ESCOLA DE GUERRA NAVAL

CMG (FN) WAGNER GRUND MARINHO

O DIREITO INTERNACIONAL DOS CONFLITOS ARMADOS E OS ATAQUES CIBERNÉTICOS

Análise no Contexto da Anexação da Crimeia (2013-2017)

Rio de Janeiro

2024

CMG (FN) WAGNER GRUND MARINHO

O DIREITO INTERNACIONAL DOS CONFLITOS ARMADOS E OS ATAQUES CIBERNÉTICOS

Análise no Contexto da Anexação da Crimeia (2013-2017)

Tese apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Política e Estratégia Marítimas.

Orientador: CMG (RM1-FN) Henrique Santos

Rio de Janeiro

Escola de Guerra Naval

2024

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

Declaro que este trabalho acadêmico: a) corresponde ao resultado de investigação por mim desenvolvida, enquanto discente da Escola de Guerra Naval (EGN); b) é um trabalho original, ou seja, que não foi por mim anteriormente utilizado para fins acadêmicos ou quaisquer outros; c) é inédito, isto é, não foi ainda objeto de publicação; e d) é de minha integral e exclusiva autoria.

Declaro também que tenho ciência de que a utilização de ideias ou palavras de autoria de outrem, sem a devida identificação da fonte, e o uso de recursos de inteligência artificial no processo de escrita constituem grave falta ética, moral, legal e disciplinar. Ademais, assumo o compromisso de que este trabalho possa, a qualquer tempo, ser analisado para verificação de sua originalidade e ineditismo, por meio de ferramentas de detecção de similaridades ou por profissionais qualificados.

Os direitos morais e patrimoniais deste trabalho acadêmico, nos termos da Lei 9.610/1998, pertencem ao seu Autor, sendo vedado o uso comercial sem prévia autorização. É permitida a transcrição parcial de textos do trabalho, ou mencioná-los, para comentários e citações, desde que seja feita a referência bibliográfica completa.
Os conceitos e ideias expressas neste trabalho acadêmico são de responsabilidade do Autor e não retratam qualquer orientação institucional da EGN ou da Marinha do Brasil.

gov.br
Documento assinado digitalmente
WAGNER GRUND MARINHO
Data: 21/11/2024 13:40:17-0300
Verifique em https://validar.iti.gov.br

RESUMO

O objeto de pesquisa dessa tese são as operações cibernéticas realizadas no contexto da anexação da Crimeia pela Rússia, e que se tem conhecimento até o momento, entre 2013 e 2017, diante do regime jurídico aplicado à condução dos conflitos armados, particularmente nas interpretações da aplicação desse regime quanto ao uso de operações cibernéticas nos conflitos armados. O estudo partiu do previsto nas Regras do Manual de Tallinn 1.0, da interpretação de alguns Estados e Organismos Internacionais, e de autores como Heather Harrison, no que se refere a aplicabilidade do Direito Internacional aos ataques cibernéticos. A partir de tal estudo chegou-se a um dos objetivos, compor um entendimento da aplicação do Direito Internacional aos ataques cibernéticos. A compreensão da crise da Crimeia como conflito armado internacional também é importante para aplicação do Direito Internacional dos Conflitos Armados (DICA), e essa interpretação é feita com base no entendimento de Yohan Dinstein, da ocorrência da guerra no sentido material, e das definições de Agressão da Assembleia Geral da ONU. A partir desse entendimento, procedeu-se a identificação dos efeitos colaterais, na população ucraniana, dos ataques cibernéticos analisados realizados na Ucrânia, no contexto da anexação da Crimeia pela Rússia, entre 2013 e 2017. Utilizando a composição um entendimento da aplicação do Direito Internacional aos ataques cibernéticos, verificou-se se tais ataques tiveram aderência ao DICA, particularmente quanto aos princípios da Distinção e da Proporcionalidade, objetivo do estudo. Dessa forma, concluiu-se que dentre os ataques cibernéticos direcionados contra a Ucrânia, o ataque de junho de 2017 por meio do NotPetya teve gravidade suficiente para contrariar o princípio da Distinção e a regra 43 do Manual de Tallinn, de proibição da utilização de Meios e Métodos Indiscriminados. Por outro lado, na análise dos demais ataques cibernéticos (Operação Armagedon – 2013; Operação Potao – 2014; e os ataques cibernéticos a infraestruturas de energia da Ucrânia - 2015 e 2016), não foram observados elementos que contrariem os Tratados, a Doutrina e a Jurisprudência do Direito Internacional dos Conflitos Armados.

Palavras-chave: Ataques Cibernéticos. Crimeia. Manual de Tallinn 1.0. Direito Internacional dos Conflitos Armados. Ucrânia.

ABSTRACT

The research object of this thesis are the cyber operations carried out in the context of the annexation of Crimea by Russia, and which are known so far, between 2013 and 2017, in view of the legal regime applied to the conduct of armed conflicts, particularly in the interpretations of the application of this regime regarding the use of cyber operations in armed conflicts. The study was based on the provisions of the Rules of the Tallinn Manual 1.0, the interpretation of some States and International Organizations, and authors such as Heather Harrison, regarding the applicability of International Law to cyber attacks. From this study we reached one of the objectives, composing an understanding of the application of International Law to cyber attacks. Understanding the Crimean crisis as an international armed conflict is also important for the application of the International Law of Armed Conflicts (LOAC), and this interpretation is made based on Yohan Dinstein's understanding of the occurrence of war in the material sense, and the definitions of Aggression of the UN General Assembly. Based on this understanding, we proceeded to identify the side effects, on the Ukrainian population, of the analyzed cyber attacks carried out in Ukraine, in the context of the annexation of Crimea by Russia, between 2013 and 2017. Using the composition an understanding of the application of International Law cyber attacks, it was verified whether such attacks adhered to the LOAC, particularly regarding the principles of Distinction and Proportionality, the central issue of the study. Thus, it was concluded that among the cyber attacks directed against Ukraine, the June 2017 attack through NotPetya was serious enough to contravene the principle of Distinction and rule 43 of the Tallinn Manual, prohibiting the use of Means and Indiscriminate Methods. On the other hand, in the analysis of other cyber attacks (Operation Armageddon – 2013; Operation Potao – 2014; and cyber attacks on energy infrastructures in Ukraine - 2015 and 2016), no elements were observed that contradict the Treaties, Doctrine and Jurisprudence of the LOAC.

Keywords: Cyber Attacks. Crimea. Tallinn Manual 1.0. International Law of Armed Conflict. Ukraine.

LISTA DE ILUSTRAÇÕES

FIGURA 1 - Método de resolução de conflito interestatal……..59

FIGURA 2 - Operações da Rússia na Crimeia…….61

SUMÁRIO

1 INTRODUÇÃO……...8

2 A DOUTRINA APLICADA AO CIBERATAQUE……...11

2.1 O MANUAL DE TALLINN……..11

2.2 A INTERPRETAÇÃO DE AUTORES, ESTADOS E ORGANISMOS INTERNACIONAIS……..……..25

2.3 COMPOSIÇÃO DA LEI DOS CONFLITOS ARMADOS NOS ATAQUES CIBERNÉTICOS……..……...37

2.4 CONSIDERAÇÕES FINAIS SOBRE A DOUTRINA APLICADA AO CIBERATAQUE……...54

3 ANÁLISE DOS ATAQUES CIBERNÉTICOS NA UCRÂNIA ENTRE 2013 E 2017……...56

3.1 A ANEXAÇÃO DA CRIMEIA PELA RÚSSIA EM 2014…….56

3.2 OS ATAQUES CIBERNÉTICOS NA UCRÂNIA ENTRE 2013 E 2017 E SEUS EFEITOS……...65

3.3 ANÁLISE DOS ATAQUES CIBERNÉTICOS NA UCRÂNIA SOB A LEI DOS CONFLITOS ARMADOS……...69

3.4 CONSIDERAÇÕES FINAIS ACERCA DOS ATAQUES CIBERNÉTICOS NA UCRÂNIA ENTRE 2013 E 2017…….……..78

4 CONCLUSÃO…….……81

5 REFLEXOS PARA A MARINHA DO BRASIL..……....86

REFERÊNCIAS……88

GLOSSÁRIO……...91

1 INTRODUÇÃO

Nas relações internacionais, as disputas entre Estados por mercados comerciais, por acesso a recursos naturais e energéticos, ou por áreas e territórios para fins econômicos ou militares, levam a tensões geopolíticas ou mesmo culminam em conflitos armados. Na história dos conflitos armados, Estados e Organismos Internacionais inicialmente buscaram regulamentar o uso da violência e de certos meios e métodos de guerra por meio de Convenções e Tratados Internacionais, como as Convenções de Haia do início do século XX. Porém, tais normas não evitaram a violência em escala mundial da Grande Guerra (1914 a 1918) e da Segunda Guerra Mundial (1939 a 1945), pois o recurso à força para a solução de disputas ainda era facultado aos Estados a seu critério. Diante disso, novas regulamentações surgiram, sendo a mais importante a Carta da Organização das Nações Unidas de 1945, na qual o recurso à força passou a ser restrito somente a duas situações: em legítima defesa; ou por autorização do Conselho de Segurança da ONU. Após esse período, seguiram-se novas regulamentações, como as quatro Convenções de Genebra de 1949 e seus Protocolos Adicionais de 1977, para a proteção de pessoas e bens durante os conflitos armados. Novos meios e métodos de guerra surgidos no século XX também tiveram restrições ou proibição de uso por Tratados e Convenções, como as minas terrestres, porém outros novos meios métodos empregados no século XXI ainda permanecem sem regulamentação, como o uso de ataques cibernéticos.

Os ataques cibernéticos, como um novo meio e método de ataque, representam um desafio para a aplicação do ordenamento jurídico internacional, enquanto não houver regulamentação do seu uso como arma nos conflitos armados. Muitos Estados não se manifestam sobre o emprego ou restrição de novos meios e métodos representados por novas tecnologias, até que possam ter entendimento das vantagens que o domínio de tais tecnologias possa lhes proporcionar na busca dos seus interesses. É nesse ambiente sem regulamentação que alguns ataques cibernéticos ocorreram ao redor do mundo, ganhando escala cada vez maior, na medida em que atingiram efeitos sobre países inteiros. Como exemplo, cita-se os ataques à Estônia em 2007, que paralisaram esse país, que já possuía diversos serviços comerciais e governamentais conectados em rede. Outros ataques

cibernéticos foram lançados no contexto de conflitos armados, como na Geórgia em 2008 e na anexação da Crimeia pela Rússia em 2014.

Nesse sentido, o uso de operações cibernéticas como meio e método de agressão traz alguns desafios, como a identificação de sua autoria ou mesmo a percepção do início do um ataque. Pode ser difícil identificar ter havido uma agressão de um Estado contra outro, o que pode gerar uma lacuna no cumprimento artigo 2-4 da Carta das Nações Unidas, de não uso da força pelos Estados Membros na solução de controvérsias. Além disso, os efeitos de ataques cibernéticos contra infraestruturas de um Estado, dentro de um conflito armado ou como ações preparatórias para uma ação cinética futura, podem atingir, de forma indiscriminada, a população civil, e causar transtornos e sofrimentos desnecessários, causando a violação de outros Tratados Internacionais. Tal evolução recente na dinâmica dos conflitos armados que motivou o presente estudo, que se propõe a compor um perfil de interpretação do Direito Internacional, sobre o uso de meios e métodos cibernéticos nos conflitos armados, e realizar a análise de um caso de emprego de operações cibernéticas conhecido. Para tanto, será analisado se os ataques cibernéticos realizados no contexto da anexação da Crimeia pela Rússia, entre 2013 e 2017, contrariaram os Tratados, a Doutrina e a Jurisprudência do Direito Internacional dos Conflitos Armados (DICA).

Esse estudo foi organizado em cinco capítulos. O primeiro capítulo é a presente introdução. No segundo capítulo serão estudados o previsto nas Regras do Manual de Tallinn 1.0; e a interpretação de alguns Estados e Organismos Internacionais; e a de autores, no que se refere a aplicabilidade do Direito Internacional aos ataques cibernéticos. A partir de tal estudo obtém-se uma síntese das interpretações levantadas, a fim de compor um entendimento da aplicação do Direito Internacional aos ataques cibernéticos. No terceiro capítulo serão descritos o conjunto de ações cinéticas e não cinéticas empregadas no contexto da anexação da Crimeia pela Rússia, entre 2013 e 2017, e avaliação dessas ações quanto a qualificação como conflito armado, entendimento importante para a aplicação do DICA. Em seguida, serão identificados os ataques cibernéticos realizados em apoio à tais ações, e os seus efeitos na população ucraniana. Por fim, será realizada a análise desses efeitos com base nos princípios do DICA, particularmente a Distinção e a Proporcionalidade, com base na síntese das interpretações do capítulo 2. O quarto capítulo é composto de uma conclusão de todo o estudo, com alguns

desafios identificados pelo vácuo normativo sobre a utilização de ataques cibernéticos, e a apresentação da análise final sobre o caso avaliado, os ataques cibernéticos sofridos pela Ucrânia entre 2013 e 2017. Por fim, o quinto capítulo trará alguns reflexos das conclusões de tal estudo sobre a Marinha do Brasil.

2 A DOUTRINA APLICADA AO CIBERATAQUE

Neste capítulo serão identificadas as referências nas quais estão previstas as normas e entendimentos referentes a aplicação do Direito Internacional aos ciberataques[1], bem como serão descritas as interpretações destas referências. A primeira parte descreverá o previsto no Manual de Tallinn. A segunda parte irá tratar da interpretação de autores que se dedicam ao estudo da aplicabilidade do Direito Internacional aos ciberataques, bem como a interpretação de alguns Estados e Organismos Internacionais, como o Comitê Internacional da Cruz Vermelha. Por fim, será realizada uma síntese das interpretações levantadas, identificando similaridades e singularidades, a fim de compor um entendimento da aplicação do Direito Internacional aos ciberataques.

2.1 O MANUAL DE TALLINN

O Manual de Tallinn 1.0 foi produzido a partir de 2009, por um Grupo de Especialistas Internacionais independente, a convite do Centro de Excelência de Defesa Cibernética Cooperativa da OTAN[2]. Este projeto teve como propósito examinar como as normas legais existentes aplicam-se a uma nova forma de guerra, a guerra cibernética, para a qual não há disposições previstas em Tratados Internacionais.

O estudo do Grupo de Especialistas Internacionais resultou em doutrina, organizadas em Regras, aprovada e publicada em 2013 e adotadas por consenso entre estes. Estas Regras são organizadas no manual em duas partes. A primeira parte, nominada Lei Internacional de Segurança Cibernética, menciona em suas seções a soberania e jurisdição no ambiente cibernético, a responsabilidade legal dos Estados sobre as operações cibernéticas, e conceitos sobre o uso da força com meios e métodos cibernéticos. A segunda parte é intitulada Lei do Conflito Armado Cibernético[3], e é composta de Regras decorrentes da análise da aplicação das

1 Ciberataque é termo comumente utilizado para referir-se a ataque cibernético.

2 Tradução do autor para *NATO Cooperative Cyber Defense Centre of Excelence* (NATO CCD COE), que é um foro de discussão cooperativa no âmbito da OTAN, porém não faz parte da estrutura desta Organização. Localizado em Tallinn, capital da Estônia, e possui como nações patrocinadoras os Estados Unidos da América e diversos outros países da OTAN.

3 Tradução do autor para *Law of Cyber Armed Conflict.*

regras existentes no Direito Internacional dos Conflitos Armados (DICA)[4] para a guerra cibernética, nas quais destacam-se: a definição de ataque cibernético; os princípios da distinção e da proporcionalidade aplicados ao ataque cibernético; os meios e métodos de ataque cibernético para evitar ataques indiscriminados a estruturas de uso civil, e as precauções para se evitar danos colaterais em desacordo com os princípios do DICA.

De acordo com o Diretor do Grupo dos Especialistas Internacionais, Prof. Michael Schmitt, o Manual de Tallinn não tem força de tratado internacional, representando tão somente a opinião do Grupo de Especialistas Internacionais, e não a visão da OTAN ou dos seus países membros.

2.1.1 Infraestrutura Cibernética

Na primeira parte do manual de Tallinn, no *caput* do capítulo I é apresentada terminologia importante para a compreensão do exposto no capítulo. Define infraestrutura cibernética como “as comunicações, armazenamento, e recursos computacionais sobre o qual o sistema de informações opera” (Tallinn, 2012, p. 24, tradução própria). Apresenta ainda o termo operações cibernéticas como “o emprego de capacidades cibernéticas com o propósito primário de atingir objetivos no espaço cibernético” (Tallinn, 2012, p. 24, tradução própria). No mesmo caput também é mencionado que “as Regras e Comentários deste Capítulo aplicam-se tanto em tempo de paz quanto em tempo de conflito armado” (Tallinn, 2012, p. 24, tradução própria).

2.1.2 Soberania, Jurisdição e Controle

De acordo com o Manual de Tallinn, “operação cibernética de um Estado direcionada contra outro Estado pode violar a soberania do último. Certamente ocorre tal violação se é causado algum dano”. (Tallinn, 2012, p. 25, tradução própria). Porém, não houve consenso entre o Grupo de Especialistas Internacionais se operações cibernéticas como as que utilizam *malware* de monitoramento, ou um

4 Conhecido no âmbito internacional como *Law of Armed Conflict* (LOAC), e no âmbito acadêmico também usa-se o termo IHL – do inglês International Humanitarian Law

DDoS, ou um *ramsonware* que não causa que não causa dano físico, constituiriam violação de soberania.

Com relação à jurisdição aplicada às operações cibernéticas, o Manual de Tallinn 1.0 prevê que “a presença física real é requerida, e suficiente, para a jurisdição baseada na territorialidade” (Tallinn, 2012, p. 28, tradução própria) Esta jurisdição territorial dividi-se em duas formas: a jurisdição territorial subjetiva ocorre quando um Estado aplica as suas leis exercendo jurisdição sobre um incidente que foi iniciado no seu território, mesmo que os efeitos da operação cibernética não tiveram efeito no território do Estado exercendo esta jurisdição; a jurisdição territorial objetiva que garante jurisdição sobre indivíduos, por parte de um Estado onde um incidente teve efeitos, mesmo que as operações cibernéticas tenham iniciado fora do território desse Estado. Como exemplo, a Geórgia poderia exercer soberania territorial objetiva sobre indivíduos envolvidos em operações cibernéticas contra esse Estado, durante o conflito desse país com a Federação Russa em 2008, com efeitos de interrupção de comunicações cibernéticas, em violação às leis da Geórgia.

Na parte de Imunidade de Soberania e Inviolabilidade, o Grupo de Especialistas Internacionais destaca o caso de objetos operados por Estados, a exemplo de satélites, que gozam de imunidade de soberania, quando possuem propósitos exclusivamente governamentais, não podendo ser usados para fins comerciais (Tallinn, 2012, p. 31, tradução própria).

Na questão da atribuição de responsabilidade de um Estado sobre operações cibernéticas, o Manual de Tallinn 1.0 estabelece a importância do controle dos Estados sobre a infraestrutura cibernética localizada no seu território, ou localizadas em outros locais mas que estejam sob seu controle exclusivo. Esse entendimento chama a atenção dos Estados para a conduta de não “permitir sabidamente que seu território seja usado para atos contrários aos direitos de outros Estados” (Tallinn, 2012, p. 33, tradução própria). De acordo com o Grupo de Especialista Internacionais, esta proibição se aplica a operações cibernéticas lançadas do território de um Estado e que produzem efeitos negativos no território de outro Estado.

2.1.3 Responsabilidade dos Estados

Responsabilidade legal por operações cibernéticas é atribuída aos Estados quando tais atos incidem em violação de obrigações internacionais previstas em tratados, que cada Estado tenha se obrigado a cumprir, ou no direito internacional consuetudinário[5]. Considera-se que tal violação pode ocorrer por ação ou omissão. O Manual de Tallinn 1.0 cita que "no domínio do espaço cibernético, um ato ofensivo internacional pode consistir […] numa violação da Carta das Nações Unidas (por exemplo: uso da força praticado por meios cibernéticos […])" (2012, p. 35, tradução própria). Esse manual também destaca a possibilidade de atos cometidos por atores não Estatais serem atribuídos a Estados, caso esse esteja provendo alguma instrução, suporte ou controle dos indivíduos ou grupos que conduzem operações cibernéticas contra outro Estado.

Sobre a utilização de estrutura cibernética governamental de um Estado para a realização de operações cibernéticas, essa situação é relatada no Manual de Tallinn 1.0 como uma "indicação de que o Estado em questão está associado com a operação" (2012, p. 39, tradução própria). Apesar do indício do envolvimento de um Estado com uma operação cibernética contra outro Estado, o mesmo Manual ressalta que isso "não serve como base legal para tomar alguma ação contra o Estado envolvido ou de outra forma considerar esse responsável pelo ato em questão" (Tallinn, 2012, p. 39, tradução própria). Essa abordagem dá-se pela possibilidade de uma estrutura cibernética governamental estar sob controle de um outro ator não Estatal ou um terceiro Estado, com o propósito de utilizar essa infraestrutura para a condução de operações cibernéticas, inclusive com a possibilidade de utilização de técnica de *spoofing* de falsificação de endereço de IP.

2.1.4 Proibição do Uso da Força

No que se refere ao uso da força, o Manual de Tallinn 1.0 preconiza que "operação cibernética que constitua a ameaça ou uso da força contra a integridade territorial ou independência política de qualquer Estado [...] inconsistente com os propósitos das Nações Unidas, é ilegal" (2012, p. 45, tradução própria). Essa definição baseia-se no princípio da não intervenção, conforme o Artigo 2(4) da Carta das Nações Unidas.[6]

5 Tradução do autor para *customary international law.*

6 O Artigo 2(4) da Carta das Nações Unidas estabelece que "Todos os [Estados] Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a independência

Para uma operação cibernética ser qualificada como uso da força, não precisa ser necessariamente conduzida por Forças Armadas. Operações cibernéticas conduzidas por agências de Inteligência de Estado ou por operadores privados a serviço de um Estado são suscetíveis a serem qualificadas como uso da força, de acordo com o Manual de Tallinn 1.0. Porém, o grupo de Especialistas Internacionais concorda com a visão de que operações de espionagem cibernética ou exploração cibernética que não tenham elemento coercitivo não violam o princípio da não intervenção, por se tratarem de mera intrusão no sistema de um Estado (Tallinn, 2012, p. 47, tradução própria).

Para a qualificação de uma operação cibernética como uso da força, segundo o Grupo de Especialistas Internacionais, “qualquer operação que ascenda ao nível de um ‘ataque armado’ […] e que seja conduzida por ou atribuída a um Estado, pode ser qualificada como ‘uso da força’” (Tallinn, 2012, p. 49, tradução própria). Para que esta qualificação se proceda, faz-se necessário o entendimento de ataque armado do Manual.

Dentre os entendimentos elencados pelo grupo de Especialistas Internacionais, esses concordam que “o uso da força que fere ou mata pessoas ou danifica ou destrói propriedade poderia satisfazer requisitos de escala e efeitos” (Tallinn, 2012, p. 55, tradução própria). Porém, o Manual não deixa claro os parâmetros de escala e efeitos. O Grupo de Especialistas Internacionais também não esclarece a partir de que ponto a extensão da morte, ferimento, dano, destruição, ou ferimento causado por uma operação cibernética faz essa constituir ~~n~~um ataque armado (Tallinn, 2012, p. 55, tradução própria). Alguns dos Especialistas Internacionais adotam a visão de que não é a natureza das consequências imediatas que importa. mas a extensão dos efeitos subsequentes. Por essa abordagem, o Manual cita que um tipo de operação cibernética direcionada a uma instalação crítica de um Estado, com efeito severo, porém não destrutivo, pode ser qualificado como ataque armado (Tallinn, 2012, p. 55, tradução própria). O Grupo de Especialistas Internacionais considera o exemplo de uma operação cibernética tendo como alvo uma estação de purificação de água, com o efeito subsequente da incidência de doença e morte causada pelo consumo de água contaminada (2012, p. 56, tradução própria).

---

política de qualquer Estado, ou qualquer outra ação incompatível com os propósitos das Nações Unidas”.

Ainda dentre os entendimentos de qualificação de operação cibernética como ataque armado, o Manual de Tallinn 1.0 faz uma comparação com outros meios e métodos não cinéticos. O Manual destaca que “é universalmente aceito que ataques químico, biológico e radiológico no requisito de escala e efeitos constituem ataque armado […] porque as consequências subsequentes podem incluir sério sofrimento ou morte. Raciocínio idêntico aplicar-se-ia para operações cibernéticas” (Tallinn, 2012, p. 54, tradução própria).

No que se refere a fatos ocorridos que podem exemplificar o efeito de dano material causado por operação cibernética, o Grupo de Especialistas Internacionais faz referência aos danos provocados às centrífugas de enriquecimento de urânio da usina nuclear de Natanz no Irã, em 2010, causados por uma operação cibernética.[7] O Grupo de Especialistas Internacionais compartilham a visão de que “estas operações tinham alcançado o limite do ataque armado” (2012, p. 56, tradução própria).

O Manual de Tallinn 1.0 apresenta uma proposta de avaliação de operação cibernética, a ser considerada por Estados, quando decidirem pelo uso de operação cibernética, para verificar se essa pode incindir em uso da força. Porém, o Manual ressalta que “eles não são critérios formais legais” (Tallinn, 2012, p. 49, tradução própria). Pelo fator da Severidade é analisada a gravidade dos efeitos de uma operação cibernética, como o dano, destruição ferimento ou morte. O fator do Direcionamento[8] analisa a relação de causa e efeito ente uma operação cibernética e os efeitos sobre uma estrutura ou população de um Estado. O fator da Invasividade refere-se ao grau de intrusão de uma operação cibernética sobre uma infraestrutura cibernética de um Estado. De acordo com o Manual, “como regra, quanto mais seguro é um sistema cibernético atingido, maior é a preocupação quanto a sua invasão” (Tallinn, 2012, p. 50, tradução própria). Pelo fator Caráter Militar verifica-se que o nexo entre a operação cibernética e operações militares aumenta a probabilidade de caracterização da operação cibernética como uso da força. Pelo fator do Envolvimento de Estado, o Manual avalia que “quanto mais claro e próximo é o vínculo entre Estado e operações cibernéticas, é mais provável que outros Estados irão caracterizar essas como uso da força por aquele Estado” (Tallinn, 2012, p. 50, tradução própria). O fator da Urgência das Consequências do

7 Essa operação cibernética constituiu-se na intrusão de um código malicioso nos computadores da usina de Natanz. Este código ficou conhecido como Stuxnet.

8 Tradução do autor para *Directness*.

Ataque, que foca no aspecto temporal dos efeitos de uma operação cibernética, se produzem efeitos imediatos ou após algum tempo, semanas ou meses. Há ainda o fator da Mensuração dos Efeitos, no qual o Manual reconhece ser mais difícil avaliar consequências subjetivas. Por fim, há o fator da Legalidade Presumida, que prevê que atos que não são proibidos são permitidos; ausência de tratado expresso ou de proibição por lei consuetudinária reconhecida, um ato é presumivelmente legal" (Tallinn, 2012, p. 52, tradução própria). Ressalta-se no Manual que estes fatores devem ser analisados de forma combinada.

2.1.5 Aplicação da Lei dos Conflitos Armados

A segunda parte do Manual de Tallinn 1.0 trata da Lei dos Conflitos Armados Cibernéticos, por meio de uma análise da aplicabilidade da Lei dos Conflitos Armados[9] às operações cibernéticas, no contexto dos conflitos armados.

De acordo com o previsto no Manual de Tallinn 1.0, o conflito armado refere-se a situações envolvendo hostilidades, inclusive aquelas conduzidas com o uso de operações cibernéticas (2012, p.68, tradução própria). Sobre a aplicabilidade da lei dos conflitos armados, o Grupo de Especialistas Internacionais tem o seguinte entendimento:

> A despeito da novidade das operações cibernéticas e da ausência de regras específicas dentro da lei dos conflitos armados explicitamente lidando com essas, o Grupo de Especialistas Internacionais foi unânime em concluir que a lei dos conflitos armados aplica-se a tais atividades nos conflitos armados internacionais e não internacionais (Tallinn, 2012, p. 68, tradução própria).

Essa parte do Manual também passa a utilizar o termo "ataque cibernético", o qual define como "uma categoria específica de operação cibernética" (Tallinn, 2012, p. 69, tradução própria). Além desse termo, o Grupo de Especialistas Internacionais também incluiu nessa parte do Manual o conceito de hostilidades: "a hostilidade constituída pode envolver qualquer combinação de operações cinéticas e cibernéticas, ou somente operações cibernéticas. Certamente, há hostilidades sempre que um Estado engaja em 'ataques cibernéticos' […] contra outro" (2012, p. 74, tradução própria).

9 Tradução do autor para *Law of Armed Conflict* (LOAC)

Para a aplicação da lei dos conflitos armados, um conflito deve ter caráter internacional[10]. O Grupo de Especialista Internacionais “concorda que um conflito é internacional se dois ou mais Estados estão envolvidos como partes em lados opostos” (2012, p. 72, tradução própria).

Esse entendimento é importante, particularmente nas situações em que há envolvimento de atores não Estatais em operações cibernéticas contra um Estado. Caso essas operações atinjam o nível de ataque armado, e seja comprovada a vinculação de tais grupos com outro Estado, agindo sob seu controle, isso pode ser qualificado como agressão entre Estados, violando o artigo2(4) da carta da ONU, com a possibilidade de caracterizar um conflito internacional. Sobre grupos ou indivíduos atuando em operações cibernética a serviço de um Estado, o Grupo de Especialistas Internacionais reconhece ser difícil comprovar se um Estado está efetivamente controlando as atividades cibernéticas de um ator não Estatal, particularmente quando a origem das operações cibernéticas não tem como origem uma infraestrutura cibernética governamental.[11]

2.1.6 Condução das Hostilidades

A lei dos conflitos armados aplica-se para qualquer meio ou método empregado. Nesse sentido, o Manual de Tallinn 1.0 menciona que “os princípios básicos como distinção e proibição de sofrimento desnecessário aplicar-se-ão para operações cibernéticas da mesma forma que para outros meios e métodos de guerra” (Tallinn, 2012, p. 91, tradução própria).

No que se refere ao ataque cibernético, esse é definido no Manual de Tallinn 1.0 partindo do conceito de “ataque” previsto no Protocolo Adicional I[12] de 1977, em seu Artigo 49 (1): “ataque significa atos de violência contra o adversário, quer sejam atos ofensivos ou defensivos” (Tallinn, 2012, p. 92). O Manual também ressalta que “atos de violência não devem ser entendidos como limitados a atividades que

10 O critério aceito da existência de conflito armado internacional advém do Artigo 2 comum às quatro Convenções de Genebra de 1949, que prevê: “A presente Convenção irá aplicar-se em caso de guerra declarada ou qualquer outro conflito armado que possa surgir entre duas ou mais Altas Partes Contratantes, ainda que o estado de guerra não seja reconhecido por uma delas”

11 O Manual de Tallinn 1.0 cita o caso das operações cibernéticas contra a Estônia em 2007, conduzido por indivíduos conhecidos como ativistas hacker – ou hackativistas -, na qual havia a suspeita de participação de outro Estado no suporte a esses indivíduos, mas não se comprovou o envolvimento estatal.

12 Protocolo Adicional I às Convenções de Genebra de 1949, Relativo à Proteção das Vítimas dos Conflitos Armados Internacionais.

liberam força cinética" (Tallinn, 2012, p. 92, tradução própria). Assim, atos de violência, ou aqueles com efeitos violentos, direcionados contra civis ou objetos civis, ou outras pessoas ou objetos protegidos, são ataques (2012, p. 93, tradução própria).

Na discussão sobre os efeitos dos ataques, o Manual traz alguns exemplos. No caso de um operação cibernética a uma instalação, com efeito sobe a sua funcionalidade, a maioria dos Especialistas Internacionais compartilha a visão de qualificação dessa operação como ataque se o reparo do dano necessitar de troca de componentes físicos da instalação (Tallinn, 2012, p. 93). Diferentemente, a discussão entre os especialistas aponta no sentido da não qualificação de uma operação cibernética como ataque, no caso de uma operação cibernética com efeito em larga escala, por exemplo, de bloqueio de acesso às comunicações por e-mail de um Estado (Tallinn, 2012, p. 94). O Manual de Tallinn aponta uma outra situação, na qual é realizada uma operação cibernética, também sem dano físico a sistemas, mas que considera como ataque. Nesse sentido, cita uma operação cibernética para desabilitar um sistema de defesa antiaérea que será atacado em seguida por um ataque cinético. O Manual aponta que a operação cibernética desse último exemplo é qualificada como ataque, por ser parte componente de um ataque cinético (Tallinn, 2012, p. 94, tradução própria).

2.1.7 Princípio da Distinção

Sobre o princípio da Distinção aplicado às operações cibernéticas, o Manual de Tallinn 1.0 adota como referência o previsto no Artigo 48 do Protocolo Adicional I:

> Com vistas a assegurar a proteção e o respeito da população civil e dos bens de caráter civil, as Partes em conflito devem sempre fazer a distinção entre população civil e combatentes, assim como bens de caráter civil e objetivos militares, devendo, portanto, dirigir suas operações unicamente contra objetivos militares (CICV, 1998, p. 39).

No âmbito das operações cibernéticas, o mesmo Manual cita algumas operações direcionadas a civis que poderiam ser legais, exemplificando uma operação psicológica por meio do envio de e-mail a população de um adversário exigindo capitulação (Tallinn, 2012, p. 96, tradução própria).

O Manual de Tallinn 1.0 também adota o previsto nos Artigos 51 e 52 do Protocolo Adicional I, referente à proteção da população e bens civis, com o

propósito de estabelecer parâmetro para a proibição de ataque a civis em decorrência de operação cibernética. O Artigo 51 prevê que “os civis e a população civil gozam de proteção geral contra os perigos resultantes de operações militares” (CICV, 1998, p. 40), enquanto que o Artigo 52 estabelece que “os bens civis não devem ser objeto de ataques ou de represálias” (CICV, 1998, p. 41).

Como forma de exemplificar a aplicação da proibição de ataque à população civil por operação cibernética, o Manual de Tallinn 1.0 cita a realização de um ataque cibernético hipotético a um sistema de transporte em massa que cause acidente com mortes e ferimentos, com o propósito de aterrorizar a população civil. De acordo com esse Manual, “tal operação também constituiria um ataque ilegal contra civis e objetos[13] civis” (Tallinn, 2012, p. 105, tradução própria).

Na regra 37, referente a Proibição de Ataque a Objetos Civis, o Manual de Tallinn 1.0 enuncia que “computadores, sistemas computacionais, e infraestrutura computacional podem ser objeto de ataque se esses forem objetivos militares” (Tallinn, 2012, p. 106, tradução própria). Nesse sentido, o Grupo de Especialistas Internacionais concorda que “a determinação de quando um objeto é um objeto civil que goza de proteção contra ataque, e não um objetivo militar, deve ser feita caso a caso” (Tallinn, 2012, p. 106, tradução própria).

No que se refere ao termo “objetivo militar”, o Manual de Tallinn 1.0 também adota como referência o previsto no Protocolo Adicional I, Artigo 52:

> No que diz respeito aos bens, os objetivos militares são limitados aos que, por natureza, localização, destino ou utilização contribuem efetivamente para a ação militar e assim sua destruição total ou parcial, sua captura ou neutralização oferecem, nestes casos, uma vantagem militar precisa (CICV, 1998, P. 42).

O Manual de Tallinn 1.0 ressalta que essa definição de objetivo militar “tem sido adotada por muitos Estados nos seus manuais militares [...]” (Tallinn, 2012, p. 107, tradução própria).

Para a qualificação de objetos, como computadores, sistemas computacionais, e infraestrutura computacional, como objetivo militar passível de ser alvo de ataque cibernético, o Manual de Tallinn 1.0 estabelece critérios de avaliação de natureza, localização, propósito ou uso. O critério da natureza é facilmente exemplificado no caso de computadores militares e infraestrutura cibernética militar,

13 O Manual de Tallinn utiliza o termo “civil *objects”* para se referir a bens civis.

que atendem a centros de comando e controle, e comunicações militares (Tallinm, 2012, p. 108).

Com relação ao critério da localização, o Manual de Tallinn ressalta que este critério refere-se a uma área geográfica de importância militar específica, não considerando um endereço de IP como uma localização, por esse critério (Tallinn, 2012, p. 108). Nesse sentido, o Manual menciona uma operação cibernética contra um sistema SCADA[14] de reservatório poderia ser empregada para liberar água numa área na qual operações militares do inimigo são esperadas, desse modo negando seu uso pelo inimigo. Nesse caso, "a área é um objetivo militar por causa da sua utilidade militar para o inimigo. Essa caracterização justifica utilizar meios cibernéticos para liberar a água do reservatório na área" (Tallinn, 2012, p. 109, tradução própria).

O Manual de Tallinn 1.0 refere-se ao critério do propósito por meio da avaliação de intenção do uso futuro de um objeto para fins militares. Esse Manual cita, como exemplo, que uma situação na qual se torna conhecida a intenção de se utilizar uma estrutura civil de transpônder em satélite de comunicações, para fins militares, pode qualificar esses transpônders como objetivo militar (Tallinn, 2012, p. 109, tradução própria).

Sobre os critérios de avaliação, o Grupo de Especialistas Internacionais expressa a opinião de que objetos que satisfazem ao critério da natureza são sempre passiveis de ataque, desde que obedecidas outras regras das lei dos conflitos armados. Para o Grupo de Especialistas Internacionais:

> Os requisitos para um objetivo militar que seja um objeto que contribui efetivamente para a ação militar e que o ataque a esse irá oferecer uma vantagem militar precisa são inerentemente atendidos para objetos que são militares na natureza. Nessa visão, por exemplo, uma rede de computadores militares necessariamente contribui efetivamente e sua destruição, dano, ou neutralização sempre oferece a um atacante uma vantagem militar precisa (2012, p. 110, tradução própria).

Uma questão importante na discussão sobre objetivo militar é a qualificação de objetos de uso dual, ou seja, civil e militar. O Manual de Tallinn 1.0 estabelece que tais objetos são objetivo militar, porém recomenda que sejam observadas algumas medidas de cautela, a fim de que sejam observados alguns princípios da lei

14 SCADA é a sigla para *Supervisory Control and Data Acquisition*, Supervisão e Aquisição de Dados. Os Sistemas SCADA utilizam software de coleta e gerenciamento de dados, e são amplamente utilizados no controle de funcionamento de diversas infraestruturas, como usinas de produção de energia, reservatórios de água, e plantas industriais.

dos conflitos armados, como o da proporcionalidade.[15] Como exemplo, esse Manual cita uma central de provedor de internet, com servidores de uso militar, mas que também possui alguns outros servidores explorados comercialmente para uso civil, e no qual um ataque cibernético para desabilitar o sistema de resfriamento dessa central poderá causar o dano por superaquecimento dos servidores nessa infraestrutura. Nesse caso, o Manual de Tallinn 1.0 recomenda que "o dano esperado aos servidores de uso civil deve ser considerado no cálculo da proporcionalidade e ser considerado quando avaliando precauções viáveis no ataque" (Tallinn, 2012, p. 114, tradução própria).

2.1.8 Princípio da Proporcionalidade

O Manual de Tallinn 1.0 adota o princípio da Proporcionalidade aplicado a operações cibernéticas a partir do conceito desse princípio previsto no Artigo 57(2)(a)(iii) do Protocolo adicional I. Sobre a observância do princípio da Proporcionalidade:

> Um ataque cibernético que tenha expectativa de causar perda acidental de vidas humanas na população civil, ferimentos nos civis, danos nos bens de caráter civil, ou uma combinação desses, que seriam excessivos em relação à vantagem militar concreta e direta esperada é proibido (Tallinn, 2012, p. 132, tradução própria).

Para a qualificação de danos excessivos, a extensão dos efeitos dos danos colaterais deve ser avaliada caso a caso, frente a vantagem militar obtida com o ataque.

Porém, o Manual de Tallinn 1.0 ressalta que a mera ocorrência de danos a civis e bens civis, também conhecidos como danos colaterais, no ataque cibernético a um objetivo militar legítimo, não caracteriza necessariamente esse ataque como ilegal (Tallinn, 2012, p. 132, tradução própria). Da mesma forma, esse Manual também reconhece que alguns efeitos decorrentes de operações cibernéticas, como inconvenientes, irritação, stress ou medo, não são enquadradas como danos colaterais (Tallinn, 2012, p. 132, tradução própria).

---

15 O Princípio da Proporcionalidade é baseado no previsto no Artigo 57(2)(a)(iii) do Protocolo Adicional I: "abster-se de lançar um ataque do qual se possa esperar que venha a causar acidentalmente perdas de vidas humanas na população civil, ferimentos nos civis, danos nos bens de caráter civil ou uma combinação dessa perdas que seriam excessivos relativamente à vantagem militar concreta e direta esperada" (CICV, 1998, p. 46).

O Manual de Tallinn 1.0 também recomenda que sejam tomadas as medidas de avaliação, por parte dos planejadores de um ataque cibernético, de possíveis efeitos indiretos sobre civis e objetos civis. Como exemplo, cita um possível ataque cibernético sobre um Sistema de Posicionamento Global por Satélite e cuja interrupção do sinal poderia causar acidentes em meios de transporte civis que utilizam tal sistema para navegação (Tallinn, 2012, p. 133). Porém, o Grupo de Especialistas Internacionais reconhece que algumas vezes difícil determinar antecipadamente os possíveis efeitos colaterais de um ataque cibernético (Tallinn, 2012, p. 135, tradução própria).

2.1.9 Meios e Métodos de Guerra

O Manual de Tallinn 1.0 define "meios de guerra cibernética[16]" como "as armas cibernéticas e seus sistemas cibernéticos associados", e "métodos de guerra cibernética" como "as táticas, técnicas e procedimento cibernéticos por meio das quais as hostilidades são conduzidas" (Tallinn, 2012, p. 118, tradução própria). O Manual define também "arma cibernética" como "meios cibernéticos de guerra projetados para uso ou intenção de uso capazes de causar ferimento ou morte de pessoas, ou danos ou destruição de objetos, ou seja, causando as consequências exigidas para qualificar uma operação cibernética como um ataque" (Tallinn, 2012, p. 119, tradução própria).

Nas questões conceituais, o Manual de Tallinn 1.0 faz a distinção entre sistema computacional, que qualifica como meio de guerra, e infraestrutura cibernética, como a internet, que conecta o sistema computacional ao alvo do ataque, mas não é considerado meio de guerra (Tallinn, 2012, p. 119, tradução própria). Da mesma forma, também é feita a distinção entre "meio de guerra" e "métodos de guerra", por meio do exemplo da utilização de um *botnet* para realizar um ataque cibernético de negação de serviço distribuído[17]. Nesse caso, "o *botnet* é o

16 O termo Guerra Cibernética aparece no Manual de Tallinn 1.0, porém sem ser definido nesse Manual. O Ministério da Defesa do Brasil (MD-31-M-08) define Gerra Cibernética como "corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2 [...]" (BRASIL, 2014, P. 19).

17 Tradução do autor para *distributed denial of service (DDoS)*, que é um método que sobrecarrega um alvo com muitas solicitações de serviço, geralmente utilizando vários *botnet*.

meio de guerra cibernética enquanto ataque de negação de serviço distribuído é o método de guerra cibernética" (Tallinn, 2012, p. 119, tradução própria).

Ainda no que se refere a meios e métodos de guerra cibernética, o Manual de Tallinn 1.0 apresenta na regra 43 a proibição de utilização de Meios e Métodos Indiscriminados, baseada no previsto no Artigo 51(4)(b) e (c) do Protocolo Adicional I[18]. Por essa regra:

> É proibido empregar meios e métodos de guerra cibernética que são indiscriminador por natureza. Meios e métodos de guerra cibernética são indiscriminados por natureza quando esses não podem ser direcionados para um objetivo militar específico, ou limitados em seus efeitos conforme estabelecido pela lei dos conflitos armados, e consequentemente são de natureza para atingir objetivos militares, civis ou objetos civis sem distinção (Tallinn, 2012, p. 121, tradução própria).

Com exemplo, o Manual de Tallinn 1.0 cita o emprego de um *malware* por um Estado para atacar uma rede de computadores específica. Embora seja direcionado para um objetivo legítimo, ao ser introduzido na rede de computadores alvo, esse código malicioso pode escapar para a rede de computadores civis, e causar efeito indiscriminado (Tallinn, 2012, p. 122, tradução própria).

Adicionalmente, também é estabelecido pelo Manual de Tallinn 1.0 na regra 49 a Proibição de Ataque Indiscriminado, baseada no previsto no Artigo 51(4)(a) do Protocolo Adicional I[19] Diferentemente da regra 43, a regra 49 designa que "ataques cibernéticos que possuem a natureza de atingir alvos legítimos, e também civis ou objetos civis sem distinção, e durante o ataque são direcionados contra um alvo legítimo e civis ou objetos civis, são proibidos" (Tallinn, 2012, p. 130,_tradução própria). Como exemplo, considera o uso de um *malware* capaz de ser direcionado contra um alvo legítimo, porém durante o ataque esse *malware* é introduzido indiscriminadamente na internet para atingir o alvo (Tallinn, 2012, p. 130).

2.1.10 Medidas de Precaução

18 O Artigo 51(4)(b) e (c) designa, respectivamente, ataques indiscriminados como: "os ataques em que forem utilizados métodos ou meios de combate que não possam ser dirigidos contra um objetivo militar determinado"; e "os ataques em que forem utilizados métodos ou meios de combate cujos efeitos não possam ser limitados […]" (CICV, 1998, P. 41).

19 O Artigo 51(4)(a) designa ataques indiscriminados como "os ataques não dirigidos contra um objetivo militar designado" (CICV, 1998, P. 41).

O Manual de Tallinn 1.0 prevê algumas regras com Medidas de Precaução aplicadas a operações cibernéticas a partir do previsto nos Artigos 57 e 58 do Protocolo adicional I.

A regra 52, Precaução na Verificação de Alvos[20], estabelece que “aqueles que decidem sobre um ataque cibernético devem tomar todas as medidas viáveis para verificar que os objetivos a serem atacados não são civis nem objetos civis nem sujeitos a proteção especial” (Tallinn, 2012, p. 139, tradução própria). Nesse sentido, quando um atacante não é capaz de reunir informação confiável sobre a natureza de um sistema cibernético proposto como alvo, o decisor seria obrigado a limitar o escopo do ataque para aqueles componentes ou capacidades do sistema sobre os quais há informação suficiente para verificar o seu status como alvo legítimo (Tallinn, 2012, p. 140, tradução própria).

A regra 56, Precaução na Escolha de Alvos[21] estabelece que para os Estados participantes do Protocolo Adicional I, quando for possível a escolha entre vários objetivos militares que proporcionem vantagem militar equivalente, o objetivo a ser selecionado para ataque cibernético deverá ser cujo ataque parece representar menor perigo para vidas civis ou objetos civis (Tallinn, 2012, p. 142, tradução própria). Sobre tal regra, o Manual de Tallinn 1.0 cita o exemplo de um ataque a um sistema de comando e controle inimigo, no qual, observando essa regra, o atacante opta por um ataque cibernético diretamente sobre esse sistema, ao invés de atacar uma central de energia que atende a tal sistema e a outros sistemas de uso civil (Tallinn, 2012, p. 143).

A regra 59, Precaução contra os Efeitos dos Ataques Cibernéticos estabelece que “as Partes de um conflito armado devem, no que for possível, tomar medidas necessárias para proteger a população civil e os bens civis sob sua autoridade, contra os riscos resultantes de um ataque cibernético” (Tallinn, 2012, p. 146, tradução própria). De acordo com o Manual de Tallinn 1.0, o cumprimento dessa regra é direcionada para o defensor “antecipadamente à possibilidade de um ataque

20 O Artigo 57(2)(a)(i) do Protocolo Adicional I estabelece que “os que preparam e decidem devem fazer tudo o que for praticamente possível para verificar se os objetivos a atacar não são civis, nem bens de caráter civil, nem se beneficiem de uma proteção especial, mas sim se são objetivos militares [...]” (CICV, 1998, p. 46).

21 O Artigo 57(2)(a)(ii) do Protocolo Adicional I estabelece que “os que preparam e decidem um ataque devem tomar todas as precauções praticamente possíveis quanto à escolha dos meios e métodos de ataque de forma a evitar ou, seja como for, reduzir ao mínimo, as perdas de vidas humanas na população civil, os ferimentos nos civis e os danos nos bens de caráter civil que puderem ser acidentalmente causados” (CICV, 1998, p. 46).

cibernético” (Tallinn, 2012, p. 146, tradução própria), como o estabelecimento de medidas de defesa cibernética dos sistemas civis e segregação desses da infraestrutura cibernética militar. Porém, o Grupo de Especialistas Internacionais ressalta que a falha de uma parte em conflito em tomar medidas de precaução para segregação de sistemas civis dos militares não isenta a outra parte de observar as demais medidas de precaução num ataque cibernético (Tallinn, 2012, p. 149).

2.2 A INTERPRETAÇÃO DE AUTORES, ESTADOS E ORGANISMOS INTERNACIONAIS

Alguns autores dedicam-se ao estudo da aplicabilidade do ordenamento jurídico internacional a novos meios e métodos de guerra, como a guerra cibernética e os ataques cibernéticos, numa situação qualificada como conflito armado e, no caso dos ataques cibernéticos, a aplicabilidade daquele ordenamento jurídico em situações não qualificadas como conflito armado. A interpretação de alguns Estados e Organismos Internacionais também será acrescentada nesse estudo.

2.2.1 O Espaço Cibernético

O espaço cibernético é definido na *US Joint Publication* 3-12 (2018, p. 100, tradução própria) como “o domínio dentro do ambiente informacional que consiste de rede independente de infraestrutura de tecnologia da informação e dados residentes, incluindo a internet, redes de comunicação, sistemas computacionais, servidores e administradores integrados”.

De acordo com Marrone e Sabatino[22] (2021, p. 10, tradução própria), a Estratégia de Segurança Nacional dos Estados Unidos da América de 2017 ressalta que no confronto geopolítico com Rússia e China o domínio cibernético é um dos principais campos de batalha.

Na terminologia aplicada ao espaço cibernético, ataques a redes de computadores são “ações tomadas através do uso de redes de computadores para interromper, negar, degradar ou destruir informações residentes em computadores e redes de computadores” (USA, 2010 *apud* Dinniss, 2023, p. 29). A mesma autora

22 Artigo Defesa Cibernética nos Países da OTAN: Modelos Comparativos, publicado em 2021 pelo *Observatorio di Politica Internazionali* (AIA), em colaboração com o Senado da República, a Câmara dos Deputados e o Ministério das Relações Exteriores e Cooperação Internacional da Itália.

também menciona a guerra centrada em redes, que usa a própria rede para fornecer uma vantagem de combate por meio de maior conscientização situacional e colaboração entre os componentes da rede, aumentando a velocidade com que as forças podem operar (Dinniss, 2023, p. 54).

2.2.2 Soberania, Jurisdição e Controle

A respeito da soberania, Alemanha[23] (2021, p. 3, tradução própria) “concorda com a visão de que operações cibernéticas atribuídas a um Estado que violam a soberania de outro Estado contrariam o Direito Internacional”. Esse Estado compartilha a visão do Manual de Tallinn 1.0 de que “operações cibernéticas atribuídas a um Estado que incidem em danos físicos e ferimentos no território de outro Estado constitui violação da soberania territorial desse Estado” (Alemanha, 2021, p. 4, tradução própria).

Sobre a questão da territorialidade, Alemanha (2021, p. 4, tradução própria) expressa que “o espaço cibernético não é um fórum desterritorializado”. Nesse sentido:

> Alemanha ressalta que não há ‘fronteira cibernética’ incongruente com fronteira física de Estado que poderia limitar ou desprezar o alcance de sua soberania. Dentro das fronteiras, um Estado tem o direito exclusivo – dentro do ordenamento jurídico internacional – de exercer plenamente sua autoridade, que inclui a proteção das atividades cibernéticas, pessoas engajadas nessas bem como estrutura cibernética no território de um Estado contra interferências cibernéticas e não-cibernéticas atribuídas a Estados estrangeiros (Alemanha, 2021, p. 3, tradução própria).

Entende-se aqui que o espaço cibernético de um Estado está contido dentro das suas fronteiras físicas, e que o Estado tem o direito de exercer autoridade e protegê-lo. Porém deve-se considerar também os sistemas que não estariam dentro dessas fronteiras físicas, como satélites de uso governamental ou militar.

Em relatório produzido pelas universidades de Bolonha, Milão e Westminster, Tanzi e outros acadêmicos[24] atribuem fundamental importância à soberania no espaço cibernético, e consideram que Estados não devem conduzir operações

23 A República Federal da Alemanha emitiu em 2021 um posicionamento (*Position Paper*) sobre A Aplicação do Direito Internacional no Espaço Cibernético, documento preparado pelo Ministério das Relações Exteriores e pelo Ministério da Defesa da Alemanha.

24 Relatório produzido em 2021 por grupo de estudo de acadêmicos das universidades de Bolonha, Milão e Westminster, com o apoio da Unidade de Planejamento Político do Ministério das Relações Exteriores e Cooperação Internacional da Itália, como proposta de posicionamento da Itália na questão do Direito Internacional e o Espaço Cibernético.

cibernéticas que produzem efeitos nocivos no território de outro Estado (Tanzi *et al*, 2021, p. 121, tradução própria).

2.2.3 Responsabilidade dos Estados

A responsabilização legal por operações cibernéticas do tipo ataques a redes de computadores depende da correta atribuição de sua autoria. Isso torna-se particularmente sensível quando refere-se aos Estados. Como Dinniss observa:

> Um dos principais problemas de qualquer ataque às redes de computadores é a imputação do ataque a um determinado ator. Enquanto a origem de alguns ataques se torna imediatamente evidente, seja porque o agressor se identifica, ou porque precedem ataques tradicionais que são facilmente atribuídos a uma determinada fonte, outros ataques são lançados anonimamente. Considerando o uso comum de *botnets* e a frequência de falsificação de IP que ocorre em ataques a redes de computadores, é difícil afirmar categoricamente que a entidade que parece ser a perpetradora do ataque é de fato o invasor final (Dinniss, 2023, p. 141).

Como exemplo, alguns endereços de IP dos ataques de negação de serviço de 2007 contra a Estônia foram atribuídos a endereços IP estatais da Rússia, mas esse país alegou que os computadores desses IP estavam comprometidos e sendo manipulados de fora da estrutura governamental (Dinniss, 2023, p. 143). Outra situação trazida por Dinniss (2023, p. 143) são os ataques cibernéticos lançados por indivíduos ou grupos em conjunto com a ação estatal tradicional. Como exemplo, quando a Rússia transferiu tropas para a Ossétia do Sul após a ofensiva georgiana em 2008, os ataques aéreos e terrestres foram acompanhados por uma série de ataques contra servidores georgianos. Embora esses ataques certamente não tenham sido sérios o suficiente para equivaler a ataques armados, dada a conectividade limitada da Geórgia à internet, eles ilustraram a capacidade de outros atores efetivamente ‘se juntarem’ a um conflito com ou sem a autorização do Estado (Dinniss, 2023, p. 143).

A mesma autora adota o exposto por Ian Brownlie, no qual “um Estado não deve permitir que seu território seja usado como santuário para terroristas ou bandos armados empenhados em atacas alvos militares ou objetos civis em outros Estados” (Brownlie, 1958 *apud* Dinniss, 2023, p. 144).

Outro fator complicador de atribuição e responsabilização é mencionado por Carr (2014, p. 4, tradução própria), sobre o qual comenta que “caso não haja

hostilidades ou tensões geopolíticas entre a vítima de um ataque cibernético e o atacante, o governo vitimado deve confiar em seus serviços de segurança e inteligência para descobrir o ator responsável".

2.2.4 Proibição do Uso da Força

Os ataques cibernéticos realizados contra a Estônia em 2007 paralisaram esse país, que já possuía diversos serviços comerciais e governamentais conectados em rede. Segundo Dinniss (2023, p. 71), o governo estoniano teria desistido de formalizar acusação contra outro Estado, embora tivesse feito acusações anteriores de que a Federação Russa estaria envolvida nesses ataques. Parece que os Estados não estavam preparados para fazer declarações públicas definitivas sobre os ataques como uso da força. Os Estados-membros da OTAN certamente não estavam preparados para aceitar que os ataques [cibernéticos] equivaliam a um ataque armado que daria início às disposições de autodefesa coletiva do Tratado do Atlântico Norte (Dinniss, 2023, p. 89).

Em decorrência disso, Dinniss (2023, p. 72) argumenta que "o advento dos ataques às redes de computadores renovou uma questão muito mais fundamental: qual é o significado de 'força' no século XXI?" Segundo essa autora, "a semântica da guerra e do armamento não são mais critérios úteis para determinar se algo é uso da força" (Dinniss, 2023, p. 95).

Para explicar tal entendimento, Dinniss (2023) cita "teorias da força" de alguns autores na sua análise sobre o uso da força. Ressalta a teoria baseada em resultados de Brownlie que exemplifica que o uso de armas químicas e biológicas produz um efeito não cinético na destruição de vidas e propriedades (Brownlie *apud* Dinniss, 2023, p. 95), a partir do qual tal autor "move o teste para além do impacto cinético das ondas de choque e do calor e em direção a uma abordagem mais ampla e orientada a resultados" (Brownlie *apud* Dinniss, 2023, p. 95). Dinstein defende uma abordagem baseada em resultados ao discutir ataques a redes de computadores no contexto de um ataque armado, e "argumenta que as consequências violentas são a chave para satisfazer a definição de ataque armado" (Dinstein *apud* Dinniss, 2023, p. 96).

> Do ponto de vista legal, não há razão para diferenciar entre os meios de ataques cinéticos e eletrônicos. Um ataque de rede de computadores

> destrutivo premeditado pode se qualificar como um ataque armado tanto quanto um ataque cinético trazendo resultados iguais ou semelhantes – o cerne da questão não é o meio disponível (um servidor de computador em vez de [...] uma bateria de artilharia), mas as consequências violentas da ação tomada. Se há uma cadeia de causa e efeito entre o ataque às redes de computadores e suas consequências violentas, pouco importa que tenha sido produzida por alta e não por baixa tecnologia (Dinstein *apud* Dinniss, 2023, p. 96).

O enquadramento dos ataques cibernéticos como ataque armado nem sempre é de fácil qualificação. Na sua análise, Dinniss (2023, p. 102) define que a intangibilidade dos ataques cibernéticos é uma das características que o distingue dos demais ataques convencionais. Para tal autora, o problema da intangibilidade existe em três níveis: primeiro, o alvo do ataque pode não existir no mundo físico, a não ser como informações mantidas em um servidor; em segundo lugar, a própria 'arma' é intangível, um pedaço de codificação binária que pode causar um efeito catastrófico; em terceiro lugar, o tipo de dano causado pelo ataque também pode ser intangível (Dinniss, 2023, p. 104).

Dinniss (2023, p. 112) considera que "quando um ataque às redes de computadores, direta ou indiretamente, resulta em uma consequência física, nomeadamente destruição de propriedade física, lesão ou perda de vidas, constituirá um uso da força nos termos do Artigo 2(4) [na Carta da ONU]". Por outro lado, quando os resultados de um ataque às redes de computadores não produzem consequências físicas, afetando somente a informação, a mesma autora se manifesta que "[tal] ataque não se enquadra claramente no teste tradicional do Artigo 2(4) e não constituirá uso da força" (Dinniss 2023, p. 112).

A respeito da qualificação de um ataque cibernético como ataque armado durante um conflito armado, o Comitê Internacional da Cruz Vermelha expôs entendimento de que ataques que resultem em perda de funcionalidade de computadores ou sistemas computacionais, mesmo sem danos físicos, constituem ataque armado (CICV, 2019, p. 7, tradução própria).

A Alemanha compartilha a visão de que a definição adotada para uso de força deve enfatizar os efeitos do ataque mais do que os meios utilizados (Alemanha, 2021, p. 6, tradução própria), bem como compartilha a visão do Manual de Tallinn 1.0 de que "o limiar do uso da força em operações cibernética é definido […] pela escala e efeitos dessa operação cibernética" (Alemanha, 2021, p. 6, tradução própria). Esse Estado sugere que uma avaliação quanto a se ter cruzado o limiar de proibição do uso da força deve ser implementada caso a caso.

> Baseado na avaliação de escala e efeitos de uma operação, o contexto mais amplo da situação e a relevância da operação cibernética maliciosa deverão ser levadas em consideração. Critérios qualitativos que podem desempenhar papel messa avaliação são […] a severidade da interferência, o imediatismo dos seus efeitos, o grau de intrusão numa estrutura cibernética estrangeira e o grau de organização e coordenação da operação cibernética maliciosa (Alemanha, 2021, p. 6, tradução própria).

Tanzi *et al* (2021, p. 128, tradução própria) considera uso da força[25] de um Estado contra outro a operação cibernética que cause dano material a objetos, morte ou ferimento de pessoas, ou perda severa de funcionalidade. Esses autores ressaltam que "operações cibernéticas causando mera perda de funcionalidade podem ser qualificadas como uso da força […] quando causa a interrupção de serviços essenciais independente da ocorrência de dano físico" (Tanzi *et al*, 2021, p. 128, tradução própria).

Na presente análise, torna-se interessante observar a forma como alguns Estados tem concebido a utilização de operações cibernéticas, por meio das suas posturas divulgadas. Como primeiro exemplo, a postura adotada pelos EUA, de acordo com Marrone e Sabatino (2021, p. 11, tradução própria) é de praticar a defesa preemptiva[26] no domínio cibernético, atacando os recursos cibernéticos de seus adversários que podem representar ameaça aos EUA ou mesmo detê-los de ações ofensivas por meio de ameaça crível ou retaliação. Esses autores também citam o uso de retaliação pelos EUA no domínio cibernético, exemplificando um ataque cibernético com *malware* sobre a rede de eletricidade da Rússia em 2019, em retaliação a um suposto ataque russo contra plantas de energia dos EUA (Marrone e Sabatino, 2021, p. 12, tradução própria).

O Reino Unido também adota postura ofensiva no domínio cibernético. Segundo Marrone e Sabatino (2021, p. 14, tradução própria), a Estratégia de Segurança Nacional do Reino Unido de 2016 prevê, além de medidas de defesa cibernética e de uma infraestrutura resiliente, o desenvolvimento de uma eficiente capacidade de dissuasão para fazer o país um alvo difícil para ataques. Nesse sentido, o Relatório Anual ao Parlamento do Comitê de Inteligência e Segurança deu uma visão geral das operações ofensivas viáveis. Estas são identificadas como as habilidades para: responder a ataques cibernéticos; negar, interromper ou degradar as comunicações adversárias ou sistemas de armas; atacar amplos sistemas ou

25 O termo "uso da força" aqui refere-se a atos que contrariam o Artigo 2(4) da Carta da ONU.
26 Preemptivo deriva da palavra *preemptive*, que significa preventivo.

infraestrutura, com a possibilidade de estender os danos ao ‘mundo real’ Marrone e Sabatino (2021, p. 15, tradução própria).

A França é outro país que decidiu, a partir de 2008, desenvolver capacidade para realizar operações cibernéticas ofensivas, além das capacidades defensivas, por meio da criação de agência interministerial, sendo mais um país com postura ofensiva (Marrone e Sabatino, 2021, p. 12, tradução própria).

2.2.5 Aplicação da Lei dos Conflitos Armados

Quanto à aplicabilidade da Lei dos Conflitos Armados aos ataques cibernéticos, Dinniss afirma que ataques a redes de computador passíveis desse enquadramento ocorrem em três situações distintas:

> (i) onde os ataques à rede de computadores são utilizados como parte de um conflito armado convencional em andamento; (ii) onde os ataques à rede de computadores são lançados por conta própria; e (iii) onde o uso de armas convencionais é insuficiente por si só para qualificar como um conflito armado, mas é acompanhado por extensos ataques à rede de computadores (Dinniss, 2023, p. 173).

Segundo Dinniss, o conflito de 2008 entre Rússia e Georgia “é comumente aceito como a primeira instância de um conflito armado acompanhado de ataques à rede de computadores”, apesar da não comprovação da autoria dos ataques. De cordo com essa autora, “na medida em que os ataques à rede de computadores possam ser seguramente atribuídos a uma das partes em conflito, […] os ataques diretamente relacionados a operações militares serão cobertos pelas leis do conflito armado assim que entrarem em vigor” (Dinniss, 2023, p. 173).

A respeito do segundo tipo de ataque à rede de computadores, quando esses são lançados por conta própria, ou seja, quando não há outro tipo de operação militar convencional em curso, Dinniss faz referência à argumentação de Schmitt:

> Os princípios do Direito Humanitário aplicam-se sempre que os ataques `rede de computadores possam ser atribuídos a um Estado e que sejam mais do que meros incidentes esporádicos e isolados e tenham a intenção de causar ferimentos, morte, danos ou destruição (e efeitos análogos), ou tais consequências sejam previsíveis. Isso ocorre mesmo que a força armada clássica não esteja sendo empregada (Schimitt *apud* Dinniss, 2023, p. 179).

Na terceira situação, “um de ataque à rede de computadores ocorre quando é lançado um ataque convencional, que por si só não o qualificaria como ataque

armado, mas que é respaldado por extensos ataques à rede de computadores" (Dinniss, 2023, p. 181). A mesma autora exemplifica um ataque cibernético a diversos serviços de uma cidade poderia multiplicar os efeitos de um pequeno ataque convencional, e que neste caso, "é provável que tal combinação de ataques seja considerada suficiente para se qualificar como um conflito armado […]" (Dinniss, 2023, p. 182).

O posicionamento dos Estados sobre a aplicabilidade da Lei dos Conflitos Armados aos ataques cibernéticos reflete uma divisão, no qual, segundo Schmitt e Vihul (2014, p. 13, tradução própria), enquanto muitos Estados do Euro-Atlântico[27] tem confirmado publicamente que a *LOAC* aplica-se a operações cibernéticas associadas a conflitos armados, Rússia e China não endossam o mesmo entendimento. Sobre a possibilidade do surgimento de novos tratados para regular os meios e métodos cibernéticos, no entendimento desses autores:

> Como todos os outros meios e métodos de guerra, Estados são hesitantes a restringir o uso de armas que podem render a esses uma vantagem no campo do conflito até que eles tenham experiência suficiente para lhes permitir pesar os benefícios das proibições e limitações no seu uso (Schmitt e Vihul, 2014, p. 20, tradução própria).

O Comitê Internacional da Cruz Vermelha compartilha a visão[28] de que "os princípios e regras do Direito Internacional Humanitário[29] aplicáveis aos conflitos armados aplicam-se 'para todas as formas de guerra e todas as formas de armas' incluindo 'aquelas do futuro' […] isso se aplica ao uso de armas cibernéticas durante os conflitos armados" (CICV, 2019, p. 4, tradução própria).

Alemanha (2021, p. 7, tradução própria) reitera sua visão de que o "Direito Internacional Humanitário aplica-se a operações cibernéticas conduzidas no contexto de um conflito armado independentemente da sua qualificação como legal ou ilegal a partir da perspectiva do *ius ad bellum*". Essa manifestação expressa sua concordância com o que é conhecido como Princípio da Separação, no qual a avaliação de uma situação de agressão quanto ao preconizado no *ius in bello* deve ser conduzida em separado da avaliação do *ius ad bellum, e vice-versa.*

---

27 Considera-se nesse estudo os países citados em Schmitt e Vihul (2014, p. 13): EUA, Reino Unido, França, Alemanha, Espanha, Itália.

28 Parecer Consultivo da Corte Internacional de Justiça sobre a Legalidade da Ameaça ou Uso de Armas Nucleares, 1996.

29 Direito Internacional Humanitário (DIH) é a denominação comumente utilizada no meio diplomático, político e nas cortes internacionais para Lei dos Conflitos Armados.

Itália (2021, p. 119, tradução própria) considera que “as regras e princípios do direito internacional […] aplicáveis a atividades no espaço cibernético não limitam-se àquelas pertencentes à proibição do uso da força nas relações internacionais”.

2.2.6 Princípio da Distinção

Sobre o princípio da Distinção aplicado às operações cibernéticas, e a seleção de alvos como objetivos militares legítimos para ataques cibernéticos, Dinniss (2023, p. 246) concorda com posicionamento dos EUA de que “quaisquer bens ou serviços que sustentam a economia de um país (e, portanto, a capacidade do governo de travar a guerra) se tornariam alvos legítimos”. Ainda segundo a autora, “essa abordagem renuncia à exigência de um nexo estreito entre o alvo e as operações militares em andamento” (Dinniss, 2023, p. 247), conforme previsto na definição de objetivo militar no Artigo 52 do Protocolo Adicional I[30]. Nesse sentido, os ataques à Estônia em 2007, que duraram mais de um mês e quase paralisaram a estrutura digital do país, seriam legalmente justificadas se ocorressem durante o curso de um conflito armado (Dinniss, 2023, p. 248). Porém, isso pode colocar em perigo o sustento da população civil, no caso de um país de matriz econômica forte em agricultura, por exemplo, o que poderia violar o Artigo 54 do Protocolo Adicional I[31], de Proteção dos bens indispensáveis à sobrevivência da população civil.

Ataques a nós de internet, a fim de interromper comunicações em sistemas atendidos dentro da distribuição desses nós, é um bom exemplo do emprego do princípio da distinção. Dinniss (2023, p. 264) avalia que “não importa quão alto o sistema ou nó-alvo esteja na rede da vítima, e qualquer que seja o efeito subsequente da sua destruição ou neutralização, cada nó deve ser avaliado por seus próprios méritos para se qualificar, ou não, como um objetivo militar”.

Sobre ataques a servidores civis de internet, Schmitt (2015, p. 11, tradução própria) admite que “se há informações confiáveis que um servidor civil de internet

30 No que diz respeito aos bens, os objetivos militares são limitados aos que, por natureza, localização, destino ou utilização contribuem efetivamente para a ação militar e assim sua destruição total ou parcial, sua captura ou neutralização oferecem, nestes casos, uma vantagem militar precisa (CICV, 1998, P. 42).

31 O Artigo 54(2) do Protocolo Adicional I estabelece que “é proibido atacar, destruir, remover ou tornar inúteis objetos indispensáveis à sobrevivência da população civil, como alimentos, áreas agrícolas para a produção de alimentos, plantações, gado, instalações e suprimentos de água potável e obras de irrigação, com o propósito específico de negar-lhes seu valor de sustento à população civil ou à Parte adversa, seja qual for o motivo, seja para matar civis de fome, para fazê-los se mudar ou por qualquer outro motivo” (CICV, 1998, p. 43).

irá em breve armazenar dados militares, o servidor é um objetivo militar que pode ser atacado mesmo antes do início do armazenamento de dados".

Pessoas envolvidas em ataques cibernéticos também podem ser qualificadas como alvos legítimos. O conflito entre Rússia e Geórgia, no qual vários civis juntaram-se ao esforço de ataques cibernéticos sobre a Geórgia e sua população, é um exemplo de que "é tão fácil 'cyber armar' a população civil como fazê-lo com armas convencionais […] muitos indivíduos tem o *know-how* para conduzir operações cibernéticas ofensivas" (Schmitt, 2015, p. 15, tradução própria). O mesmo autor defende que um indivíduo que engaja em múltiplas operações cibernéticas de uma campanha cibernética em curso, como um participante direto nas hostilidades e, portanto, alvejável durante (somente) o período em que tiver ativamente conduzindo operações cibernéticas. (Schmitt, 2016, p. 15, tradução própria).

A distinção é particularmente discutida nos ataques à rede de computadores com a utilização de código malicioso que, dependendo da sua engenharia, podem se proliferar indiscriminadamente, causando efeitos em diversas redes de computadores, ou podem ser precisamente seletivos, só causando efeito na rede-alvo. Dinniss (2023, p. 264) menciona que quando o vírus Stuxnet foi descoberto e submetido a engenharia reversa em 2010, os pesquisadores perceberam que, embora o vírus tenha sido desenvolvido para se propagar e se espalhar de forma bastante indiscriminada dentro de uma rede. Porém também constatou-se que o vírus havia sido codificado para executar sua carga útil apenas quando as condições específicas fossem cumpridas, indicando que estaria no sistema alvo. Na análise de Dinniss (2023, p. 264), embora o método de guerra pareça indiscriminado, as consequências que constituiriam um ataque são limitadas a sistemas particulares.

Diante dos exemplos de ataques expostos anteriormente, a análise quanto a observância do princípio da Distinção deve ser verificada caso a caso. Na seleção de nós de internet e servidores, como objetivo militar, deve-se analisar quais sistemas civis (não enquadrados como objetivo militar) são atendidos por tais nós, e qual parcela de serviços civis (não enquadrados como objetivo militar) são atendidos por tais servidores. Em outro exemplo, observou-se que pessoas envolvidas em ataques cibernéticos no âmbito de uma campanha cibernética ganhariam o status de combatente, e poderiam ser objeto de ataque, somente pelo período em que estiverem ativamente conduzindo tais operações cibernéticas. Isso implica num desafio de distinguir em que momentos essas pessoas estão com status de

combatente ou de pessoa protegida de ataques. Também viu-se o exemplo específico do vírus Stuxnet que parece atuar de forma indiscriminada na sua propagação e de forma seletiva no ataque final. Nesse caso específico, tal ataque observou o princípio da Distinção, ao não causar efeitos em outros sistemas quando se disseminou pelo mundo. Por fim, a seleção de quaisquer bens ou serviços que sustentam a economia de um país como alvo legítimo parece encontrar alguma concordância na doutrina internacional, mas deve-se observar o risco de ser direcionado a bens indispensáveis à sobrevivência da população civil, o que pode ferir o princípio da Distinção.

2.2.7 Princípio da Proporcionalidade

As operações cibernéticas aumentam as possibilidades de ataques a objetivos com menos danos colaterais, e maior observância do princípio da Proporcionalidade. Nesse sentido, Dinniss (2023, p. 236) observa que “alvos que estariam fora dos limites para neutralização por meios cinéticos tradicionais podem ser permitidos pelo simples expediente de desligá-los”. Tal autora levanta dois grandes problemas para os julgamentos da proporcionalidade num ataque cibernético: a extensão dos efeitos indiretos dos ataques, e os efeitos sobre sistemas de uso dual (Dinniss, 2023, p. 236). Tal julgamento complementa a análise da observância do princípio da Distinção, uma vez que, ao constatar-se que um ataque cibernético terá efeitos colaterais, a análise a partir desse ponto é quanto ao respeito ao princípio da Proporcionalidade.

Porém, alguns objetos, mesmo que constituam objetivos militares, não devem ser atacados, em virtude do risco de liberação de forças perigosas. Tais objetos gozam de medidas de proteção especial, prevista no Artigo 56(1) do Protocolo Adicional I[32], a fim de limitar a extensão dos danos colaterais permissíveis (Dinniss, 2023, p. 308). Nesse sentido, a autora adiciona que “a análise norteadora é a proteção da população civil contra danos colaterais catastróficos” (Dinstein *apud* Dinniss, 2012, p. 309). O mesmo Protocolo também prevê que não devem ser

32 O Art 56(1) estabelece que “as obras e instalações que contenham forças perigosas, tais como barragens, diques, e centrais nucleares de produção de energia elétrica, não serão objeto de ataques, mesmo que constituam objetivos militares, se esses ataques puderem produzir a liberação dessas forças em em consequência causar graves perdas na população civil. Outros objetivos militares situados sobre essas obras ou instalações, ou em suas vizinhanças, não dever ser objeto de ataques, quando estes puderem causar a liberação de forças perigosas e causar em consequência perdas graves na população civil” (CICV, 1998, P. 44).

atacados objetivos militares próximos a instalações contendo forças perigosas, como um ataque a rede de computadores que pode ter efeito colateral num sistema ou rede adjacente, com efeito indireto sobre uma barragem, dique ou gerador nuclear (Dinniss, 2023, p. 309).

Dado o exposto, observa-se a análise quanto a seleção de alvos para atender aos princípios da Distinção e da Proporcionalidade podem ser facilitadas no caso de instalações já protegidas, como no caso das que contém forças perigosas. Por outro lado, a integração de muitos sistemas civis e militares que atendem a infraestrutura de um Estado impõe certa complexidade no cálculo da proporcionalidade. Afinal, nas palavras de Dinniss (2023, p. 269), "até que ponto o fato de um Estado ter integrado deliberadamente sistemas civis e militares afeta o cálculo da proporcionalidade?"

2.2.8 Medidas de Precaução

A medida de precaução da Escolha de Armamento, como forma de minimizar a perda acidental de vidas civis, no comentário de Dinniss (2023, p. 275), "tendem a promover o uso de métodos de ataque à rede de computadores que não apresentam um risco inerente a objetos civis e não necessariamente causem destruição" (Dinniss, 2023, p. 275).

Para a aplicação da regra da Escolha de Alvos, devem ser escolhidos os objetivos que causem o menor perigo para a vida e os bens civis, quando há a opção de vários alvos selecionados para se atingir a mesma vantagem. Traz-se novamente o exemplo de ataque a nó de internet para se atingir um alvo legítimo, no qual deve-se selecionar o nó no ponto da rede que seja mais adequado para produzir os efeitos desejados no objetivo e respeitar o princípio da proporcionalidade pelos danos colaterais ocasionados a outros sistemas.

A Precaução contra os Efeitos dos Ataques Cibernéticos, de acordo com Dinniss (2012, p. 281), exigiriam que "as partes separassem os sistemas e redes militares dos civis e evitassem usar as redes civis para comunicações militares". Como exemplo , a autora cita que "a maior parte das comunicações militares dos EUA trafega por redes civis" (Dinniss, 2023, p. 269). Ressalta-se que essa regra é direcionada para o defensor, pelo estabelecimento de medidas de defesa cibernética dos sistemas civis e segregação desses da infraestrutura cibernética militar.

2.3. COMPOSIÇÃO DA LEI DOS CONFLITOS ARMADOS NOS ATAQUES CIBERNÉTICOS

2.3.1 O Espaço Cibernético

Na terminologia aplicada ao espaço cibernético, são definidos dois conceitos importantes: a infraestrutura cibernética; e o espaço cibernético. A primeira é composta pelas comunicações, o armazenamento, e os recursos computacionais sobre o qual o sistema de informações opera (Tallinn, 2012). O segundo é definido como “o domínio dentro do ambiente informacional que consiste de rede independente de infraestrutura de tecnologia da informação e dados residentes, incluindo a internet, redes de comunicação, sistemas computacionais, servidores e administradores integrados” (*US Joint Publication* 3-12, 2018, tradução própria)

Outros termos relevantes para esse estudo são as operações cibernéticas e os ataques a redes de computadores. As operações cibernéticas são definidas como o emprego de capacidades cibernéticas com o propósito primário de atingir objetivos no espaço cibernético (Tallinn, 2012). Ataques a redes de computadores são ações tomadas através do uso de redes de computadores para interromper, negar, degradar ou destruir informações residentes em computadores e redes de computadores (USA, 2010 *apud* Dinniss, 2012).

2.3.2 Soberania, Jurisdição e Controle

A respeito da soberania, observa-se que há entendimento formado por Alemanha (2021) com o Manual de Tallinn (2012) de que operações cibernéticas atribuídas a um Estado, e que incidem em danos físicos e ferimentos no território de outro Estado, constituem violação da soberania territorial desse Estado. Tanzi *et al* acrescentam que Estados não devem conduzir operações cibernéticas que produzem efeitos nocivos no território de outro Estado.

As abordagens do Manual de Tallinn 1.0 (2012) e Alemanha (2021) sobre exercício da jurisdição aplicada às operações cibernéticas convergem. Para ambos, a jurisdição é exercida de forma subjetiva quando um Estado aplica as suas leis exercendo jurisdição sobre um incidente que foi iniciado no seu território, mesmo que os efeitos da operação cibernética não tenham efeito nesse território; e a

jurisdição territorial objetiva garante jurisdição sobre indivíduos por parte de um Estado onde um incidente teve efeitos, mesmo que as operações cibernéticas tenham iniciado fora do território desse Estado. De acordo com alguns Estados, como Alemanha, o espaço cibernético não é um fórum desterritorializado. Dentro das fronteiras um Estado teria o direito exclusivo de exercer plenamente sua autoridade, que inclui a proteção das atividades cibernéticas, pessoas engajadas nessas, bem como a estrutura cibernética no seu território, contra interferências cibernéticas e não-cibernéticas atribuídas a outros Estados.

Ainda no exercício dessa soberania chama-se a atenção para a conduta dos Estados de não permitir consentidamente que seu território seja usado para a condução de operações cibernéticas com efeitos nocivos sobre outros Estados.

2.3.3 Responsabilidade dos Estados

A responsabilidade legal por meio de operações cibernéticas depende da correta atribuição de autoria dessas operações. Isso se torna particularmente sensível quando se refere aos Estados, em virtude da possibilidade de qualificação de um ataque cibernético como ataque armado (ver 2.3.4), o que poderá permitir o exercício do direito inerente de legítima defesa individual ou coletiva da vítima contra um suposto agressor, conforme previsto no Art. 51 da Carta da ONU[33]. Conforme exemplificado pelo Manual de Tallinn (2012) e outros autores, o uso da técnica de falsificação de IP (*spoofing)* que ocorre em ataques a redes de computadores torna difícil afirmar categoricamente que a entidade que parece ser a perpetradora do ataque é de fato o invasor final. Nesse caso, uma estrutura cibernética governamental pode estar sob controle de um outro ator não Estatal ou um terceiro Estado, com o propósito de utilizar essa infraestrutura para a condução de operações cibernéticas, inclusive com a possibilidade de utilização de técnica de *spoofing.* Teixeira (2024, p. 694) cita o exemplo do caso do ataque de 2007 à Estônia, no qual o rastreamento inicial apontou que o ataque estaria se originando de 178 países. Dado o exposto, a correta identificação e responsabilização do autor de um ataque cibernético é essencial para que a vítima de ataque cibernético exerça o direito de legítima defesa contra o agressor.

33 O Art. 51 da Carta da ONU estabelece que “Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva, no caso de ocorrer um ataque armado contra um membro das Nações Unidas”.

Outra situação são os ataques cibernéticos lançados por indivíduos ou grupos que se juntam a um esforço de guerra durante um conflito armado ou durante tensões geopolíticas entre Estados, mas muitas vezes sendo difícil inferir que tais ações estariam sendo controladas e coordenadas pelo ator Estatal. Há também a possibilidade de atos cometidos por atores não Estatais serem atribuídos a Estados, caso esse esteja provendo alguma instrução, suporte ou controle dos indivíduos ou grupos que conduzem operações cibernéticas contra outro Estado.

2.3.4 Proibição do Uso da Força

A proibição do uso da força elencada no Manual de Tallinn 1.0 (2012) baseia-se no princípio da não intervenção do Artigo 2(4) da Carta das Nações Unidas, e preconiza ser ilegal as operações cibernéticas que constituam a ameaça ou uso da força contra a integridade territorial ou independência política de qualquer Estado. Por outro lado, não considera como uso da força ações como a exploração cibernética, que não tenham elemento coercitivo, por se tratarem de mera intrusão no sistema de um Estado.

Para uma operação cibernética ser qualificada como uso da força, tal operação deve ascender ao nível de um ataque armado e ser conduzida por um Estado ou ser atribuída a esse, de acordo com o Manual de Tallinn 1.0. Dinniss (2023) questiona quanto ao significado de força no século XXI, particularmente com a utilização de meios e métodos cibernéticos. Nesse sentido, observa-se a análise de Dinniss quanto a intangibilidade dos ataques cibernéticos, que o torna diferente dos demais ataques convencionais. O alvo do ataque pode ser intangível quando for composto somente por dados num sistema computacional; a arma empregada para o ataque também é intangível, pois é composta de códigos de programação; por fim, o dano causado pelo ataque pode não envolver efeito físico.

Quanto aos efeitos intangíveis, interessante alusão é feita pelo Manual de Tallinn 1.0 e Dinniss com outros meios e métodos não cinéticos, como os ataques químico, biológico e radiológico, cujas consequências subsequentes podem incluir sofrimento ou morte. Dinniss (2023) parte dessa referência para fazer alusão à teoria baseada em resultados de Brownlie, que move o teste dos efeitos para além do impacto cinético das ondas de choque e do calor em direção a uma abordagem mais ampla e orientada a resultados, a exemplo do uso de armas químicas e biológicas

que produz um efeito não cinético na destruição de vidas e propriedades. Parece razoável esse posicionamento, que é reforçado pela análise baseada em resultados de Dinstein citado por Dinniss (2023), que avalia a cadeia de causa e efeito entre um ataque às redes de computadores e suas consequências violentas, sendo as consequências violentas a chave para satisfazer a definição de ataque armado. Como exemplo de ataque com efeitos subsequentes, cita-se novamente uma operação cibernética direcionada a uma instalação crítica de um Estado, como uma estação de purificação de água, e com efeito severo porém não destrutivo, da incidência de doença e morte causada pelo consumo de água contaminada. Dentre os Estados, Alemanha compartilha a visão de que a definição adotada para uso de força deve enfatizar os efeitos do ataque mais do que os meios utilizados.

Os ataques cibernéticos podem também ter efeitos tangíveis, como os danos provocados às centrífugas de enriquecimento de urânio da usina nuclear de Natanz no Irã, em 2010, causados por uma operação cibernética. Parece razoável qualificar essa operação como ataque armado, caso seja atribuída a autoria de tal operação a um ator Estatal. Dinniss (2023) e Alemanha (2021) corroboram com essa interpretação como uso da força, nos termos do Artigo 2(4), o ataque cibernético que resulta em uma consequência física, nomeadamente destruição de propriedade física, lesão ou perda de vidas.

Por outro lado, Dinniss (2023) expressa que um ataque não se enquadra claramente no teste tradicional do Artigo 2(4), e não constituirá uso da força, quando os resultados de um ataque cibernético não produzirem consequências físicas, afetando somente a informação. Nesse caso, levanta-se a questão da avaliação do ataque cibernético que causa somente perda de funcionalidade em sistemas computacionais, a exemplo dos ataques cibernéticos realizados contra a Estônia em 2007 que paralisaram esse país, que já possuía diversos serviços comerciais e governamentais conectados em rede. Há autores, como Tanzi *et al* (2014) que consideram que operações cibernéticas resultantes em mera perda de funcionalidade podem ser qualificadas como uso da força quando causam a interrupção de serviços essenciais, independente da ocorrência de dano físico. O CICV (2014) qualifica um ataque cibernético como ataque armado durante um conflito armado os ataques que resultem em perda de funcionalidade sistemas computacionais, mesmo sem danos físicos. Ressalta-se que no caso da Estônia não havia um conflito armado em curso, mas a qualificação dos ataques cibernéticos

a esse país como ataque armado poderiam caracterizar o uso da força contra tal país, nos termos do Artigo 2(4), caso fosse atribuída a autoria de tais ataques a um outro Estado.

Considerando o exposto, conclui-se que ataques cibernéticos que resultem em efeito severo porém não destrutivo, da incidência de doença e morte, são considerados ataques armados e, se forem atribuídos a um Estado, poderão ser qualificados como uso da força contra outro Estado. Da mesma forma, ataques cibernéticos que resultem em consequência física, nomeadamente destruição de propriedade física, lesão ou perda de vidas, são considerados ataques armados e, se forem atribuídos a um Estado, poderão ser qualificados como uso da força contra outro Estado. Diferentemente, se um ataque cibernético está inserido no contexto de um conflito armado já iniciado e causar perda de funcionalidade de um sistema computacional, então é considerado um ataque armado. Mas se o mesmo ataque cibernético causar perda de funcionalidade de um sistema computacional, mas fora do contexto de um conflito armado, ou seja, situação de paz, então não será considerado ataque armado.

2.3.4.1 Metodologia de avaliação

O Manual de Tallinn 1.0 (2012) apresenta uma proposta de avaliação de operação cibernética, a ser considerada por Estados, quando decidirem pelo uso de operação cibernética, para verificar se essa pode incindir em uso da força. Esses fatores devem ser analisados de forma combinada:

- Severidade - analisa-se a gravidade dos efeitos de uma operação cibernética, como o dano, destruição ferimento ou morte.

- Direcionamento - analisa-se a relação de causa e efeito entre uma operação cibernética e os efeitos sobre uma estrutura ou população de um Estado.

- Invasividade - refere-se ao grau de intrusão de uma operação cibernética sobre uma infraestrutura cibernética de um Estado. Quanto mais seguro é um sistema cibernético atingido, maior é a preocupação quanto a sua invasão.

- Caráter Militar - verifica o nexo entre a operação cibernética e operações militares em curso, na qual pode-se inferir que a operação cibernética é parte de uma operação militar.

- Envolvimento de Estado - quanto mais claro e próximo é o vínculo entre Estado e operações cibernéticas, é mais provável que outros Estados irão caracterizar essas como uso da força por aquele Estado.

- Urgência das Consequências do Ataque - foca no aspecto temporal dos efeitos de uma operação cibernética, se produzem efeitos imediatos ou após algum tempo, semanas ou meses.

- Mensuração dos Efeitos - é mais difícil avaliar consequências de efeitos não tangíveis ou subjetivos.

- Legalidade Presumida - atos que não são proibidos por tratado expresso ou de proibição por lei consuetudinária reconhecida, são permitidos.

A metodologia proposta por Alemanha (2021) é baseada na avaliação de escala e efeitos de uma operação, considerando que o contexto mais amplo da situação e a relevância da operação cibernética maliciosa deverão ser levadas em consideração. Critérios qualitativos que podem desempenhar papel nessa avaliação são a severidade da interferência, o imediatismo dos seus efeitos, o grau de intrusão numa estrutura cibernética estrangeira e o grau de organização e coordenação da operação cibernética maliciosa.

Os fatores similares nas duas metodologias podem ser assim associados: o contexto mais amplo da situação e a relevância da operação cibernética (Alemanha) pode ser relacionado ao fator Caráter Militar; a severidade da interferência (Alemanha) ao fator Severidade; o imediatismo dos seus efeitos (Alemanha) à Urgência das Consequências do Ataque; o grau de intrusão numa estrutura cibernética estrangeira ao fator Invasividade; e o grau de organização e coordenação da operação cibernética ao fator Envolvimento de Estado.

Amplia-se o fator Envolvimento de Estado a partir da análise do posicionamento de alguns Estados quanto ao uso de operações cibernéticas. Alguns países, como os EUA, Reino Unido e França, expressaram a adoção de uma postura ofensiva no domínio cibernético. EUA adotam a postura de defesa ativa, pela possibilidade de ataque de forma preemptiva aos recursos cibernéticos de seus adversários. O Reino Unido dedica-se ao desenvolvimento de uma eficiente capacidade de dissuasão para fazer o país um alvo difícil para ataques, com a possibilidade de utilização de ataques a sistemas ou infraestrutura, inclusive com a possibilidade de danos físicos. A França também concebeu o desenvolvimento de capacidade para realizar operações cibernéticas ofensivas. Embora outros Estados

não se manifestem sobre suas posturas no domínio cibernético, pode-se depreender que na competição entre os grandes atores estatais no sistema internacional tal postura também esteja sendo adotada.

Dada a similaridade das análises mencionadas, para efeito desse estudo será empregada a metodologia de avaliação de operação cibernética do Manual de Tallinn 1.0, para a análise das operações cibernéticas que serão avaliadas no capítulo 3.

2.3.5 Aplicação da Lei dos Conflitos Armados

A aplicabilidade da lei dos conflitos armados aos ataques cibernéticos, segundo Dinniss (2023), ocorrem em três situações distintas:

- onde os ataques à rede de computadores são utilizados como parte de um conflito armado convencional em andamento. Na medida em que os ataques cibernéticos possam ser seguramente atribuídos a uma das partes em conflito, os ataques diretamente relacionados a operações militares serão cobertos pelas leis do conflito armado;

- quando os ataques à rede de computadores são lançados por conta própria, e que sejam mais do que meros incidentes esporádicos e isolados, e tenham a intenção de causar ferimentos, morte, danos ou destruição, mesmo que a força armada clássica não esteja sendo empregada;

- quando o uso de armas convencionais é insuficiente por si só para qualificar como um conflito armado, mas é acompanhado por extensos ataques à rede de computadores, no qual é provável que tal combinação de ataques seja considerada suficiente para se qualificar como um conflito armado.

Na primeira situação anteriormente exposta, conclui-se que ataques cibernéticos combinados com operações militares - já há um conflito armado em curso - e cujos efeitos desse ataque cibernético o qualifiquem como ataque armado – e cuja autoria seja atribuída a um dos Estados envolvidos no conflito – são passíveis da aplicação da lei dos conflitos armados. Como exemplo pode-se citar uma operação cibernética para desabilitar um sistema de defesa antiaérea que será atacado em seguida por um ataque cinético.

A segunda situação mencionada por Dinniss envolve ataques somente com operações cibernéticas, sem que haja outras operações cinéticas em curso. Nesse caso, não há um conflito armado em andamento, no qual a lei dos conflitos armados já estaria sendo observada. Para essa análise, traz-se o posicionamento do grupo de Especialistas Internacionais do Manual de Tallinn 1.0, de que o conflito armado refere-se a situações envolvendo hostilidades, inclusive aquelas conduzidas somente pelo emprego de operações cibernéticas Observa-se que esse posicionamento dá sustentação ao enquadramento do emprego singular de operações cibernéticas na caracterização de um conflito armado, desde que não sejam mais do que meros incidentes esporádicos e isolados, e tenham a intenção de causar ferimentos, morte, danos ou destruição. Nesse caso, conclui-se que tal situação caracterizará o primeiro ataque de um conflito – uso da força de um Estado contra outro Estado - para a aplicação da lei dos conflitos armados.

Idêntica análise deve ser feita para a terceira situação, na qual o somatório dos efeitos dos ataques cinéticos e cibernéticos – nenhum desses enquadrados isoladamente como ataque armado – atinge o nível do ataque armado e, consequentemente, o uso da força de um Estado contra outro Estado, para a aplicação da lei dos conflitos armados.

2.3.5.1 Posicionamento dos Estados e Organismo Internacional

O posicionamento dos Estados sobre a aplicabilidade da Lei dos Conflitos Armados aos ataques cibernéticos reflete uma divisão. Estados do Euro-Atlântico tem confirmado publicamente seus posicionamentos. Alemanha (2021) defende o enquadramento das operações cibernéticas conduzidas no contexto de um conflito armado independentemente da sua qualificação como legal ou ilegal a partir da perspectiva do *ius ad bellum,* conforme o princípio da Separação já citado. Itália (2021) menciona que a aplicação a atividades no espaço cibernético não limitam-se àquelas pertencentes à proibição do uso da força nas relações internacionais. Observa-se que tais Estados corroboram com a aplicação da lei dos conflitos armados no uso de ataques cibernéticos, com os quais junta-se também o CICV (2019), que defende a aplicação à lei dos conflitos armados para todas as formas de

guerra e todas as formas de armas, do presente e do futuro, inclusive as cibernéticas.

Por outro lado, Estados como Rússia e China não endossam o mesmo entendimento. Sabe-se que esses e outros Estados preferem não se manifestar publicamente sobre limitações para o uso de novas tecnologias que estejam em discussão no sistema internacional, que possam levar elaboração de novos tratados para regular os meios e métodos cibernéticos, bem como restringir o seu uso. Afinal, conforme exposto por Schmitt e Vihul (2014), Estados são hesitantes até que possam pesar os benefícios das proibições e limitações no uso das das operações cibernéticas.

Considerando o exposto no Manual de Tallinn e o posicionamento de autores e Estados, pode-se admitir o entendimento a favor da aplicabilidade da lei dos conflitos armados aos ataques cibernéticos, nas duas primeiras situações descritas anteriormente, uma vez que os ataques cibernéticos nessas situações têm a qualificação de ataque armado. Para a terceira situação, não há uma métrica definida para mensurar “o somatório dos efeitos dos ataques cinéticos e cibernéticos”, tornando difícil qualificar o efeito final no nível de ataque armado.

2.3.6 Condução das Hostilidades

A partir da aplicabilidade da lei dos conflitos armados para as operações cibernéticas, entende-se que a condução das hostilidades deve observar princípios como o da distinção e da proporcionalidade, da mesma forma que para outros meios e métodos de guerra. Aqui a discussão desloca-se para a aplicabilidade de tais princípios no ambiente cibernético, pelo seu caráter intangível. Boa parte da infraestrutura de rede de computadores é de uso dual, atende a sistemas civis e militares, e ataques a redes militares teria efeitos sobre os civis. Devido a elevada probabilidade de atingir sistemas civis, Alemanha (2021) ressalta ser importante ter expertise para avaliar corretamente os potenciais efeitos indiscriminados durante o planejamento de ataque cibernético. Mas algumas situações poderão levar a decisão de ataque cibernético de um alvo, no qual seja elevada a possibilidade de danos colaterais na parte civil do sistema alvo. Nesse caso, Dinniss (2023) aponta que na discussão sobre o aspecto civil deve ser considerada como parte da equação da proporcionalidade e não como uma questão de distinção. Nos itens seguintes

serão descritas algumas regras a serem observadas pelos planejadores de operação com o uso de ataque cibernético.

2.3.7 Princípio da Distinção

O princípio da Distinção aplicado às operações cibernéticas tem como referências os Artigos 48[34], 51 e 52 do Protocolo Adicional I. O Manual de Tallinn 1.0 (2012) adota o previsto nos Artigos 51[35] e 52[36] referente à proteção da população e bens civis, com o propósito de estabelecer parâmetro para a proibição de ataque a civis em decorrência de operação cibernética.

Os planejadores de uma operação com o uso de ataque cibernético, quando fizerem a avaliação da observância de tal princípio, deverão fazer uma seleção de alvo de acordo com os parâmetros da definição de objetivo militar, conforme previsto no Artigo 52(2) do Protocolo Adicional I, o qual o Manual de Tallinn 1.0 também adota como referência.

> Art. 52(2) - "no que diz respeito aos bens, os objetivos militares são limitados aos que, por **natureza, localização, destino ou utilização** contribuem efetivamente para a ação militar e assim sua destruição total ou parcial, sua captura ou neutralização oferecem, nestes casos, uma vantagem militar precisa" (CICV, 1998, P. 42, grifo nosso).

O Manual de Tallinn (2012) propõe uma metodologia com critérios de avaliação de natureza, localização, propósito[37] ou uso[38], para a qualificação de objetos, como computadores, sistemas computacionais, e infraestrutura computacional, como objetivo militar passível de ser alvo de ataque cibernético:

- Natureza – são os computadores militares e infraestrutura cibernética militar, que atendem a centros de comando e controle, e comunicações militares;

- Localização - refere-se a uma área geográfica de importância militar específica, não considerando um endereço de IP como uma localização;

---

34 Art. 48 - Com vistas a assegurar a proteção e o respeito da população civil e dos bens de caráter civil, as Partes em conflito devem sempre fazer a distinção entre população civil e combatentes, assim como bens de caráter civil e objetivos militares, devendo, portanto, dirigir suas operações unicamente contra objetivos militares (CICV, 1998, p. 39).

35 Art. 51 - "os civis e a população civil gozam de proteção geral contra os perigos resultantes de operações militares" (CICV, 1998, p. 40).

36 Art. 52(1) - "Os bens civis não devem ser objeto de ataques ou de represálias. São bens de caráter civil todos os bens que não sejam objetivos militares […]" (CICV, 1998, p. 41).

37 Equivalente ao termo "destino" da definição do Art. 52(2).

38 Equivalente ao termo "utilização" da definição do Art. 52(2).

- Propósito - intenção do uso futuro de um objeto para fins militares, a exemplo de uma estrutura civil de transpônder em satélite de comunicações, utilizada para fins militares;

- Uso – emprego atual do objeto para fins militares.

O Manual de Tallinn exemplifica tal avaliação com uma operação cibernética contra um sistema SCADA de reservatório poderia ser empregada para liberar água na qual operações militares do inimigo são esperadas, desse modo negando seu uso pelo inimigo. Nesse caso, a área é um objetivo militar por causa da sua utilidade militar para o inimigo. De acordo com esse Manual, essa caracterização justifica utilizar meios cibernéticos para liberar a água do reservatório na área. Considera-se que nesse exemplo hipotético mencionado teriam sido atendidos outros princípios, como o da proporcionalidade. Entende-se aqui o enquadramento dessa área pelo critério do **propósito** (intenção do uso futuro para fins militares), pois espera-se que operações militares do inimigo sejam conduzidas nessa área, o que **contribuiria efetivamente para o esforço militar do inimigo**. O enquadramento dessa área como objetivo militar se completa com a identificação da **vantagem militar** obtida para a Parte autora do ataque cibernético, nesse caso pela negação da área ao uso futuro pelo inimigo, considerando que os possíveis danos colaterais atendam ao princípio da Proporcionalidade.

Sobre tais critérios de avaliação, o Grupo de Especialistas Internacionais (2012) expressa a opinião de que objetos que satisfazem ao critério da natureza são sempre passiveis de ataque, desde que obedecidos os demais critérios - contribuir efetivamente para a ação militar do inimigo, e oferecer uma vantagem militar precisa.

A partir dessa metodologia, passa-se a analisar os exemplos de ataques cibernéticos expostos em 2.2.7, pela avaliação de objetivo militar:

- Nós de internet como objetivo militar - deve-se analisar quais nós atendem a sistemas militares que se busca atingir com um ataque, buscando, sempre que possível, selecionar como alvo os nós que permitam um ataque com efeito seletivo sobre tais sistemas militares, ou com o mínimo de efeitos sobre sistemas civis atendidos por tais nós. Pode-se enquadrar esse nós no critério do **uso** – atual – para a **contribuição efetiva** em favor dos sistemas de comando e controle e comunicações militares inimigos, restando enquadrar no critério da **vantagem militar precisa** desse ataque.

- Servidores como objetivo militar - caso o servidor seja exclusivamente militar, esse já atende ao critério de objeto de **natureza** militar, atendendo automaticamente à **contribuição efetiva para o esforço militar** inimigo, restando observar o princípio da Proporcionalidade na **vantagem militar precisa** de uma ataque a esse servidor. Para servidores de uso dual, deve-se analisar quais atividades militares são atendidos por tais servidores. Avaliar pelo critério do **uso** seria recomendável, pois trata-se de objeto que não é de uso exclusivamente militar, devendo-se avaliar criteriosamente o quanto esse uso **contribui efetivamente para o esforço militar** inimigo e a **vantagem militar precisa** obtida por um ataque a esse servidor frente aos danos a sistemas e serviços civis que também são atendidos por esse servidor.

- Provedor de internet (uso dual) como objetivo militar – na situação hipotética anteriormente considerada, um ataque cibernético seria utilizado para desabilitar o sistema de resfriamento de toda a central de provedor de internet, para causar o dano por superaquecimento dos servidores nessa infraestrutura. Entende-se que houve o enquadramento pelo critério da **localização,** considerando que toda a infraestrutura **contribui efetivamente para o esforço militar** inimigo, restando avaliar o dano esperado aos servidores de uso civil no cálculo da proporcionalidade.

- Bens ou serviços que sustentam a economia de um país - o critério do **uso** ou **propósito** se enquadrariam, caso os bens ou serviços **contribuam efetivamente** para o esforço de guerra em curso ou futura, restando avaliar **vantagem militar precisa** obtida por um ataque a esse bens e serviços, com o cuidado quanto ao risco de ser direcionado a bens indispensáveis à sobrevivência da população civil, conforme exposto anteriormente.

- Pessoas envolvidas em ataques cibernéticos que, no âmbito de uma campanha cibernética ganhariam o status de combatente, e poderiam ser objeto de ataque somente pelo período em que estiverem ativamente conduzindo tais operações cibernéticas – entende-se que tais pessoas já estão **contribuindo efetivamente para o esforço militar** inimigo, e que tais pessoas seriam enquadrados pelo critério da **localização**, restando avaliar a **vantagem militar precisa** obtida por um ataque a essas pessoas frente ao dano (morte ou ferimento) causado a outras pessoas ou bens protegidos.

2.3.8 Princípio da Proporcionalidade

O Manual de Tallinn 1.0 adota o princípio da Proporcionalidade aplicado a operações cibernéticas a partir do conceito desse princípio previsto no Artigo 57 (2) (a)(iii) do Protocolo adicional I (nota 14). Esse Manual define como proporcionalidade:

> Um ataque cibernético que tenha expectativa de causar perda acidental de vidas humanas na população civil, ferimentos nos civis, danos nos bens de caráter civil, ou uma combinação desses, que seriam excessivos em relação à vantagem militar concreta e direta esperada é proibido (Tallinn, 2012, p. 132, tradução própria).

A avaliação da proporcionalidade num ataque cibernético, segundo Dinniss (2023), deve observar a extensão dos efeitos indiretos dos ataques e os efeitos sobre sistemas de uso dual (civil e militar). Nos efeitos indiretos, relembra-se o exemplo anterior do ataque ao nó de internet, no qual a inevitabilidade de atingir provedor(es) de uso civil atendidos pelo nó atacado deverá ter os efeitos indiretos sobre o sistema civil avaliados. Nos efeitos sobre sistemas dual, centrais de provedores de internet com servidores civis e militares, bem como satélites com transpônder de uso civil e militar são exemplos de sistemas nos quais deve-se avaliar os efeitos de ataque sobre a parte civil, caso não seja possível realizar ataque seletivo sobre a parte militar desses sistemas.

Por outro lado, a mera ocorrência de danos a civis e bens civis, também conhecidos como danos colaterais, no ataque cibernético a um objetivo militar legítimo, não caracteriza necessariamente esse ataque como ilegal, conforme observado no Manual de Tallinn 1.0. O próprio uso de operações cibernéticas aumentam as possibilidades de ataques a objetivos com menos danos colaterais pois, na avaliação de Dinniss (2023), alvos que estariam fora dos limites para neutralização por meios cinéticos tradicionais podem ser atingidos pelo simples desligamento desses. Aqui pode-se citar a desativação de um sistema de defesa antiaérea em área densamente povoada, cujo ataque cinético convencional incorreria em consideráveis danos colaterais. Neste caso, optando-se por um ataque cibernético, atender-se-ia ao princípio da proporcionalidade.

A proporcionalidade assume particular importância para alguns objetos que, mesmo que constituam objetivos militares, não devem ser atacados, em virtude do risco de liberação de forças perigosas. Tais objetos gozam de medidas de proteção especial, prevista no Artigo 56(1) do Protocolo Adicional I (nota 31), a fim de limitar a

extensão dos danos colaterais permissíveis. O mesmo Protocolo também prevê que não devem ser atacados objetivos militares próximos a instalações contendo forças perigosas. Pode-se fazer um contraponto ao ataque de simples “desligamento” de um sistema ou rede de computadores que supostamente atenderia ao princípio da Proporcionalidade, mas ao gerar um efeito indireto sobre uma barragem, dique ou gerador nuclear, faria com que essa instalação liberasse suas forças, incindindo na violação da proporcionalidade.

2.3.9 Meios e Métodos de Ataque

O Manual de Tallinn 1.0 (2012) define “meios de guerra cibernética” como “as armas cibernéticas e seus sistemas cibernéticos associados”, considerando como meio de guerra um sistema computacional, mas não a infraestrutura cibernética, como a internet, que conecta o sistema computacional ao alvo do ataque.

Quanto aos métodos de guerra cibernética, o mesmo Manual define como as táticas, técnicas e procedimento cibernéticos por meio das quais as hostilidades são conduzidas.

Pelo Manual de Tallinn, no caso de um *botnet* (rede de dispositivos recrutados) para realizar um ataque cibernético de negação de serviço distribuído, o *botnet* é classificado como meio de guerra cibernética enquanto o ataque de negação de serviço distribuído é o método de guerra cibernética.

Pela definição de Dinniss (2023), um *worm* é um método de ataque, pois esse é projetado para distribuir um código malicioso. Essa autora cita como exemplos o *worm Stuxnet e o worm Storm,* sendo que este último combina quatro componentes: um componente para roubar endereços de e-mail e redistribuir-se; um *Trojan de backdoor* para permitir o acesso subsequente à máquina comprometida; um recrutador de *bots* para incorporar a máquina ao *botnet Storm;* e uma ferramenta de ataque de negação de serviço (Dinniss, 2023). Parece razoável concordar com Dinniss de que os dois *worm* citados são métodos de ataque que exploram vulnerabilidades de programação por meio de componentes que permitem a intrusão nos sistemas até o computador ou sistema alvo, no qual a ferramenta de ataque que está sendo transportada pelo *worm* provocará o seu efeito.

Pelas definições citadas anteriormente, uma arma cibernética e seus sistemas cibernéticos associados são métodos de guerra cibernética. Nesse sentido, parece

adequado classificar um botnet como meio de guerra cibernética, pois uma rede de computadores recrutados será uma via para a condução de um método de ataque conjunto, como um ataque DDoS. Nesse caso o botnet funciona como uma arma cibernética para a condução do método de negação de serviço. Da mesma forma, um *worm* que transporta um conjunto de *malwares* seria um meio de transporte de tais *malwares*, que realizarão métodos de ataque diversos (roubo de endereços de e-mail para redistribuir-se, recrutador de bots para um *botnet*, negação de serviço distribuído, e outros) . Nesse caso, adotando a classificação de Tallinn, o *worm* seria uma arma cibernética para a condução dos métodos de ataque transportados.

Para efeito desse estudo, serão utilizados os termos “meios de ataque cibernético” e “métodos de ataque cibernético”.

Ainda no que se refere a meios e métodos de guerra cibernética, destaca-se a proibição utilização de Meios e Métodos Indiscriminados, baseada no previsto no Artigo 51(4)(b) e (c) do Protocolo Adicional I (nota 17). Pel regra 43 do Manual de Tallinn:

> É proibido empregar meios e métodos de guerra cibernética que são indiscriminador por natureza. Meios e métodos de guerra cibernética são indiscriminados por natureza quando esses não podem ser direcionados para um objetivo militar específico, ou limitados em seus efeitos conforme estabelecido pela lei dos conflitos armados, e consequentemente são de natureza para atingir objetivos militares, civis ou objetos civis sem distinção (Tallinn, 2012, p. 121, tradução própria).

Como exemplo, se um *malware* que é empregado por um Estado para atacar uma rede de computadores específica - que seja um objetivo legítimo - escapar para a rede de computadores civis, pode causar efeito indiscriminado.

Adicionalmente, também é estabelecido pelo Manual de Tallinn, na regra 49, a Proibição de ataque indiscriminado, baseada no previsto no Artigo 51(4)(a) do Protocolo Adicional I (nota 18) Diferentemente da regra 43, a regra 49 designa que “ataques cibernéticos que possuem a natureza de atingir alvos legítimos, e também civis ou objetos civis sem distinção, e durante o ataque são direcionados contra um alvo legítimo e civis ou objetos civis, são proibidos” (Tallinn, 2012) Como exemplo, considera o uso de um *malware* capaz de ser direcionado contra um alvo legítimo, porém durante o ataque esse *malware* é introduzido indiscriminadamente na internet para atingir o alvo (Tallinn, 2012).

2.3.10 Medidas de Precaução

As Medidas de Precaução aplicadas a operações cibernéticas baseiam-se no previsto nos Artigos 57 e 58 do Protocolo adicional I, sendo quatro as medidas que as compõem:

- Verificação de Alvos (nota 19) – o Manual de Tallinn 1.0 (2012) estabelece que devem tomar todas as medidas viáveis para verificar que os objetivos a serem atacados não são civis nem objetos civis nem sujeitos a proteção especial, ou a limitar o escopo do ataque para aqueles componentes ou capacidades do sistema sobre os quais há informação suficiente para verificar o seu status como alvo legítimo.

De acordo com Dinniss (2023), a Verificação de Alvos não seria difícil para alvos pré-selecionados, nos quais o ataque ocorre após vigilância e varredura e à rede de computadores alvo, para determinar um ponto de entrada. Ataques com *worms* e vírus não direcionados não atendem a esta medida de precaução.

- Escolha de Alvos (nota 20) – o Manual de Tallinn (2012) estabelece que quando for possível a escolha entre vários objetivos militares que proporcionem vantagem militar equivalente, o objetivo a ser selecionado para ataque cibernético deverá ser cujo ataque parece representar menor perigo para vidas civis ou objetos civis.

Sobre tal medida, considera-se o exemplo de um ataque a um sistema de comando e controle inimigo, no qual, observando essa regra, o atacante opta por um ataque cibernético diretamente sobre esse sistema, ao invés de atacar uma central de energia que atende a tal sistema e a outros sistemas de uso civil. Também enquadra-se aqui o exemplo citado anteriormente do ataque a nó de internet, optando-se por um nó mais abaixo no sistema pois, se um sistema for desligado muito acima do objetivo final, isso afetará não apenas o objetivo, mas todos os outros nós ou sistemas civis na rede.

- Escolha de Armamento – de acordo com Dinniss (2023), deve-se promover o uso de métodos de ataque à rede de computadores que não apresentam um risco inerente a objetos civis e não necessariamente causem destruição, como forma de minimizar a perda acidental de vidas civis.

- Precaução contra os Efeitos dos Ataques Cibernéticos - exige que as partes separem os sistemas e redes militares dos civis e evitassem usar as redes civis para comunicações militares.

Sobre essa última, o cumprimento dessa medida é direcionada para o defensor para o estabelecimento de medidas de defesa cibernética dos sistemas civis e segregação desses da infraestrutura cibernética militar. A falha de uma parte em conflito em tomar medidas de precaução para segregação de sistemas civis dos militares, não isenta a outra parte de observar as demais medidas de precaução num ataque cibernético. Essa é uma questão particularmente complexa, uma vez que, a partir da constatação de Dinniss (2023) que cita que a maior parte das comunicações militares dos EUA trafega por redes civis, a mesma autora deixa o seguinte questionamento: “até que ponto o fato de um Estado ter integrado deliberadamente sistemas civis e militares afeta o cálculo da proporcionalidade?”. Para efeito desse estudo, parece razoável considerar o que fora sugerido por diversos autores, de avaliar cada caso, de acordo com a situação particular de cada ataque, empregando as metodologias de avaliação recomendadas.

2.4 CONSIDERAÇÕES FINAIS SOBRE A DOUTRINA APLICADA AO CIBERATAQUE

Os ataques cibernéticos como meio e método de ataque representam um desafio para a aplicação do ordenamento jurídico internacional, de forma que não se permita a violação da soberania dos Estados pelo emprego da força, contrariando a Carta das Nações Unidas. Como novo meio e método de ataque, as operações cibernéticas são utilizadas em um novo domínio dos conflitos armados ou no qual são conduzidas as tensões geopolíticas.

Nesse contexto, a aplicabilidade da lei dos conflitos armados aos ataques cibernéticos envolve alguns desafios. O primeiro desses é avaliar o quanto um ataque cibernético é caracterizado como ataque armado. A intangibilidade dos ataques cibernéticos o torna diferente dos demais ataques convencionais, pois para os ataques cibernéticos o alvo pode ser intangível quando for composto somente por dados num sistema computacional, bem como a arma empregada para o ataque composta de códigos de programação também é intangível e, por fim, o dano causado pelo ataque pode não envolver efeito físico. Em segundo lugar, a autoria de um ataque cibernético qualificado como ataque armado deve ser corretamente atribuída a Estados, como condição necessária para caracterizar a violação de soberania de outro Estado por meio de tal ataque. Essa condição torna-se

particularmente sensível, em virtude da possibilidade do ataque ter sido lançado por grupos de dentro de um Estado e que não estejam sob seu controle, ou mesmo a estrutura cibernética governamental de um Estado estar sob controle de um outro ator não Estatal ou um terceiro Estado, para lançar ataque cibernético através do primeiro Estado, sobre o qual poderá ser atribuída equivocadamente a responsabilidade.

Apesar disso, os ataques cibernéticos podem ser empregados no âmbito dos conflitos armados, desde que sejam observadas algumas medidas de precaução como a correta seleção de alvos, a fim de evitar danos a pessoas e objetos protegidos, uma vez que os efeitos podem ser físicos. Nesse sentido, o ambiente cibernético apresenta particular desafio, pois parte da infraestrutura de rede de computadores é de uso dual, atendendo a sistemas civis e militares, e ataques a redes militares teria efeitos sobre os sistemas civis. Diante disso, a condução das hostilidades deve observar princípios como o da distinção e da proporcionalidade, da mesma forma que para outros meios e métodos de guerra.

3 ANÁLISE DOS ATAQUES CIBERNÉTICOS NA UCRÂNIA ENTRE 2013 E 2017

Neste capítulo será analisado se os ataques cibernéticos realizados no contexto da anexação da Crimeia pela Rússia, entre 2013 e 2017, contrariaram os Tratados, a Doutrina e a Jurisprudência do Direito Internacional dos Conflitos Armados (DICA). A primeira parte descreverá o conjunto de ações cinéticas e não cinéticas empregadas nesse período, e avaliação dessas ações quanto a qualificação como conflito armado, entendimento importante para a aplicação do DICA. Em seguida, serão identificados os ataques cibernéticos realizados em apoio às ações realizadas nos níveis político, estratégico e operacional, e os seus efeitos na população ucraniana. Por fim, será realizada a análise desses efeitos com base nos princípios do DICA, particularmente a Distinção e a Proporcionalidade, de acordo com a síntese das interpretações do capítulo 2.

3.1 A ANEXAÇÃO DA CRIMEIA PELA RÚSSIA EM 2014

3.1.1 Contexto Geopolítico

A descrição dos eventos que levaram à anexação da Crimeia pela Rússia em 2014 são importantes para a compreensão do contexto das tensões geopolíticas nessa região do mundo. Na história recente da Crimeia, de acordo com Medeiros (2022, p. 33), “em 1995, a região defendeu a sua separação do resto da Ucrânia que, para evitar que perdesse totalmente aquele território, cedeu o status de região autônoma com constituição própria àquela península.” Segundo Oliveira (*apud* Medeiros, 2016, p. 36), “a Crimeia conquistou mais ‘liberdade’ política, mas ainda era Kiev que possuía o território sob sua soberania”. Em 2010 Viktor Yanukovych torna-se novamente presidente da Ucrânia e, segundo Medeiros (2022, p. 35), “tinha como ‘meta’ para o seu governo estabelecer relações com os dois principais lados e protagonistas do mundo: União Europeia e Rússia”. Yanukovych decidiu por estabelecer como sua política externa um tipo de neutralidade para a Ucrânia, levando-a a cooperar com países membros da OTAN, o que representaria uma aproximação com a Europa, e com a Rússia (Medeiros, 2022, p. 38). Apesar da intenção de assinar a integração com a UE, Yanukovych declarou em novembro de 2013 que iria aprofundar as relações com Moscou (USA SOC, 2015, p. 28, tradução

própria). Setores da sociedade viram nessa intenção de aproximação uma ameaça à soberania da Ucrânia, gerando aumento da insatisfação com o governo, que culminou com o protestos iniciados na capital Kiev, cuja população apoiava a aproximação com a UE. Tais protestos não violentos logo se espalharam para o resto da Ucrânia, dando início ao que ficou conhecido como *Euromaidan*[39] (USA SOC, 2015, p. 29, tradução própria). Como consequência, em fevereiro de 2014 os Deputados ucranianos votaram para derrubar o presidente Yanukovych e realizar eleições presidenciais em 25 de maio de 2014 (BBC News Brasil, 2014), elegendo Petro Poroshenko como novo presidente do país. Ao subir ao poder, Poroshenko assinou o Acordo de Associação com a UE em 27 de junho de 2014, com oposição dos ucranianos pró-Rússia e os russos étnicos que viviam no país (USA SOC, 2015, p. 30-31, tradução própria).

Uma outra mudança que atingiu a região por diversas vezes foi em relação ao porto de Sebastopol, visto que foram formulados diversos tratados que determinavam por quanto tempo tropas russas poderiam utilizar a área como sede da esquadra russa no Mar Negro. O tratado mais recente foi assinado em 2010, e prolongou até 2042 o domínio da Rússia sobre a base naval de Sebastopol (OLIVEIRA *apud* Medeiros, 2016).

3.1.2 Método de Resolução de Conflito Interestatal

O enquadramento como conflito armado das ações empreendidas no processo de anexação da Crimeia apresenta alguma complexidade, uma vez que tais ações incluíram o emprego de vários meios e métodos de pressão política, diplomática, econômica e informacional em fases anteriores ao emprego de meios militares pela Rússia. Dessa forma, descreve-se a seguir o método de resolução de conflito utilizado nessa crise, para uma melhor compreensão da sequência das ações, e a identificação daquelas que contribuem para a correta qualificação da crise como conflito armado.

39 "Euromaidan" é uma combinação das palavras "Europa" e "Maidan", que em ucraniano significa "Praça da Independência". O movimento eclodiu após o governo ucraniano, liderado por Viktor Yanukovych, suspender a assinatura de um acordo de associação com a União Europeia. Essa decisão foi vista por muitos ucranianos como um afastamento da Europa e um alinhamento maior com a Rússia.

O novo método de guerra russa foi desenvolvido pelo General Valery Gerasimov[40], compreendendo o uso de operações híbridas, combinando atividades militares e não militares (USA SOC, 2015, p. 17, tradução própria), e de acordo com o observado na figura 1. Esse modelo compreende seis estágios de desenvolvimento do conflito, cada um caracterizado pela primazia de medidas militares e não militares mas apresentando incremento do envolvimento militar com a aproximação do conflito (USA SOC, 2015, p. 18, tradução própria):

1. Origens encobertas[41] - emprego de medidas para moldar o ambiente político e social favorável ao agente: pressão diplomática; ajuda econômica; e campanha de guerra informacional;

2. Escalada – exercício de pressão política e diplomática;

3. Início de atividades de conflito – incitação de manifestações, protestos, subversão, sabotagem, assassinatos e ataques paramilitares; movimentação estratégica de forças em direção à região do conflito;

4. Crise – inicio de operações militares, acompanhada por uma forte persuasão diplomática e económica. A guerra de informação continua com vista a tornar o ambiente propício à intervenção;

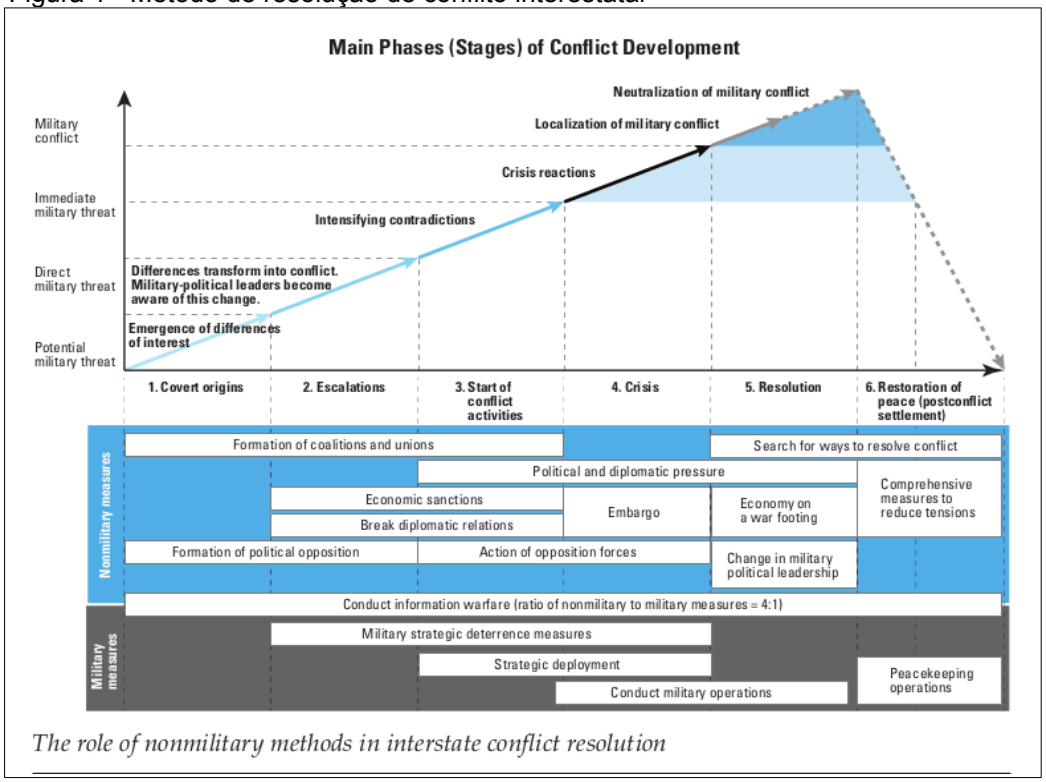
5. Resolução - Um aspecto fundamental da resolução é efetuar uma mudança na liderança militar e política do conflito região ou estado;

6. Restauração da paz – medidas para reduzir a tensão e restabelecer a paz.

40 Valery Gerasimov é Chefe do Estado-Maior das Forças Armadas Russas e Primeiro Vice-Ministro da Defesa.

41 Tradução do autor para *covert origins.*

Figura 1 - Método de resolução de conflito interestatal



Fonte - USA SOC, 2015, p. 18

3.1.3 A Intervenção da Rússa na Crimeia e a Crise no Leste da Ucrânia

O movimento do *Euromaidan* e a derrubada de Viktor Yanukovych da presidência da Ucrânia iriam possibilitar a aproximação desse país com a UE, o que era visto como inaceitável para Moscou, levando a Rússia a decidir pela anexação da Crimeia em fevereiro de 2014. Dentre as motivações da Rússia, acordo com o USA SOC:

> Os faetores estratégicos que levaram à agressão russa na Ucrânia incluíram a política interna, a reação à expansão da UE e da OTAN, o valor estratégico da no Mar Negro, a necessidade da Rússia de manter a influência nos Estados periféricos como um *buffer* contra a invasão ocidental, e o desejo do Presidente Putin de fortalecer a nova EEU[42] na antiga esfera de influência soviética (USA SOC, 2015, p. 36, tradução própria).

A Ucrânia possuía cerca de 18 mil soldados no início das tensões, e a Rússia possuía cerca de 12 mil soldados no Mar Negro, porém esses eram mais bem treinados e com melhores equipamentos (DOURADO, 2020, p. 130-131).

42 *Eurasian Economic Union* - União Econômica Eurasiática é uma união econômica dos Estados localizados principalmente no norte da Eurásia. O tratado de criação da UEE foi assinado em 29 de maio de 2014 pelos líderes da Bielorrússia, Cazaquistão e Rússia, e entrou em vigor em 1º de janeiro de 2015.

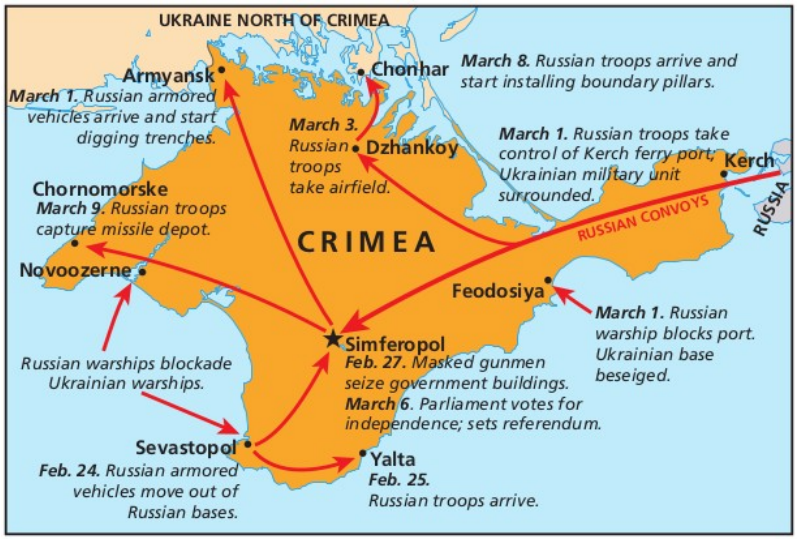
As ações empreendidas pela Rússia denotam o emprego dos estágios de desenvolvimento do conflito com medidas militares e não militares, conforme o método de resolução de conflitos interestatais descrito anteriormente. Logo após a deposição de Yanukovych, manifestações irromperam na Crimeia, nas quais os manifestantes pró-Rússia rotulavam o novo regime em Kiev como fascista. Nas ações militares, inicialmente percebeu-se que grupos de homens armados não identificados, chamados de *little green men*[43], começaram a aparecer e atuar na região da Crimeia, muitas vezes em coordenação com milícias pró-russas locais, tomando prédios do governo, instalações militares e outros pontos (USASOC, 2015, p. 31, tradução própria). Em 22 e 23 de fevereiro de 2014, Forças Aerotransportadas russas deixaram suas bases e foram aerotransportadas para perto do estreito que separa a Rússia da Crimeia (Kofman et al, 2017, p. 25, tradução própria). Em 25 de fevereiro de 2014 unidades da 810ª Infantaria Naval ocuparam uma praça em Sebastopol em veículos blindados de transporte de pessoal, violando as regras que regem as disposições de base na Crimeia (Kofman et al, 2017, p. 25, tradução própria). Em 27 de fevereiro, Forças Especiais russas tomaram o Parlamento da Criméia e hastearam a bandeira russa no prédio (Kofman et al, 2017, p. 26, tradução própria). Em 28 de fevereiro, o aeroporto de Sinferopol foi tomado por forças russas, por onde mais tropas russas passaram a chegar na península e, junto com reforços que chegaram em navios em 1º e 2 de março, ocuparam toda a península, sem resistência (Kofman et al, 2017, p. 27, tradução própria), e de acordo com o observado na figura 2. As forças russas isolaram a Crimeia da Ucrânia continental em seus pontos de travessia ao norte, cortando as comunicações terrestres entre o continente ucraniano e as bases na Crimeia, deixando a Ucrânia sem o comando efetivo e o controle sobre suas unidades na península (Kofman et al, 2017, p. 28, tradução própria).

Em 16 de Março, o governo interino da Crimeia realizou um referendo sobre secessão da Ucrânia e anexação à Rússia, anunciando que 97 por cento da população da Crimeia apoiou tal medida (USASOC, 2015, p. 57, tradução própria). Com esse instrumento político, a Rússia concluiu formalmente o processo de anexação em 18 de março (Kofman et al, 2017, p. 29, tradução própria).

---

43 *Little green men* é a denominação para grupos compostos de agentes russos não identificados que atuaram na pen(í)nsula da Crimeia, em 2013 e 2014, para organizar e liderar protestos e operações paramilitares (USASOC, 2015, p. 3, tradução própria).

Figura 2 - Operações da Rússia na Crimeia



Fonte - Kofman et al, 2017, p. 25

As potências ocidentais responderam com ameaças de novas sanções, e simultaneamente apelaram à Rússia para retirar as suas tropas e restituir a soberania ucraniana sobre a Crimeia (USASOC, 2015, p. 58, tradução própria). Apesar dessas ações das potências ocidentais, para o governo provisório de Kiev, distraído por acontecimentos no leste[44] da Ucrânia, a anexação da Crimeia aparentemente se tornou um fato consumado (USA SOC, 2015, p. 58, tradução própria).

Em resposta à anexação da Crimeia pela Rússia, a Ucrânia apresentou uma resolução à Assembleia Geral da ONU. A resolução foi aprovada em março de 2014, com uma ampla maioria, declarando o referendo da Crimeia inválido e reafirmando o compromisso da comunidade internacional com a integridade territorial da Ucrânia. (KENNEDY, 2006).

Ressalta-se que nesse período a Ucrânia estava sob um governo provisório, desde a deposição de Yanukovych em fevereiro até a eleição de Petro Poroshenko em 25 de maio de 2014. Tal situação dificultou a tomada de medidas coordenadas no nível político e estratégico para contraposição às ações da Rússia de anexação da Criméia. Destaca-se que as ações foram implementadas de forma coordenada em diversos níveis e domínios (político, diplomático, econômico e informacional) com as operações militares, conforme o método de resolução de conflito interestatal

44 Manifestações pró-Rússia e contra o novo regime em Kiev (após a deposição de Yanukovych) começaram a ocorrer no mesmo período das ações de anexação da Crimeia.

russo. A rapidez e simultaneidade das múltiplas ações desse método concorreu para a paralisia do poder político de transição em Kiev, aceitando como fato consumado o processo de anexação da Criméia pela Rússia, mesmo porque as manifestações no leste da Ucrânia já atraíam a atenção desse governo.

Após a anexação da Crimeia pela Rússia, a crise no leste da Ucrânia passa a ser a preocupação principal do poder político da Ucrânia. Durante os meses de março e abril, manifestantes pró-Rússia marcharam na região do Donbass, apreendendo edifícios governamentais em Donetsk, Luhansk, Slovyansk, Kharkiv, Kramatorsk, Horlivka e o porto de Mariupol, no Mar Negro (USA SOC, 2015, p. 58, tradução própria). Em maio as autoproclamadas Repúblicas Populares de Donetsk e Luhansk realizaram referendos, alegando que os resultados mostraram apoio popular à independência em relação à Kiev e anexação à Rússia (USA SOC, 2015, p. 60, tradução própria). Observadores reportaram a presença de tropas de operações especiais russas fomentando essas ações, o que caraterizaria a condução das primeiras etapas do método de resolução de conflito interestatal russo. De junho a agosto a Rússia apoiou as forças separatistas com material mecanizado, blindados, e defesa antiaérea de alto alcance (operado pelas próprias unidades russas), e o governo da Ucrânia os combatia com uma campanha que denominavam Operação Anti-Terrorista (Kofman et al, 2017, p. 62, tradução própria). A presença de tropas regulares da Rússia nessas áreas foram percebidas, e o novo presidente da Ucrânia Petro Poroshenko, declarou que a Rússia tinha lançado uma invasão em grande escala do país. (USASOC, 2015, p. 60, tradução própria), situação negada pela Rússia. Porém, segundo Kofman et al (2017, p. 62, tradução própria), a Rússia passou a operações convencionais, invadindo com convencionais e derrotando forças ucranianas na Batalha de Ilovaisk. Um acordo de cessar fogo[45] foi assinado em 5 de setembro, seguido de uma nova ofensiva russa em 13 de janeiro, e a assinatura de um segundo acordo de cessar fogo em 12 de fevereiro de 2015 (Tratado de Minsk II). Com a suspensão das hostilidades, a situação permaneceria como um conflito suspenso até a invasão da Rússia à Ucrânia em fevereiro de 2022. Desde os eventos de 2014, a Ucrânia tem trabalhado com aliados ocidentais para impor sanções econômicas e diplomáticas à Rússia, alegando que a

45 O Protocolo de Minsk I ou Tratado de Minsk I foi um acordo assinado por representantes da Ucrânia, da Rússia, da República Popular de Donetsk (DNR), e da República Popular de Lugansk (LNR) para pôr fim à guerra no leste da Ucrânia, em 5 de setembro de 2014.

Rússia violou a Carta da ONU e outras normas internacionais ao anexar a Crimeia e apoiar os separatistas no leste da Ucrânia (Kennedy, 2006).

Quanto a qualificação da crise da Crimeia como conflito armado, faz-se necessário identificar uma situação de hostilidades entre as partes ou ato de agressão por uma dessas. Para tanto, traz-se inicialmente o posicionamento de Dinstein:

> A experiência mostra que existem dois diferentes tipos de sentido de guerra: o material e o técnico. A guerra no sentido técnico se inicia com uma declaração de guerra e termina com um Tratado de Paz ou qualquer outro ato formal indicando que a guerra está terminada. A guerra no sentido material acontece independentemente de atos formais. Sua ocorrência é contingente somente da erupção das hostilidades entre as partes, mesmo na ausência da declaração de guerra (Dinstein, 2004, p. 12-13).

Analisando as ações militares de ambos os lados na Crimeia, a fase das operações militares ocorreram com o uso de tropas pela Rússia na península, porém sem grandes conflitos ou violência entre as partes. Conforme as bases e aquartelamentos das tropas ucranianas foram sendo cercadas pelas ações coordenadas das forças russas, houve um período de resistência pelos ucranianos, porém sem grades hostilidades, até a retirada das forças ucranianas da península após a conclusão do processo de anexação pela Rússia. O governo em Kiev deu ordens para sua tropas na Crimeia não escalarem o conflito e, de acordo com USASOC (2015, p. 56), em 9 de março o governo de Kiev confirmou que não pretendia enviar forças militares ucranianas para a Crimeia. Apesar da extensiva presença de tropas da Rússia na península, não se observou o irrompimento de hostilidades, sendo ainda duvidoso afirmar que houve uma situação de conflito armado.

Porém, de acordo com a definição de Agressão da Assembleia Geral da ONU, adotada em 1974, “agressão é o uso da força armada por um Estado contra a soberania, integridade territorial ou independência política de um outro Estado […]” (Disntein, 2004, p. 173). O Art. 3º dessa definição de 1974 cita dentre os atos específicos de agressão, a invasão ou ataque pelas Forças Armadas de um Estado ao território de outro, ou qualquer ocupação militar, mesmo que temporária, resultante de tal invasão ou ataque, ou ainda qualquer anexação pelo uso da força do território de um Estado ou parte dele (Dinstein, 2004, p. 179).

Portanto, com base nesse entendimento, pode-se afirmar que a ocupação militar da península da Crimeia pelas tropas russas, caracterizando as ações

cinéticas no conjunto das ações coordenadas, que resultaram na anexação desse território, caracterizou um ato de agressão, qualificando-o como um conflito armado internacional. O protesto das potências ocidentais à Rússia pela retirada das suas tropas e restituição da soberania ucraniana sobre a Crimeia reforçam o reconhecimento de que houve violação da soberania desse Estado pelo uso da força. Adicionalmente, com a assinatura do Memorando de Budapeste[46] de 1994, na qual a Ucrânia aderiu ao Tratado de Não Proliferação de Armas Nucleares em troca de garantias contra agressão, a Rússia assumiu o compromisso de respeitar as fronteiras ucranianas.

Da mesma forma, a crise no leste da Ucrânia entre fevereiro de 2014 e fevereiro de 2015 também pode ser qualificada como conflito armado internacional, em virtude do envolvimento direto de tropas russas na região realizando operações convencionais, e pelo acordos de cessar fogo entre as Partes em conflito, que é um instrumento para suspensão de hostilidades. De acordo com Dinstein (2004, p. 78), suspensão das hostilidades não deve ser confundida com término das hostilidades (ou término da guerra), pois a suspensão significa que o estado de guerra continua, pois não houve um devido processo de paz. Segundo esse mesmo autor, o irromper de hostilidades entre períodos de acordos cessar fogo ocasiona combates individuais dentro de uma mesma guerra (Distein, 2004, p. 78). Dessa forma, parece razoável afirmar que o conflito de anexação da Crimeia pela Rússia e os conflitos no leste da Ucrânia (entre fevereio de 2014 e fevereiro de 2015) são um único conflito armado entre Rússia e Ucrânia. Ampliando mais a análise, o rompimento do acordo de cessar fogo de 12 de fevereiro de 2015 (Tratado de Minsk II), com invasão da Ucrânia pela Rússia em fevereiro de 2022, pode ser considerado como a retomada do conflito armado entre Rússia e Ucrânia iniciado em fevereiro de 2014.

Sobre a aplicabilidade da Lei dos Conflitos Armados, segundo Dinstien (2004, p. 14), as leis do estado de guerra (constituindo o núcleo do *jus in bello* internacional) são aplicadas tão logo a guerra no sentido material seja engatilhada, apesar da ausência do estado de guerra do ponto de vista técnico. Esse princípio é descrito no art. 2º comum às Convenções de Genebra de 1949 para a Proteção das

46 No dia 05 de dezembro de 1994, a Grã-Bretanha, a Rússia e os Estados Unidos assinaram em Budapeste, o Memorando sobre as Garantias de Segurança em virtude da adesão da Ucrânia ao Tratado de Não Proliferação de Armas Nucleares (TNP). Os países signatários do Memorando de Budapeste se comprometeram a abster-se de recorrer à ameaça ou uso da força contra a integridade territorial ou a independência política da Ucrânia.

Vítimas de Guerra[47]. Diante do exposto, conclui-se que os Tratados, a Doutrina e a Jurisprudência do Direito Internacional dos Conflitos Armados (DICA) aplicam-se à crise que levou à anexação da Crimeia pela Rússia.

3.2 OS ATAQUES CIBERNÉTICOS NA UCRÂNIA ENTRE 2013 E 2017 E SEUS EFEITOS

De acordo com Casalunga (2020, p. 77), a campanha de intrusão cibernética da Rússia na Ucrânia teve início a partir da decisão do então presidente Viktor Yanukovych em aceitar o Acordo de Associação entre a Ucrânia e a União Europeia em 2013. Análise de documentos evidenciaram a presença de ferramentas espionagem de *spear phishing* contra alvos do governo central desde 2013 (LOOKINGGLASS *apud* Casalunga, 2015, p. 4). Desde 2013, uma campanha russa, denominada Operação Armagedon, supostamente visando o governo ucraniano**(,)** e autoridades policiais e militares, provavelmente ajudou a proporcionar uma vantagem militar à Rússia em relação à Ucrânia, com segredos obtidos por meio de espionagem cibernética (Weedon, 2015, p. 73).

Corroborando com o exposto, Perlroth (2023, p. 14) menciona que “por anos, hackers russos bombardearam os ucranianos com milhares de ataques cibernéticos por dia e rastrearam as redes do país incessantemente em busca de sinais de vulnerabilidade – uma senha fraca, uma brecha de segurança, softwares pirateados”. Sobre tais ações, ressalta-se que uma campanha de levantamento e acompanhamento de informações sensíveis de outro Estado proporciona vantagem para a realização de futuras campanhas (inclusive futuras operações cibernéticas), nos níveis político, estratégico e tático. Apesar da Operação Armagedon ter fornecido acesso a dados e vulnerabilidades que pudessem ser explorados posteriormente, essa operação não possibilitou uma situação política permanentemente favorável à Rússia, conforme se sucederam os eventos de fevereiro de 2014, com a deposição do presidente Viktor Yanukovych.

Durante a crise e conflito de 2014 na Crimeia, as operações militares russas ocorreram concomitante com ataques cibernéticos que atingiram os setores de comunicação, sistemas bancários, e comprometeram o funcionamento de

47 A presente Convenção será aplicada a todos os casos de guerra declarada, ou qualquer outro conflito armado, que possa ocorrer entre duas ou mais Partes Contratantes, mesmo que o estado de guerra não seja reconhecido por uma delas.

infraestruturas críticas (CROWDSTRIKE, 2014 *apud* Casalunga, 2020, p. 75). Tais ataques cibernéticos realizados em 2014 e a Operação Armagedon (em curso desde 2013) caracterizaram a utilização de grupos conhecidos como APT[48], dentre as quais destaca-se o APT29:

> O APT29 é um grupo russo de espionagem cibernética sofisticado e altamente capaz, com um conjunto de ferramentas diversificado e em constante evolução e operadores talentosos. As ferramentas do APT29 muitas vezes aproveitam serviços web legítimos para comando de *malware* e mecanismos de controle, o que pode torná-los mais difíceis de detectar, por parecem ser comunicações benignas à primeira vista. (Weedon, 2015, p. 69).

Uma das armas cibernéticas utilizadas pelas APT na Ucrânia é o BlackEnergy (BE), interferindo nos serviços de telefonia celular dos membros do parlamento dificultando a comunicação e o processo de decisório de resposta à invasão russa à Crimeia (Casalunga, 2020, p. 80). A Operação Potao desativou vários *websites* governamentais ucranianos e bloqueou telefones celulares e computadores de funcionários do governo, pouco antes das forças militares russas entrarem na península (Unwala & Ghori, 2015 apud Ramos, 2018, p. 48). Tais ataques ocorreram durante as ações iniciais no terreno pelos *little green men*, principais responsáveis pela tomada de controle da Crimeia (Casalunga, 2020, p. 80).

Diante do exposto, nos eventos que se sucederam desde 2013 até a incorporação da Crimeia pela Rússia em fevereiro de 2014, observa-se a utilização de operação cibernética, inicialmente no nível político, com a deflagração da Operação Armagedon, e posteriormente a realização de ataques cibernéticos pela Operação Potao em apoio a ações táticas no terreno. Durante a crise subsequente no leste da Ucrânia, ataques cibernéticos ocorreriam em apoio às ações nos níveis político, estratégico e tático.

Em 21 maio de 2014, logo após a declaração de independência dos territórios do Donbass em relação ao governo central de Kiev, a APT CyberBerkut assumiu a autoria dos ataques que atingiram a rede da Comissão Central de Eleições (CEC) (KOVAL, 2015, p. 56 *apud* Casalunga, 2020, p. 81). Essa APT assumiu o controle da página da CEC para anunciar uma notícia falsa da vitória do conservador Dmitry

48 Ameaças Persistentes Avançadas (APT, do inglês Advanced Persistent Threats) são grupos com alto grau de especialização, alta capacidade de adaptação e recursos para atuarem por muito tempo (Weedon, 2015). São atores estatais e não-estatais como espiões, hackers, criminosos e terroristas cibernéticos que atuam em esquemas altamente organizados, capazes de orquestrar ataques sofisticados sem que sua presença seja notada até que a ação tenha ocorrido e os danos causados (CAVELTY, 2013, *apud* Casalunga, 2020).

Yarosh nas urnas, que imediatamente foi compartilhada pelos canais de TV russos (KOVAL, 2015, p. 56 *apud* Casalunga, 2020, p. 81).

Outra arma cibernética utilizada, dessa vez pela APT FancyBear/Sofacy/PawnStorm, foi o X-Agent, ferramenta de acesso remoto capaz de infectar sistemas operacionais diversos como Windowns, iOS e MacOS (MEYERS, 2016, p. 1 *apud* Casalunga, 2020, p. 85). Em 2014, o X-Agent infectou um aplicativo utilizado por integrantes da artilharia ucraniana, fornecendo aos hackers russos a localização em tempo real das tropas ucranianas, permitindo às tropas russas antecipar os movimentos do adversário no campo de batalha (MEYERS, 2016, p. 4 *apud* Casalunga, 2020, p. 85).

No prosseguimento das tensões geopolíticas entre Rússia e Ucrânia, partir de 2015, ocorreram uma série de ataques cibernéticos às infraestruturas críticas da Ucrânia. Nesse contexto, uma APT identificada como Sandworm foi apontada como responsável por obter códigos de execução e senhas de acesso remoto para atacar setores de infraestrutura crítica da Ucrânia em meados de 2015 (LIPOVSKY, 2014 *apud* Casalunga, 2020, p. 87). O primeiro desses ataques cibernéticos ocorreu em 23 de dezembro de 2015, conforme relata Perlroth:

> Em 23 de dezembro de 2015, os mesmos hackers russos se infiltraram nas centrais elétricas da Ucrânia, invadindo os computadores que controlavam a rede elétrica do país e desligando os disjuntores até que milhares de ucranianos ficassem sem energia. Também desligaram os geradores de reserva nos centro de distribuição, fazendo com que encarregados de manutenção trabalhassem no escuro (Perlroth, 2023, p. 16).

As operações não autorizadas resultantes provocaram falta de energia para aproximadamente 225.000 consumidores em regiões do oeste da Ucrânia e na capital Kiev (Whitehead et al, 2017, p. 1). O efeito provocado foi uma falta de energia que durou menos de seis horas, porém esse ataque representou algo inédito pois, de acordo com Perlroth (2023, p. 16) “o que aconteceu no oeste da Ucrânia naquele dia não tem precedentes na história [...] até aquele 23 de dezembro de 2015, nenhum Estado-nação com meios para fazê-lo tivera coragem de realmente lançar o ataque”. Ainda segundo essa autora, “o desligamento de energia na Ucrânia tinha era um trabalho de impacto político, de demonstração de força por parte da Rússia, de que seria capaz de deixar a Ucrânia no escuro quando quisessem” (Perlroth, 2023, p. 17).

Em 2016 ocorreria o segundo desses ataques à Ucrânia. O incidente atingiu novamente no oeste do país, na região de Ivano-Frankivsk, no qual houve desligamento de sete subestações 110kV e 23 subestações 35K, e durante mais de duas horas o sistema teve de operar em modo manual (ICS, 2016, p.1 *apud* Casalunga, 2020, p. 88). Simultaneamente, houve um ataque do tipo de negação de serviço (DDoS) no sistema de comunicação telefônica, congestionando o serviço de central de atendimento da empresa de energia com milhares de chamadas, garantindo que os usuários atingidos não conseguissem relatar as interrupções (E-ISAC, 2016, p. 12 *apud* Casalunga, 2020, p. 90). A exposição da vulnerabilidade do Sistema de Supervisão e Aquisição de Dados (SCADA) para infraestruturas críticas limitou a confiabilidade público-privada na segurança do mesmo e, sob essa perspectiva, os ataques foram considerados críticos (E-ISAC, 2016, p. 3 *apud* Casalunga, 2020, p. 89).

Em junho de 2017, um ataque cibernético que ficou conhecido como NotPetya causou grande impacto na Ucrânia. Computadores em diversos sistemas apresentaram telas pretas em caixas eletrônicos, em sistemas de pagamento diversos em postos de gasolina, em estações de trem e supermercados, em sistemas de pagamentos de benefícios ou distribuição de correspondência (Perlroth, 2023, p. 20). Em Chernobyl 2500 computadores apagaram num intervalo de sete minutos, inclusive os que monitoravam os níveis de radiação do local do acidente nuclear que ocorreu três décadas antes. “Ninguém sabia se os níveis de radiação eram seguros ou se aquilo era algum tipo de sabotagem sinistra”, segundo o gerente de tecnologia de Chernobyl, Sergei Goncharov (Perlroth, 2023, p. 22). O *malware* do NotPetya apresentou um efeito indiscriminado, inicialmente atingindo empresas na Ucrânia e depois ao redor do mundo. Segundo Perlroth (2023, p. 20), computadores foram invadidos na *Pfizer* e na *Merck*, uma indústria farmacêutica, na empresa de navegação Maersk, na FedEx e numa fábrica de chocolates da Calbury na Tasmânia, e teria custado um bilhão de dólares à Maersk e FedEx.

Também foram relatados efeitos duradouros em decorrência do ataque cibernético NotPetya.

Segundo Perlroth (2023, p. 20), em 2019 os sistemas marítimo e ferroviário ainda não tinham se recuperado totalmente, bem como ainda havia pacotes de correspondência extraviados pela Ucrânia desde a queda do sistema de

rastreamento, e pagamentos de aposentadorias ainda não tinham sido restabelecidos, devido ao apagamento dos registros.

Apesar da amplitude geográfica dos efeitos dos ataques cibernéticos de dezembro de 2015 e 2016, e dos efeitos prolongados do ataque de junho de 2017, não foram relatados, até o presente momento, danos físicos ou mortes resultantes de tais ataques, apesar dos efeitos nos monitores de Chernobyl.

3.3 ANÁLISE DOS ATAQUES CIBERNÉTICOS NA UCRÂNIA SOB A LEI DOS CONFLITOS ARMADOS

A análise dos ataques cibernéticos na Ucrânia, descritos em 3.2, será realizada com base na síntese obtida no capítulo 2, a partir das interpretações dos Tratados, da Doutrina e da Jurisprudência do Direito Internacional dos Conflitos Armados. Inicialmente será analisado o quanto cada um dos ataques cibernéticos ultrapassou limites que o caracterizem como ataque armado. Em segundo lugar, será verificada a autoria desses ataques cibernéticos, pois a correta atribuição a um Estado é condição necessária para caracterizar a violação de soberania de outro Estado por meio de tal ataque pelo uso da força. Uma vez que a ocupação da Crimeia pelas tropas russas e a subsequente crise no leste da Ucrânia, entre fevereiro de 2014 e fevereiro de 2015, foram qualificadas como conflito armado internacional em 3.1.3, os ataques cibernéticos relacionados no período 2013-2017 ocorreram no âmbito desse conflito[49], o que caracteriza a condição para a aplicação do DICA. A partir dessa condição, serão analisadas a observância das medidas de precaução na condução das hostilidades, como a correta seleção de alvos, para o atendimento dos princípios da Distinção e da Proporcionalidade e outras medidas de precaução.

A primeira operação cibernética analisada é a Operação Armagedon. Do ponto de vista técnico, essa caracterizou-se por uma campanha visando agentes do Estado, para levantamento e acompanhamento de informações sensíveis. Mas as ações não foram direcionadas somente contra autoridades civis e militares, pois segundo o que foi exposto por Perlroth (2023), hackers russos já vinham atacando os ucranianos com ataques cibernéticos diários para rastrear as redes do país em busca de vulnerabilidades. Torna-se razoável afirmar que dados e vulnerabilidades

49 Em 2017 esse conflito estava suspenso desde o acordo de cessar fogo de 2015 (Tratado de Minsk II).

obtidos nesses ataques cibernéticos sobre a população ucraniana teriam sido usados para a realização da Operação Armagedon. Sobre os efeitos dessa operação, esses caracterizaram-se pela violação de dados e informações sensíveis, sem efeitos conhecidos sobre a funcionalidade de sistemas ou danos físicos, o que afasta a sua qualificação como ataque armado. Quanto a atribuição de autoria, as tensões geopolíticas entre a Rússia e a Ucrânia no período e os seus desdobramentos futuros a partir de 2014 tornam críveis a condução de uma campanha de espionagem cibernética em 2013 pela Rússia, a fim de apoiar as operações que se seguiram em 2014. Apesar dissso, não cabe a aplicação da Lei dos Conflitos Armados, pois de acordo com o grupo de Especialistas Internacionais de Manual de Tallinn 1.0 (2013), operações de espionagem cibernética ou exploração cibernética que não tenham elemento coercitivo não violam o princípio da não intervenção, por se tratarem de mera intrusão no sistema de um Estado.

Durante as ações no terreno para a tomada da Crimeia, pelos *little green men* e posteriormente por outras tropas russas, as operações militares russas ocorreram concomitantemente com ataques cibernéticos que atingiram os setores de comunicação, sistemas bancários, e comprometeram o funcionamento de infraestruturas críticas. Uma das armas cibernéticas utilizadas foi a BlackEnergy (BE), com a qual a Operação Potao desativou vários *websites* governamentais ucranianos e bloqueou telefones celulares e computadores de funcionários do governo e membros do parlamento.

Analisando-se esses ataques de fevereiro de 2014, enquanto a Operação Armagedon visou o espaço cibernético para a busca de dados residentes, a Operação Potao atuou sobre a infraestrutura cibernética, buscando efeitos de negação de serviço (DDoS). Destaca-se aqui para análise, dois efeitos conhecidos até o momento: a interrupção de serviços governamentais disponíveis nos seus *websites;* e a inoperância do serviço de telefonia celular no país. De acordo com o exposto em 2.3.4, um ataque cibernético inserido no contexto de um conflito armado já iniciado e que cause perda de funcionalidade de um sistema computacional, pode ser considerado um ataque armado. Diante disso, será feita a análise desse ataque, utilizadando a metodologia constante em 2.3.4.1:

- Severidade - nos efeitos sobre a interrupção da telefonia celular, esse tinha como provável propósito dificultar o comando e controle do nível político estratégico, das autoridades decisoras ucranianas, nas ações de contraposição à investida russa

na península da Crimeia. Tal ação teve efeitos severos, porém considera-se uma ação legítima sobre a função de combate comando e controle[50] durante um conflito armado. O outro efeito da operação Potao ocorreu sobre os serviços governamentais, e dentre esses podem ter sido atingidos aqueles utilizados pela população, como o acesso a benefícios sociais, previdenciários, serviços de saúde pública ou serviços de emergência – esses também possivelmente atingidos pela interrupção na telefonia celular. No entanto não se conhece, até o momento, a gravidade desses efeitos, como o dano, destruição ferimento ou morte, que possam ter sido causados pela falta de acesso a tais serviços no período que os efeitos foram sentidos.

- Direcionamento – é clara a relação da operação Potao com os efeitos sobre os *websites* governamentais ucranianos e o bloqueio da telefonia celular, pelo que se conhece.

- Invasividade - considera-se elevado o grau de intrusão da operação Potao, pois atingiu a infraestrutura cibernética de outro Estado, que geralmente possui requisitos elevados de segurança.

- Caráter Militar – a operação Potao ocorreu durante as ações no terreno para a tomada da Crimeia, o que lhe atribui o caráter militar.

- Envolvimento de Estado – as tensões geopolíticas entre a Rússia e a Ucrânia e a operação Armagedon desde 2013 apontam para o vínculo da Rússia como coordenadora da operação Potao.

- Urgência das Consequências do Ataque - a operação Potao produziu efeitos imediatos sobre os *websites* governamentais ucranianos e na telefonia celular.

- Mensuração dos Efeitos - não se conhece, até o momento, a gravidade dos efeitos sobre a população ucraniana, como o dano, destruição ferimento ou morte, que possam ter sido causados pela falta de acesso aos serviços governamentais ou de emergência, no período que os efeitos foram sentidos.

- Legalidade Presumida - não há tratado internacional ou lei consuetudinária reconhecida que torne ilegal a operação Potao, perante a comunidade internacional. Ressalta-se que a Rússia é um dos Estados que preferem não se manifestar publicamente sobre limitações para o uso de novas tecnologias que estejam em

50 Comando e Controle é uma das funções de combate, nos níveis de condução da guerra, nacional, estratégico, operacional e tático (*UNIVERSAL NAVAL TASK LIST, Department of the Navy, USA).*

discussão no sistema internacional, que possam levar elaboração de novos tratados para regular os meios e métodos cibernéticos, bem como restringir o seu uso.

A partir dessa análise, pode-se afirmar que a operação Potao foi lançada como parte de um conflito armado em andamento, e a sua atribuição a uma das partes em conflito – Rússia – torna tal operação cibernética coberta pelas leis do conflito armado, conforme o critério estabelecido em 2.3.5. Prossegue-se adiante a análise das medidas de precaução na condução desse ataque, para o atendimento dos princípios da Distinção e da Proporcionalidade. Conforme exposto em 2.3.7, a avaliação do princípio da Distinção inicia-se pela análise da seleção de alvo, conforme os parâmetros da definição de objetivo militar:

- Natureza – entende-se que a infraestrutura atingida pela operação Potao não é militar, por trata-se de infraestrutura civil que atende a sites governamentais e comunicações civis.

- Localização – sabe-se que a área geográfica atingida foram só centros governamentais na capital Kiev.

- Propósito – a infraestrutura atingida, sendo parte das comunicações do nível político e estratégico, provavelmente seriam utilizadas na gestão da crise na península da Criméia, com ordens fluindo das autoridades desses níveis para as forças militares no terreno, por meio da telefonia celular e outros meios de cominucação dessa estrutura governamental. É razoável afirmar que tal canal seria utilizado no comando e controle e comunicações militares, com fins militares.

- Uso – não há conhecimento do uso da infraestrutura atingida para fins militares.

Entende-se o enquadramento dessa infraestrutura pelo critério do propósito (intenção do uso futuro para fins militares), pois espera-se que o esforço militar ucraniano na península fosse coordenado no nível político e estratégico utilizando também as comunicações civis. Ressalta-se também que os websites governamentais também podem ser usados no esforço do conflitos, por meio dos quais podem fluir orientações à população e esforço de mobilização. Tais ações também contribuiriam efetivamente para o esforço militar ucraniano, atendendo ao segundo critério de alvo. O enquadramento como objetivo militar se completa com a identificação da vantagem militar obtida pela Rússia - autora do ataque cibernético - pela interferência no comando e controle ucraniano por ocasião do ataque à

Crimeia. Dessa forma, pode-se afirmar que a operação Potao atendeu ao princípio da Distinção.

Passa-se a analisar a observância ao princípio da Proporcionalidade, pela avaliação de possíveis danos colaterais. Os sites governamentais que foram derrubados podem ter sido atingidos por meio de ataque cibernético direto aos websites ou à infraestrutura de sistemas de uso dual, como provedores de internet que atendem a servidores do governo e civis. Nesse caso, ocorre o dano colateral a servidores civis, porém não se conhece até o momento a extensão de tais possíveis danos. Da mesma forma, o ataque de inetrrupção da telefonia celular de membros do governo teria atingido a disponibilidade desse serviço para a população, mas também não há dados suficientes da extensão desse efeito colateral na população ucraniana. Ressalta-se que o uso de operações cibernéticas aumentam as possibilidades de ataques a objetivos com menos danos colaterais, na medida em que são uma alternativa a ataques a sistemas de comunicações por meios cinéticos tradicionais, como bombardeios a infraestrutura física de comunicações na área atendida por tal sistema, a exemplo do ataque aéreo a uma torre de televisão no conflito entre Rússia e Ucrânia em 2022[51]. Diante disso, é razoável afirmar que a operação Potao atendeu ao princípio da Proporcionalidade.

Para completar a análise da operação Potao, verifica-se quanto ao meio e metodo de ataque e outras medidas de precaução. O meio de ataque utilizado foi o *malware* BlackEnergy (BE), com utilização de e-mails de spear-phishing com anexos maliciosos para infectar computadores do governo e da imprensa ucrânia[52], para a condução de método de ataque DDoS. Tal forma de ataque foi direcionado aos sistemas alvo, o que caracteriza o atendimento de medidas de precaução de verificação de alvo e escolha de alvo, bem como a da escolha de armamento (BE). Acressenta-se o fato de não se conhecer, até o momento, efeitos indiscriminados decorrentes desse ataque sobre a população civil, o que corrobora o atendimento ao princípio da Proporcionalidade.

Os ataques cibernéticos a infraestruturas de energia ocorridos em 2015 e 2016 serão analisados conjuntamente, em virtude da similaridade entre ambos. Uma APT identificada como Sandworm foi apontada como responsável por obter códigos de execução e senhas de acesso remoto para atacar setores de

51 Uma torre de televisão de 240 metros na cidade ucraniana de Kharkiv quebrou ao meio e caiu no chão depois de um ataque aéreo russo à essa infraestrutura (https://www.cnnbrasil.com.br / acesso em 26/7/24).

52 Fonte: https://www.kaspersky.com.br/resource-center/threats/blackenergy / acesso em 26/7/24.

infraestrutura crítica da Ucrânia. No ataque de dezembro de 2015, computadores que controlavam a rede elétrica do país foram invadindos, desligando os disjuntores e geradores de reserva, causando a falta de energia por seis horas para 225.000 ucranianos no oeste do país e na capital Kiev. Ataque semelhante ocorreu em dezembro de 2016, com efeito sentido no oeste do país por duas horas, com o sistema tendo que operar em modo manual. Nesse evento de 2016, também ocorreu um ataque simultaneo do tipo DDoS no sistema de comunicação telefônica, congestionando o serviço de central de atendimento da empresa de energia com milhares de chamadas, para que os usuários atingidos não conseguissem relatar as interrupções de energia.

- Severidade – 225.000 ucranianos ficaram sem energia no ataque de 2015, e provavelmente um efetivo menor - que 225.000 - da população ficou sem energia no ataque de 2016, que atingiu uma área menor - o oeste do país. Sobre o congestionamento da telefonia, parece que esse ataque ocorreu somente no serviço de central de atendimento da empresa de energia. No entanto não se conhece, até o momento, a gravidade desses efeitos, como mortes que possam ter sido causados pela falta de energia em hospitais. Diante disso, considera-se os efeitos não foram severos (dano destruição ferimento ou morte), limitando-se ao inconveniente causado à população.

- Direcionamento – é clara a relação da APT Sandworm com os efeitos sobre o fornecimento de energia na Ucrânia, pois esse tipo de *malware* vem sendo utilizado em ataques a infraestruturas de energia pelo mundo[53].

- Invasividade - considera-se elevado o grau de intrusão do Sandworm, pois atingiu a infraestrutura crítica de outro Estado.

- Caráter Militar – os ataques ocorreram durante o período de vigência do acordo de cessar fogo de 2015 (Tratado de Minsk II). Como o conflito armado estava suspenso, o ataque cibernético não esteve relacionado a uma operação militar em andamento, o que não lhe confere caráter militar.

- Envolvimento de Estado – as tensões geopolíticas entre a Rússia e a Ucrânia desde a anexação da Crimeia apontam para o vínculo da Rússia com a APT Sandworm e seus ataques cibernéticos.

- Urgência das Consequências do Ataque – o ataque por meio do Sandworm produziu efeitos imediatos de interrupção no fornecimento de energia.

53 Kaspersky, op. cit., acesso em 26/7/24.

- Mensuração dos Efeitos – a extensão conhecida dos efeitos foram a interrupção no fornecimento de energia para parcela da população, sendo 225.000 na primeira ocasião, e um número possivelmente menor na segunda ocasião. Não se conhece, até o momento, a extensão de outros efeitos sobre demais serviços essenciais ou de emergência.

- Legalidade Presumida – não há ainda proibição prevista no direito internacional pois, de acordo com Teixeira (2024, p. 864), “as zonas cinzentas são a prova concreta de que o direito posto não consegue responder todos os fenômenos jurídicos gerados com as operações cibernéticas maliciosas.”

Conforme mencionado anteriormente, os ataques cibernéticos à Ucrânia no perído 2013-2017 ocorreram no âmbito de um conflito armado, o que caracteriza a condição para a aplicação do DICA. A partir da análise dos ataques de 2015 e 2016, pode-se aribuir a autoria a uma das partes em conflito – Rússia. Porém os efeitos observados e conhecidos até o momento limitaram-se aos incovenientes causados à população, o que não possui gravidade suficiente para caracterizaR tais ataques cibernéticos como ataque armado. Caso fosse considerado ataque armado à época, isso poderia significar um rompimento no acordo de cessar fogo vigente. Dentro dessa situação hipotética, será conduzida a análise das medidas de precaução na condução desse ataque, de acordo com os princípios da Distinção e da Proporcionalidade, pela análise da seleção de alvo, conforme os parâmetros da definição de objetivo militar:

- Natureza – entende-se que a infraestrutura atingida por meio do Sandworm não é militar, por se trata de infraestrutura crítica de fornecimento de energia.

- Localização – a área geográfica atingida foram o oeste do país e a capital Kiev.

- Propósito – não há indício da intenção de uso futuro, à época, da infraestrutura atingida para fins militares.

- Uso – não há conhecimento do uso da infraestrutura atingida para fins militares.

Não verifica-se o enquadramento das infraestrututras atingidas pelos critério da natureza, propósito ou uso. Com relação ao critério da localização, o fato do primeiro ataque ser direcionado a capital do país poderia ser critério válido caso a Rússia tivesse a intenção de atingir o centro político do país a fim de obter uma vantagem militar numa retomada do conflito no leste da Ucrânia. Entende-se

também que a infraestrutura de energia na capital contribuiria efetivamente para o esforço militar ucraniano, na coordenação das ações numa retomada do conflito no leste do país. Nessa situação hipotética, poder-se-ia enquadrar as infraestruturas de energia atingidas como objetivo militar. Pelos efeitos avaliados na corrente análise, o ataque cibernético por meio do Sandworm teria atendido aos princípio da Distinção e da Proporcionalidade, caso esse ataque fosse qualificasdo como ataque armado – na análise em curso não foi considerado ataque armado.

Diante disso, conclui-se que, devido ao estado de conflito vigente, tal ataque cibernético foi direcionado ao cento político e outra região do país como meio de coreção sobre o estamento político e sobre a população, como forma de criar tensões internas e mantê-los sob pressão.

O mais severo ataque cibernético sobre a Ucrânia foi lançado em 2017. O NotPetya causou grande impacto na Ucrânia. Ressalta-se que no período desse ataque ainda havia um estado de conflito armado suspenso por acordo de cessar fogo, mantendo a condição para a aplicação do DICA.

- Severidade – o ataque atingiu sistemas de diversos serviços no país, em estações de trem e outros meios de transporte, pagamentos em postos de gasolina e supermercados, em sistemas de pagamentos de benefícios ou distribuição de correspondência, e também no sistema de monitoramento de radiação em Chernobyl. Porém não se conhece, até o momento, efeitos como danos, ferimentos ou mortes que possam ter sido causados. Pela abrangência dos efeitos sobre a população, considera-se que esses foram severos.

- Direcionamento – o efeito das telas pretas nos computadores dos diversos serviços impactados na Ucrânia é associado ao do NotPetya em outros ataques pelo mundo.

- Invasividade - considera-se elevado o grau de intrusão do NotPetya, pois atingiu sistemas de diversos serviços comerciais e de empresas sediados em no Estado da Ucrânia, além do sistema de monitoramento de radiação em Chernobyl.

- Caráter Militar – os ataques ocorreram durante o período de vigência do acordo de cessar fogo de 2015 (Tratado de Minsk II). Como o conflito armado estava suspenso, o ataque cibernético não esteve relacionado a uma operação militar em andamento, o que não lhe confere caráter militar.

- Envolvimento de Estado – as tensões geopolíticas entre a Rússia e a Ucrânia desde a anexação da Crimeia apontam para o vínculo da Rússia com o NotPetya.

- Urgência das Consequências do Ataque – o ataque por meio do NotPetya produziu efeitos imediatos de interrupção de diversos serviços, alguns dos quais ainda sentiam efeitos duradouros. Em 2019, os sistemas marítimo e ferroviário ainda não tinham se recuperado totalmente, bem como ainda havia pacotes de correspondência extraviados pela Ucrânia desde a queda do sistema de rastreamento, e pagamentos de aposentadorias ainda não tinham sido restabelecidos, devido ao apagamento dos registros.

- Mensuração dos Efeitos – os efeitos do NotPetya atingiram grande amplitude geográfica, além da Ucrânia. Computadores foram invadidos na *Pfizer* e na *Merck*, uma indústria farmacêutica, na empresa de navegação Maersk, na FedEx e numa fábrica de chocolates da Calbury na Tasmânia, e teria custado um bilhão de dólares à Maersk e FedEx. Considerando os efeitos imediatos e duradouros dentro e fora da Ucrânia, pode-se afirmar que a mensuração de prejuízos são da ordem de bilhões de dólares.

- Legalidade Presumida – não há proibição prevista no direito internacional, ressaltando-se que o emprego de operações cibernéticas maliciosas vale-se da zona cinzenta na legislação.

Considerando-se a análise do ataque do NotPetya, pode-se aribuir a autoria a uma das partes em conflito – Rússia. Os efeitos observados e conhecidos até o momento foram severos, por sua extensão geográfica e duração na Ucrânia, além de outros efeitos ao redor do mundo. Seria razoável afirmar que tais aspectos atribuem gravidade suficiente para caracteriza tal ataque cibernético como ataque armado. Ressalta-se que à época isso não foi interpretado como um rompimento no acordo de cessar fogo vigente. Segue-se a análise das medidas de precaução na condução desse ataque, de acordo com os princípios da Distinção e da Proporcionalidade, pela análise da seleção de alvo, conforme os parâmetros da definição de objetivo militar:

- Natureza – entende-se que os sistemas atingidos por meio do NotPetya não são militares, por se tratarem de sistemas de serviços e de empresas.

- Localização – a área geográfica atingida estendeu-se por todo o país e outras empresas pelo mundo.

- Propósito – não há indício da intenção de uso futuro de qualquer dos sistemas atingidos para fins militares.

- Uso – não há conhecimento do uso dos sistemas atingidos para fins militares.

Não verifica-se o enquadramento dos sistemas atingidos pelos critério da natureza, localização, propósito ou uso, dessa forma não havendo qualificação desses sistemas como objetivo militar. Diante disso, e considerando a qualificação anterior como ataque armado, tal ataque não atende ao princípio da Distinção, por atacar sistemas não considerados objetivo militar. Acrescenta-se à análise dois fatos decorrentes do ataque pelo NotPetya: o efeito indiscriminado causado ao redor do mundo; e o efeito sobre os computadores que monitoravam os níveis de radiação do local do acidente nuclear que ocorreu em Chernobyl. No primeiro caso, seria contrariada a regra 43 do Manual de Tallinn, de proibição da utilização de Meios e Métodos Indiscriminados. Quanto aos monitores de Chernobyl, por fazer parte de uma instalação com forças perigosas, a discussão seria em torno do princípio da proporcionalidade. Porém, não há elementos suficientes que se conheçam de que tal instalação esteve em risco de liberar tais forças em decorrência dos efeitos do ataque pelo NotPetya.

Diante do exposto, conclui-se que o ataque cibernético pelo NotPetya atingiu o nível do ataque armado, e a sua autoria apontada para uma das partes do conflito armado – Rússia - o qualifica como uso da força, apesar de não ter sido considerado, à época, um rompimento no acordo de cessar fogo (Tratado de Minsk II). Conforme exposto por Teixeira (2024, p. 698), “o ciberrespaço proporciona um tipo de coerção mais sofisticada, passível de atingir diversas expressões do poder nacional”. Dessa forma, destaca-se novamente que a zona cinzenta no direito internacional torna viável tal ataque cibernético, sem caracterizar claramente o uso da força e a retomada das hostilidades, mas como forma de manter a pressão sobre o oponente, a fim de enfraquecê-lo.

3.4 CONSIDERAÇÕES FINAIS ACERCA DOS ATAQUES CIBERNÉTICOS NA UCRÂNIA ENTRE 2013 E 2017

As ações empreendidas no processo de anexação da Crimeia incluíram o emprego de vários meios e métodos de pressão política, diplomática, econômica e

informacional, em fases anteriores ao emprego de meios militares pela Rússia, de acordo com o método de resolução de conflito interestatal concebido pelo General Valery Gerasimov. No escopo dessas ações, foram empregados ataques cibernéticos direcionados ao Estado ucraniano, em várias fases desse método de resolução de conflito. O relacionamento desses ataques cibernéticos nessas fases permite avaliar o seu enquadramento dentro de uma situação de conflito armado, o que é condição para a aplicação do DICA. Nesse sentido, a qualificação da crise da Crimeia como conflito armado internacional deveu-se à ocupação militar e anexação da península da Crimeia pelas tropas russas, que caracterizou um ato de agressão, tomando por base o entendimento de Dinstein (2004) da ocorrência da guerra no sentido material, e definições de Agressão da Assembleia Geral da ONU (1974), entendimento corroborado pelos protestos das potências ocidentais à Rússia. Da mesma forma, a crise no leste da Ucrânia entre fevereiro de 2014 e fevereiro de 2015 também foi qualificada como conflito armado internacional, em virtude do envolvimento direto de tropas russas na região realizando operações convencionais, e pelo acordos de cessar fogo entre as Partes em conflito (Tratados de Minsk I e II).

Os ataques cibernéticos relacionados para análise no perído 2013-2017 foram a Operação Armagedon (2013), a Operação Potao (BlackEnergy - 2014), os ataques cibernéticos a infraestruturas de energia (Sandworm - 2015 e 2016), e o ataque pelo NotPetya (2017). Quanto a atribuição de autoria de tais operações, as tensões geopolíticas entre a Rússia e a Ucrânia no período e os seus desdobramentos no conflito armado a partir de 2014 tornam críveis a condução de uma campanha de espionagem cibernética por meio da Operação Armagedon pela Rússia, bem como as demais operações cibernéticas citadas anteriormente, a fim de apoiar as operações cinéticas no terreno em 2014, e como forma de conduzir as pressões políticas a partir do cessar fogo de 2015. Com relação a aplicação do DICA, esse não aplica-se à Operação Armagedon, pois operações de espionagem cibernética que não tenham elemento coercitivo não violam o princípio da não intervenção, por se tratarem de mera intrusão no sistema de um Estado, de acordo com o Manual de Tallinn (2013), e também por ter sido conduzida no período anterior ao conflito armado de 2014. Para as os ataques pelo BlackEnergy, Sandworm e NotPetya, concluiu-se pela aplicação do DICA, pois tais ataques cibernéticos ocorreram no peíodo a parrtir do conflito armado entre Rússia e Ucrânia.

Na análise das medidas de precaução na condução de tais ataques, conclui-se que, no caso da operação Potao, essa atendeu aos princípios da Distinção e da Proposrcionalidade, na medida em que os seus efeitos se fizeram sentir no comando e controle ucraniano durante as ações no terreno para a tomada da Crimeia pela Rússia - o que lhe confere o caráter militar -, com danos colaterais considerados aceitáveis - *websites* governamentais ucranianos e telefonia celular foram impactados. Diferentemente, os ataques cibernéticos a infraestruturas de energia ocorridos em 2015 e 2016 não estiveram relacionados a uma operação militar em andamento, em virtude da vigência do acordo de cessar fogo já em 2015, o que não confere caráter militar a esse ataque cibernético. Acrescendo-se que a análise dos seus efeitos não os consideraram de gravidade suficiente para caracterizar tais ataques cibernéticos como ataque armado, pois limitaram-se aos inconvenientes causados à população. Já o ataque pelo NotPetya foi considerado um ataque severo devido aos efeitos abrangentes e duradouros sobre a população, e a extensão geográfica desses efeitos sobre sistemas operacionais de diversos serviços na Ucrânia e empresas ao redor do mundo, com prejuízos estimados na ordem de bilhões de dólares. Tal gravidade seria suficiente para caracterizar esse ataque cibernético como ataque armado. Acrescendo-se a ausência de enquadramento dos sistemas atingidos como objetivo militar - critérios da natureza, localização, propósito ou uso -, tal ataque não atende ao princípio da Distinção, com efeito indiscriminado causado ao redor do mundo. Apesar do resultado dessa análise, como o ataque pelo NotPetya não foi considerado um rompimento no acordo de cessar fogo vigente (Tratado de Minsk II), torna-se difícil confirmar a qualificação desse ataque como uso da força e a retomada das hostilidades.

Por fim, pode-se concluir que, dentre os ataques cibernéticos direcionados contra a Ucrânia, o ataque de junho de 2017 por meio do NotPetya teve gravidade suficiente para contrariar os princípio do DICA, particularmente a Distinção e contrariando a regra 43 do Manual de Tallinn, de proibição da utilização de Meios e Métodos Indiscriminados.

4 CONCLUSÃO

O presente estudo teve como objetivo analisar se os ataques cibernéticos realizados no contexto da anexação da Crimeia pela Rússia, entre 2013 e 2017, tiveram aderência ao Direito Internacional dos Conflitos Armados, particularmente quanto aos princípios da Distinção e da Proporcionalidade. Tal análise torna-se instigante na medida em que os ataques cibernéticos, como um novo meio e método de ataque, representam um desafio para a aplicação do ordenamento jurídico internacional. Inicialmente, muitos Estados abstêm-se em emitir posicionamento sobre o emprego ou restrição de novos meios e métodos representados por novas tecnologias, até que possam ter entendimento das vantagens que o domínio de tais tecnologias possa lhes proporcionar na condução das disputas entre Estados, como as disputas comerciais, as tensões geopolíticas em paz ou os conflitos armados. Enquanto não houver norma ou tratado reconhecido pelo Estados acerca do emprego e restrições dessas novas tecnologias, Estados poderão desenvolver capacidades em torno delas e fazer experimentações do seu uso, em testes ou emprego real. Foi nesse ambiente sem regulamentação que alguns ataques cibernéticos ficaram conhecidos no mundo, como os ataques à Estônia em 2007, que paralisaram esse país, que já possuía diversos serviços comerciais e governamentais conectados em rede. Tais ataques ocorreram num contexto de tensões políticas envolvendo esse país e a Rússia, mas não se comprovou o envolvimento estatal, seja em suporte ou coordenando as ações conduzidas por indivíduos denominados como ativistas hacker – ou hackativistas. Isso traz o grande desafio da atribuição de autoria de um ataque cibernético, que depende de análises técnicas para identificar a sua origem. A exemplo dos ataques à Estônia, Teixeira (2024) menciona que o rastreamento inicial apontou que o ataque estaria se originando de 178 países; e Dinniss (2023) descreve que alguns dos ataques de negação de serviço contra a Estônia foram atribuídos a endereços IP estatais da Rússia, mas esse país alegou que os computadores desses IP estavam comprometidos e sendo manipulados de fora da estrutura governamental. Observa-se como pode ser difícil a correta atribuição de autoria de um ataque cibernético, e de forma segura. Diante disso, o governo estoniano teria desistido de formalizar acusação contra outro Estado, embora tivesse feito acusações anteriores de que a Federação Russa estaria envolvida nesses ataques. Na apreciação de Dinniss

(2023), os Estados-membros da OTAN certamente não estavam preparados para aceitar que os ataques [cibernéticos] equivaliam a um ataque armado que daria início às disposições de autodefesa coletiva do Tratado do Atlântico Norte. Observa-se que, devido ao vácuo normativo, os Estados não estavam preparados para fazer declarações públicas definitivas sobre tais tipos de ataques como uso da força.

Para contornar esse desafio, uma iniciativa foi tomada no Centro de Excelência de Defesa Cibernética Cooperativa da OTAN, que convidou um Grupo de Especialistas Internacionais independente para conduzir um projeto de estudo sobre o problema. Tal projeto teve como propósito examinar como as normas legais existentes aplicam-se a uma nova forma de guerra, a guerra cibernética, para a qual não há disposições previstas em Tratados Internacionais. O estudo do grupo de especialistas internacionais resultou em Regras, aprovadas e publicadas em 2013 e organizadas no Manual de Tallinn 1.0. Apesar de não ter força de Tratado Internacional, representando tão somente a opinião do grupo de especialistas internacionais, e não a visão da OTAN ou dos seus países membros, o Manual de Tallinn tornou-se uma referência para as discussões acerca do assunto por parte de Estados e Organismos Internacionais. Foi a partir do previsto nas Regras do Manual de Tallinn 1.0, e da interpretação, de alguns Estados e Organismos Internacionais, e de autores, da aplicabilidade do Direito Internacional aos ataques cibernéticos, que o presente estudo realizou uma síntese das interpretações levantadas, a fim de compor um entendimento da aplicação do Direito Internacional aos ataques cibernéticos. A partir dessa síntese, foi conduzida a análise dos ataques cibernéticos realizados no contexto da anexação da Crimeia pela Rússia, entre 2013 e 2017.

Pelo entendimento adotado nesse estudo, para um operação cibernética ser qualificada como uso da força – contrariando o princípio da não intervenção do Artigo 2(4) da Carta da ONU - , tal operação deve ascender ao nível de um ataque armado – a partir daí mencionada como ataque cibernético - e ser conduzida por um Estado ou ser atribuída a esse. Dentre as situações nas quais operações cibernéticas foram consideradas como ataques armados estão: ataques cibernéticos que resultem em efeito severo porém não destrutivo, da incidência de doença e morte (a exemplo de um ataque cibernético a um sistema de purificação de água); ataques cibernéticos que resultem em consequência física, nomeadamente destruição de propriedade física, lesão ou perda de vidas; ataques cibernéticos

inseridos no contexto de um conflito armado já iniciado e que cause perda de funcionalidade de um sistema computacional.

Para a avaliação dos operações cibernéticas como ataque armado, foi adotada a metodologia do Manual de Tallinn 1.0, que utiliza fatores: Severidade; Direcionamento; Invasividade; Caráter Militar; Envolvimento de Estado; Urgência das Consequências do Ataque; Mensuração dos Efeitos; e Legalidade Presumida. A partir da qualificação como ataque armado, passa-se a analisar se o ataque cibernético atendeu aos princípios da Distinção e da Proporcionalidade, pela observância das medidas de precaução na condução das hostilidades, como a correta seleção de alvos. Para tal análise, utilizou-se a avaliação quanto ao correto enquadramento de alvos do ataque cibernético pelos parâmetros da definição de objetivo militar (natureza, localização, propósito, uso). A partir da definição dessa metodologia, obteve-se a análise dos ataques cibernéticos propostos e as conclusões desse estudo.

Os ataques cibernéticos analisados foram a Operação Armagedon (2013), a Operação Potao (BlackEnergy - 2014), os ataques cibernéticos a infraestruturas de energia da Ucrânia (Sandworm - 2015 e 2016), e o ataque pelo NotPetya (2017). Inicialmente, considerou-se a qualificação da crise da Crimeia como conflito armado internacional, devido à ocupação militar e anexação da península da Crimeia pelas tropas russas, o que caracterizou um ato de agressão, pelo entendimento da ocorrência da guerra no sentido material, e definições de Agressão da Assembleia Geral da ONU (1974), e pelos protestos das potências ocidentais à Rússia quanto à violação de soberania da Ucrânia. Da mesma forma, a crise no leste da Ucrânia entre fevereiro de 2014 e fevereiro de 2015 também foi qualificada como conflito armado internacional, em virtude do envolvimento direto de tropas russas na região realizando operações convencionais, e pelo acordos de cessar fogo entre as Partes em conflito, materializados pelos Tratados de Minsk I e II (2014 e 2015 respectivamente). Tal entendimento foi importante para enquadrar alguns dos ataques cibernéticos analisados como parte de um conflito armado.

No que se refere à atribuição de autoria de tais operações, as tensões geopolíticas entre a Rússia e a Ucrânia no período e os seus desdobramentos no conflito armado a partir de 2014 tornam críveis a condução de uma campanha de espionagem cibernética por meio da Operação Armagedon pela Rússia, bem como as demais operações cibernéticas citadas anteriormente, a fim de apoiar as

operações cinéticas no terreno em 2014, e como forma de conduzir as pressões políticas a partir do cessar fogo de 2015. Com relação a aplicação do DICA, concluiu-se que esse não aplica-se à Operação Armagedon, pois operações de espionagem cibernética que não tenham elemento coercitivo não violam o princípio da não intervenção, e também por ter sido conduzida no período anterior ao conflito armado de 2014. Para as os ataques pelo BlackEnergy, Sandworm e NotPetya, concluiu-se pela aplicação do DICA, pois tais ataques cibernéticos ocorreram no período a partir do conflito armado entre Rússia e Ucrânia.

Na análise das medidas de precaução na condução de tais ataques, conclui-se que, no caso da operação Potao, essa atendeu aos princípios da Distinção e da Proporcionalidade, na medida em que os seus efeitos se fizeram sentir no comando e controle ucraniano durante as ações no terreno para a tomada da Crimeia pela Rússia - o que lhe confere o caráter militar -, com danos colaterais considerados aceitáveis - *websites* governamentais ucranianos e telefonia celular foram impactados. Diferentemente, os ataques cibernéticos a infraestruturas de energia ocorridos em 2015 e 2016 não estiveram relacionados a uma operação militar em andamento, em virtude da vigência do acordo de cessar fogo já em 2015, o que não confere caráter militar a esse ataque cibernético. Acrescendo-se que a análise dos seus efeitos não os consideraram de gravidade suficiente para caracterizar tais ataques cibernéticos como ataque armado, pois limitaram-se aos incovenientes causados à população. Já o ataque pelo NotPetya foi considerado um ataque severo devido aos efeitos abrangentes e duradouros sobre a população, e a extensão geográfica desses efeitos sobre sistemas operacionais de diversos serviços na Ucrânia e empresas ao redor do mundo, com prejuízos estimados na ordem de bilhões de dólares. Tal gravidade seria suficiente para caracterizar esse ataque cibernético como ataque armado. Acrescendo-se a ausência de enquadramento dos sistemas atingidos como objetivo militar - critérios da natureza, localização, propósito ou uso -, tal ataque não atende ao princípio da Distinção, com efeito indiscriminado causado ao redor do mundo. Apesar do resultado dessa análise, como o ataque pelo NotPetya não foi considerado um rompimento no acordo de cessar fogo vigente (Tratado de Minsk II), torna-se difícil confirmar a qualificação desse ataque como uso da força e a retomada das hostilidades.

Por fim, pode-se concluir que, dentre os ataques cibernéticos direcionados contra a Ucrânia, o ataque de junho de 2017 por meio do NotPetya teve gravidade

suficiente para contrariar os princípio do DICA, particularmente a Distinção e contrariando a regra 43 do Manual de Tallinn, de proibição da utilização de Meios e Métodos Indiscriminados. Por outro lado, na análise dos demais ataques cibernéticos (Operação Armagedon – 2013; Operação Potao – 2014; e os ataques cibernéticos a infraestruturas de energia da Ucrânia - 2015 e 2016), não foam observados elementos que contrariem os Tratados, a Doutrina e a Jurisprudência do Direito Internacional dos Conflitos Armados.

5 REFLEXOS PARA A MARINHA DO BRASIL

O estudo de um fenômeno ainda recente, como a utilização de ataques cibernéticos em apoio à ações realizadas em diferentes níveis (estratégico ou político) contra um Estado e suas instituições, podem melhorar a compreensão sobre a forma como esses ataques se desenvolvem e na identificação dos seus efeitos sobre as estruturas do Estado e da sociedade. Tal entendimento também é importante para a segurança cibernética da Marinha do Brasil (MB), seja para manter a operacionalidade das suas capacidades, ou para proteger os seus ativos de informação, como os de Ciência e Tecnologia. Dessa forma, esse trabalho visou colaborar com a MB com uma melhor compreensão dos desafios que envolvem o emprego eficiente de ações de defesa cibernética que não incorram em conflito com o ordenamento jurídico internacional.

De acordo com a Doutrina Militar de Defesa Cibernética (MD-31-M-08), a Guerra Cibernética é empregada pelas Forças Armadas, nas ações nos níveis operacional e tático, para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Durante as ações de anexação da Crimeia pela Rússia, previamente às ações no terreno foi lançada a operação Potao, cujos efeitos se fizeram sentir no comando e controle ucraniano sobre as suas forças localizadas na península da Crimeia. Tais efeitos contribuiram para que a iniciativa das ações cinéticas estivessem do lado das tropas russas. De acordo com o MD-31-M-08, as atividades no espaço cibernético podem criar liberdade de ação para atividades em outros domínios, como o terrestre, como forma de alavancar capacidades nesses domínios, para que sejam criados efeitos únicos e, frequentemente, decisivos. Dessa forma, observa-se que a MB, como Força que pode estar operando, de forma conjunta ou singular, num teatro de operações distante dos centros decisores nos níveis político e estratégico, deve possuir resiliência cibernética diante do que a referida doutrina refere-se como insegurança latente dos sistemas computacionais. A MB, como uma Força que está se modernizando com novas plataformas de combate com mais sistemas informatizados, deve permanecer atenta para a possibilidade de ser surpreendida com base nas vulnerabilidades dos próprios sistemas de

informação. Tal ameaça, nominada “Dia-Zero” na doutrina, decorre de algo comum na atualidade, que é a descoberta de tais vulnerabilidades por algum ator (Estatal ou não Estatal), que a mantém em segredo com a possibilidade de explorá-la em ataques cibernéticos futuros. Por outro lado, caso a MB possua a capacidade de explorar uma vulnerabilidade, pela utilização de um “Dia-Zero” numa ação de guerra cibernética contra um oponente, a Força também estaria sujeita ao que a doutrina denomina de “Dilema do Atacante”. Isso significa que a manutenção de um “Dia-Zero”, como segredo, com a possibilidade de tal uso, não permite que o desenvolvedor ou fabricante tome conhecimento e disponibilize a correção da vulnerabilidade, o que pode deixar vulnerável a ataques semelhantes os próprios sistemas do atacante. Além dessa possível vulnerabilidade da própria defesa cibernética, essa questão também envolve outro risco, que é a possibilidade de produzir efeitos indiscriminados. Nesse sentido, a utilização, por parte de nossas forças, de um “Dia-Zero” que não é de conhecimento por outros atores, tem a possibilidade de gerar efeitos colaterais em sistemas fora do alvo designado, conforme observado nos efeitos ao redor do mundo no ataque pelo NotPetya em junho de 2014. Diante dessa possibilidade, a MB e o Estado brasileiro correriam risco de violar o princípio da Distinção durante uma ação de Guerra Cibernética. Dessa forma, o desenvolvimento da resiliência cibernética e o emprego eficiente das ações de defesa cibernética, conforme a nossa doutrina, devem considerar os ensinamentos obtidos do emprego de operações cibernéticas em conflitos armados pelo mundo.

REFERÊNCIAS

BBC News Brasil. **Parlamento destitui presidente da Ucrânia e convoca eleições para maio**. Disponível em: https://www.bbc.com/portuguese/noticias/2014/02/140222_presidente_deposto. Acesso em: 26 jun. 2024.

BRASIL. Ministério da Defesa. **MD31-M-08** – Doutrina de Defesa Cibernética. 1. ed. Brasília, DF, 2014.

CASALUNGA, Fernando. **Guerra Hibrida-cibernética: Uma análise do conflito Rússia-Ucrânia (2014-2015) sob a perspectiva da tecnologia da informação.** Dissertação (Pós-graduação em Ciência Política) - Universidade Federal de Pernambuco, Recife, 2020.

CARR, Jeffrey. Responsible Attribution: **A Prerequisite for Accountability**. NATO Cooperative Cyber Defence Centre of Excellence, 2014.

CICV. **Convenções de Genebra de 12 de Agosto de 1949**. Comitê Internacional da Cruz Vermelha, 1992.

CICV. **Protocolos Adicionais às Convenções de Genebra de 12 de Agosto de 1949**. Comitê Internacional da Cruz Vermelha, 1998.

CNN Brasil. **Torre de TV despenca na Ucrânia ao ser atingida por ataque russo**. Disponível em: https://www.cnnbrasil.com.br/internacional/video-torre-de-tv-despenca-na-ucrania-ao-ser-atingida-por-ataque-russo/#:~:text=Uma%20torre%20de%20televis%C3%A3o%20de,russo%20%C3%A0%20infraestrutura%20de%20televis%C3%A3o. Acesso em: 26 jul. 2024.

DINNISS, Heather. **Guerra Cibernética e as Leis da Guerra**. 1. ed. Rio de Janeiro, Biblioteca do Exército, 2023.

DISNTEIN, Yoham; DAHL, Arne. **Oslo Manual on Select Topics of the Law of Armed Conflict. Rules and Comentary**. 2020.

DISNTEIN, Yoham. **Guerra, Agressão e Legítima Defesa**. 3. ed. Barueri, SP, Manole, 2004.

DOURADO, Maria; LEITE, Alexandre; NOBRE, Fábio. Guerra Híbrida vs. Gibridnaya Voyna: os diferentes significados dos conceitos híbridos para o ocidente e a Rússia. **Revista da Escola de Guerra Naval**, Rio de Janeiro, RJ, v. 26, n. 1, p. 39-64, 2020.

Embaixada da Ucrânia no Brasil. **Declaração do Ministério das Relações Estrangeiros da Ucrânia por ocasião do 20º aniversário da assinatura do Memorando de Budapeste**. Disponível em: https://brazil.mfa.gov.ua/pt/news/2546-

zajava-mzs-z-nagodi-20-ji-richnici-pidpisannya-budapeshtsykogo-memorandumu. Acesso em: 10 jul. 2024.

Jusbrasil. **O rompimento do memorando de Budapeste sobre garantias de segurança e suas consequências**. Disponível em: https://www.jusbrasil.com.br/artigos/o-rompimento-do-memorando-de-budapeste-sobre-garantias-de-seguranca-e-suas-consequencias/1402058979**.** Acesso em: 28 jun. 2024.

Karpersky. **O que são vírus de computador e worm de computador**. Disponível em: https://www.kaspersky.com.br/resource-center/threats/computer-viruses-vs-worms. Acesso em: 13 jul. 2024.

KOFMAN, Michael; MIGACHEVA, Katya; NICHIPORUK, Brian; RADIN, Andrew; TKACHEVA, Olesya; OBERHOLTZER, Jenny. **Lessons from Russia's Operations in Crimea and Eastern Ukraine**. RAND Corporation. Santa Monica , 2017.

GERNANY, German Federal Foreign Office, German Federal Ministry of Defense. **Position Paper on the Application of International Law in Cyberspace**. 2021.

ICRC. **International Humanitarian Law and Cyber Operations durind Armed Conflicts. ICRC Position Paper.** Comitê Internacional da Cruz Vermelha, 2019.

MARRONE, Alessandro; SABATINO, Ester. **Cyber Defense in NATO Countries: Comparing Models**. Observatorio di Politica Internazionali (AIA), Italia, 2021.

MEDEIROS, Manuelle. **A Guerra Cibernética: um estudo de caso a partir da anexação da Crimeia.** 2022. 58 fl. Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) – Faculdade Damas da Instrução Cristã, Recife, 2022.

NATO. Cooperative Cyber Defence Centre of Excellence. **TALLINN MANUAL on the International Law Applicable to Cyber Warfare**. Cambridge University Press, UK, 2013.

PERLROTH, Nicole. **É Assim que me Disseram que o Mundo Acaba: hackers, mercenários e governos na disputa pelo controle cibernético global**. 1. ed. Porto Alegre, Arquipélago, 2023.

ROCHA, Marcio; FONSECA, Daniel. A Questão Cibernética e o Pensamento Realista. Revista da Escola de Guerra Naval, Rio de Janeiro, RJ, v. 25, n. 2, p. 517-543, 2019.

SCHMITT, Michael; VIHUL, Liis. **The Nature of International Law Cyber Norms**. NATO Cooperative Cyber Defence Centre of Excellence, 2014.

SCHMITT, Michael; VIHUL, Liis. **The Law of Cyber Targeting**. NATO Cooperative Cyber Defence Centre of Excellence, 2015.

TANZI, Attila (org.). **International Law and Cyberspace**. Relatório, Universidades de Bolonha, Milão e Westminster, e Unidade de Planejamento Político do Ministério das Relações Exteriores e Cooperação Internacional da Itália, 2021.

TEIXEIRA, Alexandre. **Poder, Tecnologia e Direito: a força cibernética e a disrupção nos principais paradigmas de sustentação do direito aplicável aos conflitos armados**. 1. ed. São Paulo, Dialética, 2024.

TIAGO, Filipe. **Análise da Intervenção Russa na Crimeia.** 2019. Relatório Científico Final do Trabalho de Investigação Aplicada (Mestrado Integrado em Ciências Militares) – Academia Militar, Lisboa, 2019.

United Nations. Office for Disarmament Affairs. Tratado de Não Proliferação de Armas Nucleares (TNP). Disponível em: https://disarmament.unoda.org/wmd/nuclear/npt. Acesso em: 10 jul. 2024.

USA. Department of the Navy. **OPNAVINST 3500.38C** - Universal Naval Task List. Washington, DC, 2022.

USA. Joint Chiefs Of Staff. **Joint Publication 3-12** – Cyberspace Operations. 2018.

USA. United States Army Special Operations Command. **“Little Green Men” a prime on Modern Russian Unconventional Warfare Ukraine 2013-2014**. Johns Hopkins University Apllied Physics Laboratory, North Carolina, 2015.

WEEDON, Jean. Beyond ‘Cyber War’: Russia’s Use of Strategic Cyber Espionage and Information Operations in Ukraine. **Cyber War in Perspective: Russian Aggression Against Ukraine**. NATO CCD COE, Tallinn, p. 67-78, 2015.

WHITEHEAD, David; OWENS, Kevin; GAMMEL, Dennis; SMITH, Jess. **Interrupção de Energia Induzida por Ataque Cibernético na Ucrânia: Análise e Estratégias Práticas de Mitigação.** Schweitzer Engineering Laboratories. Annual Western Protective Relay Conference, Texas, 2016.

GLOSSÁRIO

Ataque Cibernético - compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente.

Ataques de DDoS - método de ataque cibernético para impedir o funcionamento de sites depois de enviar diversas solicitações que excedem a capacidade da rede.

***Botnet* -** é uma rede dispositivos recrutados, por meio de um ataque cibernético, com capacidade de conexão em rede computacional, para utilizá-los para replicar e amplificar um ataque cibernético a um número maior de computadores. Um smartphone, uma smart TV, uma câmera de segurança conectada a uma rede, ou qualquer dispositivo que tem a capacidade de se conectar em rede, ou realizar acesso, ou fazer solicitação de acesso a essa rede, podem ser utilizados como botnet.

Dia-Zero - designação atribuída à situação na qual há uma ameaça capaz de explorar uma vulnerabilidade de segurança descoberta em sistemas computacionais e que não teve, ainda, correção disponibilizada pelo desenvolvedor ou fabricante.

Espionagem cibernética - ação cibernética usada para conduzir atividades de espionagem para roubar dados sigilosos e confidenciais ou propriedade intelectual de um indivíduo, organização ou sistema de computador do governo. O objetivo do roubo de dados geralmente é obter vantagem estratégica, econômica, política ou militar.

Exploração cibernética - consiste em ações de busca ou coleta, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter a consciência situacional do ambiente cibernético.

Guerra Cibernética - corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir

capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2.

***Malware* -** software malicioso projetado para danificar ou explorar vulnerabilidades em qualquer rede ou dispositivo programável.

Ramsonware - um tipo de *malware* utilizado para negar à vítima o acesso aos seus arquivos e exigir um resgate em troca da restauração desse acesso.

Resiliência Cibernética - capacidade de manter as infraestruturas críticas de tecnologia da informação e comunicações opera

***Spoofing* -** técnica de falsificação de endereço IP, fazendo com que um computador destinatário de um pacote de dados receba um endereço de remetente diferente daquele da real origem dos dados.

***Worm* -** métodos de ataque projetado para distribuir um *malware*. Um *worm* explora vulnerabilidades como erros de configuração de rede ou brechas de segurança no sistema operacional ou aplicativos, que permitem a intrusão nos sistemas até o computador ou sistema alvo, no qual o *malware* que está sendo transportado pelo *worm* provocará o seu efeito.