur Rodrigues. **Guerra Cibernética e o Direito Internacional: Aplicabilidade do Jus ad Bellum e do Jus in Bello** / Contra-Almirante (FN) Luiz Artur Rodrigues Nunes. - Rio de Janeiro: ESG, 2015. Disponível em:https://repositorio.esg.br/bitstream/123456789/1277/1/Luiz%20Artur%20RODRIGUES%20Nunes.pdf. Acesso em 20 de jan. de 2022.

NYE, Joseph S. **Cyberpower.** *Harvard Kennedy School*, 2010. Disponível em: <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf>. Acesso em 05 out. 2021.

NYE, Joseph S. **The future of power.** New York: Public Affairs, 2011.

OLSON, P. **We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency, 2012**. New York: Little, Brown and Company.

OTAN. **Cyber Defense.** 2021. Disponível em <https://www.nato.int/cps/en/natohq/topics_78170.htm>. Acesso em 25 de mar. 2021.

OTAN. **Tratado do Atlântico Norte.** 1949. Disponível em < https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=pt>. Acesso em 26 de mar. 2021.

ONU. **One place where the world's nations can gather together, discuss common problems and find shared solutions,** 2021. Disponível em <https://www.un.org/en/about-us>. Acesso em: 26 mar. 2021.

ONU. **Carta das Nações Unidas.** 1945. Disponível em < http://www.planalto.gov.br/ccivil_03/decreto/1930-1949/d19841.htm>. Acesso em 03 mar. 2022.

ONU. **Cyberconflicts and National Security.** 2013. Disponível em < https://www.un-ilibrary.org/content/journals/15643913/50/2/4/read>. Acesso em 12 mar. 2022

PETERS, Michele et al. **Research into headache: the contribution of qualitative methods.** Headache: The Journal of Head and Face Pain, v. 42, n. 10, p. 1051-1059, 2002.

PARET, P. **Expansão da Guerra – Clausewitz. Construtores da estratégia moderna. t.1**. Rio de Janeiro: Biblioteca do Exército, 2015.

PERKOVICH, George. **Understanding Cyber Conflict**, 2017. Disponível em < https://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_FullText.pdf. Acesso em 12 jan. 2022.

PIERRE, Luis Saint-Pierre & VITTELLI, Mariana G. **Dicionário de Segurança e Defesa.** Editora UNESP, 2018.

POLIT, D. F.; BECK, C. T.; HUNGLER, B. P. **Fundamentos de pesquisa em enferma- gem: métodos, avaliação e utilização**. Trad. de Ana Thorell. 5. ed. Porto Alegre: Artmed, 2004.

POLITICO. **DOD could use force in cyber war**, 2011. Disponível em < https://www.politico.com/story/2011/07/dod-could-use-force-in-cyber-war-059035> . Acesso em 26 jan. de 2022.

POUGET, Émile. **Le Syndicat.** Nancy: Reveil Ouvrier, 1910.

QUIVY, R.; CAMPENHOUDT, L. V. **Manuel de recherche en sciences sociales**. Paris: Du- nod, 2005.

REUTERS. **U.S. blames North Korea for 'WannaCry' cyber attack, 2017**. Disponível em <https://www.reuters.com/article/us-usa-cyber-northkorea-idUSKBN1ED00Q>. Acesso em 03 de out. 21.

REUTERS. **U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials.** 2019. Disponível em <https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive-idUSKBN1WV0EK . Acesso em 11 jan. 2022.

REUTERS. **Iran admits cyberattack on nuclear plants,** 2010. Disponível em <https://www.reuters.com/article/us-iran-idUSTRE6AS4MU20101129>. Acesso em 03 mar. 2022.

REUTERS. **Iran's U.N. mission rejects 'unfounded' U.S. claim over Gulf of Oman tanker attacks.** 2019. Disponivel em < https://www.reuters.com/article/mideast-tankers-iran-un-idINKCN1TE3D3>. Acesso em 12 fev. 2022.

RID, T. **Cyberwar will not take place!**. Journal of Strategic Studies, 2012.

RID, T.; BUCHANAN, B. **Attributing cyber attacks. Journal of Strategic Studies**, v. 38, n. 1-2, p. 4-37, 2015.

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

SCHNEIER, Bruce. **Cyberconflits and National Security**. 2013. ONU. Disponível em< https://www.un-ilibrary.org/content/journals/15643913/50/2/4/read>. Acesso em 15 de jun. de 2021.

SILVA, Júlio Cezar Barreto Leite da. **Guerra cibernética: a guerra no quinto domínio, conceituação e princípios.** Revista da Escola de Guerra Naval 20, no. 1: 193-211 (Jan./Jun.). Rio de Janeiro. 2014.

SILVA, Teixeira F. **Dicionário de Segurança e Defesa**. São Paulo. Editora Unesp Digital, 2018.

SILVA, Douglas Luís da. **O mundo globalizado da Indústria 4.0 e as guerras tecnológicas: as potencialidades e os desafios da Artilharia de Campanha do Brasil**. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2020.

SINGER, P.; FRIEDMAN, A. **Cybersecurity and Cyberwar: What Everyone Needs to Know.** Oxford University Press. 1. ed., jan. 2014.

STEVENS, Tim. **Cyberweapons: Power and the governance of the invisible**. International Politics, 55(3-4), 482-502. 2018.

STONE, John. **Cyber War *Will* Take Place!** In: The Journal of Strategic Studies, Vol. 36, n. 1, p. 101-108, 2013.

STRANGE, S. **States and Markets.** 2a. edição, Londres: Pinter Publishers, 1994.

SILVA, Carlos M. V. **A transformação da guerra na passagem para o século XXI. Um estudo sobre a atualidade do paradigma de Clausewitz.** Dissertação de Mestrado. Orientador: Prof. Dr. João Roberto Martins Filho. São Carlos-SP Julho 2003.

TABANSKY, Lior. **Basic Concepts in Cyber Warfare**. Military and Strategic. Affairs, v. 3, n. 1, p. 75-92, 2011.

TEIXEIRA JÚNIOR, A. W. M.; VILAR-LOPES, G.; FREITAS, M. T. D. **As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica**. Carta Internacional. Belo Horizonte, v. 12, n. 3, p. 30-53, 2017.

THE TELEGRAPH. **Georgia: Russia 'conducting a cyberwar',** 2008. Disponível em <https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html>. Acesso em 26 fev. 2022.

THE GUARDIAN. **Titan Rain - how Chinese hackers targeted Whitehall**, 2007. Disponível em < https://www.theguardian.com/technology/2007/sep/04/news.internet>. Acesso em 23 mar. 2022.

THE GUARDIAN. **Russia accused of unleashing cyberwar to disable Estonia**, 2007. Disponível em <https://www.theguardian.com/world/2007/may/17/topstories3.russia> Acesso em 23 fev. 2022.

THE GUARDIAN. **Ukrainian blackout caused by hackers that attacked media company, researchers say,** 2016. Disponível em https://www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company. Acesso em 14 mar. 2022.

THE GUARDIAN. **Donald Trump calls Iran attack on US drone a 'big mistake'.** 2019. Disponível em < https://www.theguardian.com/world/2019/jun/20/iran-claims-us-drone-shot-down-missile-strike-saudi-arabia-trump-yemen>. Acesso em 05 fev. 2022.

THE GUARDIAN. **Two oil tankers attacked in Gulf of Oman,** 2019. Disponível em https://www.theguardian.com/world/2019/jun/13/oil-tankers-blasts-reports-gulf-of-oman-us-navy. Acesso em 23 fev. 2022.

THE GUARDIAN. **Iran deal: Trump breaks with European allies over 'horrible, one-sided' nuclear agreement,** 2018. Disponível em https://www.theguardian.com/world/2018/may/08/iran-deal-trump-withdraw-us-latest-news-nuclear-agreement. Acesso em 22 fev. 2022.

THE GUARDIAN. **Trump says US response to oil attack depends on Saudi Arabia's assessment,** 2019. Disponível em < https://www.theguardian.com/world/2019/sep/16/iran-trump-saudi-arabia-oil-attack-assessment-latest. Acesso em 23 fev. 2022.

THE WASHINGTON POST. **Trump approved cyber-strikes against Iranian computer database used to plan attacks on oils tankers**, 2019. Disponível em < https://wapo.st/37AMW0D. Acesso em 21 fev. 2022.

THE WASHINGTON POST. **IAEA says foreign expertise has brought iran to threshold of nuclear capability,** 2011. Disponível em https://wapo.st/3tgniGY. Acesso em 12 mar. 2022.

THE WASHINGTON POST. **Trump authorizes offensive cyber operations to deter foreign adversaries Bolton says,** 2019. Disponível em https://wapo.st/3ustTfB. Acesso em 04 de maio de 2021.

VENTRE, D. **Ciberguerra.** In: Academia General Militar. Seguridad global y potências emergentes em um mundo multipolar. XIX Curso Internacional de Defensa. Espanha: Universidad Zaragoza. 2011.

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

WALTZ, Kenneth. **Teoria das Relações Internacionais**. Trad. Port. Lisboa: Gradiva, 2002.

WEEDON, J. **Beyond Cyber War: Russia´s use of Strategic Cyber Espionage and Information Operations in Ukraine**. In: Geers, K (ed.). Cyber War in Perspective: Russian Aggression Against Ukraine. p.67-77NATO CCDCOE Publications. Tallinn. 2015.

WHITEHEAD, David E.; OWENS, Dennis G.; SMITH, Jess. **Interrupção de Energia Induzida por Ataque Cibernético na Ucrânia: Análise e Estratégias Práticas de Mitigação.** Schweitzer Engineering Laboratories, Inc. A edição revisada anterior foi lançada em outubro de 2016. Originalmente apresentado na 43rd Annual Western Protective Relay Conference, outubro de 2016.

WIRED. **Ahmadinejad's getty pretty tired of this dead scientist crap,** 2010. Disponível em <https://www.wired.com/2010/12/ahmadinejads-getting-pretty-tired-of-this-dead-scientist-crap/>. Acesso em 01 mar. 2022

WIRTZ, J. J. **Life in the "Gray Zone": observations for contemporary strategists.** Defense & Security Analysis, v. 33, n. 2, p. 106-114, 2017.

WRIGHT, Quincy. **A Guerra**. Condensado por Louise Leonard Wright e traduzido por Delcy G. Doubrawa. 1988.

WOLOSYN, André Luís. **Guerra nas Sombras:** Os bastidores dos serviços secretos internacionais. São Paulo : Contexto, 2013.

YAKEMTCHOUK, Romain. **La Politique Etrangère de La Russie**. Paris; L'harmattan. 2008.

YAHOO NEWS. **US launched cyber attacks on Iran after drone shootdown**. 2019. Disponível em <https://news.yahoo.com/us-launched-cyberattacks-iran-drone-shootdown-reports-232123877.html>. Acesso em 10 jul. 2021.

ZETTER, Kim. **Contagem Regressiva até Zero Day**. Editora Brasport, 2014.