

UNIVERSIDADE FEDERAL DE MINAS GERAIS – UFMG

FACULDADE DE DIREITO

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

LUCAS MENDES DE FARIA ROSA SOARES

A LEGÍTIMA DEFESA EM FACE DAS OPERAÇÕES CIBERNÉTICAS E A NOVA
LÓGICA DA GUERRA:

CONSIDERAÇÕES À LUZ DO MANUAL DE TALLINN

BELO HORIZONTE

2022

UNIVERSIDADE FEDERAL DE MINAS GERAIS – UFMG

FACULDADE DE DIREITO

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

LUCAS MENDES DE FARIA ROSA SOARES

A LEGÍTIMA DEFESA EM FACE DAS OPERAÇÕES CIBERNÉTICAS E A NOVA
LÓGICA DA GUERRA:
CONSIDERAÇÕES À LUZ DO MANUAL DE TALLINN

Dissertação de Mestrado submetida ao Programa de Pós-Graduação em Direito da Universidade Federal de Minas Gerais **Linha 4. Estado, Razão e História**, sob a orientação da Profª. Dra. Carla Ribeiro Volpini Silva.

BELO HORIZONTE

2022

Ficha catalográfica elaborada pela bibliotecária Meire Luciane Lorena Queiroz - CRB-6/2233.

S676l Soares, Lucas Mendes de Faria Rosa
A legítima defesa em face das operações cibernéticas e a nova lógica da guerra [manuscrito]: considerações à luz do Manual de Tallinn / Lucas Mendes de Faria Rosa Soares. - 2022.
129 f.: il.

Dissertação (mestrado) - Universidade Federal de Minas Gerais, Faculdade de Direito.
Bibliografia: f. 122-129.

1. Direito internacional público - Teses. 2. Guerra de informação - Teses. 3. Cibernética - Teses. 4. Guerra (Direito internacional público) - Teses. 5. Legítima defesa - Teses. I. Silva, Carla Ribeiro Volpini.
II. Universidade Federal de Minas Gerais - Faculdade de Direito. III. Título.

CDU: 341.36



ATA DA DEFESA DA DISSERTAÇÃO DO ALUNO LUCAS MENDES DE FARIA ROSA SOARES

Realizou-se, no dia 13 de julho de 2022, às 14:00 horas, Faculdade de Direito da UFMG, da Universidade Federal de Minas Gerais, a defesa de dissertação, intitulada *A LEGÍTIMA DEFESA EM FACE DAS OPERAÇÕES CIBERNÉTICAS E A NOVA LÓGICA DA GUERRA: CONSIDERAÇÕES À LUZ DO MANUAL DE TALLINN*, apresentada por LUCAS MENDES DE FARIA ROSA SOARES, número de registro 2019652140, graduado no curso de CIENCIAS DO ESTADO, como requisito parcial para a obtenção do grau de Mestre em DIREITO, à seguinte Comissão Examinadora: Prof(a). Carla Ribeiro Volpini Silva - Orientador (UFMG), Prof(a). Jose Luiz Borges Horta (UFMG), Prof(a). Paulo Roberto Cardoso (Universidade Federal de Minas Gerais).

A Comissão considerou a dissertação:

() Aprovada, tendo obtido a nota 100.

() Reprovada

Finalizados os trabalhos, lavrei a presente ata que, lida e aprovada, vai assinada por mim e pelos membros da Comissão.
Belo Horizonte, 13 de julho de 2022.


Prof(a). Carla Ribeiro Volpini Silva (Doutora) nota 100 (cem)


Prof(a). Jose Luiz Borges Horta (Doutor) nota 100 (cem)


Prof(a). Paulo Roberto Cardoso (Doutor) nota 100 (cem)

AGRADECIMENTOS

A meus professores, em todos os níveis de minha formação, arautos do conhecimento que em todos os momentos me instigaram a chama da dúvida, os despertaram amor e paixão pelo conhecimento, pela ciência, tecnologia e inovação, as quais hoje, tenho o orgulho de servir.

A Faculdade de Direito da Universidade Federal de Minas Gerais - UFMG, por ter me proporcionado experiências acadêmicas e políticas indispensáveis a uma formação cidadã, questionadora e transformadora.

Aos meus amigos, verdadeiros refúgios em meio as inconstâncias da vida, especialmente neste triste momento que nos acomete, de uma Pandemia.

A minha família, por servir de base de formação, por ser símbolo de orgulho e honra e que neste momento busco dar continuidade a seu legado.

Aos alunos que tive o prazer de lecionar enquanto estagiário docente, despertando a paixão e o orgulho do magistério.

Aos meus Mestres intelectuais, que dispuseram de tempo, paciência, carinho e que nunca desacreditaram de minha capacidade. Na figura dos queridos professores José Luiz Borges Horta, Paulo Roberto Cardoso, Onofre Batista Alves, Antônio Gomes de Vasconcelos, Jamile, dentre tantos outros que dividiram os corredores da Vetusta Casa de Afonso Pena e suas salas.

A minha mãe, Anna Paola que com todas as adversidades da vida que lhe acometeram se impõe como figura inabalável, digna das mais altas bênçãos e virtudes, que me acompanha e me incentiva a sempre a melhorar, que nunca se abalou pelas intempéres da vida.

As minhas origens, que nunca abandonaram meu modo de ser e de agir, assumindo caráter inabalável.

A minha amiga e Orientadora de graduação e agora de Mestrado, Carla Ribeiro Volpini Silva, que me abriu portas dentro da Universidade, confiou em mim sua intelectualidade e conhecimento.

RESUMO

A presente Dissertação de Mestrado tece considerações concernentes aos limites do Direito Internacional Público no campo dos conflitos armados, considerando a aplicação das normativas internacionais em particular aquelas que delimitam os campos do Uso da Força e da Legítima Defesa tomando por base uma nova realidade da teoria da guerra e dos conflitos, não mais atrelados ao campo de batalha clássico e cinético, neste pesquisa, focalizados nas lógicas das Guerras Híbridas e das Guerras Omnidimensionais, tratando-se ainda, em particular, no uso do ciberespaço enquanto novo campo de batalha, no que, hoje, podemos denominar como *cyberwar*, *ciberguerra* (guerra cibernética) e derivados.

Ademais, a pesquisa baliza-se nos estudos realizados pelos Manuais de Tallinn, particularmente, pelo Manual de Tallinn 2.0, documento seminal à pesquisa, criados por iniciativa do Centro de Excelência de Ciberdefesa Cooperativa vinculado à OTAN, formulados por especialistas em cibersegurança de vários países e coordenado pelo professor Michael N. Schmitt. Os Manuais através de um estudo da normativa internacional, buscam um entendimento interpretativo do problema relacionado as operações cibernéticas nos campos do *jus ad bellum* e do *jus in bello*, de forma analógica às operações cinéticas e sua possível “responsabilização” em face das normativas existentes que regem estes campos.

Palavras-Chave: Guerra Cibernética; Manual de Tallinn; Guerras Híbridas; Guerras Omnidimensionais; Uso da Força e Legítima Defesa

ABSTRACT

This Master's Dissertation makes considerations concerning the limits of Public International Law in the field of armed conflicts, considering the application of international norms, in particular those that delimit the fields of Use of Force and Self Defense, based on a new reality of the theory of war and conflicts, no longer tied to the classic and kinetic battlefield, in this research, focused on the logics of Hybrid Wars and Omnidimensional Wars, dealing with, in particular, the use of cyberspace as a new battlefield, in what, today, we can denominate as *cyberwar*, and its derivatives.

In addition, the research is based on studies carried out by the Tallinn Manuals, particularly by the Tallinn Manual 2.0, seminal document to the research, created on the initiative of the Cooperative Cyber Defense Center of Excellence linked to NATO, formulated by cybersecurity experts from several countries. and coordinated by Professor Michael N. Schmitt. The Manuals, through a study of international regulations, seek an interpretive understanding of the problem related to cybernetic operations in the fields of *jus ad bellum* and *jus in bello*, in an analogous way to kinetic operations and their possible "accountability" in the face of existing regulations that govern these fields.

Key Words: Cyber Warfare; Tallinn Manual; Hybrid Wars; Omnidimensional Wars; Use of Force and Self-Defense

SUMÁRIO

INTRODUÇÃO	9
CAPÍTULO I – A GUERRA, DA CINÉTICA À CIBERNÉTICA E A NOVA NARRATIVA DAS TEORIAS DA GUERRA.....	12
1.1 – A GUERRA CINÉTICA O MILITAR NO FRONTE	16
1.2 – A GUERRA CIBERNÉTICA, O MILITAR FORA DO FRONTE.....	33
1.3 – GUERRAS HÍBRIDAS E GUERRAS OMNIDIMENSIONAIS NO CONTEXTO DE GUERRA NO CIBERESPAÇO.....	54
CAPÍTULO II – O USO DA FORÇA E A LEGÍTIMA DEFESA SOB A ÓTICA DAS OPERAÇÕES CIBERNÉTICAS.....	65
2.1 – O PROBLEMA DO LIMITE DO USO DA FORÇA NO CIBERESPAÇO	67
2.2 – O PROBLEMA DA CAPACIDADE RESPONSIVA EM MATÉRIA DE LEGÍTIMA DEFESA SOB A NOVA LÓGICA DA GUERRA	80
CAPÍTULO III – TALLINN E UM NOVO MARCO NORMATIVO	94
3.1 – O PROBLEMA DA SOBERANIA NO CIBERESPAÇO E A PROPOSTA EM TALLINN .	96
3.2 – TALLINN ENQUANTO “RULE OF ENGAGEMENT” DA GUERRA NO CIBERESPAÇO.....	108
CONSIDERAÇÕES FINAIS	119
REFERÊNCIAS	122

INTRODUÇÃO

Esta Dissertação de Mestrado intende tecer considerações acerca das limitações do Direito Internacional Público no concernente ao campo dos conflitos armados, considerando a aplicação das normativas internacionais em particular aquelas que delimitam os campos do Uso da Força e da Legítima Defesa em uma nova realidade da teoria da guerra, do conflito, em particular, no uso do ciberespaço no que, hoje, podemos denominar como *cyberwar*, *ciberguerra* e derivados.

Ademais, a pesquisa concentra-se nos estudos fundamentais presentes nos Manuais de Tallinn, criados por iniciativa do Centro de Excelência de Ciberdefesa Cooperativa vinculado à OTAN, formulados por especialistas em cibersegurança de vários países e coordenado pelo professor Michael N. Schmitt. Os Manuais buscam um entendimento do problema relacionado as ações cibernéticas nos campos do *jus ad bellum* e do *jus in bello* e sua possível “responsabilização” em face das normativas existentes que regem estes campos.

O trabalho realizado por Tallinn, apesar do esforço monumental, não representa aplicação jurídica factual, apresentando apenas aplicação analógica. É sobre esse problema chave em que se assenta o presente esforço acadêmico: um estudo do campo de batalha moderno, que faz uso dos vários campos de ação, e a limitação normativa internacional aplicável na atualidade.

Esta pesquisa assenta-se em duas grandes perguntas que estão interconectadas: a primeira, se a presente normativa internacional é suficiente em face dos novos conflitos armados e se Tallinn de fato preencheu as lacunas com seu ideário de aplicação analógica (ou se seria necessário uma nova normativa tomando Tallinn como base) e a segunda, como os novos conflitos armados podem ser tratados frente a esta nova proposta interpretativa, vez que, como apresentado pelos conceitos de guerra a serem tratados nesta pesquisa, os conflitos não mais se limitam ao campo de batalha, ao estado belicoso, muito menos a lógica cinética da guerra clássica, ou, em outras palavras, seriam as operações cibernéticas de um Estado sobre outro limitadas pelas normas internacionais vigentes? Essas ações no campo virtual seriam atos de agressão, tendo em mente a Carta das Nações Unidas e, caso sejam, quais os limites aplicáveis no concernente ao uso da força e da legítima defesa? Tallinn assenta-se sobre esses problemas (e outros), na busca por solucionar lacunas, que serão investigadas ao longo da dissertação.

A relevância deste trabalho encontra-se no aspecto da atualidade da temática, e na necessidade de adequação tanto da esfera nacional quanto da internacional à nova realidade, agora cibernética, no que tange o conflito armado. Inicialmente, o problema da guerra ou do conflito armado (de forma pertinentemente, o Direito Internacional distingue ambos) não é recente e não carece de trabalhos densos que estudem e interpretem a temática¹. Contudo, no Brasil, pouco se tem acerca do tema sob a ótica de Tallinn, menos ainda, sob o prisma analítico dos novos conflitos para além do campo de batalha física da lógica clássica da guerra cinética *per se*.

Não há que se negar que atos de agressão não se limitam ao lançamento de mísseis ou a fricções em fronteiras. O que não faltam são exemplos de ações por meios virtuais, não se restringindo somente à *world wide web* ou à internet, no intuito de influenciar eleições, limitar operações financeiras e atacar o funcionamento de infraestruturas críticas².

Nessa linha, a normativa Internacional define o entendimento de soberania, à uma ideia de limitação dos poderes (outrora *supremos*³) e competências, como o próprio exercício da soberania:

a soberania – no seu sentido original de autoridade suprema – não existe, nem pode existir, na ordem externa, porque, nela, os Estados são submetidos ao Direito Internacional, por um processo semelhante ao que submete, na ordem interna, os indivíduos às normas do direito[...]⁴.

Contudo, a nova realidade não se limita ao espaço real, físico, tangível, pelo contrário, encontramos grande parte de nossas operações em execução no espaço virtual, nossos documentos, informações, estruturas, dentre outros. Entretanto, resta compreender as limitações da teoria clássica de soberania e seu entendimento pela doutrina internacional. Francisco Suárez entende o conceito de modo que “quando não há outro que lhe seja superior, pois esta palavra significa negação de um poder superior ao qual devesse obedecer quem o

¹ A esse respeito ver: A nova ordem mundial e os conflitos armados/El nuevo orden mundial y los conflictos armados/ Coordenadores Daniel Amin Ferraz [e] Denise Hauser. Belo Horizonte: Mandamentos, 2002. BUZAN, Barry. A evolução dos estudos de segurança internacional/ Barry Buzan, Lene Hansen; tradução Flávio Lira. São Paulo: Editora Unesp, 2012. KENNEDY, Paul. Ascensão e queda das grandes potências: transformação econômica e conflito militar de 1500 a 2000/ Paul Kennedy; tradução de Waltésir Dutra, 5ª ed. Rio de Janeiro: Campus, 1991. WALZER, Michael. Guerras justas e injustas: uma argumentação moral com exemplos históricos/ Michael Walzer; tradução Waldéa Barcellos. São Paulo: Martins Fontes, 2003 e MORRIS, Ian. Guerra: o horror da guerra e seu legado para a humanidade/ Ian Morris; tradução de Luis Reyes Gil. São Paulo: LeYa, 2015.

² A esse respeito ver: MUELLER, Robert S. Report On The Investigation Into The Russian Interference In The 2016 Presidential Election. U.S. Departamento f Justice. Washington D.D. 2019. Disponível em < <https://www.justice.gov/storage/report.pdf> >. Acessado em: 10/05/2020 e UNITED STATES. Joint Chiefs of Staff. Cyberspace Operations. 2018. Disponível em: < https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf > Acessado em 10/05/2020

³ BODIN, apud BONAVIDES, Paulo. Ciência Política. 10. Ed. São Paulo: Malheiros, 2001, p. 125.

⁴ RUSSOMANO, Gilda M C, Meyer. Direito Internacional Público. 1. Vol, Rio de Janeiro: Forense, 1989, p. 104

detém”⁵. Por fim, vale citar Pereira, que resume de forma inequívoca a matéria ao comentar a citação à Suárez:

Este é, pois, o sentido lato da palavra soberania. Em sentido restrito, o termo aparece para indicar, em toda a sua plenitude, o poder do Estado moderno, que, mediante sua lógica absolutista interna, suplantou a antiga ordem medieval, cuja natureza e dinâmica assentavam-se nas duas vertentes universalistas do poder medieval, a Igreja e o Império.⁶

Vivemos em uma realidade onde o espaço digital se constitui enquanto uma nova lógica “territorial”, ele é uma extensão da própria soberania de um país, porém, essa nova realidade parece ser um problema para a teoria clássica da soberania que apresenta certa dificuldade de explicar a questão, seja em limitação seja em extensão. Essa dificuldade acaba se traduzindo enquanto oportunidade na execução de operações cibernéticas que poderiam caracterizar-se enquanto ato de agressão e violação da soberania de outro país, contudo, essa lacuna conceitual acaba por dificultar a compreensão de uma limitação.

A realidade conflituosa global em que vivemos, onde o conflito não se limita à fricção cinética, e em que a ideia de “ataque” que poderia ensejar a aplicação do direito à defesa, presente na Carta da ONU, hoje não encontra escopo de ação em medidas análogas.

O problema assenta-se na questão da limitação da teoria clássica da soberania para compreender o espaço virtual enquanto espaço soberano e em qual extensão, tendo Tallin vislumbrado essa problemática e compreendendo (e delimitando) o espaço digital enquanto espaço soberano. Por fim essas questões são trabalhadas dentro da dissertação sob a ótica de uma nova lógica da guerra, não mais somente cinética, a partir de duas grandes teorias, que demonstram que a guerra é um fenômeno cultural, digital, tecnológico e social, não mais limitado a ideia clássica de soberania e escapando a atual possibilidade de legítima defesa fundamentada pela ONU.

⁵ SUÁREZ, Francisco Apud PEREIRA, Antônio Celso Alves. Soberania e Pós-Modernidade pp. 619-662, in O Brasil e os novos desafios do direito internacional / Leonardo Nemer Caldeira Brant (coordenador). Rio de Janeiro: Forense, 2004, p. 622.

⁶ Ibidem

CAPÍTULO I – A GUERRA, DA CINÉTICA À CIBERNÉTICA E A NOVA NARRATIVA DAS TEORIAS DA GUERRA

Que o homem a muito busca a resolução de seus conflitos mediante o uso da força é inegável, passando da aplicação da força bruta em seus primórdios⁷, à sofisticação do uso da coerção psicossocial, muito bem explanada por Joseph Nye.

A este respeito, o que parece ter mudado não é necessariamente o conceito da Guerra enquanto instrumento de dominação, expansão, agressão ou imposição, mas, tão somente sua natureza, é, sob essa afirmação que parte este capítulo, uma breve análise da alteração estrutural da guerra, entendida inicialmente pelo seu fulgor do combate cinético, passando para a frieza do combate cibernético, estritamente sob a ótica daqueles que vivem o combate. Cumpre analisar o conflito sob o prisma da realidade vigente, como a guerra se configura na atualidade, será ela um confronto cinético, cibernético ou ambos?

Na mesma linha do apresentado essa aparente estabilidade no concernente à natureza, à ciência, às razões e às justificativas para se adentrar e travar um conflito sofreram alterações, tanto de caráter moral⁸ quanto normativo. Passando da criação do Comitê da Cruz Vermelha e as Convenções de Haia e Genebra bem como seus Protocolos Adicionais⁹, aos crimes julgados pelos Tribunais de Tóquio e Nuremberg¹⁰ até ao Estatuto de Roma e a criação de uma jurisdição Internacional competente para julgar aqueles responsáveis pelos Crimes de Guerra e Crimes Contra a Humanidade¹¹. Sob a ótica de Clausewitz o conflito pode ser compreendido de forma exógena, abarcando, ainda, conceitos vitais para melhor compreender a problemática moderna.

A guerra, então, é apenas um verdadeiro camaleão, que modifica um pouco a sua natureza em cada caso concreto, mas é também, como fenômeno de conjunto e relativamente às tendências que nela predominam, uma surpreendente trindade em que se encontra, antes de mais nada, a violência original de seu elemento, o ódio e a animosidade, que é preciso considerar como um cego impulso natural, depois, o jogo das probabilidades e do acaso, que fazem dela uma livre atividade da alma, e, finalmente, a sua natureza subordinada de instrumento da política por via da qual ela pertence à razão pura.¹²

Clausewitz vislumbra a guerra como um ato político, ela não deve ser compreendida como um “infortúnio”, como uma falha da diplomacia, mas como um possível desdobramento

⁷ A esse respeito ver MORRIS, Ian, Guerra O Horror da Guerra e seu Legado para a Humanidade. p. 12. 2014

⁸ WALZER, Michael. Guerras justas e injustas: uma argumentação moral com exemplos históricos. Tradução de Waldéa Barcellos. São Paulo: Martins Fontes, 2003.

⁹ CICV, Comitê Internacional da Cruz Vermelha. Disponível em: < <https://www.icrc.org/pt> >.

¹⁰ FERRO, Ana Luiza Almeida. O Tribunal de Nuremberg: precedentes, características e legado. Com exemplos de provas da acusação e ilustrações. 2. Ed. Rev. Atual. e amp. Belo Horizonte: Del Rey, 2019.

¹¹ O Tribunal Penal Internacional: Comentários ao Estatuto de Roma. Coordenadores: Sylvia Helena Steiner e Leonardo Nemer Caldeira Brant. Belo Horizonte: Konrad Adenauer Stiftung, CEDIN, Del Rey, 2016.

¹² CLAUSEWITZ, Carl Von. Da Guerra. São Paulo: Editora WMF Martins Fontes, 2010, p.30.

dela, como parte do pragmatismo e da vontade de um Estado. Evidente que a compreensão da guerra como tal não é adequada aos dias atuais.

Afirmamos, pelo contrário, que a guerra é simplesmente a continuação das relações política, com o acréscimo de outros meios. Empregamos deliberadamente a expressão “com o acréscimo de outros meios” porque queremos deixar claro também que a guerra por si só não interrompe as relações políticas nem transforma-as em algo totalmente diferente. É essencial que continue a haver estas relações, independentemente dos meios que empregue. As principais linhas ao longo das quais os acontecimentos militares evoluem, e às quais eles estão restritos, são as linhas políticas que continuam durante toda a guerra e durante a paz subsequente. Como poderia ser diferente? As relações políticas entre os povos e entre os seus governos cessam quando não são mais trocadas notas diplomáticas? Não é a guerra apenas uma outra expressão dos seus pensamentos, uma outra forma de falar ou de escrever? A sua gramática pode ser, na realidade, a sua própria, mas não a sua lógica.¹³

Porém, a necessidade de se adentrar em conflitos de forma direta e presente parece ter se tornado uma fatalidade do passado, se Clausewitz afirma ser a guerra continuidade da política, a política tem demonstrado pouca necessidade de empregar a guerra. Hoje, vemos o emprego da dissuasão como máxima da força dos Estados.

O Direito à Guerra, também conhecido como *Jus ad Bellum*, ou, ainda, de forma questionável, Doutrina da Guerra Justa¹⁴ é um termo que representa o estado em que uma nação pode declarar ou entrar em guerra ante outra nação. Para além de um estado de possibilidade política, é um ato de possibilidade jurídica, ou seja, não se limita somente a vontade de um ente de se impor frente a outro, mas demanda uma justificativa para o ato. Justificativa esta que deve ser referendada pela comunidade internacional (atualmente na figura do Conselho de Segurança ou da Assembleia das Nações Unidas).

O Capítulo VII da Carta da ONU torna clara as possibilidades de se aplicar o Direito à Guerra, sendo o principal deles o da legítima defesa como definido pelo art. 51 da Carta¹⁵. Isto é, da preservação do Estado e de sua soberania territorial, fica, porém, aberta a garantia de *Jus ad Bellum* pelo Conselho de Segurança ou pela Assembleia da ONU, se apresentadas as razões para a necessidade do conflito. Pode-se, dessa forma, compreender o *Jus ad Bellum* como o direito do uso da força, como direito, não devendo ser tratado como ato de agressão e sim como ato de resposta, ato de defesa, ato justo legitimado por princípios quais sejam:

O instituto da legítima defesa é definido, de forma geral, como o meio pelo qual alguém, “usando moderadamente dos meios necessários, repele injusta agressão atual

¹³ *Ibidem*. p.717-718.

¹⁴ A esse respeito ver: AQUINO, S.T. *Suma teológica*. II, II,q.40, a.1, ad 1, 3. p. 2000 e WALZER, Michael. *Guerras justas e injustas: uma argumentação moral com exemplos históricos*. Tradução de Waldéa Barcellos. São Paulo: Martins Fontes, 2003.

¹⁵ ONU, Organização das Nações Unidas. Carta das Nações Unidas. < <https://www.un.org/en/sections/un-charter/chapter-vii/index.html> >. Acessado em 10 de maio de 2020. Ainda sobre a legítima defesa ver: BETHLEHEM, Daniel. *Notes and Comments Principles Relevant to the Scope of a State’s Right of Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors*. U.N. 2012. Disponível em < <https://www.un.org/law/counsel/Bethlehem%20-%20Self-Defense%20Article.pdf> >. Acessado em 10/05/2020.

ou iminente, a direito seu ou de outrem.” Da definição se pode inferir algumas condições necessárias ao exercício de tal direito: 1. A existência de uma agressão atual ou iminente; 2. A necessidade do meio utilizado para se repelir a agressão; 3. A proporcionalidade da reação; 4. Um direito pessoal, ou alheio, a proteger.¹⁶

Todo Direito à Guerra precede de um ato de agressão, de violação e violência. Esse por sua vez garante ao Estado vitimado o *Casus Belli*, ou seja, o fato e a justificativa para se responder à agressão pelos meios proporcionais auferidos mediante uma agressão em resposta, ou seja, guerra. É, pois, o ato que justifica a guerra, tão antigo quanto o próprio conceito de Guerra Justa. A apresentação de um ato que justifique a guerra é complexa, primeiro pela possibilidade de fraude no próprio ato¹⁷, em contrapartida, outros atos não são derivados de fraudes, a exemplo da Guerra dos Seis dias¹⁸.

É importante ter em mente primeiro a evolução do conceito, de algo amplo e questionável, onde as razões e motivos para se declarar (ou a capacidade declaratória) guerra de forma justa e aceitável pela comunidade, para algo cada vez mais estrito e evitável. De fato, os canais diplomáticos nos dias atuais, em especial com o avanço das redes de comunicação, hoje, de caráter instantâneo garantiram preponderância nas resoluções pacíficas pelas negociações. Contudo, como termo em constante evolução, sua aplicação muitas vezes se dá de forma a garantir interesses específicos e questionáveis, à exemplo da Doutrina Bush e a noção de Guerra Preventiva na lógica de combate ao terror¹⁹.

Essa evolução não se limitou à questão doutrinária ou legal, tendo o avanço tecnológico acompanhado e servido aos propósitos bélicos. Também a ideia da cibernética e do uso dos espaços digitais não passou ao largo da aplicação militar, seja em tempos de paz ou de guerra.

Nos subcapítulos que se seguem, iremos trazer uma análise das novas doutrinas aplicadas à guerra e a posição dos Estados em relação a elas, é, pois, uma contextualização da

¹⁶ VELOSO, Ana Flávia. O Terrorismo Internacional e a Legítima Defesa no Direito Internacional: O Artigo 51 da Carta das Nações Unidas pp. 183-207. In Terrorismo e direito: os impactos do terrorismo na comunidade internacional e no Brasil/ Coordenador, Leonardo Nemer Caldeira Brant. Rio de Janeiro: Forense, 2003. p. 189.

¹⁷ Exemplo disso foi o incidente de Gleiwitz, onde, a mando de Hitler, uma estação de rádio alemã, fronteira com a Polônia foi atacada por soldados da SS vestidos de uniformes poloneses e assassinaram os funcionários do local. Na época, o Governo declarou que este havia sido um ato de agressão contra o povo Alemão, ato que justificava a guerra, anos depois tudo teria sido comprovado como um ato planejado com o intuito de garantir a Alemanha o direito de declarar guerra à Polônia. A esse respeito ver: BUTLER, Rupert. A Gestapo: a história da polícia secreta de Hitler: 1933-1939/Ruper Butler; tradução de Emanuel Mendes Rodrigues. São Paulo: Editora Escala, 2008. p. 49

¹⁸ A Guerra dos Seis Dias foi um conflito entre Israel, Egito, Síria e Jordânia, onde, após o fechamento do porto do estreito de Tirana somado ao bloqueio de mercadorias, a expulsão dos agentes de paz da UNEF e a mobilização e militarização em Sharm el-Sheikh tornaram claras suas pretensões de agressão, Israel, isolado e nesta situação vê a clara presença de *Casus belli*.

¹⁹ A este respeito ver: RECORD, Jeffrey. The Bush Doctrine and War with Iraq. 2003. BRIGAGÃO, Clóvis. O 11 de Setembro: Novas Ameaças à Paz. pp. 347-355 in Terrorismo e direito: os impactos do terrorismo na comunidade internacional e no Brasil/ Coordenador, Leonardo Nemer Caldeira Brant. Rio de Janeiro: Forense, 2003 e UNITED STATES OF AMERICA. The National Security Strategy of The United States of America. 2002.

transição que nos trouxe ao problema vigente, da desconfiguração do conceito clássico da guerra, travada entre soberanos, seja por interesses nacionais seja pela defesa de sua própria existência.

Por fim, cumpre-nos analisar um importante fator da guerra, seus atores, quem são os agentes ativos e passivos nos conflitos e sua subsequente transformação sob os prismas que buscamos analisar neste estudo, o combatente, outrora facilmente identificável por sua farda, hoje parece ter se mesclado ao cidadão comum ou, ainda, tornou-se um indivíduo sem rosto, como os muitos outros que trafegam nos canais e espaços virtuais. A guerra, antes muito bem regida e regulamentada parece querer escapar de suas amarras “civilizatórias”, esgueirando-se por novos meios e, é este o fenômeno que buscamos analisar ao longo deste capítulo, junto das novas teorias da guerra que se apresentam.

1.1 – A GUERRA CINÉTICA O MILITAR NO FRONTE

Para uma melhor compreensão do cenário em que nos encontramos, é imperioso demonstrar de onde viemos, qual o caminho percorrido pela humanidade no concernente aos conflitos armados e às guerras. Não há dúvida de que a natureza evolutiva do homem, especialmente nos campos da ciência e tecnologia tem influência direta em todas as esferas sociais, ainda nesta linha, parece-nos inegável que o conflito é característica intrínseca ao humano, a este respeito, devemos compreender o conflito em seu sentido *lato*, ou seja, não restrito somente à violência, sem, contudo, excluir a mesma enquanto *última ratio*. A violência enquanto coerção, constitui parte importante da formação das sociedades modernas²⁰.

Ademais, a natureza da guerra está diretamente ligada a aquele que a trava, ou seja, é o partícipe direto, o combatente que, em grande medida, define a natureza da guerra, as decisões podem ser tomadas e travadas pelos comandantes, generais e lideranças políticas, em grande medida, distantes dos combates “corpo a corpo”, mas a forma de se travar o combate e de se tratar o combatente, são respostas definidas por aqueles que jazem na linha de frente:

Entre soldados que escolhem lutar, restrições de várias naturezas surgem com facilidade e, por assim dizer, com naturalidade, resultantes do **respeito e reconhecimento mútuos**. As histórias de cavaleiros fidalgos são em sua maior parte histórias, mas não resta dúvida de que no final da Idade Média estava amplamente disseminado um **código militar**, que por vezes era respeitado. O código foi criado para atender aos guerreiros aristocratas, mas também refletia a noção de que eles tinham de si mesmos como pessoas de um certo tipo, **envolvidas em atividades de sua própria escolha**. (...) ²¹ (grifo nosso)

A colocação de Walzer à primeira vista parece dicotômica ao apresentado anteriormente, contudo, é preciso compreender a evolução da guerra neste contexto. É importante entender o papel do “militar” no contexto pré-estatal para o pós-estatalização da organização social. O cavaleiro feudal é não somente um líder político, como também um comandante militar e soldado, mas, o é, por livre adesão, suas regras, ou, “código militar” como o autor bem coloca, não um conjunto de costumes acordados entre seus iguais para garantir um combate “civilizado” entre “profissionais” ou, aqueles que se envolveram em atividades de sua própria volição.

Contudo, vale compreender que essa “escolha” perde espaço com o fim da fidalguia e o início da massificação militar, os conflitos de voleio²² dão lugar às artilharias e baionetas. Os

²⁰ A este respeito ver MORRIS. Ian, GUERRA O horror da guerra e seu legado para a humanidade e WALZER. Michael, guerras justas e injustas uma argumentação moral com exemplos históricos.

²¹ WALZER, Michael. Guerras justas e injustas: uma argumentação moral com exemplos históricos. p. 57. Tradução de Waldéa Barcellos. São Paulo: Martins Fontes, 2003

²² Tática militar de voleio ou tiros de voleio, enfileiramento de soldados de mosquete, em que ondas de tiros são disparadas uns contra os outros, sem a utilização de coberturas, marca das guerras napoleônicas.

mercenários, tão empregados na Europa até os idos do século XVI²³ dão lugar aos exércitos nacionais, a este respeito, trazemos a baila duas visões acerca dessa transição, a primeira sob um prisma positivo da necessidade de exércitos nacionais e outra da natureza dos exércitos mercenários profissionais.

No concernente ao primeiro, talvez não tenha havido maior defensor em seu tempo, que o próprio Nicolau Maquiavel que, em sua obra, o Príncipe (1532), afirmou:

Digo, pois, que as armas com as quais um príncipe defende o seu Estado, ou são suas próprias ou são mercenárias, ou auxiliares ou mistas. As mercenárias e as auxiliares são inúteis e perigosas e, se alguém tem o seu Estado apoiado nas tropas mercenárias, jamais estará firme e seguro, porque elas são desunidas, ambiciosas, indisciplinadas, infiéis; galhardas entre os amigos, vis entre os inimigos; não têm temor a Deus e não têm fé nos homens, e tanto se adia a ruína, quanto se transfere o assalto; na paz se é espoliado por elas, na guerra, pelos inimigos. A razão disto é que elas não têm outro amor nem outra razão que as mantenha em campo, a não ser um pouco de soldo, o qual não é suficiente para fazer com que queiram morrer por ti. Querem muito ser teus soldados enquanto não estás em guerra, mas, quando esta surge, querem fugir ou ir embora.

Para persuadir de tais coisas não me é necessária muita fadiga, eis que a atual ruína da Itália não foi causada por outro fator senão o de ter, por espaço de muitos anos, repousado sobre as armas mercenárias. Elas já fizeram algo em favor de alguns e pareciam galhardas nas lutas entre si; mas, quando surgiu o estrangeiro, mostraram-lhe o que eram. Por isso foi possível a Carlos, rei de França, tomar a Itália com o giz; e quem disse que a causa disso foram os nossos pecados, dizia a verdade, se bem que esses pecados não fossem aqueles que ele julgava, mas sim esses que eu narrei, e como eram pecados de príncipes, estes sofreram o castigo.²⁴

Não há de se negar que na visão de Maquiavel, os exércitos nacionais, vinculados ao príncipe (soberano), constituiriam a melhor forma de organização das armas, contudo, sua fala traz alguns aspectos importantes da natureza do mercenário, principalmente a sua suposta postura em combate para com seus pares, especialmente no que tange a ideia de sacrifício em nome de terceiros “... fazer com que queiram morrer por ti.”

À primeira vista, um soldado que não está disposto a morrer pela causa, não tem interesse também em eliminar ou aniquilar de igual, esta mesma causa, sendo este, um ponto que merece reflexão, a guerra ou, o combate ao mercenário é, nada mais que seu trabalho, a ele não interessa nem a sua própria morte, nem a de seus “inimigos”, isso, pois, ela acarretaria a inexistência de futuros contratos, por sua vez, o soldado estatal batalha pelos interesses primários sempre de terceiros, seja de seu “príncipe” como diria Maquiavel, seja de sua pátria, as paixões e aspirações para além do soldo, levam a ações possivelmente mais cruéis ou finalísticas, em uma lógica diferente da de seus antecessores (mercenários).

²³ A este respeito ver especialmente o artigo de SKJELVER. Danielle Mead, Landsknecht German mercenary pikeman, disponível em: < <https://www.britannica.com/topic/Landsknechte> >. acessado em 15 de março de 2021.

²⁴ MAQUIAVEL. Nicolau, O Príncipe Maquiavel ao Magnífico Lorenzo de Medici, pp. 47 – 48 LCC Publicações Eletrônicas, disponível em: < <http://www.dominionpublico.gov.br/download/texto/cv000052.pdf> >, acessado em 20 de março de 2021.

Contudo, essa lógica de paixões contaminantes no campo de batalha, dicotômicas dos códigos e ritos medievais e dos interesses pessoais dos mercenários trouxe à tona uma nova lógica de combatente, a este respeito, cumpre explicitar a visão trazida por Walzer, previamente mencionada como dicotômica à de Maquiavel:

A fidalguia, costuma-se dizer, caiu vítima da revolução democrática e da guerra revolucionária: a paixão popular sobrepujou a honra aristocrática. Isso situa o limite antes de Waterloo e Appomattox, embora não com total correção. É o sucesso da coação que torna a guerra repugnante. A democracia é um fator somente na medida em que ela aumenta a legitimidade do Estado e, daí, a eficácia de seu poder coercitivo, não por ser o povo armado uma corja sedenta de sangue, insuflada pela devoção política e empenhada na guerra total (em contraste com seus oficiais, que lutariam com comedimento se pudessem). [...] ²⁵

A alusão trazida à democracia é dispensável, como o próprio autor bem expõe, mas a massificação das forças, o combatente do fronte, não mais é o nobre cavaleiro feudal, senhor de terras, em um combate firmado pela honra e pelos rígidos pactos de sangue, tão pouco é o fidalgo mercenário, comerciante de suas armas, combatendo pelos seus ganhos pessoais com seus homens, vinculados a firmes laços de fidalguia aristocrática e contratos de serviço. Agora o combatente é um membro da população, é um ator da máquina coercitiva do Estado na mesma medida em que se constituiu enquanto agente político mundano, suscetível às paixões e aos discursos que o lançam à própria sorte nos campos de batalha e o obrigam a lutar a “qualquer custo”. Aqui, vislumbra-se algo análogo à dicotomia entre o “apolíneo e o dionisíaco”²⁶, dicotomia que, como demonstra José Luiz Borges Horta, é inteligível através da história, na própria concepção do Estado.

Uma das grandes diferenças está no detentor da capacidade de editar normas e costumes no campo de batalha, com o fim da fidalguia e da preponderância dos exércitos mercenários, os costumes e normativas militares não mais são ditados eminentemente por aqueles que jazem no fronte de batalha, o soldado nacional nada mais é do que uma peça no grande tabuleiro da estratégia militar, tendo pouca ou nenhuma volição frente a seus superiores e inimigos:

[...] Não é o que as pessoas fazem quando entram na arena do combate que transforma a guerra num “circo de carnificina”, mas, como já ressaltai, o simples fato de que elas se encontram ali. **Soldados morreram aos milhares em Verdun e no Somme simplesmente porque estavam disponíveis, a vida de cada um, por assim dizer, nacionalizada pelo Estado moderno. Lançar-se contra arame farpado e fogo de metralhadora em acessos de entusiasmo patriótico não foi escolha deles.** O sangue doeu nos seus ossos, também. **Eles, também, lutariam com comedimento se pudessem.** Seu patriotismo é, naturalmente, uma explicação parcial de sua disponibilidade. **Não se trata de que a disciplina do Estado lhes seja meramente imposta. Ela também é uma disciplina que eles aceitam, supondo que seja o que devem fazer em nome da família e do país.** No entanto, os traços comuns aos combates contemporâneos: o ódio ao inimigo, a impaciência diante de quaisquer

²⁵ WALZER, Michael. Guerras justas e injustas: uma argumentação moral com exemplos históricos. p. 58. Tradução de Waldéa Barcellos. São Paulo: Martins Fontes, 2003

²⁶ HORTA, José Luiz Borges. História do Estado de Direito. p. 22 São Paulo: Alameda, 2011.

limitações, o empenho pela vitória – esses são produtos da própria guerra, onde quer que massas de homens sejam mobilizadas para a batalha. São tanto uma contribuição da guerra moderna à política democrática quanto uma contribuição da democracia à guerra.²⁷

Aqui, mais uma vez, Walzer parece feliz ao constatar a natureza dos conflitos pós Estados-Nação, a despeito do contínuo uso do termo “democracia”, em nada a questão trazida se limita a ela, de certo, o autor tem a mesma compreensão dos combatentes sob um prisma pré-democrático, do contrário, não traria exemplos como Waterloo²⁸, Appomattox²⁹, Verdun³⁰ e Somme³¹. Aqui, nos interessa a mudança da lógica do combatente em sua evolução histórica.

Ainda nesta linha e, para uma melhor compreensão do enquadramento destes combatentes e da lógica da guerra cinética em um horizonte evolutivo, façamos uma breve análise do quadro a seguir:

Figure 1. The evolution of the concept of war over time³²

1. Phase	2. Phase	3. Phase	4. Phase	5. Phase
Wars before nation-states	Generarion Classic Wars (1648 – 1830) Top point: Napolyon Wars	war 2. Generation war All together Industry Wars (1830 – 1918) Top point: I. World War	3. Generation war Maneuver Wars (1918 – 1948) Top point: 1941 II World War	4. Generation war Unconventional Wars (from 1948 to our days especially aftermath of 11 september), Top point: US Afghanistan and Iraq Occupations.

²⁷ *Ibidem*, pp. 58 – 59.

²⁸ Aqui, como na referência de Walzer, Waterloo se refere à Batalha de Waterloo, confronto militar ocorrido de 18 de junho de 1815, nas imediações de Waterloo, no então Reino Unido dos Países Baixos, onde Napoleão, derrotado, viu seu fim e o término do seu reinado de Cem Dias.

²⁹ A campanha de Appomattox diz respeito à campanha militar travada entre 29 de março de 1865 a 9 de abril de 1865 no Estado Norte Americano da Virgínia, culminando na rendição do Exército Confederado sob o comando de Robert E. Lee para o Exército da União, sob o comando de Ulysses S. Grant, o fim da campanha marcou efetivamente o fim da Guerra de Secessão ou Guerra Civil Americana.

³⁰ A batalha de Verdun foi um dos muitos campos de batalha travados durante a Primeira Guerra Mundial na Frente Ocidental, tendo durado de 21 de fevereiro de 1916 à 18 de dezembro de 1916 entre as tropas do Império Alemão e da França, totalizando perdas entre mortos e feridos superiores a 700.000 (setecentos mil) combatentes.

³¹ A Batalha do Somme também conhecida como Ofensiva do Somme, foi uma das maiores batalhas travadas durante a Primeira Guerra Mundial, totalizando mais de 3.000.000 (três milhões) de combatentes das forças do Império Britânico, da França e do Império Alemão, datada de 1º de julho de 1916 a 18 de novembro de 1916, a ofensiva buscava dar uma vitória concisa às tropas anglo-francesas sobre as tropas Alemãs e dar fim à guerra, estima-se que a batalha deixou um legado de mais de 1.000.000 (um milhão) entre mortos e feridos.

³² LIND, W.S., NIGHTENGALE, K., SCHMITT, J. F. SUTTON, J. W. The Changing Face of War: Into the Fourth Generation, *Marine Cops Gazette*. apud KURU, Huseyin. Evolution of war and cyber-attacks in the concept of conventional warfare. p. 13. *Journal of Learning and Teaching in Digital Age*, 2018, 3(1), 12-20

Até este momento, apresentamos a lógica da guerra presente na primeira fase, as guerras precedentes à formação dos Estado-nação. As guerras de segunda fase ou primeira geração, são marcadas pelos confrontos de largos exércitos nacionais nos campos de batalha, organizados em linhas de soldados portando mosquetes, acompanhados pelos assaltos de cavalaria e pelo suporte dos canhões de artilharia, são batalhas sangrentas, marcadas pelos tiros de voleio e pela pouca mobilidade das tropas, contudo, a tecnologia começa a ser empregada em larga escala aos conflitos, são somente modificando o tipo de munição e de explosivos, como o próprio emprego em massa de armas de fogo e de canhões cada vez mais destrutivos. As disputas militares, aqui, deixam de ser somente regionalizadas e personalistas, passando a conflitos em larga escala, envolvendo vastas regiões do planeta, mobilizando milhares de homens e toneladas de materiais e equipamentos, tendo as guerras napoleônicas representado o ápice deste período.

Contudo, é a partir de 1648 (data que marca o início dessa fase) que vemos o surgimento de dois marcos relevantes para a compreensão da guerra e de sua lógica, aqui, após o fim das Guerras Religiosas que devastaram a Europa, também conhecida como Guerra dos 30 Anos, a paz estabelecida a seu término foi a responsável pelo surgimento dos Estados Nacionais modernos (como os conhecemos), munidos de soberania e territorialidade, bem como pelo surgimentos de princípios basilares ao Direito Internacional Público, especialmente aquele aplicado à lógica dos conflitos, é aqui que vemos a fecundação do princípio da não intervenção e, conseqüentemente, do Direito de resposta e, ou, da legítima defesa:

Surgido em 1648 com os tratados de Münster e Osnabruck, que consagraram a Paz de Westphalia, o Direito Internacional clássico se ocupava, sobretudo, de estabelecer normas de coexistência entre os Estados Soberanos.

A Paz de Westphalia estabeleceu os princípios que caracterizam o Estado moderno, destacando-se as normas de soberania, da igualdade jurídica entre os Estados, da territorialidade e, por consequência, de não-intervenção³³

A despeito da turbulência do período, as contribuições em matéria de Direito Internacional foram inegáveis, com o desenvolvimento e, ou, o aperfeiçoamento de teorias que continuam vigentes (resguardadas suas limitações). Dentre essas contribuições, há de se legar atenção à obra de Hugo Grotius, *De jure belli ac pacis*³⁴, publicado em 1625, aqui Grotius irá trabalhar a ideia de Guerra Justa³⁵, as limitações e extensões pelas quais um soberano poderia

³³ JUBILUT, Liliana Lyra. Os Fundamentos do Direito Internacional Contemporâneo: da Coexistência aos Valores Compartilhados. Anuário Brasileiro de Direito Internacional 1, 2006, pp 203-219 (205). Disponível em: < <https://www.corteidh.or.cr/tablas/r27213.pdf> >. Acessado em: 03 de fevereiro de 2021.

³⁴ Tradução livre: Das leis de guerra e paz

³⁵ Cumpre destacar que o termo não é cunhado por Grotius e sim trabalhado por ele tomando por base trabalhos anteriores aos próprios, valendo destaque a Santo Ambrósio em *De Officiis*, Santo Agostinho em *De Civitate Dei* e *Contra Faustum*, até o aperfeiçoamento da doutrina por Santo Tomás de Aquino, na obra *Suma Teológica*.

declarar, travar e lutar uma guerra de forma justa, a este dá-se o nome de *Jus ad Bellum* que, para ele, são justificáveis em quatro situações:

- a) Quando o objetivo seja a defesa em face de ameaça ou da iminência de uma ameaça, ou seja, em caráter de legítima defesa:

E, novamente, o que pode se opor à força, senão a força? Ulpiano observa que Cassius diz que é lícito repelir a força pela força, e é um direito aparentemente dado pela natureza repelir as armas com armas, com quem Ovídio concorda, observando que as leis nos permitem pegar em armas contra aqueles que as portam.³⁶

Ora, o excesso de retaliação não pode, mais do que o medo do perigo incerto, dar uma cor de direito à primeira agressão, o que pode ser ilustrado pelo caso de um malfeitor, que não pode ter o direito de ferir ou matar os oficiais da justiça em suas tentativas de levá-lo, insistindo como um argumento que ele temia que a punição excedesse a ofensa.

O primeiro passo, que deve ser dado pelo agressor, deve ser a oferta de indenização ao lesado, mediante arbitragem de algum Estado independente e desinteressado. E se esta mediação for rejeitada, então sua guerra assume o caráter de uma guerra justa.³⁷

- b) Com o objetivo de recuperar um bem injustamente expropriado:

Um espectador, de fato, está mal qualificado para julgar até que ponto, mesmo na guerra mais justa, a autodefesa, a obtenção de indenização ou a punição de um agressor, pode ser levada. São pontos que, em muitas ocasiões, senão na maioria, devem ser deixados à consciência e ao arbítrio dos próprios beligerantes: um modo muito preferível ao de apelar à mediação e à decisão de poderes desinteressados e neutros. Lívio deu um discurso dos aqueus ao senado, no qual eles perguntam: “como os irados dos direitos da guerra podem ser questionados com justiça ou objeto de discussão?”³⁸

- c) Para se fazer valer uma convenção ou acordo, em respeito aos tratados e ao pactuado:

[...] Daí os romanos inferiram que, embora a convenção feita com Asdrúbal, pela qual ele foi proibido de passar o Ibero, não lhes serviu de nada, pois não havia sido ratificada pelos cartagineses, ainda se os cartagineses sancionaram a conduta de Aníbal em seu ataque ao povo de Saguntum com o qual os romanos, após a celebração dessa convenção, fizeram aliança, eles devem se considerar autorizados a declarar guerra aos cartagineses por terem violado um tratado solene. Sobre o que Lívio raciocina da seguinte maneira: “Pela cláusula a favor dos aliados de ambos os lados, havia segurança suficiente para os Saguntinos. Pois não havia limitação de palavras para aqueles que eram aliados na época, nem eram de molde a excluir qualquer poder de fazer novas alianças. Mas se ambos os lados tivessem liberdade para fazer novas alianças, quem poderia pensar que seria justo privar os novos aliados daquela proteção

³⁶ GROTIUS, Hugo. On the Law of War and Peace. pp. 21 Translated from the original Latin *De Jure Belli ac Pacis* by A.C. Campbell, A.M. Batoche Books. Kitchener. 2001. Tradução livre de: “And again, what can be opposed to force, but force? Ulpian observes that Cassius says, it is lawful to repel force by force, and it is a right apparently provided by nature to repel arms with arms, with whom Ovid agrees, observing that the laws permit us to take up arms against those that bear them.”

³⁷ *Ibidem*. pp. 70. Tradução livre de: “Now the excess of retaliation cannot, any more than the fear of uncertain danger, give a colour of right to the first aggression, which may be illustrated by the case of a malefactor, who can have no right to wound or kill the officers of justice in their attempts to take him, urging as a plea that he feared the punishment would exceed the offense. The first step, which an aggressor ought to take, should be an offer of indemnity to the injured party, by the arbitration of some independent and disinterested state. And if this mediation be rejected, then his war assumes the character of a just war.”

³⁸ *Ibidem*. pp. 284 Tradução livre de: “A spectator indeed is but ill qualified to judge, how far, even in the most just war, self-defence, the attainment of indemnity, or the punishment of an aggressor, may be carried. These are points, which, on many, if not most, occasions must be left to the conscience and discretion of the belligerents themselves: a mode far preferable to that of appealing to the mediation, and decision of disinterested and neutral powers. Livy has given an address of the Achaeans to the senate, in which they ask, “how the iravailing themselves of the rights of war can ever be fairly called in question, or made a subject of discussion?””

a que teriam direito pelos tratados de amizade? A exclusão não poderia ir além de declarar que os aliados dos cartagineses não deveriam ser seduzidos a renunciar a seus compromissos, nem, se o fizessem, serem admitidos em aliança com os romanos.”³⁹

d) Para se aplicar uma punição que seja justa

Agora, como a guerra pública nunca pode ocorrer, mas onde os remédios judiciais deixam de existir, muitas vezes ela é prolongada, e o espírito de hostilidade inflamado pelo aumento contínuo de perdas e danos. Além disso, a guerra privada se estende apenas à autodefesa, enquanto os poderes soberanos têm o direito não apenas de evitar, mas de punir os erros. De onde eles estão autorizados a impedir uma agressão remota e imediata. Embora a suspeita de intenções hostis por parte de outra potência possa não justificar o início de uma guerra real, exige medidas de prevenção armada e autoriza a hostilidade indireta. Pontos, que serão discutidos em outro lugar.⁴⁰

A concepção de Grotius muito se assemelha a visão aquiniana do preceito, expandindo as possibilidades de interpretação da aplicação da teoria, visto que, para Santo Tomás de Aquino, só seria compreensível três justificativas para uma Guerra Justa sendo:

a) Ser declarada pelo poder do soberano, visto que, para o autor, somente a mais elevada autoridade teria legitimidade de declarar guerra, a guerra não deve ser movida por interesses particulares:

Primeiro, a autoridade do chefe, por cuja ordem a guerra deve ser feita. Pois, não pertence a uma pessoa privada mover a guerra, porque pode buscar o seu direito particular, no tribunal do superior. Semelhantemente, também não pertence a uma pessoa privada convocar a multidão, o que deve ser feito, nas guerras. Por onde, como o cuidado da república foi cometido aos chefes, a eles lhes pertence defender a coisa pública da cidade, do reino ou da província que lhe está submetida. Ora, eles a defendem materialmente com a espada, contra os perturbadores internos, quando punem os malfetores, segundo aquilo do Apóstolo: Não é de balde que ele traz a espada; porquanto ele é ministro de Deus, vingador em ira contra aquele que obra mal. Assim também, com a espada da guerra, pertence-lhes defender a coisa pública contra os inimigos externos. Por isso, a Escritura diz aos príncipes. Tirai ao pobre e livrai ao desvalido da mão do pecador. Donde o dizer Agostinho: A ordem natural, acomodada à paz dos mortais, exige se atribua ao príncipe a autoridade e a deliberação para empreender uma guerra.⁴¹

³⁹ Ibidem. pp. 145 – 147 Tradução livre de: “[...] Hence the Romans inferred that although the convention made with Asdrubal, by which he was prohibited from passing the Iberus, had been of no service to them, as it had not been ratified by the Carthaginians, yet if the Carthaginians sanctioned the conduct of Hannibal in his attack upon the people of Saguntum with whom the Romans, after the making of that convention, had entered into an alliance, they should consider themselves as authorised to declare war against the Carthaginians for having violated a solemn treaty. Upon which Livy reasons in the following manner, “By the clause in favour of allies on both sides, there was sufficient security for the Saguntines. For there was no limitation of the words to those, who were allies at that time, nor were they such as to exclude either power from making new alliances. But if both sides were at liberty to make new alliances, who could think it just to deprive the new allies of that protection to which they would be entitled from treaties of amity? The exclusion could reasonably go no further than to declare that the allies of the Carthaginians should not be seduced to renounce their engagements, nor if they did so, be admitted into alliance with the Romans.”

⁴⁰ Ibidem. pp. 69-70 Tradução livre de: “Now as public war can never take place, but Where judicial remedies cease to exist, it is often protracted, and the spirit of hostility inflamed by the continued accession of losses and injuries. Besides, private war extends only to self-defence, whereas sovereign powers have a right not only to avert, but to punish wrongs. From whence they are authorised to prevent a remote as well as an immediate aggression. Though the suspicion of hostile intentions, on the part of another power, may not justify the commencement of actual war, yet it calls for measures of armed prevention, and will authorise indirect hostility. Points, which will be discussed in another place.”

⁴¹ AQUINO, Santo Tomás. Suma Teológica, p. 2000. Disponível em: < <https://sumateologica.files.wordpress.com/2017/04/suma-teolc3b3gica.pdf> >. Acessado em: 19 de maio de 2021

- b) Ter uma causa ou motivação justa, em grande medida, retributiva, ou seja, que busca retificar uma injustiça:

Segundo, é necessária uma causa justa; isto é, que os atacados mereçam sê-lo, por alguma culpa. Por isso diz Agostinho: Costumam definir as guerras justas como as que vingam injúrias, quando uma nação ou uma cidade, que vai ser atacada pela guerra, ou deixou de castigar o que foi iniquamente feito pelos seus membros, ou de restituir o de que se apoderou injustamente.⁴²

- c) Ter como objetivo o bem ou evitar o mal, objetivando a realização do bem supremo e em prol de uma coletividade:

Terceiro, é necessário seja reta a intenção dos beligerantes, pelo que se entende o promoverem o bem ou evitarem o mal. Por isso diz Agostinho: Os verdadeiros adoradores de Deus consideram justas também as guerras feitas, não por cobiça ou crueldade, mas por desejo de paz, para que os maus sejam reprimidos e os bons socorridos. Pode contudo acontecer que, mesmo sendo legítima a autoridade de quem declara a guerra e justa a causa, ela venha a tornar-se ilícita por causa da intenção depravada. Pois, diz Agostinho: O desejo de danificar, a crueldade no vingar-se, o ânimo encolerizado e implacável, a fereza na revolta, a ânsia de dominar e causas semelhantes são as que, nas guerras, são condenadas pelo direito.⁴³

Aqui é importante compreender que, a despeito da temporalidade e do caráter analítico moral em que pese a análise dos autores, muito do cerne de suas preposições permanece em vigência quando vamos trabalhar a lógica da compreensão da guerra. Ambos reconhecem que compete somente ao poder soberano a capacidade de se declarar um conflito, que para que o mesmo seja declarado, é preciso que uma motivação justa exista, essa, em grande medida em razão de um direito violado ou da eminência da violação de um direito em caráter internacional e, por fim, que o objetivo seja benéfico ou que busque o bem, neste caso, em caráter coletivo, ou seja, que este bem não tenha em vistas a assunção de vantagens pessoais.

Tomando por paralelo as normas vigentes que compreendem a normativa do Direito à Guerra, veremos a presença destes mesmos fatores, limitando seu escopo de atuação, nos Arts. 39 a 51 da Carta das Nações Unidas, em particular nos Arts. 39 e 51, em que observamos a limitação da busca pelo bem comum ou evitar o mal e, a garantia de resposta a um direito violado, respectivamente:

Artigo 39: O Conselho de Segurança determinará a existência de qualquer ameaça à paz, ruptura da paz ou ato de agressão e fará recomendações, ou decidirá que medidas devem ser tomadas de acordo com os artigos 41 e 42, para manter ou restabelecer paz e segurança internacionais.

[...]

Artigo 51: Nada na presente Carta prejudicará o direito inerente à legítima defesa individual ou coletiva se ocorrer um ataque armado contra um Membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para manter a paz e a segurança internacional. As medidas tomadas pelos membros no exercício deste direito de autodefesa serão imediatamente comunicadas ao Conselho de Segurança e não afetarão de forma alguma a autoridade e responsabilidade do Conselho de Segurança sob a presente Carta de tomar a qualquer momento as medidas

⁴² *Ibidem*.

⁴³ *Ibidem*, p. 2001.

que julgar convenientes. julgar necessário para manter ou restaurar a paz e a segurança internacionais.⁴⁴

É exatamente durante esse período que Lind denomina de “Guerras Clássicas” em que essas teorias assumem sua sofisticação máxima, onde vemos a aplicação da lógica da Guerra Justa e das justificativas de guerra para a garantia de *Casus Belli*, de forma que os Estados, agora devidamente constituídos, se viam no direito legal, de defender seus interesses e suas fronteiras.

A segunda geração, denominada de Guerras Industriais foi marcada em grande medida pelos inúmeros avanços tecnológicos no campo de batalha, e neste íterim, de 1830-1918, que vemos o surgimento das metralhadoras, dos grandes encouraçados de guerra, do submarino, dos aviões, das largas malhas ferroviárias e de novas tecnologias de comunicação.

As novas armas e estratégias advindas do período também garantiram novas formas de matar e, com elas, a preocupação de que não bastava manter as velhas normativas de guerra, pouco garantidoras aos combatentes e, em grande medida, limitadas aos soberanos e suas capacidades beligerantes.

É exatamente neste contexto que surgem as primeiras normas de proteção ao combatente, nas formas da Primeira Convenção de Genebra e da Segunda Convenção de Genebra. A primeira surge através dos esforços hercúleos de Jean-Henri Dunant, conhecido como patrono do hoje conhecido Comitê Internacional da Cruz Vermelha:

Não há homem que mereça mais esta honra, pois foi você, há quarenta anos, que pôs em pé a organização internacional de socorro aos feridos no campo de batalha. Sem vocês, a Cruz Vermelha, a suprema conquista humanitária do século XIX, provavelmente nunca teria sido realizada.⁴⁵

Dunant, após breve viagem pelo norte da Itália viu nos restos do campo da Batalha de Solferino, apesar de não ter presenciado a batalha em si, Dunant pode caminhar pelos destroços e vislumbrar em primeira mão os horrores típicos das novas guerras, e do trato indiscriminado para com os combatentes. Os horrores foram tão impactantes, que pelo resto de seus dias, o

⁴⁴ ONU. Carta das Nações Unidas, Capítulo 7, 1945. Disponível em: < <https://www.un.org/en/about-us/un-charter/chapter-7> >. Acessado em: 07 de fevereiro de 2021. Tradução livre de: “Article 39: The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.[...]Article 51: Nothing in the presente Charter shall impair the inherent right of individual or collective self-defence if na armed attack occurs Against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the presente Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

⁴⁵ DUNANT, Henry. A Memory of Solferino, p. 12. International Committee of the Red Cross. Geneva 1959. Tradução livre de: “There is no man who more deserves this honour, for it was you, forty years ago, who set on foot the international organization for the relief of the wounded on the battlefield. Without you, the Red Cross, the supreme humanitarian achievement of the nineteenth century, would probably never have been undertaken.”

humanitário se dedicou pela luta dos direitos dos combatentes e feridos em guerras, tendo influenciado diretamente na construção da Convenção de Genebra:

Em 1863, quatro anos após a batalha de Solferino e um ano após a publicação do livro de Dunant, um comitê privado formado pelo general Dufour, Gustave Moynier, os médicos Théodore Maunoir e Louis Appia e o próprio Henry Dunant organizou uma conferência em Genebra, à qual 16 países enviaram seus representantes. A conferência recomendou a criação de sociedades nacionais de socorro e pediu aos governos que lhes dessem proteção e apoio. Além disso, a conferência expressou o desejo de que, em tempos de guerra, as partes beligerantes declarem os estabelecimentos de controle sanitário e os hospitais de campanha neutros, ou seja, invioláveis, que proteção semelhante seja estendida ao pessoal médico do exército, aos voluntários e aos próprios feridos e, finalmente, que os governos escolham um sinal distintivo comum marcação de pessoas e objetos a serem protegidos.

Em 1864, o Conselho Federal convocou uma Conferência Diplomática em Genebra, com a participação de plenipotenciários de 16 países; esta conferência elaborou a “Convenção de Genebra para a Melhoria da Condição dos Feridos nos Exércitos em Campo”, que foi assinada em 22 de agosto daquele ano seguinte. A Convenção formalizou as recomendações da conferência de 1863 e deu início ao princípio – crucial para todo o empreendimento – de que soldados feridos e doentes devem ser acolhidos e atendidos sem distinção de nacionalidade. Em homenagem à Suíça, o signo heráldico de uma cruz vermelha sobre fundo branco – na verdade, a bandeira suíça com as cores invertidas – foi escolhido como emblema garantindo proteção e assistência.⁴⁶

Genebra representou um marco nos direitos dos combatentes e o início de um movimento global por limitações e normatizações claras acerca do *Jus in Bello* ou seja, do Direito na Guerra, a garantia de que limitações seriam aplicadas pelos beligerantes, garantindo a amortização de perdas e danos indiscriminados à vida dos combatentes ainda na lógica da Segunda Geração. Aqui teremos ainda a adoção das Convenções de Haia de 1899 e de 1907, que limitaram, inclusive, o tipo de armamento, explosivo e dano que poderia ser implicado a um combatente.

Assim como as instituições da Cruz Vermelha mudaram ao longo dos anos de acordo com as novas necessidades, a Convenção de 1864 também foi adaptada às circunstâncias em mudança e complementada por novos instrumentos jurídicos. Em 1899, uma nova convenção “para a Adaptação à Guerra Marítima dos Princípios da Convenção de Genebra de 22 de agosto de 1864” foi assinada pelos representantes dos Estados participantes da primeira Conferência Internacional de Paz, realizada em Haia. A Convenção de Genebra de 1864 foi revisada em 1906 e, pela primeira vez, as

⁴⁶ *Ibidem*. pp. 129 - 130. Tradução livre de: “In 1863, four years after the battle of Solferino and a year after Dunant’s book was published, a private Committee consisting of General Dufour, Gustave Moynier, physicians Théodore Maunoir and Louis Appia, and Henry Dunant himself, organized a conference in Geneva, to which 16 countries sent their representatives. The conference recommended that national relief societies be set up, and asked the governments to give them their protection and support. In addition, the conference expressed the wish that in wartime belligerent parties declare lazarets and field hospitals neutral, i.e. inviolate, that similar protection be extended to army medical staff, voluntary helpers and the wounded themselves, and finally that the governments choose a common distinctive sign marking persons and objects to be protected.

In 1864, the Federal Council convened a Diplomatic Conference in Geneva, with plenipotentiaries from 16 countries taking part; this conference drew up the “Geneva Convention for the Amelioration of the Condition of the Wounded in Armies in the Field”, which was signed on 22 August of that year that followed. The Convention formalized the recommendations of the 1863 conference and started the principle – crucial for the whole undertaking – that wounded and sick soldiers must be taken in and cared for without distinction of nationality. As a tribute to Switzerland, the heraldic sign of a red cross on a white ground – in effect, the Swiss flag with colours reversed – was chosen as the emblem guaranteeing protection and assistance.”

sociedades voluntárias de socorro foram mencionadas nela. A segunda Conferência de Paz (Haia, 1907) adotou os “regulamentos relativos às leis e costumes da guerra em terra” que proíbem meios de travar a guerra que causam sofrimento cruel e desnecessário e estipulam o tratamento humano dos prisioneiros de guerra e a observância de certos direitos fundamentais dos habitantes dos territórios ocupados. Em 1929, uma Conferência Diplomática convocada pelo Conselho Federal comprometeu-se a revisar a Convenção de Genebra de 1906 e adotou a “Convenção de Genebra Relativa ao Tratamento dos Prisioneiros de Guerra”, que acrescentou e detalhou as regras contidas nos regulamentos de Haia sobre a guerra em terra, levando em conta a experiência da Primeira Guerra Mundial.⁴⁷

O fim da segunda geração possui como marco o fim de um dos conflitos mais sangrentos da humanidade, a Primeira Guerra Mundial, conflito que viu mudanças significativas nos regramentos de guerra, como mencionado anteriormente, desde as questões relativas às batalhas marítimas, especialmente no emprego de submarinos, bem como nos direitos dos prisioneiros de guerra.

A terceira geração da guerra compreendida pelos anos de 1918 – 1945, a despeito do seu curto espaço de tempo pode ser considerada a geração mais sangrenta dentre as propostas, seu período histórico definidor é, sem sombra de dúvidas, a Segunda Guerra Mundial, aqui, observamos igualmente a mudança de uma chave, que caminhará até os dias atuais, sendo a linha tênue constantemente tencionada pelos conflitos contemporâneos, especialmente aqueles que compreendemos como cibernéticos.

A despeito da inserção do civil enquanto objetivo de guerra, a Segunda Guerra também representa o ápice do conflito cinético, apesar de a Guerra de Trincheira, marca da Primeira Grande Guerra, soar melhor à lógica cinética, é a guerra de mobilidade que melhor a representa. Aqui, a palavra de ordem é mobilização, as tropas estão em constante movimento, as máquinas de guerra são velozes e estratégicas, as divisões trabalham em conjunto em uma unidade de

⁴⁷ *Ibidem*, pp. 134 – 135. Tradução livre de: “Just as the Red Cross institutions have changed over the Years in accordance with new needs, the 1864 Convention has also been adapted to changing circumstances and supplemented by new legal instruments. In 1899, a new convention “for the Adaptation to Maritime Warfare of the Principles of the Geneva Convention of August 22 1864” was signed by the representatives of the States taking part in the first International Peace Conference, held at The Hague. The 1864 Geneva Convention was revised in 1906, and for the first time voluntary relief societies were mentioned in it. The second Peace Conference (The Hague, 1907) adopted the “regulations concerning the laws and customs of war on land” which prohibit means of waging war which cause cruel and unnecessary suffering, and stipulate humane treatment of prisoners of war and the observance of certain fundamental rights of inhabitants of occupied territories. In 1929, a Diplomatic Conference convened by the Federal Council undertook to revise the 1906 Geneva Convention and adopted the “Geneva Convention Relative to the Treatment of Prisoners of War”, which added to and set out in greater detail the rules contained in the regulations of The Hague on war on land, taking into account experience of World War I.”

terra, água e ar, a “*Sitzkrieg*”⁴⁸ da lugar a *Bewegungskrieg*⁴⁹. A ideia é de que a mobilidade por si, permitiria a captura de pontos estratégicos de abastecimento do inimigo, conjuntamente ao passo que o avanço combinado pelo fechamento de bolsões de unidades inimigas garantiria a rendição e a destruição da moral⁵⁰, sem a necessidade de utilização massiva de equipamentos.

Se a trincheira, os grandes encouraçados, zepelim e os canhões de proporções gigantescas marcaram a Primeira Guerra em perspectiva de armamento, a Segunda Guerra foi representada pelo sonar, pela comunicação, pelos avanços tecnológicos no campo da aeronáutica (incluindo o desenvolvimento dos mísseis⁵¹) e, especialmente, pelo tanque de guerra:

Neste ano de 1929, convenci-me de que os tanques trabalhando sozinhos ou em conjunto com a infantaria nunca poderiam alcançar importância decisiva. Meus estudos históricos, os exercícios realizados na Inglaterra e nossa própria experiência com maquetes me convenceram de que os tanques nunca seriam capazes de produzir todo o seu efeito até que as outras armas, em cujo apoio eles deveriam inevitavelmente confiar, fossem levadas ao seu padrão. de velocidade e de desempenho pelo país. Nessa formação de todas as armas, os tanques devem desempenhar papel primordial, sendo as demais armas subordinadas às exigências da blindagem. Seria errado incluir tanques nas divisões de infantaria; o que era necessário eram divisões blindadas que incluíssem todas as armas de apoio necessárias para permitir que os tanques lutassem com pleno efeito.⁵²

É em face dos horrores perpetrados e da necessidade de limitar a aplicação dos armamentos empregados, que mais uma vez as Convenções são readequadas, dessa vez, por compreender que para além do sofrimento do combatente, o civil é, em *última ratio* uma vítima e um combatente em potencial, que os plenipotenciários discutem a aplicabilidade da normativa

⁴⁸ Termo alemão para “Guerra de Mentira”, em tradução literal significa “Guerra Sentada”, termo adotado pelos soldados alemães sediados na fronteira franco-germânica em 1939, antes do início das mobilizações alemãs, para ambos os lados, durante um período, as tropas mesmo que em guerra ficaram paradas, sem demonstrar qualquer ato de agressão, o termo foi utilizado também em referência analógica à Primeira Guerra Mundial, quando, em determinado período do conflito, as tropas muitas vezes ficavam mais tempo estáticas que em combate, a despeito de estarem nas linhas de frente.

⁴⁹ Termo alemão para “Guerra de Movimento”, conhecida por jornalistas e pesquisadores como Blitz Krieg, contudo, o real termo empregado pela escola militar alemã e pelos estrategistas à época fora de *Bewegungskrieg* ou, guerra de movimento, a este respeito ver: FRIESER, Karl-Heiz. *The Blitzkrieg Legend: The 1940 Campaign in the West* [Blitzkrieg-legende: der westfeldzug 1940] translation. J. T. Greenwood. Annapolis: Naval Institute Press.

⁵⁰ A este respeito ver: CLARK, Alan. *Barbarossa: The Russian-German Conflict, 1941-45*. New York: Quill. 1965; TOOZE, Adam. *The Wages of Destruction: The Making and Breaking of the Nazi Economy*, London: Allen Lane. 2006; GLANTZ, David. *Operation Barbarossa: Hitler’s Invasion of Russia 1941*. Stroud, Gloucestershire, UK: The History Press. 2012; WALZER, Michael. *Guerras justas e injustas: uma argumentação moral com exemplos históricos*. Tradução de Waldéa Barcellos. São Paulo: Martins Fontes, 2003 e MORRIS. Ian, *Guerra: o horror da guerra e seu legado para a humanidade*; tradução Luis Reyes Gil. São Paulo: LeYa, 2015.

⁵¹ A este respeito ver: NEUFELD, Michael J. *The Rocket and the Reich: Peenemünde and the Coming of the Ballistic Missile Era*. New York: The Free Press. 1995.

⁵² GUDERIAN, Heinz. *Panzer Leader*. New York: Da Capo Press. 2001. Tradução livre de: “In this year, 1929, I became convinced that tanks working on their own or in conjunction with infantry could never achieve decisive importance. My historical studies, the exercises carried out in England and our own experience with mock-ups had persuaded me that the tanks would never be able to produce their full effect until the other weapons on whose support they must inevitably rely were brought up to their standard of speed and of cross-country performance. In such formation of all arms, the tanks must play primary role, the other weapons being subordinated to the requirements of the armour. It would be wrong to include tanks in infantry divisions; what was needed were armoured divisions which would include all the supporting arms needed to allow the tanks to fight with full effect.”

aos civis e aos combatentes eventuais, como *Partizans* e grupos de resistência, garantindo nestes casos resguardo ao respectivos grupos e à aqueles que venham a combater-los:

Em 1949 outra Conferência Diplomática, também convocada pelo governo suíço, procedeu a uma ampla revisão da Lei de Genebra já em vigor e acrescentou um novo instrumento legal, a “Convenção de Genebra relativa à proteção de pessoas civis em tempos de guerra”. Esta Convenção refere-se novamente à regulamentação da Haia sobre a guerra em terra, mas abrange também alguns novos fundamentos, como a proteção dos hospitais civis e dos transportes médicos civis, a criação de hospitais e zonas de segurança, o estatuto jurídico dos estrangeiros em o território de uma parte em conflito, e o tratamento de internados civis e populações de territórios ocupados. [...]

As Convenções de Genebra de 1949 foram complementadas em 1977 por dois Protocolos Adicionais, adotados pela Conferência Diplomática sobre a Reafirmação e Desenvolvimento do Direito Internacional Humanitário Aplicável em Conflitos Armados, que se reunia em Genebra desde 1974 a convite do Conselho Federal. O Protocolo I trata dos conflitos armados internacionais e o Protocolo II dos conflitos armados não internacionais. Eles contêm 130 artigos ao todo, que incluem – além de disposições sobre proteção e assistência aos feridos, presos e doentes – regras relativas à condução da guerra, visando principalmente evitar sofrimentos desnecessários e dar à população civil maior proteção contra os efeitos da guerra. [...] ⁵³

Por fim chegamos ao que Lind, Nightengale, Schmitt e Sutton denominaram como Guerra de Quarta Geração. Aqui nos ateremos somente à análise do desenvolvimento do período e da concepção cinética concernente à guerra, vez que, a quarta geração constitui linha limítrofe entre a guerra cinética e a cibernética, é aqui em que as palavras de Clausewitz mais ganham corpo “A guerra, então, é apenas um verdadeiro camaleão, que modifica um pouco a sua natureza em cada caso concreto”⁵⁴. Para tanto, vale trazer a definição dos autores acerca da temática:

Em termos gerais, a guerra de quarta geração parece ser amplamente dispersa e amplamente indefinida; a distinção entre guerra e paz será borrada a ponto de não ter campos de batalha ou frentes definíveis. A distinção entre “civil” e “militar” pode desaparecer. As ações ocorrerão simultaneamente em toda a profundidade dos participantes, incluindo sua sociedade como entidade cultural, não apenas física. As principais instalações militares, como aeródromos, locais fixos de comunicação e grandes quartéis-generais, tornar-se-ão raridades devido à sua vulnerabilidade; o mesmo pode ser verdade para equivalentes civis, como sedes do governo, usinas de energia e locais industriais (incluindo conhecimento, bem como indústrias

⁵³ DUNANT, Henry. *A Memory of Solferino*, pp. 135 - 136. International Committee of the Red Cross. Geneva 1959. Tradução livre de: “In 1949 another Diplomatic Conference, also convened by the Swiss government, undertook an extensive revision of the Law of Geneva already in force and added a new legal instrument, the “Geneva Convention Relative to the Protection of Civilian Persons in Time of War”. This Convention again relates to the regulation of the Hague on war on land, but it also covers some new grounds, such as the protection of civilian hospitals and civilian medical transports, the setting-up of hospital and safety zones, legal status of foreigners on the territory of a party to a conflict, and the treatment of civilian internees and populations of occupied territories.[...] The 1949 Geneva Conventions were supplemented in 1977 by two Additional Protocols, adopted by the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, which had been meeting in Geneva since 1974 on invitation by the Federal Council. Protocol I deals with international armed conflicts, and Protocol II with non-international armed conflicts. They contain 130 articles in all, which include – besides provisions on giving protection and assistance to the wounded, prisoners and the sick – rules relative to the conduct of war, aimed primarily at avoiding unnecessary suffering, and giving to the civilian population greater protection from the effects of war.[...]”

⁵⁴ CLAUSEWITZ, Karl von. *Loc. cit.* p. 30

manufatureiras). O sucesso dependerá muito da eficácia nas operações conjuntas, pois as linhas entre responsabilidade e missão se tornam muito tênues. Novamente, todos esses elementos estão presentes na guerra de terceira geração; quarta geração irá apenas acentuá-los.⁵⁵

Aqui duas questões merecem destaque nesta definição, a primeira é o caráter de continuidade das características presentes na terceira geração, com um incremento às mesmas, ou seja, a indistinção entre civis e militares, a pluralidade dos campos de batalha, não mais limitados ao fronte e a redução dos contingentes operacionais, se comunicação era a palavra de ordem e mobilidade a doutrina da terceira geração, aqui, comunicação é a doutrina e informação a palavra de ordem.

As bombas nucleares lançadas em 1945⁵⁶ representaram a mudança de chave na compreensão de como guerras seriam travadas, o medo do inverno nuclear e a corrida armamentista trouxe à tona a Guerra Fria, um conflito marcado pela lógica da dissuasão, em um mundo que se encontrava em um constante estado de “guerra pacífica”, aqui, vimos o surgimento dos conflitos periféricos, as desestabilizações regionais e, conseqüentemente, o fenômeno do terrorismo⁵⁷, bem como as guerras de *proxy*:

No novo ambiente de segurança global, o desejo dos Estados-nação de diminuir os problemas por meios indiretos, em vez das guerras convencionais, que agora custam caro para resolver questões políticas, levou ao nascimento do conceito de "guerras por procuração". O melhor exemplo das “guerras por procuração” são as relações EUA-Irã. O general Mohammed Caferi, do Exército da Guarda Republicana, afirma que "se há aqueles que pensam que os Estados Unidos resolverão seus problemas no Iraque, Afeganistão e Israel e depois se voltarão para o Irã, eles podem estar errados. Porque

⁵⁵ LIND, William S; NIGHTENGALE, Keith; SCHMITT, John F.; SUTTON, Joseph W.; WILSON, Gary I. The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette. pp. 23-24. Oct. 1989; 73, 10. Tradução livre de: “In broad term, fourth Generation warfare seems likely to be widely dispersed and largely undefined; the distinction between war and peace will be blurred to the point of having no definable battlefields or fronts. The distinction between “civilian” and “military” may disappear. Actions will occur concurrently throughout all participants depth, including their society as a cultural, not just a physical, entity. Major military facilities, such as airfields, fixed communications sites, and large headquarters will become rarities because of their vulnerability; the same may be true of civilian equivalents, such as seats of government, power plants, and industrial sites (including knowledge as well as manufacturing industries). Success will depend heavily on effectiveness in joint operations as lines between responsibility and mission become very blurred. Again, all these elements are present in third Generation warfare; fourth generation will merely accentuate them.”

⁵⁶ Corresponde ao lançamento das únicas duas bombas nucleares contra outra nação, pelos Estados Unidos da América contra o Império do Japão, resultando em definitivo no fim da Segunda Guerra Mundial. Em 06 de agosto de 1945, foi lançado sob a cidade de Hiroshima a bomba conhecida como Little Boy, resultando na devastação da cidade e na morte e ferimento de 66.000 (sessenta e seis mil) e 69.000 (sessenta e nove mil) japoneses respectivamente. Em 09 de agosto de 1945, os Estados Unidos lançaram sob Nagasaki o segundo e último artefato nuclear, a Fat Man, aniquilando a cidade e resultando na fatalidade de 40.000 (quarenta mil) japoneses no primeiro impacto e mais 80.000 (oitenta mil) em decorrência de problemas ligados à radiação. A respeito do tema ver: The Atomic Bombings of Hiroshima and Nagasaki, by The Manhattan Engineer District, June 29, 1946. Disponível em: < <https://www.gutenberg.org/cache/epub/685/pg685.html> >. Acessado em: 20 de fevereiro de 2021.

⁵⁷ Aqui vale destacar que o terrorismo não surgiu com o fim da segunda guerra, sendo um fenômeno presente ao longo da história, contudo, o terrorismo em escala global, enquanto uma ameaça real ao “mundo civilizado” é um fenômeno típico do fim do século XX e do século XXI, a este respeito ver: LARA, Antônio de Sousa, O Terrorismo e a ideologia do ocidente. Edições Almedina, SA. Coimbra. 2007; A nova ordem mundial e os conflitos armados/El nuevo orden mundial y los conflictos armados/Coordenadores Daniel Amin Ferraz e Denise Hauser. Belo Horizonte: Mandamentos, 2002 e BUZAN, Barry. A evolução dos estudos de segurança internacional; tradução Flávio Lira. São Paulo: Ed. Unesp, 2012.

o Irã nunca permitirá que os EUA terminem seu trabalho no Iraque, Afeganistão e Israel” (Kazemzadeh, 2007). Nesse caso, as táticas iranianas são determinar as estratégias que permitirão aos EUA consumir recursos de guerra e vontades de combate nas ruas de Bagdá e Líbano, e nas montanhas do Afeganistão. De fato, muitas vezes é mencionado que o Irã está por trás da vitória esmagadora do Hezbollah contra Israel na Guerra do Líbano de 2006 (Cordesman, 2006).⁵⁸

Hoje é difícil de se distinguir um conflito regular de uma insurreição, uma revolução, um atentado ou um ataque cibernético, são esses fenômenos guerras? São conflitos “armados”? onde podemos enquadrá-los? A guerra hoje está presente enquanto um *continuum*, a vitória está no convencimento da população muito mais que na destruição de um alvo estratégico, está na disrupção de um satélite e de um serviço muito mais que no empunhar de armas. A guerra cinética pode não ter acabado, mas, sem sombra de dúvida o seu elevado custo financeiro e moral deu lugar a uma nova forma de se guerrear, mais palatável, econômica e convincente, a nova lógica de “conquistar mentes e corações” foi muito bem interpretada pelo General David Petraeus, na guerra do Afeganistão:

A orientação reconhece que o terreno decisivo no Afeganistão é o que os militares chamam de "terreno humano" - a população de onde as operações de contrainsurgência estão ocorrendo.

"As pessoas são o centro de gravidade", escreveu Petraeus na orientação divulgada ontem. Separar o Talibã e outros grupos inimigos do povo e protegê-los de ameaças é o caminho a seguir, disse ele.

[...]

A orientação também diz que tomar território e depois deixá-lo não vencerá a batalha. A coalizão e as forças afegãs devem tomar e manter uma área para permitir que organizações governamentais internacionais e afegãs estabilizem a área. Empregos e um bom governo vencerão a batalha a longo prazo, escreveu o general, e os militares e civis devem pensar a longo prazo.

O dinheiro é munição em uma contrainsurgência, observa o guia. E assim como o fogo direcionado é mais eficaz do que as rodadas de pulverização, também é investir nos lugares certos com as pessoas certas, disse Petraeus.⁵⁹

⁵⁸ KURU, Huseyin. Evolution of war and cyber-attacks in the concept of conventional warfare. p. 14. Journal of Learning and Teaching in Digital Age, 2018, 3(1), 12-20. Tradução livre de: “In the new global security environment, nation-states’ desire to wear down the woe by means of indirect ways rather than the conventional wars which are now costly to settle political issues, has led concept of "proxy wars" born. The best example of the “proxy wars” is the US-Iran relations. General Mohammed Caferi of the Republican Guard Guards Army claims that "If there are those who think that the United States will solve his problems in Iraq, Afghanistan and Israel and then turn to Iran, they might be wrong. Because Iran will never allow the US to end its work in Iraq, Afghanistan and Israel”(Kazemzadeh, 2007). In that case, the Iranian tactics are to determine the strategies that will enable the US to consume war resources and fighting wills in the streets of Baghdad and Lebanon and on the mountains of Afghanistan. Indeed, it is often mentioned that Iran is behind the overwhelming victory of Hezbollah against Israel in the 2006 Lebanon War (Cordesman, 2006).”

⁵⁹ GARAMONE, Jim. Petraeus puts protecting people at strategy’s center. U.S. Army, American Forces Press Service. August 03, 2010. Disponível em: < https://www.army.mil/article/43205/petraeus_puts_protecting_people_at_strategys_center > Acessado em: 04 de fevereiro de 2021. Tradução livre de: “The guidance recognizes that the decisive terrain in Afghanistan is what the military calls the the "human terrain" - the population where counterinsurgency operations are taking place. "The people are the center of gravity," Petraeus wrote in the guidance issued yesterday. Separating the Taliban and other enemy groups from the people and protecting them from threats is the way forward, he said.[...] The guidance also says that taking territory and then leaving it will not win the battle. Coalition and Afghan forces must take and hold an area to allow international and Afghan government organizations to stabilize the area. Jobs and good government will win the battle in the long run, the general wrote, and servicemembers and civilians must think in

Talvez o mais importante para compreendermos a transfiguração da cinética para a cibernética em relação ao conflito é, sobretudo, na lógica da mudança do combatente e, conseqüentemente do combatido. Na guerra cinética o combatente é um indivíduo facilmente identificável, as próprias normas internacionais obrigam que o seja:

ARTIGO 13: A presente Convenção aplicar-se-á aos feridos e enfermos que se incluam nas seguintes categorias: 1) os membros das forças armadas de uma Parte em luta, da mesma forma que os membros das milícias e corpos de voluntários que façam parte dessas forças armadas; 2) os membros de outras milícias e de outros corpos voluntários, inclusive os de movimentos de resistência organizados, pertencentes a uma das Partes em luta e que atuam fora ou no interior de seu próprio território, mesmo que êsse território se ache ocupado, contanto que essas milícias ou corpos de voluntários, inclusive os movimentos de resistência organizados, preencham as seguintes condições: [...]

b) ter um emblema distintivo fixo e reconhecível a distância;⁶⁰

ARTIGO 13: A presente Convenção aplicar-se-á aos náufragos, feridos e doentes no mar, pertencentes às categorias seguintes: 1) Os membros das forças armadas de uma Parte no conflito, bem como os membros das milícias e dos corpos de voluntários que façam parte dessas forças armadas; 2) Os membros das outras milícias e dos outros corpos de voluntários, incluindo os dos movimentos de resistência organizados, que pertençam a uma Parte no conflito e atuem fora do seu próprio território, mesmo que este território esteja ocupado, contanto que essas milícias ou corpos de voluntários, incluindo esses movimentos de resistências organizados, satisfaçam às seguintes condições:[...]⁶¹

b) Possuírem um sinal distintivo fixo e susceptível de ser reconhecido a distância;

ARTIGO 4º A. São prisioneiros de guerra, no sentido da presente Convenção, as pessoas que, pertencendo a uma das categorias seguintes, tenham caído em poder do inimigo: 1) Os membros das forças armadas de uma Parte no conflito, assim como os membros das milícias e dos corpos de voluntários que façam parte destas forças armadas; 2) Os membros das outras milícias e dos outros corpos de voluntários, incluindo os dos outros corpos de voluntários, incluindo os dos movimentos de resistência organizados, pertencentes a uma Parte no conflito operando fora ou no interior do seu próprio território, mesmo se este território estiver ocupado, desde que estas milícias ou corpos voluntários, incluindo os dos movimentos de resistência organizados, satisfaçam as seguintes condições:[...]

b) Ter um sinal distinto fixo que se reconheça à distância;⁶²

Já na nova realidade, o combatente pode ser um militar tradicional, fardado e municiado, como pode muito bem ser um insurgente, descaracterizado entre a população ou, ainda, um jovem sem rosto atrás de um teclado. Ademais, o alvo não necessariamente precisa ser uma base militar ou um grande hangar de aviões, pode ser o coração financeiro de uma nação⁶³, ou ao sistema político institucional de um país⁶⁴, os objetivos se mantiveram em certa escala, as táticas não e, no cerne delas está a informática.

Aqui, não pretendemos afirmar que a guerra cinética terminou, muito pelo contrário, a virada do século não viu o desemprego das armas, pelo contrário, tivemos um período

the long run. Money is ammunition in a counterinsurgency, the guidance notes. And just as aimed fire is more effective than spraying rounds, so too is investing in the right places with the right people, Petraeus said.

⁶⁰ Convenção de Genebra I.

⁶¹ Convenção de Genebra II.

⁶² Convenção de Genebra III.

⁶³ A exemplo do atentado ao World Trade Center.

⁶⁴ A exemplo das primaveras coloridas, que viram a derrubada de vários governos no oriente médio.

conturbado de insurreições e guerras civis eclodindo em muitas partes do mundo, contudo, o fenômeno digital em matéria disruptiva tem assumido o frontispício do problema. Podemos, em grande medida, dimensionar, punir e encontrar os combatentes regulares que extrapolam qualquer normativa internacional, bem como seus Estados e lideranças. Contudo, o mesmo não pode ser dito das operações no ciberespaço.

1.2 – A GUERRA CIBERNÉTICA, O MILITAR FORA DO FRONTE

Representada originalmente pelo termo *cyberwarfare*, do inglês, a guerra cibernética, *lato sensu*, é um conceito que engloba quaisquer ações cibernéticas nocivas tomadas por um ou contra um Estado⁶⁵. Podemos compreender à luz da teoria de Clausewitz, ciberguerra como um ato de violência conduzida por, ou que tem como alvo, a tecnologia da informação e comunicação visando compelir seu oponente a seguir sua vontade.⁶⁶

A guerra cibernética deve ser percebida com cautela, primeiro, pela dificuldade técnica de seu combate e asserção, segundo, pelos alvos e objetivos. Esse último, em grande medida, concentra-se nas funcionalidades estatais, contudo, essas mesmas funcionalidades estão intrinsecamente ligadas às necessidades básicas da população civil, pelo que denominam-se infraestruturas críticas, ou seja, redes elétricas, de gás, de água, telecomunicações, transportes, serviços financeiros, de saúde, etc⁶⁷. A problemática está em se definir e comprovar que tal ataque partiu de um Estado ou fez uso da infraestrutura de rede de um Estado com o conhecimento e, ou consentimento desse.

Outro grave problema está ligado a questão da função do Estado dentro da rede e em resguardar esses serviços. Importa ressaltar que na atualidade, grande parte desses serviços, apesar de interesse público, estão concentradas em instituições privadas, que devem resguardar seus sistemas internos por conta própria. Dessa forma, a despeito de se tratar de questões estatais, um ataque a essa infraestrutura estará invariavelmente causando danos à propriedade privada em primeiro momento, mesmo que o objetivo final seja o da interrupção de serviços públicos. Some-se a isso a realidade global da presença física de servidores, onde muitas vezes, Estados contratam serviços que possuem seus servidores em território estrangeiro, sendo este, o foco da operação.

O ciberespaço é um território desregulamentado em grande medida, neste espaço, vários atores individuais, com seus interesses (pessoais ou de terceiros) são responsáveis por operacionalizar ações, muitas vezes a serviço de Estados em uma lógica de ataques cibernéticos, seja roubar informações, seja para danificar as estruturas de outros Estados.

Para concluir, observa-se que a guerra cibernética se molda conforme as características do espaço cibernético, e tem como principal ator o Estado e se caracteriza por suas motivações políticas. Como os sistemas de informação são essenciais na infraestrutura crítica de um país, o país se torna cada vez mais impotente diante dos ataques cibernéticos. Por infraestrutura crítica consideram-se os sistemas

⁶⁵ ALHOFF, Fritz. *Binary bullets: the ethics of cyberwarfare*. Nova York: Oxford University Press, 2016. p.35.

⁶⁶ *Ibidem*, p.3.

⁶⁷ ICRC. *The Potential Human Cost of Cyber Operations*. ICRC Expert Meeting 14-16 November 2018. Geneva. 2018

bancários, econômicos, de transporte, de defesa, de telecomunicação etc. Deste modo, o computador é uma arma muito potente na Era da Informação permitindo que um ator, seja estatal ou não estatal, inicie um conflito cibernético que cause danos às infraestruturas críticas de um país.⁶⁸

Por sua vez, o alvo operacional acaba sendo a população civil, muito em conformidade com o ideário dos novos conflitos, o civil não somente é um objetivo militar a ser conquistado, como também um possível aliado, ainda que sem ter conhecimento disso. Contudo, operações que tenham como alvo civis e, ou, que seu efeito colateral resulte em danos à civis são expressamente proibido pelo normativo internacional em se tratando de operações militares ou paramilitar, seja em um conflito internacional seja nacional, como dispõe o art. 51 do Protocolo Adicional I à Convenção de Genebra⁶⁹ bem como o art. 3º comum às quatro convenções de Genebra⁷⁰.

Como podemos observar, a guerra cibernética é o ápice do que foi trabalhado enquanto as Guerras de Quarta Geração, não há que se falar mais em um “agente” da guerra na forma de um soldado fardado, aqui, a guerra está inserida em uma lógica onde cada cidadão é um soldado e um alvo em potencial. A própria utilização de infraestrutura civil para o emprego de operações cibernéticas é uma realidade que merece atenção, afinal de contas, um dispositivo móvel, um computador ou qualquer aparelho que possa ser conectado a rede mundial de computadores, pode servir de “posto avançado” para a dispersão de ferramentas maliciosas como vírus, malwares e spywares.

Façamos um breve exercício, suponhamos que em uma central de monitoramento de lançamento de mísseis, o oficial encarregado, observa um vasto painel, contendo uma imagem do globo terrestre, com pequenos sensores ligados a cada localidade que disponha de arsenais nucleares, caso um desses mísseis seja disparado, uma luz se acende e, caso vários sejam disparados um alerta é disposto na tela. Em um determinado instante, uma luz começa a piscar, então duas, três, dez e, em breve, todas as luzes de uma superpotência nuclear estão cintilantes, um alerta de ataque iminente começa a disparar na tela. O operador, confuso, aflito e desesperado não sabe como interpretar aquilo, um inverno nuclear parece próximo, mas, igualmente inconcebível. Parece um relato dantesco ou, pelo menos, vindo de páginas de ficção científica, contudo, não é o caso, reservadas as liberdades autorais, um caso semelhante ocorreu.

⁶⁸SANDRONI, Gabriela Araujo. Prevenção da Guerra no Espaço Cibernético. <https://www.jurisway.org.br/v2/dhall.asp?id_dh=12381> acessado em 28/10/2019

⁶⁹ CICV, Comitê Internacional da Cruz Vermelha. Protocolos Adicionais às Convenções de Genebra de 12 de agosto de 1949. Genebra, Suíça. 2017. P. 39

⁷⁰ CICV, Comitê Internacional da Cruz Vermelha. Artigo 3º comum às quatro Convenções de Genebra. 12 de agosto de 1949. Disponível em < <https://www.icrc.org/pt/doc/resources/documents/treaty/treaty-gc-0-art3-5tdlrm.htm>>. Acessado em: 22/04/2020.

Em 26 de setembro de 1983, o sistema de alerta nuclear da União Soviética passou pela mesma ocorrência, no momento o Tenente Coronel Stanislav Petrov era o oficial responsável pelo sistema, quando as luzes do monitor dispararam, o militar teve duas opções, iniciar a terceira guerra mundial ou aceitar que aquela era uma falha do sistema, Petrov, como nossa própria existência demonstra, escolheu a última:

Todos os dados verificados, ao que parece, o sistema estava certo no alvo - ou melhor, os mísseis relatados estavam. Alguns pensamentos passaram pela mente de Petrov.

"Eu simplesmente não conseguia acreditar que assim, de repente, alguém iria lançar cinco mísseis contra nós. Cinco mísseis não nos eliminariam. Os EUA não tinham cinco, mas mil mísseis em prontidão para a batalha." Simplesmente não parecia nenhum cenário considerado pela inteligência militar antes.

O segundo pensamento na mente de Petrov toda vez que estava de serviço era o seguinte:

"Imaginei que assumiria a responsabilidade de desencadear a Terceira Guerra Mundial - e disse que não, não o faria."

A tensão deve ter sido avassaladora - ele realmente teve tempo para considerar o contexto global de suas ações?

"Sempre pensei nisso. Sempre que vinha de plantão, sempre refrescava na memória. Naquele momento, não havia tempo para pensar, tinha que trabalhar, trabalhar, trabalhar."

Petrov relatou o alarme a seus superiores e o declarou falso. Se ele estivesse enganado, o erro teria se tornado óbvio em minutos: o sistema de detecção do posto tinha uma vantagem de 15 minutos sobre os radares terrestres. Nenhum míssil caiu sobre a União Soviética em um quarto de hora; em vez disso, em uma hora, o alto comando desceu ao posto de comando.⁷¹

Petrov viveu em uma época em que suas opções eram de um lançamento real ou uma falha no sistema, a despeito da existência de computadores, a ideia de vírus tão mortais como os que enfrentamos na atualidade era, de fato, um produto da imaginação de escritores, contudo, hoje esse cenário seria um pouco diferente e, de certo, mais assustador. O medo de um inverno nuclear pode ter ficado nas páginas da Guerra Fria, mas os arsenais nucleares não, tão pouco seus sistemas de lançamento, computadorizados, nessa lógica, e se a nos deparássemos não com uma falha de sistema, nem com um lançamento planejado e, sim, com um ataque cibernético disruptivo, ou que tenha tomado controle de uma central de lançamento. Podemos não ter

⁷¹ LEBEDEV, Anastasiya. The man Who Saved the World Finally Recognized. MosNews. 21 de maio de 2004. Disponível em: < <https://web.archive.org/web/20110721000030/http://www.worldcitizens.org/petrov2.html> >. Acessado em 20 de junho de 2021. Tradução livre de: "All the data checked out, to all appearances, the system was right on target - or rather, the missiles it reported were. A couple of thoughts flashed past Petrov's mind. "I just couldn't believe that just like that, all of a sudden, someone would hurl five missiles at us. Five missiles wouldn't wipe us out. The U.S. had not five, but a thousand missiles in battle readiness." It just didn't seem like any scenario considered by military intelligence before. The second thought on Petrov's mind every time he was on duty was this: "I imagined if I'd assume the responsibility for unleashing the third World War - and I said, no, I wouldn't." The tension must have been overwhelming - did he really have the time to consider the global context of his actions? "I always thought of it. Whenever I came on duty, I always refreshed it in my memory. At that moment, there was no time to think, I had to work, work, work." Petrov reported the alarm to his superiors and declared it false. Had he been mistaken, the mistake would have become obvious in minutes: the post's detection system had a 15-minute advantage over the ground radars. No missiles rained on Soviet Union in a quarter hour; rather, in an hour, high command descended on the command post."

passado por essa realidade ainda, mas, vamos apresentar alguns exemplos de operações conhecidas que demonstram a letalidade do problema.

A grande diferença é que o temor de um ataque (apesar de improvável) era real, as linhas limítrofes entre guerra e paz tangíveis, a guerra cibernética não carrega consigo a representação de um cavaleiro apocalíptico, pelo contrário, é silenciosa, mas tão destrutiva quanto. As condições de vitória e derrota, subjetivas, isso não foi inaugurado pela guerra cibernética, mas sem sombra de dúvidas, aperfeiçoado, como apresentamos anteriormente, essa é uma marca da quarta geração. Quem venceu a Guerra do Vietnã? Ao se perguntar para um americano, sem sombra de dúvidas, orgulhosamente, seremos informados que os Estados Unidos, mas, para boa parte do mundo, o discurso será de uma derrota retumbante, não em escala e operação militar, mas no cerne das doutrinas militares da quarta geração, no combate interno, na guerra de “mentes e corações”⁷²:

A ofensiva radical em todo o país contra o ROTC e o treinamento de oficiais universitários é bem conhecida. Os eventos do ano passado na Universidade de Stanford, no entanto, demonstram os extremos a que esta campanha (que atingiu o pico após o Camboja) chegou. Depois que o corpo docente de Stanford votou para aceitar um programa ROTC modificado e especialmente reestruturado, a universidade foi submetida a um ciclone de violência contínua que incluiu pelo menos US \$ 200.000 em danos finais a edifícios (destacados pela destruição sistemática de 40 vitrais de vinte pés na biblioteca). No final, liderada pelo reitor da universidade Richard W. Lyman, a faculdade se inverteu. Lyman foi citado na época que "ROTC está custando muito a Stanford". A "Indústria do Entretenimento pela Paz e Justiça", a frente do show biz antiguerra organizada por Jane Fonda, Dick Gregory e Dalton Trumbo, agora reivindica mais de 800 filmes, TV e nomes de músicas. Esta organização está apoiando a turnê antimilitar da senhora Fonda que foi aberto do lado de fora dos portões de Ft. Bragg, N.C., em meados de março.⁷³

É pois um claro exemplo de Guerra Assimétrica, ou seja, não há que de se falar em equidade entre os beligerantes, seja ela técnica, econômica ou em contingente, a questão é que as novas tecnologias disruptivas e, especialmente a comunicação, possibilitaram que muitos Estados ou atores de menor poderio, pudessem entrar em um conflito de forma eficiente, visto que, a vitória pode ser alcançada, não por batalhas decisivas ou conquistas espaciais

⁷² A este respeito ver: FINK, Bob. Vietnam – a View from the Walls: a History of the Vietnam Anti-War Movement. Greenwich Publishing. 1982.

⁷³ HEINL, Robert D. Jr. The Collapse of the Armed Forces. p. 4. Armed Forces Journal, 07 June 1971. Disponível em: < <https://msuweb.montclair.edu/~furg/Vietnam/heinl.pdf> > Acessado em: 20 de junho de 2021. Tradução livre de: “The nation-wide campus-radical offensive against ROTC and college officer-training is well known. Events last year at Stanford University, however, demonstrate the extremes to which this campaign (which peaked after Cambodia) has gone. After the Stanford faculty voted to accept a modified, specially restructured ROTC program, the university was subjected to a cyclone of continuing violence which included at least \$200,000 in ultimate damage to buildings (highlighted by systematic destruction of 40 twenty-foot stained glass windows in the library). In the end, led by university president Richard W. Lyman, the faculty reversed itself. Lyman was quoted at the time that "ROTC is costing Stanford too much." "Entertainment Industry for Peace and Justice," the antiwar show-biz front organized by Jane Fonda, Dick Gregory, and Dalton Trumbo, now claims over 800 film, TV, and music names. This organization is backing Miss Fonda's antimilitary road-show that opened outside the gates of Ft. Bragg, N.C., in mid-March.”

estratégicas, mas pelo desgaste político, social e militar de uma guerra que busca vencer pelo convencimento da população de seu adversário, como visto logo acima.

O ciberespaço acaba por se constituir enquanto uma nova frente de batalha, enquanto a primeira geração tinha a terra e o mar como campo de batalha, a segunda geração inaugurou o céu e a terceira o espaço como centros de operações, a quarta geração, por sua vez, viu o ciberespaço como ambiente de oportunidade, mas aqui, o combatente não está no atrito do conflito, é um campo que dispensa qualquer tato com a ideia da cinética, aqui, o militar (se é que de fato é um militar), não está no front.

Contudo, um outro problema se apresenta sob essa nova perspectiva, por se constituir enquanto um campo de batalha completamente novo e, de certo modo, desvinculado das amarras presentes no mundo físico, o ciberespaço não compreende barreiras, se não as compreende, de certo não as considera. As linhas limítrofes que tão bem definem os limites entre os Estados, não se apresentam no ciberespaço, a ideia de soberania (e da violação da mesma), parecem perder qualquer relevância nesse novo ambiente, aqui, em razão dessa nova “cyber-geografia”, a concepção de uma violação, ataque ou agressão à soberania de terceiros é algo extremamente complexo de se definir, como posso argumentar a violação da soberania de um Estado e, conseqüentemente evocar um princípio de legítima defesa, se não posso quantificar as linhas limítrofes entre o “meu” cyber espaço e o seu?

Não obstante, a dificuldade de identificação de barreira físicas em sentido geográfico não são o único problema, visto que, operações e ataques que visam danificar estruturas ou, causar distúrbios político-sociais, podem muito bem ter, enquanto alvo focal, a sociedade civil de uma nação, a ideia de inexistência de limites físicos, criou verdadeiro campo de oportunidade para que se fizessem alvos civis enquanto alvos militares. A guerra assimétrica não vê qualquer limitação ou distinção entre um civil e um militar, enquanto alvo operacional, tendo o terrorismo enquanto seu precursor no século XXI, o ciberespaço virou campo de recrutamento e treinamento desses grupos⁷⁴.

Acerca desse novo campo de oportunidade, vale destacar a eficácia de uma operação cibernética bem executada, não somente o combatente no ciberespaço é uma incógnita, um indivíduo, indivíduos ou Estados não identificados, como uma operação cibernética pode

⁷⁴ A este respeito ver SETTE CÂMARA, Thiago. Terrorismo na era da internet: O uso de redes sociais pelo Estado Islâmico. Revista Relações Internacionais no Mundo Atual, n. 21, v.1, p. 196-221, 2016.

permanecer indetectável por meses, em alguns casos, anos, até ser “oficialmente” disparada (posteriormente iremos trabalhar exemplos deste caso):

[...] Explosões nucleares também apresentam sua própria evidência bastante irrefutável de que armas atômicas foram usadas, enquanto uma operação cibernética bem-sucedida pode permanecer sem ser detectada por meses ou anos.⁷⁵

Vale destacar que segundo dados, o complexo de cibersegurança, veio para ficar e, em grande medida substituiu o clássico complexo de defesa. Com a cada vez maior dependência de interconectividade e de dispositivos e armamentos conectados à rede, basta observar os VANTS ou Drones, bem como os obuseiros autopropulsados a exemplo do sueco Archer⁷⁶, o emprego convencional destes dispositivos em larga escala, estaria em franca desvantagem a ataques precisos e cyber soldados, some-se a isso os elevados custos de manutenção e de emprego destes armamentos, ainda que extremamente avançados, isso, sem mencionar, a suscetibilidade de identificação e rastreamento de potenciais agressores, no caso de utilização de armamentos clássicos, a este respeito vale destacar a assertiva análise de Singer e Friedman:

A ascensão da segurança cibernética como um problema anda de mãos dadas com um boom no número de empresas que tentam ganhar dinheiro com isso. E há muito dinheiro a ser feito. De fato, o mercado de segurança cibernética de 2013 somente nos Estados Unidos foi estimado em US\$ 65 bilhões e projetado para crescer a uma taxa de 6% a 9% ao ano por pelo menos os próximos cinco anos. Em apenas dez anos, a segurança cibernética poderá ser um mercado de US\$ 165 bilhões. Outras estimativas já colocam a escala global do complexo ciber-industrial em “algo entre US\$ 80 bilhões e US\$ 150 bilhões anualmente”.

O que é notável é que esse crescimento está acontecendo ao mesmo tempo em que os orçamentos de defesa tradicionais estão caindo. “Em um mercado de defesa global estéril, o domínio da segurança cibernética forneceu um oásis raro” é como uma revista líder do setor de defesa descreveu o mundo da segurança cibernética. E, como muito mais em segurança cibernética, o boom não é apenas um fenômeno americano. Por exemplo, mesmo em um ambiente de austeridade e cortes dramáticos em todo o governo do Reino Unido, a revisão de Defesa e Segurança Estratégica de 2010 recomendou um aumento no financiamento de segurança cibernética de US\$ 1,7 bilhão. Como escreveu o professor Peter Sommer, da London School of Economics: “Em termos de envolvimento das grandes companhias militares, você tem que perceber que eles estão achando extremamente difícil vender equipamentos grandes e pesados do tipo que eles estão vendendo. Estamos acostumados porque o tipo de guerra em que estamos envolvidos tende a ser contra insurgentes. E assim eles estão procurando desesperadamente por novas áreas de produtos – e a área de produtos óbvia, eles pensam, é a guerra cibernética.”⁷⁷

⁷⁵ SINGER, P. FRIEDMAN, A. *Cybersecurity and cyberwar: What everyone needs to know*. New York: Oxford University Press. p. 162. 2014. Tradução livre de: “[...] Nuclear explosions also present their own, rather irrefutable evidence that atomic weapons have been used, while a successful covert cyber operation could remain undetected for months or years.”

⁷⁶ A este respeito ver VOLKVEIS, José Henrique Antunes. *Emprego de Obuseiros Autopropulsados*, Trabalho de Conclusão de Curso apresentado à Academia Militar das Agulhas Negras. Academia Militar das Agulhas Negras, Resende. 2016. Disponível em: < <https://bdex.eb.mil.br/jspui/bitstream/1/1142/1/TCC%203105%20Antunes.pdf> > Acessado em: 20 de maio de 2021.

⁷⁷ SINGER, P. FRIEDMAN, A. *Cybersecurity and cyberwar: What everyone needs to know*. New York: Oxford University Press. p. 163. 2014. Tradução livre de: “The rise of cybersecurity as an issue has gone hand in hand with a boom in the number of companies trying to make money from it. And there is a lot of money to be made. Indeed, the 2013 cybersecurity market in the United States alone was estimated to be \$65 billion and projected to grow at a 6 percent to 9 percent rate per year for at least the next five years. In only ten years, cybersecurity could

Tendo em mente o completo descolamento do combatente com a linha de frente e, sua difícil identificação bem como conexão real e direta com o campo de batalha, assim como a nova abertura de oportunidade para operações encobertas de desestabilização em uma lógica de guerra assimétrica, até que ponto eventos como a Primavera Árabe ou golpes de Estado e Revoluções não são orquestrados por esses agentes estatais (ou não estatais) sem face, é um questionamento que deve ser feito. Em uma realidade em que a concepção do Estado Nação tem se fragilizado frente as novas tecnologias e novas esferas supra-estatais, onde se encontram esses novos atores da guerra? E os Estados? Seriam esses vítimas ou algozes? Ao que se apresenta nos encontramos em um cenário de constante estado de guerra, de uma guerra que é ao mesmo tempo Assimétrica e Irregular, onde não há uma “batalha decisiva” como afirmava Clausewitz, muito menos de campos de batalha bem delimitados e agentes identificados.

Sem sombra de dúvidas, uma das características mais marcantes dessa nova modalidade de agressão é a capacidade de gerar danos indiretos. A degradação do sistema em si nem sempre é o alvo desejado do ataque. Desse modo um ataque pode tanto pretender apagar dados sensíveis obtidos por outro Estado quanto cortar o acesso a serviços básicos ao desabilitar *software* com essa finalidade, como expõe Biazatti:

O ataque cibernético tem a característica particular de afetar o funcionamento regular de um software, produzindo consequências negativas devido ao seu mau funcionamento ou permitindo que o invasor o controle, usando-o para atacar outro alvo. É o que acontece quando o sistema de controle das comportas de uma empresa é haqueado e o invasor libera a água contra cidades ou instalações relevantes ou quando o sistema de navegação de aeronaves é propositalmente comprometido, as levando a se chocar umas contra as outras ou simplesmente perder estabilidade e cair. Pode-se mencionar ainda a manipulação do sistema GPS de um satélite, a fim de desviar mísseis inimigos de seu alvo original ou a alteração dos dados sanguíneos dos pacientes de um hospital, fazendo com que enfermeiros apliquem sangue de tipo incorreto nos internados. Todos esses exemplos envolvem um ato que demanda uma outra ação a ser tomada por um terceiro ou necessita do objeto o qual o sistema conecta para que o resultado pretendido seja alcançado. Daí dizer que os ataques cibernéticos possuem um caráter indireto.⁷⁸

be a \$165 billion market. Other estimates already place the global scale of the cyber-industrial complex at “somewhere between \$80 billion and \$150 billion annually.” What is notable is that this growth is happening at the same time that traditional defense budgets are going down. “In a barren global defence market the cyber security domain has provided a rare oasis” is how a leading defense industry magazine described the world of cybersecurity. And, like much else in cybersecurity, the boom is not just an American phenomenon. For instance, even in an environment of austerity and dramatic cuts across the UK government, the 2010 Strategic Defence and Security review recommended an increase in cybersecurity funding of \$1.7 billion. As Professor Peter Sommer of the London School of Economics wrote, “In terms of the involvement of the big military companies, you have to realize that they are finding it extremely difficult to sell big, heavy equipment of the sort they are used to because the type of wars that we’re involved in tend to be against insurgents. And so they are desperately looking for new product areas—and the obvious product area, they think, is cyber warfare.”

⁷⁸ BIAZATTI, Bruno. Operações cibernéticas à luz da proibição internacional do uso da força: um estudo sobre o direito à legítima defesa. Trabalho de Conclusão de Curso (Graduação em Direito) - Faculdade de Direito, Universidade Federal de Minas Gerais. Belo Horizonte, 2015. pp.48 - 49.

Fica evidente que um dos fatores relevantes para se delimitar a extensão de um ataque não mais está atrelado aos aspectos logísticos e estratégicos em que as tropas se colocam na operação, ou até mesmo quanto ao seu alvo primário, mas sim os alvos secundários que sofrem indiretamente com o ataque ou se colocam como campos de oportunidade para a desestabilização de um inimigo internamente.

Ciente dessa nova lógica, os EUA através do vice-presidente do Estado-Maior Conjunto emitiu para seus dirigentes militares, comandantes e diretores um memorando⁷⁹ em que definiu um conceito para “alvos críticos”. Segundo o documento seria considerado “*Critical Cyber System/Asset/Function*” um sistema informático que, se atacado, implicaria negativamente e significativamente na segurança nacional, estabilidade econômica, confiança da população, saúde pública e preservação ambiental. No mesmo caminho “*Critical Infrastructure*” seriam sistemas ou bens com a mesmas características.⁸⁰ Vemos aqui, mais uma vez, a preocupação americana com a lógica de uma guerra que tenha como enfoque a desestabilização enquanto campo de batalha decisivo.

Passemos então a analisar esse teatro de guerra cibernético, através de exemplos concretos de ataque que resultaram de alguma forma, em danos diretos e indiretos aos alvos pretendidos. A este respeito, trabalharemos o ataque à Estônia (2007)⁸¹, o *Titan Rain* (2003-2007)⁸² e as operações envolvendo os vírus *Stuxnet* no Programa Nuclear Iraniano e demais infraestruturas do país (2009-2012)⁸³.

a) O ATAQUE À ESTÔNIA:

O ataque à Estônia, inicialmente atribuído à Rússia (apesar desta negar), ocorreu supostamente em decorrência da retirada de um monumento em homenagem aos combatentes soviéticos (monumento que simbolizava a vitória da URSS sobre o Nazismo), foi caracterizado por uma série de ataques cibernéticos à infraestrutura crítica do país. A Estônia é um país altamente dependente de seu sistema digital, integrado virtualmente, o ataque que perdurou por

⁷⁹ ESTADOS UNIDOS. Memorandum on Joint Terminology for Cyberspace Operations for Chiefs of the Military Services, Commanders of the Combatant Commands and Directors of the Joint Staff Directorates, General James E. Cartwright, Vice Chairman of the Joint Chiefs of Staff, Washington D.C., 2011

⁸⁰ *Ibidem.* p.5.

⁸¹ http://www.bbc.com/portuguese/reporterbbc/story/2007/05/070517_estoniaataquesinternetw.shtml acesso em 26 de fevereiro de 2020

⁸² <https://www.theguardian.com/uk/2007/sep/05/topstories3.politics> acesso em 26 de fevereiro de 2020

⁸³ <https://oglobo.globo.com/sociedade/tecnologia/virus-stuxnet-que-atacou-usinas-nucleares-no-ira-foi-criado-em-parceria-por-eua-israel-2836696> acesso em 26 de fevereiro de 2020

semanas, suspendeu uma série de serviços essenciais, levou milhares de pessoas às ruas e o sistema bancário e financeiro do país foi afetado com grandes perdas econômicas⁸⁴.

Apesar de mediatizado enquanto uma resposta à questão do monumento, vale apresentar algumas questões que parecem contradizer essa justificativa. A Estônia é um país dividido culturalmente, após a separação do país da União das Repúblicas Socialistas Soviéticas - URSS em 1991, o país optou por um caminho de aproximação do ocidente, e de rápida expansão tecnológica e digital, contudo, à época, um quarto da população se considera de origem étnica russa, tendo como sua primeira língua, inclusive o russo, esses cidadãos passaram a se sentir excluídos do rápido desenvolvimento tecnológico desfrutado pelo país:

Mas nenhuma nação está isenta de problemas. Cerca de um quarto da população da Estônia não se considera estoniana. Eles são geralmente classificados como “russos”, pois embora em termos de etnia sejam originários de vários países, a maioria fala russo como primeira língua. Um núcleo duro deles acredita que são tratados pelo Estado como cidadãos de segunda classe.⁸⁵

Sem sombra de dúvidas a escalada de tensões teve seu ápice com a execução de decisão de mudança de local do monumento, com forte resistência de uma minoria étnica russa no país, protestos acabaram saindo das ruas e indo para o espaço cibernético. No dia 27 de abril de 2007, o maior ataque cibernético até então teve início, a operação consistiu em um volume nunca antes visto de Ataques de Negação de Serviço (DDoS). Normalmente, esse tipo de operação tem como objetivo provocar a queda de serviços e servidores, emulando ou coordenando acessos em massa, levando os servidores a uma impossibilidade de resposta em face do volume de acessos e de solicitações de dados.

Inicialmente, as autoridades imaginaram que estavam diante de ações descoordenadas de grupos revoltosos internos, não levou muito tempo para que as constatações iniciais se apresentassem como falsas e os traços de um ataque altamente coordenado, planejado e de proporções nunca antes vistas estava em curso.

O que poderia ser considerado o Pearl Harbor dos ataques cibernéticos, teve um efeito devastador no sistema financeiro e de comunicação do país, inicialmente as páginas do governo,

⁸⁴ OTTIS, Rain. Analysis of the 2007 Cyber Attacks Against Estonia from the information Warfare Perspective. Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. Disponível em < <https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/> >. Acessado em: 10/02/2020.

⁸⁵ Steve Mansfield-Devine, “Estonia: What Doesn’t Kill You Makes You Stronger,” Network Security 7 (July 2012): 13, p. 12. disponível em: < [https://doi.org/10.1016/S1353-4858\(12\)70065-X](https://doi.org/10.1016/S1353-4858(12)70065-X) > Acessado em: 27 de junho de 2021. Tradução livre de: “But no nation is without its problems. Around a quarter of Estonia’s population does not consider itself Estonian. They are generally classed as ‘Russian’, as although in terms of ethnicity they originate from a number of countries, most speak Russian as a first language. A hard core of them believe they are treated by the state as second-class citizens.”

órgãos oficiais e autoridades foram retirados do ar, a prática de *de-facing*⁸⁶ foi constatada em várias páginas e, em certo momento, a imprensa oficial do Estado bem como demais órgãos de comunicação privados ficaram completamente inoperantes, o país ficou às escuras, sem conseguir se comunicar com a população e sem conseguir uma comunicação adequada com o exterior:

Os primeiros ataques consistiram em inundações de negação de serviço – algumas usando lixo eletrônico – contra sites de alto perfil, a maioria deles com conexões com o governo. Eles incluíam sites para o Presidente, Parlamento, polícia e partidos políticos. A 'sala de reuniões pública', onde o governo estoniano publica seus comunicados de imprensa, foi um dos primeiros atacados e logo ficou inacessível de fora do país. Houve também uma série de desfigurações do site.

Muito disso foi coordenado por hackers russos usando fóruns online. Usando uma metodologia que mais tarde seria adotada por grupos hacktivistas como o Anonymous, os hackers incentivaram os “patriotas” – muitos sem habilidades técnicas, mas compartilhando o desejo de agir – a baixar software pronto. Essas eram principalmente ferramentas DDoS pré-existentes que empregavam ping ou inundação de SYN, mas algumas foram especialmente modificadas para participar do ataque à Estônia.

Os meios de comunicação, incluindo o jornal diário Postimees, também foram atacados e, a certa altura, a mídia se viu isolada do mundo exterior. Isso, avalia Almann, é indicativo de quão bem planejados foram os ataques. “Foi perturbador”, diz ele. “Já era difícil ler notícias lá dentro, mas também era difícil ler notícias para quem estava fora do país. Havia um sentimento de pânico começando a crescer.[...]”⁸⁷

O pior momento da crise ocorreu no dia 09 de maio (coincidentalmente, o dia em que a Rússia comemora a vitória da Segunda Guerra Mundial), existem estimativas de que um milhão de *botnets*⁸⁸, foram empregados no ataque somente neste dia, os computadores “zumbis” contaminados por malware, espalhados pelo mundo, se transformaram instantaneamente em misseis teleguiados, prontos para desestabilizar toda a rede da Estônia mais uma vez:

Os russos comemoram a vitória na Segunda Guerra Mundial em 9 de maio, razão pela qual os estonianos de etnia russa se reuniram no memorial naquela data no ano anterior. Os botnets que entraram em ação naquele dia eram agora muito maiores: como uma estimativa aproximada, de que até um milhão de computadores podem ter

⁸⁶ Prática de se mudar o “rosto” de uma página, normalmente um ataque dessa natureza costuma sequestrar a página pretendida e alterar sua estrutura, seu layout, apresentando alguma mensagem.

⁸⁷ Steve Mansfield-Devine, “Estonia: What Doesn’t Kill You Makes You Stronger,” Network Security 7 (July 2012): 13. p. 13 disponível em: < [https://doi.org/10.1016/S1353-4858\(12\)70065-X](https://doi.org/10.1016/S1353-4858(12)70065-X) > Acessado em: 27 de junho de 2021. Tradução livre de: “The first attacks consisted of denial of service floods – some using junk mail – against high-profile websites, most of them with connections to the Government. They included websites for the President, Parliament, police and political parties. The ‘public briefing room’, where the Estonian Government posts its press releases, was among the first hit and was soon inaccessible from outside of the country. There were also a number of site defacements. Much of this was co-ordinated by Russian hackers using online forums. Using a methodology that would later be adopted by hacktivist groups such as Anonymous, the hackers encouraged ‘patriots’ – many without technical skills but sharing a desire to take action – to download ready-made software. These were mostly pre-existing DDoS tools that employed ping or SYN flooding, but some had been specially modified to participate in the attack on Estonia. Media outlets, including the daily newspaper Postimees, also came under attack and at one point the media found itself cut off from the outside world. This, Almann reckons, is indicative of how well planned the attacks were. “It was disturbing,” he says. “It was already difficult to read news inside, but it was also difficult to read news for those people who were outside of the country. There was a panicky feeling starting to grow.[...]”

⁸⁸ Botnets são computadores conectados em rede, infectados, que podem ser controlados e acessados remotamente e utilizados na operacionalização de ações maliciosas na rede de computadores.

participado do ataque principal, e alguns cálculos colocam o número total de máquinas envolvidas em toda a campanha em dois milhões.⁸⁹

Apesar das manifestações da Estônia de que o ataque de fato teria partido da Rússia, nenhuma prova concreta foi apresentada pelo país, a despeito das evidências tangíveis, incluído o rastreamento de IPs advindos do país, a natureza do ataque cibernético garantiu a seus operadores o seu anonimato. Contudo, os danos não foram anônimos, o país se viu em um verdadeiro apagão de comunicação por dias, seu sistema financeiro foi danificado, causando danos reais ao mercado nacional, sem mencionar aos cidadãos, que já desfrutavam à época, de um sistema bancária altamente digital.

Ademais, a gravidade do ataque aos órgãos de Governo do país, levou o então Secretário de Segurança Interna dos Estados Unidos (Homeland Security), Michael Chertoff a se manifestar:

Este ataque foi além de simples travessuras. Representava uma ameaça real à segurança nacional e à capacidade do governo estoniano de governar seu país. Enfrentamos no século 21 um problema muito difícil: um único indivíduo, um pequeno grupo de pessoas e certamente um estado-nação podem potencialmente causar o tipo de dano ou interrupção que nos anos anteriores só acontecia quando você jogava bombas ou detonava explosivos.⁹⁰

Ainda nessa linha o Centro de Excelência em Comunicações Estratégicas da OTAN lançou em 06 de junho de 2019, um documento intitulado de “Hybrid Threats: 2007 cyber attacks on Estonia”, em que define bem os objetivos vislumbrados pelo ataque, bem como sua visão acerca dos atores passivos e ativos:

Fluxo de informações interrompido: Ao impedir o acesso a muitas formas de informação (sites de jornais, mensagens, saldos bancários), esse ataque cibernético atingiu o coração da economia dependente de tecnologia da Estônia, onde o fluxo irrestrito de informações e dados é vital. Isso ameaçou afetar a psicologia dos cidadãos e a confiança das empresas e investidores.

[...]

Este primeiro ataque cibernético significativo causou alguma interrupção e custo para a Estônia, mas nunca teve a intenção de causar danos irreversíveis e duradouros. Foi antes de tudo um ato de comunicação. A mensagem pretendida era que a Federação Russa tinha a capacidade de isolar efetivamente um estado, interrompendo o fluxo de dados, como transferências financeiras, notícias, e-mail, etc. Esse isolamento poderia ser iniciado sem aviso prévio e ser impossível de manobrar.⁹¹

⁸⁹ Op.cit, p. 14. Tradução livre de: “Russians celebrate victory in World War Two on 9 May, which is why ethnic Russian Estonians had gathered at the memorial on that date the previous year. The botnets that swung into action that day were now much bigger: as a rough estimate, as many as one million computers may have participated in the main attack, and some calculations put the total number of machines involved over the whole campaign at two million.”

⁹⁰ ESPINER, Tom. Estonia’s Cyberattacks: Lessons learned, a year on. 1 may, 2008. Disponível em: < <https://www.zdnet.com/article/estonias-cyberattacks-lessons-learned-a-year-on/> > Acessado em: 10 de junho de 2021. Tradução livre de: “This attack went beyond simple mischief. It represented an actual threat to the national security and the ability of the Estonian government to govern its country. We face in the 21st century a very difficult problem: a single individual, a small group of people and certainly a nation state can potentially exact the kind of damage or disruption that in years past only came when you dropped bombs or set off explosives.

⁹¹ PAMMENT, James. Et. Al. Hybrid Threats: 2007 cyber attacks on Estonia. p. 66 e 68. 2019. Disponível em: < <https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86> > Acessado em: 15 de junho

Ambas as manifestações apresentadas possuem pontos de extrema importância, a primeira, em relação à gravidade do ataque, a despeito de não ter gerado danos físicos aparentes, a constatação é de que a operação cibernética atingiu o coração do Estado-Nação, sua soberania, se estivéssemos tratando de um ataque cinético, não há dúvida que qualquer ato que ponha em risco a soberania de outro Estado, estará diretamente violando a normativa internacional, garantindo ao Estado atacado, a capacidade responsiva de se proteger, invocar o instituto da legítima defesa.

O Outro ponto de grande relevância é a estratégia empregada, a ideia de como bem aponta o documento da Otan, de atacar o psicológico da população, desestabilizar, atuar como um ataque preciso ao coração de uma nação em um grande teatro de guerra.

Contudo, o mesmo documento apresenta uma passagem preocupante em sua conclusão, que vai de encontro com a ideia de que uma escalada nas operações cibernéticas enquanto atos de resposta é algo previsível no horizonte próximo:

[...] Nos últimos dez anos, a OTAN e a UE percorreram um longo caminho na compreensão de como as diferentes fontes de avaliação se unem e qual a melhor forma de determinar o grau de probabilidade. Os governos tornaram-se mais maduros para lidar com ataques cibernéticos. **Os governos aprenderam que as opções de resposta não se limitam a medidas militares (por exemplo, acionando o Artigo V) e legais, mas que ferramentas diplomáticas mais amplas e uma resposta internacional consistente podem ter mais impacto.**⁹² (Grifo nosso).

A ideia de que a saída considerada mais eficiente seria a da aplicação do vasto rol de oportunidades em matéria de Relações Internacionais à primeira vista pode não parecer desconfortante, contudo, essa parece ser uma saída a ineficácia ou incompletude da legislação vigente, contudo, o que acontece quando a diplomacia falha? O que impediria de um estado afetado por um ataque nessas proporções e com essas suspeições acerca de terceiros, respondesse em pé de igualdade. Decerto, há uma busca na manutenção da suposta paz internacional, mas, como veremos posteriormente, parece haver ainda mais um interesse no uso desse novo campo de oportunidades.

de 2021. Tradução livre de: “Disrupted information flow: By preventing access to many forms of information (newspaper websites, messaging, bank balances), this cyber attack struck at the heart of Estonia’s technology-dependent economy where the unrestricted flow of information and data is vital. This threatened to have effects on the psychology of citizens and the confidence of businesses and investors.[...] This first significant cyber attack caused some disruption and cost to Estonia, but was never intended to cause irreversible and lasting damage. It was first and foremost an act of communication. The intended message was that the Russian Federation had the capabilities to effectively isolate a state by disrupting the flow of data such as financial transfers, news, email, etc. This isolation could be initiated with no warning and be impossible to out-manoeuvre.”

⁹² *Ibidem*, p.68. Tradução livre de: “[...] In the last ten years, NATO and the EU have come a long way in understanding how different sources of assessment come together, and how best to determine the degree of probability. Governments have grown more mature in dealing with cyber attacks. Governments learned that response options are not limited to military (for instance triggering Article V) and legal measures, but that broader diplomatic tools and a consistent international response can have more impact.”

b) TITAN RAIN

O *Titan Rain* foi uma falha explorada, presumivelmente pelo governo Chinês para espionar os Estados Unidos e seus aliados, a falha, detectada em 2004, afetou setores como o Departamento de Defesa Americano. A demora e a continuidade do ataque acabou por possibilitar que uma série de informações confidenciais caíssem em domínio de outro Estado⁹³. O uso dessa falha é considerado até o hoje o maior caso de espionagem digital do mundo, com danos incalculáveis à segurança dos países afetados, a China e seus aliados negaram qualquer participação.

A falha pode ser considerada um marco no tocante a temática das operações cibernéticas, visto que representa o primeiro grande exemplo de espionagem cibernética atribuído a China. Ainda que não tenha gerado danos físicos, ou qualquer gargalo nos equipamentos e redes, os alvos tiveram dados sensíveis roubados, possivelmente expostos à nações adversárias e, ou, inimigas, informações essas confidenciais, ligadas a pesquisas no setor de defesa, dados estruturais das falhas de segurança de vários atores estatais e de interesse estatal, dentre outros:

[...] O resultado final da operação é que a propriedade intelectual foi roubada, o que tem um impacto muito limitado nas outras camadas do ciberespaço, pois nenhum sistema está sendo danificado ou pessoas individuais foram prejudicadas. Mas, a longo prazo, o ataque à camada de conteúdo pode ser suficiente para fornecer ao adversário a vantagem estratégica de ter uma visão das capacidades e desenvolvimento de armamento do destinatário.⁹⁴

Ainda que o ataque tenha se dado no início dos anos 2000, sua repercussão foi massiva, primeiro, como anteriormente mencionado, por ter sido considerado uma das primeiras operações cibernéticas, com a finalidade de espionagem com o roubo de dados sensíveis. A operação teve primariamente como alvos, informações e infraestrutura digital restritas a agências governamentais e militares, dentre elas o Departamento de Estado, Departamento de Energia, Departamento de Segurança, NASA, bem como algumas empresas ligadas ao setor de defesa, com contratos com o Governo Americano como a *Lock Head Martin*.

Após investigações iniciais, com envolvimento de agências especializadas como o FBI e profissionais do setor de tecnologia das empresas afetadas, constatou-se que os ataques teriam

⁹³ SAPORITO, Laura e LEWIS James A. Cyber Incident Attributed to China. Center for Strategic and International Studies.

⁹⁴ LOMANS, Marieke. Investigating Titan Rain Cyber Security & Cyber Operations. Master MSS – Class 2015. 2017.pp.Disponível:<10.https://www.academia.edu/32222445/_Investigating_Titan_Rain_Cyber_Espionage_Cyber_Security_and_Cyber_Operations > Acessado em, 14 de fevereiro de 2021. Tradução livre de: “[...] The end result of the operation is that intellectual property has been stolen, which has very limited impact on the other layers of cyber space as no systems are being damaged or individual persona have been harmed. But in the long term, the attack on the content layer might just be enough to provide the adversary with the strategic advantage of having insight in the capabilities and development of weaponry of the addressee.”

partido diretamente de agentes chineses, especificamente de servidores localizados na província de Guangdong. Ainda que a rastreabilidade tenha levado os especialistas a localizarem a origem do ataque, essa informação, ainda que relevante, somente apresenta a localização de onde partiram as operações, não necessariamente de seus agentes.

A capacidade de utilização de infraestruturas terceiras para a operacionalização de um ataque cibernético, como já mencionado anteriormente, dificulta a localização de seus agentes, ao passo que acaba por gerar desconfiança em casos como esse. Contudo, especialistas entendem que a capacidade e a extensão das operações do *Titan Rain*, só poderiam partir de uma organização altamente disciplinada e organizada, possivelmente de caráter militar.

O volume de informações obtidas pelos “hackers”, demandaria uma filtragem especializada, para garantir observância das informações relevantes e de interesse específico. É sob esta ótica que especialistas supõem, não somente baseado na localização dos servidores do ataque, mas do grau de especialização das organizações chinesas, que o ataque tenha sido perpetrado e dirigido por autoridades governamentais.

Não obstante, a prática de espionagem digital, parece ser uma das especialidades da China, em matéria de operações cibernéticas. Segundo os pesquisadores Robert Lai e Syed (Shawon) Rahman, a capacidade operacional chinesa, bem como a especialidade na obtenção e tratamento de dados sensíveis, acabou por possibilitar um grau de especialização, particular ao modelo chinês:

A China é o estado-nação mais ativo em atividades de espionagem cibernética com uma abordagem de “grão de areia” – rouba o máximo de dados possível e infere informações valiosas a partir dos dados roubados. A maioria dos especialistas acredita que a China é responsável pelos dez piores eventos de invasão de computadores: (1) Titan Rain; (2) Escritório da Ásia Oriental do Departamento de Estado; (3) Escritórios do Rep. Frank Wolf; (4) Departamento de Comércio; (5) Escola de Guerra Naval; (6) o secretário de Comércio Carlos Gutierrez e o apagão de 2003; (7) campanhas presidenciais de McCain e Obama; (8) Gabinete do Senador Bill Nelson; (9) Rede Fantasma; e (10) programa F-35 da Lockheed Martin. A espionagem cibernética é uma ameaça que oferece aos adversários vantagens assimétricas na obtenção de tecnologia crítica, segredo comercial, propriedade intelectual, dados financeiros, informações de identificação pessoal (PII) e dados confidenciais de empresas, instituições, contratados de defesa ou do governo para que possam nivelar o campo de jogo.⁹⁵

⁹⁵ LAI, Robert. RAHMAN, Syed (Shawon). Analytic of China Cyberattack. The International Journal of Multimedia & Its Application (IJMA) Vol. 4, No. 3, June 2012. Pp 37 – 56. P. 38. Tradução livre de: “China is the most active nation-state on cyber espionage activities with a “grain of sands” approach—steals as much data as possible, and infers valuable information from the stolen data. Most experts believe that China is responsible for the ten worst computer hacking events: (1) Titan Rain; (2) State Department’s East Asia Bureau; (3) Offices of Rep. Frank Wolf; (4) Commerce Department; (5) Naval War College; (6) Commerce Secretary Carlos Gutierrez and the 2003 blackout; (7) McCain and Obama presidential campaigns; (8) Office of Sen. Bill Nelson; (9) Ghostnet; and (10) Lockheed Martin’s F-35 program. Cyber espionage is a threat that gives adversaries the asymmetric advantages on gaining critical technology, trade secret, intellectual property, financial data, personal identifiable information (PII), and classified data from corporations, institutions, defense contractors, or the government so that they can level the playing field.”

Isso fica evidente quando levamos em consideração a natureza do tratamento de dados dada pelo Partido Comunista Chinês, sua doutrina de controle total dos meios de comunicação, bem como dos aspectos culturais da nacionalidade, levou ao desenvolvimento de uma verdadeira rede de vigilância do ciberespaço, com um sistema de censura bem desenvolvido, em uma rede de multicamadas:

Censura na Internet com características chinesas – a maioria dos analistas se concentra apenas na liberdade de expressão, mas ignoram que a capacidade de censura da China lhes oferece uma vantagem assimétrica. A China iniciou atividades de censura desde que os chineses começaram a usar a Internet. Desde a captura de cada pacote até a inspeção do conteúdo e a aplicação de regras ao bloqueio, a China ganhou muita experiência prática com atividades de censura. A infraestrutura de Internet da China possui um sistema de monitoramento de conteúdo distribuído completo, multicamada, multicanal e distribuído integrado para realizar inspeção profunda de pacotes, que também pode ser uma defesa.⁹⁶

Para melhor compreender a logística operacional do Titan Rain e as razões de sua imputação enquanto uma operação de origem estatal, mister analisar o seguinte excerto:

Para realizar footprinting, scanning e enumeração, os hackers envolvidos no Titan Rain recorreram a versões customizadas de softwares projetados para executar automaticamente tais tarefas. Embora grande parte da investigação do Titan Rain permaneça confidencial, os investigadores divulgaram a seguinte linha do tempo de um dia típico de reconhecimento cibernético para a revista Time que começou em 1º de novembro de 2004:

- 22h23: Hackers identificam vulnerabilidades em sistemas no Comando de Engenharia de Sistemas de Informação do Exército dos EUA em Fort. Huachuca, AZ.
- 1h19: Hackers identificam as mesmas vulnerabilidades na Defense Information Systems Agency em Arlington, VA.
- 3h25: Hackers escaneiam o Naval Oceanic Systems Center em San Diego, CA.
- 4h46: Hackers escaneiam a instalação de Defesa Estratégica e Espacial do Exército dos EUA em Huntsville, AL.

Uma vez que a fase de reconhecimento cibernético de uma missão estivesse completa, o próximo passo para os hackers do Titan Rain era se infiltrar nos sistemas de interesse. Com base em relatórios de código aberto, sabemos que os sistemas infiltrados na operação Titan Rain provavelmente foram feitos com um software (ou malware) aparentemente inócuo (ou seja, jogos, software comercial pirata, arquivos de dados etc.), mas em vez disso, contém código que permite que o hacker acesse o sistema que executa o software. Muitas vezes, depois que o usuário clica em algum ícone ou link comum, um Trojan pode começar a ser executado no sistema, mas permanecer completamente imperceptível – simplesmente residindo na memória de um computador desconhecido para o usuário. Em novembro de 2003, um alerta do governo descreveu uma infecção generalizada dos sistemas de computador do Departamento de Defesa dos EUA (DoD) por um Trojan.⁹⁷

⁹⁶ *Ibidem*. P. 44. Tradução livre de: “Internet censorship with Chinese characteristics—most analysts only focus on freedom of speech, but they ignore that China’s censorship capability offer them an asymmetric advantage. China has begun censorship activities even since Chinese start using Internet. From capturing every packet to inspecting the content, and applying rules to blockage, China has gained much practical experience from censorship activities. China’s Internet infrastructure has a complete, multi-layer, multi-channel, and distributed content monitor system built-in to perform deep packet inspection, which can be a defense as well.”

⁹⁷ SHAKARIAN, Paulo. SHAKARIAN, Jana. RUEF, Andrew. Introduction to Cyber-Warfare a Multidisciplinary Approach. Elsevier, Syngress. Waltham, MA. US. 2013, p. 126. Tradução livre de: “To perform footprinting, scanning, and enumeration, the hackers involved in Titan Rain resorted to customized versions of software designed to automatically perform such tasks. Though much of the Titan Rain investigation remains confidential, the investigators disclosed the following time line of a typical day of cyber reconnaissance to time magazine that started on November 1, 2004: 10:23 pm: Hackers identify vulnerabilities on systems at the U.S. Army Information

Ainda que aparentemente uma simples operação de invasão de computadores, por intermédio de um software malicioso, a capacidade de se infiltrar em um sistema sofisticado como de um órgão governamental, foge da alçada de muitos programadores ainda que experientes, não somente isso, o grau de sofisticação e disciplina por parte dos agentes invasores, em analisar os computadores das Instituições alvo das ações, com operacionalização coordenada, em curtos espaços de tempo, como bem demonstra o supracitado, bastou para as suspeitas de uma operação com características estatais e militares. Isso se tornou ainda mais evidente, no momento em que especialistas não conseguiram detectar traços das operações, o que, de acordo com eles, não é uma característica comum em ações de hackers, que costumam deixar rastros ou pistas de suas ações:

Shawn Carpenter, um veterano da Marinha dos EUA, trabalhou como especialista em segurança de redes de computadores para os Laboratórios Nacionais Sandia. Ele se envolveu pela primeira vez na investigação de Titan Rain em setembro de 2003, quando ajudou a investigar uma invasão de sistemas de computador na Lockheed Martin. Um evento semelhante ocorreu posteriormente em Sandia apenas alguns meses depois. Ele observou que os hackers iriam rapidamente para o arquivo e carregariam as informações desejadas de um determinado sistema – gastando meros 10 a 30 minutos conectados ao sistema do alvo. Carpenter observou que, ao contrário dos hackers amadores, cujos erros se tornam visíveis quando eles comprometem um sistema, os hackers do Titan Rain sabiam qual era seu trabalho e o que queriam – eles “nunca apertam uma tecla errada”.⁹⁸

Fica evidente a relevância do ataque para a compreensão do problema, primeiro em razão do ineditismo quanto ao tipo de operação e seu suposto agente, segundo, pela temporalidade dos atos, que se prolongaram por anos, até sua detecção e, como as fontes nos revela, nem todos os detalhes do que foi e qual foi a extensão dos dados roubados pelo Titan Rain.

System Engineering Command in Ft. Huachuca, AZ. 1:19 am: Hackers identify the same vulnerabilities at the Defense Information Systems Agency in Arlington, VA. 3:25 am: Hackers scan the Naval Oceanic Systems Center in San Diego, CA. 4:46 am: Hackers scan U.S. Army Space and Strategic Defense installation in Huntsville, AL. Once the cyber reconnaissance phase of a mission was complete, the next step for the Titan Rain hackers was to infiltrate the systems of interest. Based on open source reports, we know that the systems infiltrated in the Titan Rain operation were most likely done with a piece of software (or malware) appear to be innocuous (i.e., games, pirated commercial software, data files, etc.) but instead contain code that allows the hacker to access the system running the software. Often, after the user clicks on some ordinary appearing icon or link, a Trojan may start running on the system but remain completely unnoticeable – simply residing in memory of a computer unknown to the user. In November 2003, a government alert described a wide-spread infection of U.S. Department of Defense (DoD) computer systems by such a Trojan.”

⁹⁸ *Ibidem*. P. 126. Tradução livre de: “Shawn Carpenter, a veteran of the U.S. Navy, worked as a computer network security specialist for Sandia National Laboratories. He first became involved in the Titan Rain investigation in September of 2003 when he helped investigate a break-in of computer systems at Lockheed Martin. A similar event subsequently occurred at Sandia only a few months later. He noted that the hackers would move quickly to the archive and upload the desired information from a given system – spending a mere 10 – 30 min logged on to the target’s system. Carpenter noted that unlike amateur hackers, whose mistakes become visible once they compromised a system, the Titan Rain hackers knew what their job was and what they wanted – They “never hit a wrong key.””

c) STUXNET

O *Stuxnet* é um dos vírus mais destrutivos já desenvolvidos, foi utilizado na disrupção do programa nuclear iraniano⁹⁹, sendo utilizado para infectar o sistema operacional da Siemens em 14 empresas Iranianas, furtando dados e causando instabilidade no sistema, causando danos estruturais às usinas e ao programa de enriquecimento. Acredita-se que o vírus foi projetado e plantado pelos Estados Unidos da América e, ou, Israel, ambos negaram o fato:

Sendo uma proposta inédita, a intenção era de, inicialmente, retardar os planos iranianos e ganhar tempo. Nesse sentido, desenvolveu-se um dos mais secretos programas dentro do governo dos EUA, o *Olympic Games* (Sanger 2012, 188-225), o qual possui dois objetivos políticos: sabotar, ainda que temporariamente, o programa nuclear iraniano e convencer Israel de que há uma maneira mais eficaz e menos custosa de lidar com o problema nuclear iraniano do que lançar ataques aéreos (Sanger 2012, *passim*). Em tese, o projeto se mostrou eficaz, mas, na prática, não havia garantias de que *de facto* funcionasse. Mesmo assim, Washington e Tel Aviv consideraram essa a melhor opção (Sanger 2012, 190-193).¹⁰⁰

É importante observar que um vírus capaz de infectar instalações nucleares sem ser detectado, bem como causar danos estruturais que ultrapassam os limites do espaço digital, apresenta claras características do que pode ser entendido como “weaponização” dos aparatos digitais. O Stuxnet poderia ter sido o grande trunfo nas operações de contenção do programa nuclear iraniano, contudo, como um vírus biológico, sua contenção acabou por fugir da alçada de seus desenvolvedores, uma vez solto, foi possível identificá-lo:

Nesse contexto, surgiu o que ficou conhecido depois por Stuxnet, um verme de computador (*worm*) utilizado como arma cibernética, cujos alvos são as centrífugas para enriquecimento de urânio, situadas em Natanz (Clarke e Knake 2012, 291-294; Foltz 2012, 44). O objetivo dos engenheiros especialistas em computação e física nuclear, dos EUA e de Israel, era explorar a vulnerabilidade das máquinas iranianas mapeadas pelos informantes israelenses. A intenção era fazer com que as centrífugas parassem de funcionar, de modo a parecer acidental, e que os engenheiros iranianos não desconfiassem imediatamente que estariam sob ataques cibernéticos. O Stuxnet seria introduzido no sistema computacional em Natanz, fazendo com que elas funcionassem de maneira inesperada, até quebrar. Com sorte, para EUA e Israel, parte dessas infraestruturas explodiriam e os iranianos demorariam a descobrir a origem do problema (Clarke e Knake 2012, 291, 295; Sanger 2012, 189).

Em 2010, o *worm* se comportou de maneira inesperada – espalhando-se para além de Natanz –, quando foi identificado e divulgado por especialistas em computação. A partir daí, o Stuxnet foi “capturado” por especialistas, os quais o perceberam como um sofisticado instrumento para proferir ataques em rede a ser direcionado a outros alvos (Clarke e Knake 2012, 296).¹⁰¹

A capacidade do vírus em se espalhar e contaminar computadores desconectados da rede mundial de computadores (internet), demonstra o poder destrutivo dessa ferramenta enquanto arma, especialmente quando levamos em considerações que boa parte da infraestrutura crítica

⁹⁹ BRASIL. Congresso Nacional. Senado Federal. Comissão de Relações Exteriores e Defesa Nacional. Rumos da política externa brasileira: temas da agenda internacional, política externa brasileira. Brasília: Senado Federal, 2012, p. 114

¹⁰⁰ LOPES, Gills; OLIVEIRA de, Carolina Fernanda Jost. Stuxnet e defesa cibernética estadunidense à luz da análise de política externa. Ver. Bra. Est. Def. ano 1, jul./dez., pp 55 – 69. p 60.

¹⁰¹ *Ibidem*. P. 60 – 61

dos Estados, hoje, é dependente de hardwares, com suas funcionalidades todas atreladas à softwares, controlando cada pequena operação. O desenvolvimento de tal ferramenta, segunda especialistas, demandaria uma equipe treinada, com capacidade de operar no desenvolvimento em tempo integral, especialmente em razão das particularidades do Stuxnet:

É difícil, se não impossível, saber exatamente como o malware foi desenvolvido, mas não há dúvida de que seu desenvolvimento exigiu recursos consideráveis em mão de obra, tempo e finanças. Especialistas avaliando o desenvolvimento do worm estimam que deve ter exigido uma equipe de cinco a dez programadores trabalhando em tempo integral por pelo menos seis meses.¹⁰²

Ainda nesta linha, mister desvelar as características do vírus para melhor compreender sua sofisticação, visto que, um *malware* que explora o que é conhecido como “*0-day exploit*”, ou “vulnerabilidade 0-day”, que significaria a exploração de uma falha que ainda não é conhecida, dificultando sua identificação e posterior resolução:

O Stuxnet tem tamanho considerável – maior do que worms comparáveis – e foi escrito em várias linguagens de programação diferentes com alguns componentes criptografados (Chen, 2010, p. 3). Ele explorou não uma, mas quatro vulnerabilidades de dia zero para infectar computadores: um processo automático de unidades USB conectadas, uma conexão com impressoras compartilhadas e duas outras vulnerabilidades relacionadas ao escalonamento de privilégios. Este último é um processo de computador que permitiu que o worm executasse software em computadores mesmo quando eles estavam bloqueados (Naraine, 2010). O Stuxnet procurou infectar computadores que executam o sistema operacional Microsoft Windows por meio de um desses vetores. Quando identificou uma abertura, usou certificados de driver válidos, mas roubados, da RealTek e JMicron para baixar seu rootkit. Usando esses certificados de driver, o worm foi capaz de procurar o software Siemens Simatic WinCC/Step-7, um programa usado para controlar equipamentos industriais (Falliere et al., 2011, p. 33; Matrosov et al., 2010, p. 68). Ao infectar os arquivos utilizados por esse software, o worm conseguiu acessar e controlar os Controladores Lógicos Programáveis (CLPs), ou seja, pequenos computadores usados para regular a energia em dispositivos industriais (De Falco, 2012, p. 6). Além disso, o worm também foi capaz de se comunicar com outras máquinas infectadas e servidores C&C na Dinamarca e Malásia para se atualizar e transmitir informações sobre o que havia encontrado (Chen e Abu-Nimeh, 2011, p. 93).¹⁰³

¹⁰² BAEZNER, Marie; ROBIN, Patrice: Hotspot Analysis: Stuxnet, October 2017, Center for Security Studies (CSS), ETH Zürich. p. 7. Tradução livre de: “It is difficult, if not impossible, to know exactly how the malware was developed, but there can be no doubt that its development required considerable resources in manpower, time and finance. Specialists evaluating the development of the worm estimate it must have required a team of five to ten programmers working full-time for at least six months.”

¹⁰³ *Ibidem*. p. 7. Tradução livre de: “Stuxnet is sizeable – larger than comparable worms – and it was written in several different programming languages with some encrypted components (Chen, 2010, p. 3). It exploited not one but four zero-day vulnerabilities to infect computers: an automatic process from connected USB drives, a connection with shared printers, and two other vulnerabilities concerning privilege escalation. The latter is a computer process that allowed the worm to execute software in computers even when they were on lock-down (Naraine, 2010). Stuxnet looked to infect computers running the Microsoft Windows operating system via one of these vectors. When it identified an opening, it used valid, but stolen, driver certificates from RealTek and JMicron to download its rootkit. Using these driver certificates, the worm was then able to search for the Siemens Simatic WinCC/Step-7 software, a program used to control industrial equipment (Falliere et al., 2011, p. 33; Matrosov et al., 2010, p. 68). By infecting files used by this software, the worm was able to access and control the Programmable Logic Controllers (PLCs), i.e. small computers used to regulate power in industrial devices (De Falco, 2012, p. 6). Furthermore, the worm was also able to communicate with other infected machines and C&C servers in Denmark and Malaysia in order to update itself and transmit information about what it had found (Chen and Abu-Nimeh, 2011, p. 93).”

É, contudo, a capacidade de dano no mundo real causada pelo *Stuxnet* que merece atenção. Semelhante ao caso do *Titan Rain*, a extensão dos ataques e danos, não é conhecida na integralidade, contudo, existem dados suficientes quanto aos danos causados à centrífugas de enriquecimento de urânio iranianas, ainda que o ataque não tenha resultado no término em definitivo como seus possíveis criadores haviam imaginado, foi possível mensurar danos reais ao programa:

O efeito físico mais direto e único do Stuxnet foi o dano causado às centrífugas. Acreditava-se que o malware, que foi claramente projetado para afetar a instalação nuclear em Natanz, afetava a velocidade das centrífugas, fazendo com que alternassem entre velocidades altas e baixas (Farwell e Rohozinski, 2011, pp. 24–25). Essa mudança de velocidade foi mascarada pelo rootkit do worm, fazendo com que os operadores acreditassem que as centrífugas estavam operando em sua velocidade normal. A mudança de velocidade faria com que as centrífugas se desgastassem mais rapidamente e sofressem danos irreparáveis. Natanz tinha entre 6.000 e 9.000 centrífugas em operação na época, das quais cerca de 1.000 precisavam ser substituídas (De Falco, 2012, p. 23; Nakashima e Warrick, 2012). Especialistas da AIEA avaliando as plantas notaram que o Irã substituiu cerca de 10% de suas centrífugas a cada ano devido a quebras, mas trocou um pouco mais de centrífugas do que o habitual entre meados de 2009 e meados de 2010 (Nakashima e Warrick, 2012). O ISIS informou que o nível de produção de urânio de baixo enriquecimento permaneceu estável e até aumentou durante o período do ataque do Stuxnet. No entanto, os níveis de produção foram menos eficientes, pois poderiam ter sido com centrífugas em pleno funcionamento. Em outras palavras, a produção de urânio de baixo enriquecimento só aumentou devido aos ciclos de trabalho acelerados para compensar a perda das centrífugas danificadas. Mesmo em fevereiro de 2010, os níveis de produção ainda eram mais baixos do que antes do ataque em novembro de 2009. O Irã levou aproximadamente um ano para se recuperar totalmente dos efeitos do ataque Stuxnet e retornar a um nível de produção comparável ao de novembro de 2009.¹⁰⁴

Ainda que o dano às centrífugas não aparente ter sido significativo, é inegável que o mesmo tem extensões assustadoras, levando em consideração que ao menos 1 ano de produção foi afetado, pela ação de uma ferramenta de computador, comparativamente, do tamanho de um organismo unicelular, sendo “operado” a milhares de quilômetros de distância. É importante salientar, como apresentado na citação supracitada, que possivelmente os danos teriam sido

¹⁰⁴ *Ibidem*. p. 10. Tradução livre de: “The most direct and only physical effect of Stuxnet was the damage caused to the centrifuges. The malware, which was clearly designed to affect the nuclear facility in Natanz, was believed to affect the speed of the centrifuges, causing them to alternate between high and low speeds (Farwell and Rohozinski, 2011, pp. 24–25). This change in speed was masked by the worm’s rootkit, making the operators believe that the centrifuges were operating at their normal speed. The change of speed would have caused the centrifuges to wear out faster and suffer damage beyond repair. Natanz had between 6,000 and 9,000 operating centrifuges at the time, about 1,000 of which needed to be replaced (De Falco, 2012, p. 23; Nakashima and Warrick, 2012). IAEA experts assessing the plants noted that Iran replaced about 10% of its centrifuges each year due to breakage, but exchanged slightly more centrifuges than usual between mid-2009 and mid-2010 (Nakashima and Warrick, 2012). ISIS reported that the level of production of low enriched uranium remained steady and even increased during the period of the Stuxnet attack. However, production levels were less efficient as they could have been with fully working centrifuges. In other words, the output of low enriched uranium only increased because of accelerated working cycles to compensate for the loss of the damaged centrifuges. Even by February 2010, production levels were still lower than before the attack in November 2009. It took Iran approximately one year to recover fully from the effects of the Stuxnet attack and to return to a level of production comparable to November 2009.”

consideravelmente maiores, caso o vírus não tivesse se espalhado e conseqüentemente sido detectado.

Ainda nessa linha, existem relatos divergentes quanto ao *Stuxnet*, contendo especulações de danos causados pelo vírus, muito mais significativos que os ao Irã, contudo, empresas de segurança da informação desconsideraram tal possibilidade à época. A este respeito, é necessário levar em consideração que “armas cibernéticas” existem em uma zona cinzenta de operacionalização e oportunidade, desta feita, especulações merecem a devida análise e atenção, especialmente em razão da possibilidade de veracidade das mesmas:

Em outubro de 2012, o secretário de Defesa dos EUA, Leon Panetta, alertou que os Estados Unidos eram vulneráveis a um “ciber Pearl Harbor” que poderia descarrilar trens, envenenar o abastecimento de água e danificar as redes elétricas. No mês seguinte, a Chevron confirmou a especulação ao se tornar a primeira corporação dos EUA a admitir que o *Stuxnet* havia se espalhado por suas máquinas. Isso pode possivelmente negar o envolvimento dos EUA nesta guerra cibernética. Segundo algumas fontes, o *Stuxnet* é o motivo do naufrágio da *Deepwater Horizon* e causa do derramamento de óleo mexicano. Mas especialistas em segurança como F-Secure e Kaspersky Lab negam tais possibilidades.¹⁰⁵

Possivelmente em razão da velocidade em que o vírus foi descoberto, bem como da rápida resposta e do relativo baixo resultado operacional, outros vírus foram desenvolvidos tendo o *Stuxnet* como base, todos com a finalidade de causar danos a infraestruturas críticas, a alvos estratégicos e todos explorando vulnerabilidade de dia 0. Nesta linha, foram desenvolvidos o *Duqu*, *Flame* e *Shamoon*:

Em outubro de 2011, um malware com semelhanças com o *Stuxnet* conhecido como *Duqu* foi descoberto. *Duqu* criou backdoors que poderiam ser explorados para destruir a rede em um momento arbitrário e também tinha um keylogger embutido nele. Uma vulnerabilidade de dia zero foi explorada para distribuir o trojan *Duqu*. Um mês depois, o Irã admitiu que suas instalações nucleares haviam sido atingidas pelo *Duqu*. Em dezembro de 2011, ataques cibernéticos à empresa ferroviária *Northwest* interromperam os sinais ferroviários por dois dias.

Em maio de 2012, o malware *Flame* supostamente criado por Israel e pelos EUA, com o objetivo de diminuir a capacidade do Irã de desenvolver uma arma nuclear, foi descoberto. O *Flame* explorou bugs existentes e uma vulnerabilidade de dia zero no sistema operacional *Windows* para infectar sistemas no Irã, Líbano, Síria, Sudão, territórios ocupados por Israel e outros países do Oriente Médio e Norte da África há dois anos. Em agosto de 2012, o produtor de petróleo *Saudi Aramco* foi alvo do malware *Shamoon* para interromper a produção de petróleo. O malware infectou 30.000 estações de trabalho sem interromper nenhuma produção. “*Cutting Sword of Justice*” reivindicou a responsabilidade pelo ataque, embora tenha sido atribuído a um ator desconhecido de estado-nação.

Em maio de 2013, foi revelado que o acesso não autorizado aos bancos de dados do Inventário Nacional de Barragens permitiu que invasores colocassem as mãos em informações confidenciais. No mesmo mês, Israel declarou que havia evitado

¹⁰⁵ RAO, Siddharth Prakash. *Stuxnet, A new Cyberwar weapon: Analysis from a technical point of view*. Technical Report. May. 2014. Aalto University. 2014. P. 3. Tradução livre de: “In October 2012, U.S. defense secretary Leon Panetta warned that the United States was vulnerable to a “cyber Pearl Harbor” that could derail trains, poison water supplies, and cripple power grids. The next month, Chevron confirmed the speculation by becoming the first U.S. Corporation to admit that *Stuxnet* had spread across its machines. This might possibly deny the involvement of USA in this cyberwar. According to some sources *Stuxnet* is the reason for sink of *Deepwater Horizon* and cause the Mexican oil spill. But security experts like F-Secure, Kaspersky Lab deny such possibilities.”

ciberataques do Exército Eletrônico Sírio visando computadores do sistema de águas para a cidade de Haifa.¹⁰⁶

Semelhante ao seu antecessor, o *Duqu*, resultou em danos no mundo real, ainda que não tão sérios, é importante lembrar o temor do Secretário de Defesa Americano Leon Panetta, sobre um possível Pearl Harbor cibernético, a capacidade de adentrar e desabilitar o um sistema ferroviário por determinado período pode parecer pequeno, perto de danos à centrífugas nucleares, contudo, a possibilidade destrutiva de ambos é semelhante. Basta imaginar a possibilidade de modificar a trajetória de trilhos e o conseqüente choque de locomotivas, causando danos econômicos consideráveis e, ou, ceifar vidas.

É mediante ataques como o do *Stuxnet* e seus sucessores que demonstram a capacidade de operações cibernéticas, especialmente porque mediante estas, efeitos no mundo real podem ser sentidos, ataques como o sofrido pelo Irã, muito se assemelham aos sofridos pela Estônia, neste sentido, é preciso imaginar quais as possíveis repercussões de se manter o espaço digital, desregulado no campo do Direito da Guerra.

¹⁰⁶ VAIDYA, Tavish. 2001-2013: Survey and Analysis of Major Cyberattacks. Georgetown University. 1 Sep. 2015. P. 8-9. Tradução livre de: "In October 2011, a malware with similarities to Stuxnet known as Duqu was discovered. Duqu created back doors which could be exploited to destroy the network at an arbitrary time and also had a keylogger built in to it. A zero-day vulnerability was exploited to distribute Duqu trojan. A month later, Iran admitted that its nuclear sites had been hit by Duqu. In December 2011, cyberattacks on Northwest rail company disrupted railway signals for two days. In May 2012, Flame malware allegedly created by Israel and the US, aimed at slowing down Iran's ability to develop a nuclear weapon was discovered. Flame exploited existing bugs and a zero-day vulnerability in Windows operating system to infect systems in Iran, Lebanon, Syria, Sudan, the Israeli Occupied Territories and other countries in the Middle East and North Africa two years ago. In August 2012, oil producer Saudi Aramco was targeted with Shamoon malware to disrupt oil production. The malware infected 30,000 workstations without disrupting any production. Cutting Sword of Justice claimed responsibility for the attack, though it was attributed to unknown nation-state actor. In May 2013, it was revealed that unauthorized access to databases of National Inventory of Dams allowed attackers to get their hands on sensitive information. In the same month, Israel stated that it had prevented cyberattacks from Syrian Electronic Army targeting computers of water systems for city of Haifa."

1.3 – GUERRAS HÍBRIDAS E GUERRAS OMNIDIMENSIONAIS NO CONTEXTO DE GUERRA NO CIBERESPAÇO

Nesta seção nos importa contextualizar a inserção da lógica das operações cibernéticas à lógica da guerra. Como havíamos trabalhado anteriormente, na primeira seção deste capítulo, a evolução na conceituação dos conflitos pode ser dividida em 4 (quatro) gerações, sendo a 4ª geração a correspondente ao que entendemos como guerras híbridas, guerras não convencionais, guerras irregulares e, até certa medida, as guerras omnidimensionais.

É neste contexto em que se inserem as guerras operacionalizadas no ciberespaço, conflitos que se expandiram para um novo teatro de operações, a transmutação da guerra cinética para a guerra cibernética. Contudo, é importante ressaltar que esse salto não pressupõe um abandono ou uma “superação” do que entendíamos como guerras clássicas, com as características das demais gerações das guerras, tampouco com o fim da cinética, aqui, o que apresenta-se é a plena sinergia das várias dimensões dos teatros de operação, é a ação conjunta da cinética e da cibernética, da ação e da dissuasão, da simetria e da assimetria.

As Guerras Híbridas passaram a ser um conceito em disputa, sua definição, ainda que variada, tanto no espectro temporal quando geográfico, parece se assemelhar, ao menos em *ultima ratio*. A esse respeito, vamos trabalhar uma visão ocidental e uma oriental da temática, ainda que muito semelhantes, a temporalidade parece ter permitido um aperfeiçoamento conceitual.

Em 2010, o Escritório de Responsabilidade do Governo dos Estados Unidos (United States Government Accountability Office), emitiu um relatório¹⁰⁷ destrinchando o entendimento do Departamento de Defesa dos Estados Unidos, quanto ao termo (e seu emprego), das Guerras Híbridas, no entendimento americano, baseado tanto em pareceres emitidos pelos departamentos, órgãos e secretarias responsáveis, quanto pelas manifestações das autoridades competentes junto ao Congresso Nacional Americano, os EUA parecem divergir internamente quanto ao termo.

o De acordo com oficiais da Força Aérea, a guerra híbrida é mais potente e complexa do que a guerra irregular devido ao aumento do ritmo, complexidade, diversidade e orquestração através das fronteiras nacionais, que são todos exacerbados pela facilidade com os quais os adversários podem se comunicar, acessar recursos internacionais e financiamento e adquirir armamento mais letal e sofisticado.

¹⁰⁷ U.S. Government Accountability Office, 2010. Hybrid Warfare Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives, 10 de setembro de 2010. United States Government Accountability Office, Washington, DC. Acessado em: 12/12/2021, disponível em: < <https://www.gao.gov/assets/gao-10-1036r.pdf> >.

o Oficiais do Comando de Operações Especiais afirmaram que a guerra híbrida não é diferente das atuais formas doutrinárias de guerra empregadas em todo o espectro de conflito.

o Oficiais da Marinha afirmaram que híbrido é sinônimo de espectro completo e abrange tanto a guerra convencional quanto a guerra não convencional.

o Os oficiais do Corpo de Fuzileiros Navais usam o termo “híbrido” para descrever a ameaça potencial apresentados por atores estatais e não estatais e acreditam que a guerra híbrida não é uma nova forma de guerra; em vez disso, é sinônimo de conflito de espectro total e já é devidamente contemplado na doutrina atual.¹⁰⁸

Nessa mesma linha, o relatório buscou agregar um (ainda que pequeno), compilado de definições não oficiais do conceito em trabalhos acadêmicos:

Guerra Híbrida—Conflito executado por ameaças estatais e/ou não-estatais que emprega vários modos de guerra para incluir capacidades convencionais, táticas irregulares e desordem criminal. (Comando das Forças Conjuntas dos EUA, comunicado do Centro Conjunto para Análise Operacional sobre “Adaptação Conjunta à Guerra Híbrida”)

Ameaça Híbrida—Um adversário que emprega simultaneamente e de forma adaptativa alguma combinação fundida de (1) meios políticos, militares, econômicos, sociais e de informação e (2) métodos convencionais, irregulares, terroristas e de conflito disruptivo/criminoso. Pode incluir uma combinação de atores estatais e não estatais. (Definição de trabalho derivada do Comando das Forças Conjuntas dos EUA, Centro de Guerra Irregular Conjunta, 2008-2009)

Ameaça Híbrida—Uma ameaça que emprega simultaneamente forças regulares e irregulares, incluindo elementos terroristas e criminosos para atingir seus objetivos usando uma variedade em constante mudança de táticas convencionais e não convencionais para criar múltiplos dilemas. (Ambiente Operacional do Comando de Treinamento e Doutrina do Exército dos EUA, 2009-2025)

Ameaças híbridas—Ameaças que incorporam uma gama completa de diferentes modos de guerra, incluindo capacidades convencionais, táticas e formações irregulares, atos terroristas, incluindo violência e coerção indiscriminadas, e desordem criminal, conduzidas por ambos os estados e uma variedade de atores não estatais.¹⁰⁹

Fica claro por essas definições, que a ideia central é de que as Guerras Híbridas compreenderiam a lógica das guerras convencionais com as guerras irregulares, ainda que, para

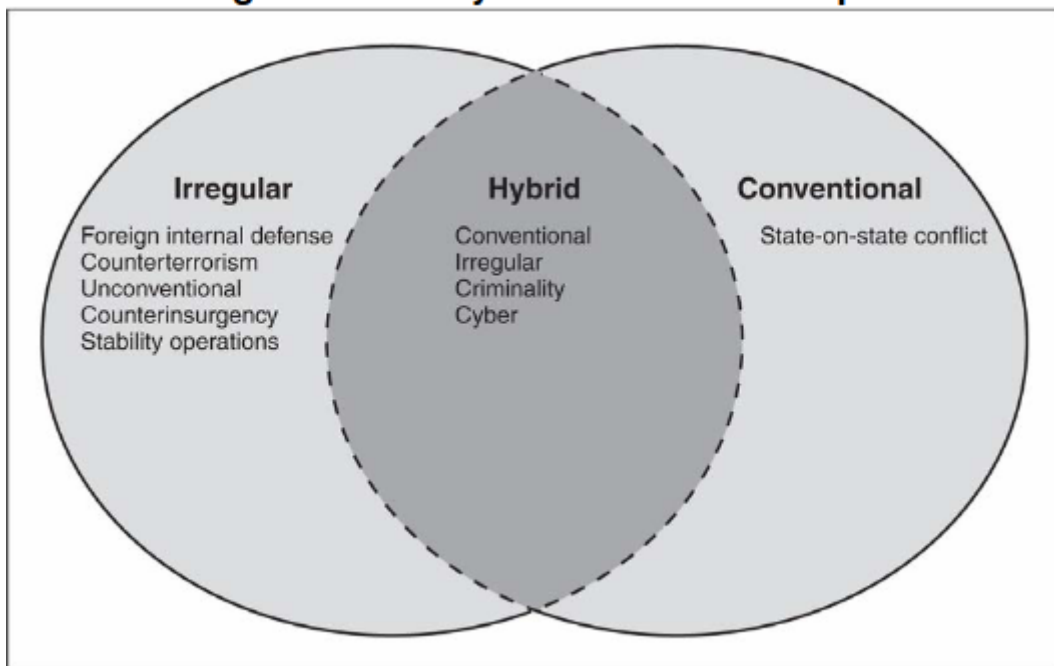
¹⁰⁸ *Ibidem*. p. 17. Tradução livre de: “o According to Air Force officials, hybrid warfare is more potent and complex than irregular warfare due to increased tempo, complexity, diversity, and wider orchestration across national borders, which are all exacerbated by the ease with which adversaries can communicate, access international resources and funding, and acquire more lethal and sophisticated weaponry. o Special Operations Command officials stated that hybrid warfare is no different from current doctrinal forms of warfare employed across the spectrum of conflict. o Navy officials stated that hybrid is synonymous with full spectrum and encompasses both conventional warfare and unconventional warfare. o Marine Corps officials use the term “hybrid” to describe the potential threat posed by both state and non-state actors and believe that hybrid warfare is not a new form of warfare; rather it is synonymous with full spectrum conflict and is already adequately covered in current doctrine.”

¹⁰⁹ *Ibidem*. p. 18. Tradução livre de: “Hybrid Warfare—Conflict executed by either state and/or non-state threats that employs multiple modes of warfare to include conventional capabilities, irregular tactics, and criminal disorder. (U.S. Joint Forces Command, Joint Center for Operational Analysis briefing on “Joint Adaptation to Hybrid War”) Hybrid Threat—An adversary that simultaneously and adaptively employs some fused combination of (1) political, military, economic, social and information means and (2) conventional, irregular, terrorism and disruptive/criminal conflict methods. It may include a combination of state and non-state actors. (Working definition derived by U.S. Joint Forces Command, Joint Irregular Warfare Center, 2008-2009) Hybrid Threat—A threat that simultaneously employs regular and irregular forces, including terrorist and criminal elements to achieve their objectives using an ever-changing variety of conventional and unconventional tactics to create multiple dilemmas. (U.S. Army Training and Doctrine Command’s Operational Environment, 2009-2025) Hybrid Threats—Threats that incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder, conducted by both states and a variety of non-state actors.”

boa parcela dos levantamentos realizados pelo Documento, o entendimento é de que o conceito não possui uma definição clara, bem como não careceria, igualmente, de tal definição, estando muito mais atrelado ao risco e, ou, complexidade operacional, do que realmente uma nova lógica de guerra, na mesma linha, o termo vincula-se a ideia de práticas já historicamente consolidadas.

Por fim, o documento traz uma representação figurativa, com base nos levantamentos dos documentos oficiais e dos estudos acadêmicos analisados, que parece bastante explicativa:

Figure 2: The Hybrid Warfare Concept



Source: GAO analysis of DOD military concept and briefing documents and academic writings.

110

Como o próprio nome sugere, as guerras híbridas seriam a junção de práticas tanto das guerras convencionais quanto das irregulares, aqui, particularmente, nos interessa o aspecto “Cyber” trazido na figura, exatamente por compreender uma problemática, visto que o mesmo não está presente, nem no espectro irregular, nem no convencional. Seriam então as operações cibernéticas no contexto dos conflitos uma prática da guerra irregular ou convencional?

A ideia do campo digital assume particularidade às guerras híbridas, não que ela se limite a tal, contudo, se a mesma estivesse vinculada às guerras regulares, o problema de sua regulamentação e sua delimitação no campo do Direito Internacional estaria pacificado, se fosse uma prática restrita ao campo da guerra irregular, não se configuraria enquanto campo de oportunidade operacional em conflitos Estado contra Estado, desta feita, restando enquanto

¹¹⁰ *Ibidem.* p. 16.

campo de operação das guerras híbridas, as operações cibernéticas podem ser oportunizadas por agentes estatais, enquanto ações legítimas.

É sob esse prisma que a problemática foi alvo de discussão em 2014, pela OTAN, em documento oficial, dispondo tanto sobre questões pertinentes ao conceito de Guerras Híbridas, quanto acerca das operações e segurança cibernética de seus membros:

13. Garantiremos que a OTAN seja capaz de enfrentar com eficácia os desafios específicos colocados pelas ameaças de guerra híbrida, em que uma ampla gama de medidas militares, paramilitares e civis abertas e secretas são empregadas em um projeto altamente integrado. É essencial que a Aliança possua as ferramentas e procedimentos necessários para dissuadir e responder eficazmente às ameaças de guerra híbrida e as capacidades para reforçar as forças nacionais. Tal incluirá também o reforço das comunicações estratégicas, o desenvolvimento de cenários de exercício à luz das ameaças híbridas e o reforço da coordenação entre a OTAN e outras organizações, em conformidade com as decisões relevantes tomadas, com vista a melhorar a partilha de informações, consultas políticas e a comunicação entre funcionários coordenação. Congratulamo-nos com o estabelecimento do Centro de Excelência de Comunicações Estratégicas acreditado pela OTAN na Letônia como uma contribuição significativa para os esforços da OTAN nesta área. Encarregamos o trabalho de guerra híbrida a ser revisto juntamente com a implementação do Plano de Ação de Prontidão.

[...]

104. Aguardamos com expectativa o diálogo e a cooperação contínuos entre a OTAN e a UE. Nossas consultas se ampliaram para abordar questões de interesse comum, incluindo desafios de segurança como defesa cibernética, proliferação de armas de destruição em massa, combate ao terrorismo e segurança energética. Também buscaremos trabalhar mais de perto em várias outras áreas, incluindo segurança marítima, defesa e capacitação de segurança relacionada, e abordando ameaças híbridas, de acordo com as decisões tomadas.¹¹¹

Aqui, muito semelhante ao abordados pelos Americanos, a OTAN entende as guerras híbridas como a congregação de operações típicas das guerras convencionais e não convencionais, com particular preocupação e relação as ameaças híbridas, vale destacar ainda a temporalidade do documento, em período posterior aos ataques cibernéticos à Estônia, ataque que poderia, muito bem, estar enquadrado a sistemática das guerras híbridas.

¹¹¹ NATO, 2014. North Atlantic Treaty Organization. Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. Acessado em: 12/12/2021. Disponível em: < https://www.nato.int/cps/en/natohq/official_texts_112964.htm >. Tradução livre de: “13. We will ensure that NATO is able to effectively address the specific challenges posed by hybrid warfare threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design. It is essential that the Alliance possesses the necessary tools and procedures required to deter and respond effectively to hybrid warfare threats, and the capabilities to reinforce national forces. This will also include enhancing strategic communications, developing exercise scenarios in light of hybrid threats, and strengthening coordination between NATO and other organisations, in line with relevant decisions taken, with a view to improving information sharing, political consultations, and staff-to-staff coordination. We welcome the establishment of the NATO-accredited Strategic Communications Centre of Excellence in Latvia as a meaningful contribution to NATO's efforts in this area. We have tasked the work on hybrid warfare to be reviewed alongside the implementation of the Readiness Action Plan.[...] 104. We look forward to continued dialogue and cooperation between NATO and the EU. Our consultations have broadened to address issues of common concern, including security challenges like cyber defence, the proliferation of weapons of mass destruction, counter-terrorism, and energy security. We will also seek to work more closely together in several other areas, including maritime security, defence and related security capacity building, and addressing hybrid threats, in line with decisions taken.”

Não por outra razão, o documento se preocupa em expandir a questão cibernética em sede das intenções da OTAN, particularmente em solo Europeu:

72. À medida que a Aliança olha para o futuro, as ameaças e ataques cibernéticos continuarão a se tornar mais comuns, sofisticados e potencialmente prejudiciais. Para enfrentar esse desafio em evolução, endossamos uma Política de Defesa Cibernética Aprimorada, contribuindo para o cumprimento das principais tarefas da Aliança. A política reafirma os princípios da indivisibilidade da segurança aliada e da prevenção, detecção, resiliência, recuperação e defesa. Recorda que a responsabilidade fundamental da defesa cibernética da OTAN é defender as suas próprias redes, e que a assistência aos Aliados deve ser abordada de acordo com o espírito de solidariedade, enfatizando a responsabilidade dos Aliados em desenvolver as capacidades relevantes para a proteção das redes nacionais. Nossa política também reconhece que o direito internacional, incluindo o direito internacional humanitário e a Carta da ONU, se aplica ao ciberespaço. Os ataques cibernéticos podem atingir um limite que ameaça a prosperidade, a segurança e a estabilidade nacionais e euro-atlânticas. Seu impacto pode ser tão prejudicial às sociedades modernas quanto um ataque convencional. Afirmamos, portanto, que a defesa cibernética faz parte da tarefa central de defesa coletiva da OTAN. Uma decisão sobre quando um ataque cibernético levaria à invocação do Artigo 5 seria tomada pelo Conselho do Atlântico Norte caso a caso.

73. Estamos empenhados em desenvolver ainda mais as nossas capacidades nacionais de defesa cibernética e reforçaremos a segurança cibernética das redes nacionais das quais a OTAN depende para as suas tarefas principais, a fim de ajudar a tornar a Aliança resiliente e totalmente protegida. A estreita cooperação bilateral e multinacional desempenha um papel fundamental no aprimoramento das capacidades de defesa cibernética da Aliança. Continuaremos a integrar a defesa cibernética nas operações da OTAN e no planejamento operacional e de contingência, e aumentaremos o compartilhamento de informações e a conscientização situacional entre os Aliados. Parcerias fortes desempenham um papel fundamental na abordagem de ameaças e riscos cibernéticos. Continuaremos, portanto, a nos envolver ativamente em questões cibernéticas com nações parceiras relevantes caso a caso e com outras organizações internacionais, incluindo a UE, conforme acordado, e intensificaremos nossa cooperação com a indústria por meio de uma parceria cibernética da indústria da OTAN. As inovações tecnológicas e a experiência do setor privado são cruciais para permitir que a OTAN e os Aliados alcancem os objetivos da Política de Defesa Cibernética Aprimorada. Melhoraremos o nível das atividades de educação, treinamento e exercícios de defesa cibernética da OTAN. Desenvolveremos a capacidade de alcance cibernético da OTAN, baseando-nos, como primeiro passo, na capacidade de alcance cibernético da Estônia, levando em consideração as capacidades e os requisitos da Escola CIS da OTAN e de outros órgãos de treinamento e educação da OTAN.¹¹²

¹¹² *Ibidem*. Tradução livre de: 72 As the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, we have endorsed an Enhanced Cyber Defence Policy, contributing to the fulfillment of the Alliance's core tasks. The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. It recalls that the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks. Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis. 73 We are committed to developing further our national cyber defence capabilities, and we will enhance the cyber security of national networks upon which NATO depends for its core tasks, in order to help make the Alliance resilient and fully protected. Close bilateral and multinational cooperation plays a key role in enhancing the cyber defence capabilities of the Alliance. We will continue to integrate cyber defence into NATO operations and operational and contingency planning, and enhance information sharing and situational awareness among Allies. Strong partnerships play a key role in addressing cyber threats and risks. We will therefore continue to engage actively

As Guerras Híbridas acabam por operacionalizar pelos Estados todos os métodos típicos das guerras não convencionais. Ações e tratativas de desestabilização, de mudanças de regime, de suporte a insurreições, acabam assumindo um espaço de tática e prática militar estatal, operada em boa medida por agentes externos (para estatais), ainda que operacionalizada por agentes estatais. A desestabilização política, econômica e a erosão estrutural, passam a ser partes do teatro de guerra, para além da conquista de objetivos estratégicos, a conquista de “mentes e corações” passa a ser objeto militar, ainda que para tal, seja necessário o emprego de métodos não tradicionais.

A guerra no Século XXI acontece no campo da cultura, através dos oligopólios, em escala planetária de um sistema de comunicação dirigido a partir dos centros mundiais de poder, interferindo e alterando matrizes e elementos de identificação cultural brasileiros.

O conceito de defesa cultural, como nos propomos a refletir, visando a uma atualização da Política Nacional de Defesa, necessariamente há de incorporar a ideia de soberania cultural, visto ser ela o alvo prioritário das ações ofensivas de diatética cultural, com foco no estímulo e criação de falsas contradições no seio da sociedade, objetivando a criação artificial de cisões e fragmentações, notadamente através de instrumentos próprios de guerra psicológica, os quais objetivam fragilizar a soberania cultural de determinado país.¹¹³

Essa, como já mencionada, não é uma perspectiva nova, contudo, é uma estratégia estatal nova, a constrição causada pela normativa, parece ter levado os Estados a adotar a Guerra Híbrida enquanto novo *modus operandi*, visto que, como bem abordou o Major Hugo Miguel Moutinho Fernandes, do exército português:

Nas guerras híbridas, um dos principais objetivos é destabilizar os governos oponentes e as suas instituições, criando o caos e um vazio de poder. (Blum, et al., 2015).

Através de um documento do European External Action Service (Countering hybrid threats, food-for-thought paper), de maio de 2015, a UE caracterizou a guerra híbrida como o uso centralmente concebido e controlado de várias táticas encobertas e abertas, decretadas por meios militares e não-militares, que vão desde operações de informações e cibernéticas através de pressão econômica para o uso de forças convencionais (European External Action Service, 2015, p. 2).

Apesar de o conceito não ser consensual e novo, e de não enfrentarmos um alargamento do número de desafios distintos, eles convergem para uma nova maneira de fazer a guerra. Estas guerras híbridas misturam a letalidade do conflito de Estado com o fervor fanático e prolongado da guerra irregular.¹¹⁴

on cyber issues with relevant partner nations on a case-by-case basis and with other international organisations, including the EU, as agreed, and will intensify our cooperation with industry through a NATO Industry Cyber Partnership. Technological innovations and expertise from the private sector are crucial to enable NATO and Allies to achieve the Enhanced Cyber Defence Policy's objectives. We will improve the level of NATO's cyber defence education, training, and exercise activities. We will develop the NATO cyber range capability, building, as a first step, on the Estonian cyber range capability, while taking into consideration the capabilities and requirements of the NATO CIS School and other NATO training and education bodies.”

¹¹³ CARDOSO, Paulo Roberto. *Diatética Cultural: Estado, soberania e defesa cultural*. Belo Horizonte: Universidade Federal de Minas Gerais, 2016, p. 108. (Tese, Doutorado em Direito).

¹¹⁴ Fernandes, H., 2016. As Novas Guerras: O Desafio da Guerra Híbrida. Revista de Ciências Militares, novembro de 2016 IV (2), pp. 13-40. p. 22. Acessado em: 12/12/2021. Disponível em: < <http://www.iesm.pt/cisdi/index.php/publicacoes/revista-de-ciencias-militares/edicoes> >

Comumente empregada por forças não estatais, agora a guerra irregular, ou guerra não convencional se transformou em tática militar estatal, para tanto, é importante conceituarmos essa visão, visto que, é parte integral utilizada por Korybko, autor que melhor caracterizou as Guerras Híbridas enquanto teoria:

A guerra irregular é a forma mais antiga de se combater e, desde meados do século passado, também, a mais usual. [...] Terrorismo, guerrilha, insurreição, movimento de resistência, combate não convencional e conflito assimétrico, por exemplo, são alguns dos conceitos ou práticas abarcados pelo conjunto de ideias, mais amplo e muito pouco compreendido, denominado guerra irregular¹¹⁵

Já segundo Korybko, a Guerra Não Convencional, na forma abordada em sua obra, possui uma definição menos abrangente, cabendo ainda uma pequena ressalva, visto que, o autor, tangenciou sua análise acerca das práticas americanas, muitas vezes adotando conceitos mais restritivo, muitas vezes soando de forma parcial, sem, contudo, que isso causa demérito ao aperfeiçoamento trazido ao conceito:

A Guerra Não Convencional é definida neste livro como qualquer tipo de força não convencional (isto é, grupos armados não oficiais) envolvida em um combate largamente assimétrico contra um adversário tradicional. Se consideradas em conjunto em uma dupla abordagem, as Revoluções Coloridas e a Guerra Não Convencional representam os dois componentes que darão origem à teoria da Guerra Híbrida, um novo método de guerra indireta sendo perpetrado pelos EUA.¹¹⁶

Para ele, parte indissociável dessa tática, é a desestabilização dos Estados tidos como inimigos, através de infiltração social, especialmente na opinião pública, a essa estratégia, Korybko dá o nome de Revoluções Coloridas, essas, seriam uma etapa necessária para a consecução das Guerras Híbridas:

Um dos mais novos modelos para desestabilização de Estado. Elas permitem que atores externos manifestem negações plausíveis quando acusados de interferir ilegalmente nos assuntos domésticos de um Estado soberano, e a mobilização em massa do “poder do povo” faz delas altamente eficazes na ótica de mídia mundial. Além disso, o aglomerado de muitos civis protestando contra o governo também aumenta a pressão sobre o mesmo e limita suas opções para lidar com eficiência contra a desestabilização em andamento. Todas as Revoluções Coloridas seguem à risca o mesmo modelo, e entender a natureza dessa tática de desestabilização na prática permitirá elaborar contramedidas adequadas para se defender contra ela.¹¹⁷

Vale ressaltar que para os observadores, segundo o próprio autor, muitas vezes a percepção de que uma possível guerra híbrida esteja em curso, só será perceptível ao final do conflito, ao se analisar que a deterioração das estruturas governamentais e da opinião popular, nada mais eram do que estratégias e operações realizadas no bojo das “revoluções coloridas” ou das guerras não convencionais.

¹¹⁵ VISACRO, A. Guerra Irregular. São Paulo: Contexto, 2009. p. 7

¹¹⁶ KORYBKO, Andrew. Guerras Híbridas: das Revoluções Coloridas aos Golpes. Editora Expressão Popular, São Paulo, 2018. p. 15.

¹¹⁷ *Ibidem*. p. 115

[...] A guerra híbrida levanta a hipótese de que o conflito pré-existente em questão é uma revolução colorida fabricada externamente e que a guerra não convencional pode ser iniciada de forma secreta quase que imediatamente após o início da revolução colorida para atuar como um multiplicador de forças. A campanha de uma guerra não convencional cresce em intensidade até que o governo alvo seja derrubado. Se a revolução colorida fracassa, contudo, a guerra não convencional, por fim, assume seu estágio de levante e começa a enfatizar a letalidade extrema em seus métodos. A guerra não convencional basicamente se desenvolve a partir de uma revolução colorida, que, em si, é uma semente plantada estrategicamente com a justificativa da “luta pela libertação democrática”, como é habitualmente retratado de maneira enganosa pela mídia ocidental.¹¹⁸

Instalada a instabilidade, ou, o que o autor recorrentemente sinalizará como “o caos”, as táticas de guerras convencionais passam a fazer parte do novo xadrez, dando origem a Guerra Híbrida:

[...] A guerra híbrida consiste em uma parte assimétrica singular da dominação de espectro total que pode ser melhor resumida como a armatização do caos e a tentativa de administrá-lo. Ela é um novo plano de guerra que transcende todos os outros e os incorpora em seu ser multifacetado.¹¹⁹

Dentro deste escopo, o que nos interessa é o fator digital em meio à questão das Guerras Híbridas, ainda que Korybco não trabalhe a ideia de “armatização” dos meios digitais ou do espaço cibernético de forma direta, ele não deixa de tangenciar a questão, dando relevância ao espaço digital, enquanto ambiente, se não, campo de ação, de operações ligadas às revoluções coloridas. Para ele, as mídias sociais assumem um papel preponderante enquanto ferramenta de desestabilização, se apresentando como verdadeiro campo de ação, de insurgentes e milícias digitais, ali, o espaço pode ser configurado em uma base de operações:

[...] As mídias sociais e tecnologias afins substituirão as munições de precisão guiadas como armas de “ataque cirúrgico” da parte agressora, e as salas de bate-papo online e páginas no Facebook se tornarão o novo “covil dos militantes”. Em vez de confrontar diretamente os alvos em seu próprio território, conflitos por procuração serão promovidos na vizinhança dos alvos para desestabilizar sua periferia. As tradicionais ocupações militares podem dar lugar a golpes e operações indiretas para troca de regime, que tem um melhor custo-benefício e são menos sensíveis do ponto de vista político.¹²⁰

O conceito de Guerra Híbrida parece não compreender na totalidade o espaço cibernético enquanto um verdadeiro campo de batalha, ainda que entenda como campo de oportunidade para operacionalização, especialmente no campo da guerra não convencional. Ainda que apresente problemas graves, especialmente na ideia de operações de desestabilização das estruturas políticas de um Estado, como bem alerta Korybko, o objeto que nos preocupa é o da materialização de danos, realizados por operações cibernéticas, em um contexto análogo ao de um ataque cinético e, a este respeito, a Guerra Híbrida parece não ser suficiente para enquadrar essa nova lógica de guerra.

¹¹⁸ *Ibidem.* p. 73-74

¹¹⁹ *Ibidem.* p. 45

¹²⁰ *Ibidem.* p. 14

Contudo, resta analisar mais uma teoria que busca compreender a 4ª geração dos conflitos, sendo essa a teoria da Guerra Omnidimensional. Como o próprio nome sugere, omnidimensional é uma referência a multiplicidade de dimensões em que a guerra ocorre, de forma simultânea, diferente do que é entendido como a Guerra Híbrida, representada pela aplicação de duas lógicas da guerra, a Guerra Omnidimensional é travada na pluralidade dos campos de batalha, nas dimensões do campo de batalha.

Nessa lógica, é preciso compreender o que os autores entendem por dimensões do campo de batalha, para tanto, vamos referenciar o trazido pelo Tenente-Coronel Franco Azevedo e o Major Martins da Mota. Os autores fazem a divisão em 4 (quatro) dimensões ao campo de batalha, a primeira, compreendida pela frente de batalha, é uma dimensão linear, de confronto direto, limitado “aos pontos físicos do terreno”¹²¹:

Num primeiro momento, a limitação tecnológica dos armamentos em termos de alcance e letalidade restringiu tão somente o espaço de combate à frente de batalha, que se constituía, portanto, na única dimensão empregada nos combates daquele momento.¹²²

A 2ª dimensão, por sua vez, referencia-se à profundidade, desenvolvida especialmente em razão da evolução tecnológica dos armamentos, o emprego de forças que vão além da linha de frente do campo de batalha, exemplificados pelo emprego da artilharia, e das guerras de movimento, com máquinas de mobilidade:

Posteriormente, as inovações tecnológicas, tais como o desenvolvimento dos canhões e dos tiros de Artilharia e o aumento do alcance das armas de fogo, em conjugação com as inovações não tecnológicas, como a concepção de novo emprego doutrinário para os carros de combate, possibilitaram a incorporação de uma segunda dimensão ao campo de batalha (2ª DCB) - a profundidade. [...] Esta nova capacidade resultou em transformações militares profundas, uma vez que se tornou possível atingir o centro de gravidade do inimigo valendo-se de meios indiretos ou de aproximação indireta, que potencializam a surpresa.¹²³

A 3ª dimensão é compreendida pelos novos espaços em que a guerra passou a ser travada, não mais ela se limitava à terra, agora, o conflito poderia ser travado no ar e no mar, o desenvolvimento dos aviões, dos navios de guerra e dos submarinos, são as representações desse espaço de oportunidade do conflito:

Ininterruptamente, as inovações continuaram se conjugar e a impulsionar a dinâmica das guerras e a organização dos exércitos e, assim, uma terceira dimensão foi incorporada. O desenvolvimento dos meios da aviação militar e dos submarinos permitiu a atuação militar nos vetores aeroespacial e subaquático, dando forma à terceira dimensão do campo de batalha (3ª DCB).¹²⁴

¹²¹ AZEVEDO, C.E.F. e MOTA, R.M. As dimensões do campo de batalha e a guerra omnidimensional. Coleção Meira Mattos, revista das ciências militares, nº 26, 2º quadrimestre 2012. Rio de Janeiro: ECEME, 2012. p. 5

¹²² *Ibidem.* p. 5

¹²³ *Ibidem.* p. 5

¹²⁴ *Ibidem.* p. 6

Por fim, a 4ª dimensão é representada pelo espaço físico e não físico, é a própria consciência humana, na forma do pensamento psicológico, é a guerra psicológica, da conquista de mentes e corações, do convencimento, do terror, mas é também a guerra travada no espaço digital, nas redes físicas e digitais:

O desenvolvimento recente de inovações tecnológicas, como o domínio do espectro eletromagnético e das redes lógicas, conjugadas com a implantação de inovações não tecnológicas, particularmente de caráter doutrinário, tais como a exploração dos vetores psicológicos e humanos, tornou possível a exploração de aspectos não físicos do campo de batalha, caracterizando o início da incorporação de uma quarta dimensão ao campo de batalha (4ª DCB) – a dimensão não tangível.

Portanto, os vetores do espectro eletromagnético, as estruturas das redes lógicas, os sistemas de comando e controle e o processo decisório inimigo se tornaram alvos a serem conquistados. De forma semelhante, o próprio pensamento do oponente, suas opiniões e a disposição de seus soldados e de sua população para um conflito passaram a se constituir em objetivos estratégicos de guerra. Alvos anteriormente inimagináveis e até mesmo inatingíveis foram estabelecidos, a partir de então, tendo em vista sua vulnerabilidade, com efeitos favoráveis surpreendentes. Com base na 4ª DCB, novos conceitos de guerra estão em desenvolvimento: **Guerra Eletrônica, Guerra Cibernética**, Guerra Psicológica, Guerra da Informação, Guerra Biológica e outros. (grifo nosso)¹²⁵

É sob a ótica da congregação da multiplicidade destas dimensões, de forma indissociável, que se assenta a Guerra Omnidimensional:

Com certeza, há uma aceitação da redução do uso da violência armada para resolução de conflitos e a interpretação de que há outro caminho para se atingir o mesmo resultado. Este caminho é representado pela Guerra Omnidimensional. Uma guerra que não será caracterizada por dimensões ou espaços (tangíveis ou não); nem por uma ou por outra tecnologia. Será uma guerra caracterizada pela multidimensionalidade e pela utilização de toda tecnologia disponível em todo espaço possível.

A guerra parece estar renascendo com outro formato. O ataque financeiro realizado por George Soros no Sudeste Asiático, os ataques terroristas conduzidos por Osama Bin Laden às embaixadas norte-americanas e ao World Trade Center, o ataque com gás Sarin no metrô de Tóquio, realizado pelos discípulos de Aum Shinri Kyo, **os ataques cibernéticos de 2007 e 2009 e a devastação causada por Morris Jr. na Internet, todos estes são eventos cujos graus de destruição são comparáveis aos de uma guerra convencional**. Estes acontecimentos representam uma forma embrionária de um novo tipo de guerra, na qual os Princípios de Guerra não mais indicarão “o emprego da força armada para compelir um inimigo a submeter-se”, e sim, “a utilização de todos os meios, militares e não militares, letais e não letais, para compelir o adversário a submeter-se” [...].¹²⁶ (grifo nosso)

Ainda nessa linha e, em caráter semelhante ao já abordado na questão da guerra híbrida, a análise quanto ao emprego do tipo do conflito, só pode ser analisada e compreendida ao passo em que o conflito se desenvolve, ao passo em que o mesmo se escala, ou seja, não se declara uma guerra omnidimensional, da mesma forma que não se declara uma guerra híbrida, contudo, é a medida que novas táticas e métodos são aplicados, que a guerra começa a assumir suas características de multiplicidade dimensional, até o momento em que podemos vislumbrar uma verdadeira “guerra total”, não no sentido Gobeliano, e sim no do emprego de todo e qualquer

¹²⁵ *Ibidem*. p. 6

¹²⁶ *Ibidem*. p. 8

método para alcançar os objetivos, na mesma medida em que todo e qualquer método se torna objeto militar:

A análise da Guerra Omnidimensional é diacrônica, ou seja, deve ser realizada levando-se em consideração a evolução temporal do conflito: ataques financeiros; **cibernéticos; batalhas baseadas em rede, com alvos estratégicos; suspensão temporária ou total da rede de internet ou de suas funcionalidades;** ataques terroristas discretos ou de grande impacto. Todas estas ações fazem parte de uma escalada do conflito, que pode culminar num combate militar tradicional de segunda e terceira dimensão. Em outras palavras, em dado momento, a guerra pode estar sendo travada em uma dimensão e noutro, ser consolidada em uma dimensão distinta. O conflito poderá ser vencido sem um único disparo, evidenciando competência de uma das partes para **obter a vitória sem a violência militar, o que não quer dizer que não tenha havido violência política, econômica, tecnológica ou de outra ordem.** (grifo nosso)¹²⁷

Como os autores demonstram, ainda que a violência física, cinética, não tenha ocorrido, ainda que os agentes não sejam soldados fardados, ainda que a operação não se restrinja a terra, ar e mar com emprego militar, há violência análoga à violência operada pela lógica da guerra clássica. A Guerra Ominidimensional, assim como a Guerra Híbrida, lança mão de todos os meios possíveis para a conquista dos velhos e novos objetivos militares e, se para isso for necessário o emprego dos meios cibernéticos e no espaço cibernético, o mesmo será feito, não em caráter sucessório ou de exceção, e sim em caráter complementar.

¹²⁷ *Ibidem.* p. 8

CAPÍTULO II – O USO DA FORÇA E A LEGÍTIMA DEFESA SOB A ÓTICA DAS OPERAÇÕES CIBERNÉTICAS

Neste capítulo serão apresentadas questões concernentes à temática do uso da força, em matéria de Direito Internacional, a este respeito, mister apontar que a legítima defesa, bem como as operações cibernéticas, aqui, deve ser abordada como desdobramentos da própria lógica do uso da força, não por derivarem da mesma, mas por lançar mão da prática para sua efetividade.

É importante aqui levar em consideração a ideia de que o uso da força, ainda que aplicado à lógica da legítima defesa em matéria internacional, representa a ideia de uma falha dos princípios basilares da diplomacia, é inegável que a ideia de que um Estado faça uso de meios coercitivos cinéticos (ou que possam ser traduzidos como tal), façam parte do arcabouço de uma comunidade internacional coerente.

Ainda assim, o “legislador”, representado pelos plenipotenciários vitoriosos da Segunda Guerra Mundial, entenderam por bem garantir a possibilidade e a aplicação do uso da força, dentro da Carta fundacional da Organização das Nações Unidas – ONU, para tanto, pensou-se em uma lógica restritiva, de modo a limitar ao máximo as possibilidades pelas quais os Estados poderiam declarar guerra. Ainda que extremamente progressista para a época, o texto acabou por perder parte de sua eficácia, se levarmos em consideração o volume de conflitos no pós-guerra, ainda que esses façam uso do argumento da legítima defesa, como veremos ao longo deste capítulo, esta parece ser só uma forma de “legitimar” as vontades beligerantes dos Estados.

Cumprido destacar que, ainda que a intenção tenha se consolidado com a Carta da ONU, a ideia de uma limitação da capacidade jurídica de se declarar guerra, já fora objeto de tentativa, na construção da Liga das Nações, ainda nessa linha, as convenções de Haia e Genebra (já trabalhadas anteriormente), reforçaram a ideia de uma limitação à prática belicosa.

Aqui cabe um questionamento, há de se falar em soberania internacional? É possível conceber a ideia de que a soberania de um Estado possa extrapolar suas fronteiras, fazendo valer sua vontade sob a soberania de outro Estado? Há de se falar em alguma legitimidade quanto a essa questão?

É preciso de detida atenção às particularidades do ciberespaço, aplicadas à temática da legítima defesa e do uso da força. Como mencionado anteriormente, a guerra e os conflitos armados sofreram enormes mutações aos longos das décadas, não sendo diferente com o advento do ciberespaço, tendo esse proporcionado um novo ambiente em que os conflitos poderiam ser travados.

É nesse novo campo de oportunidade que surgem problemas objetos desta pesquisa, quais as limitações do uso da força no ciberespaço? Há de se falar em tradução do conceito de uso da força dentro do ciberespaço? Uma operação cibernética pode ser respondida com um ataque cinético? Quais os limites dos Estados em matéria de uso da força e legítima defesa sob a ótica das operações cibernéticas? Essas são algumas das questões que buscaremos tangenciar ao longo deste capítulo, sem, contudo, buscar esgotar a questão.

Para tanto, alguns termos serão definidos ao longo deste capítulo, de forma a possibilitar uma melhor compreensão da temática, dentre eles, o conceito de força e legítima defesa, em matéria de Direito Internacional e sua lógica aplicada ao ciberespaço.

2.1 – O PROBLEMA DO LIMITE DO USO DA FORÇA NO CIBERESPAÇO

É importante destacar que a tentativa de se restringir a guerra e, conseqüentemente o uso da força enquanto uma prerrogativa dos Estados surgiu primeiramente com o Pacto Briand-Kellogg, também conhecido como Pacto Multilateral de Renúncia a Guerra, como uma resposta direta à Primeira Grande Guerra:

Profundamente conscientes de seu dever solene de promover o bem-estar da humanidade;
 Convencidos de que é chegado o momento em que se deve renunciar francamente à guerra como instrumento da política nacional, a fim de que se perpetuem as relações pacíficas e amistosas que agora existem entre os seus povos;
 Convencidos de que todas as mudanças em suas relações mútuas devem ser buscadas apenas por meios pacíficos e ser o resultado de um processo pacífico e ordeiro, e que qualquer potência signatária que, a partir de agora, procure promover seus interesses nacionais por meio da guerra deve ser negada a benefícios proporcionados por este Tratado;
 Esperançosos de que, encorajados por seu exemplo, todas as outras nações do mundo se unam a este esforço humano e, aderindo ao presente Tratado, tão logo ele entre em vigor, traga seus povos para o âmbito de suas disposições benéficas, unindo assim as nações civilizadas do mundo em uma renúncia comum à guerra como instrumento de sua política nacional;¹²⁸

Ressalta-se que o pacto buscou adotar o abandono ao recurso da guerra, enquanto uma política estatal dos Estados, concebendo que, ainda que a guerra seja um ato com conseqüências internacionais, sua razão parte de uma lógica puramente estatal, a do uso da força e, ou, da legítima defesa. A ideia da renúncia do uso da força e a doção de meios diplomáticos para a resolução de conflitos e controvérsias à luz do Pacto, assumiu uma característica vanguardista e, em certa medida, utópica, especialmente se observarmos os acontecimentos vindouros.

ARTIGO 1.

As Altas Partes Contratantes declaram solenemente nas marinhas de seus respectivos povos que condenam o recurso à guerra para a solução de controvérsias internacionais e a renunciam como instrumento de política nacional em suas relações recíprocas.

ARTIGO 2.

¹²⁸ INTERNATIONAL TREATY FOR THE RENUNCIATION OF WAR AS NA INSTRUMENT OF NATIONAL POLICY. Paris, agosto, 1928. p. 2-3. Disponível em: <<https://web.archive.org/web/20121016045106/http://www.fco.gov.uk/resources/en/pdf/treaties/TS1/1929/29>>. Acessado em: 17 de fevereiro de 2022. Tradução livre de: “Deeply sensible of their solemn duty to promote the wel-fare of mankind;Persuaded that the time has come when a frank renunciation of war as an instrument of national policy should be made to the end that the peaceful and friendly relations now existing between their peoples may be perpetuated;Convinced that all changes in their relations with one another should be sought only by pacific means and be the result of a peaceful and orderly process, and that any signatory Power which shall hereafter seek to promote its national interests by resort to war should be denied the benefits furnished by this Treaty;Hopeful that, encouraged by their example, all the Other nations of the world will join in this humane endeavour and by adhering to the present Treaty as soon as it comes into force bring their peoples within the scope of its beneficentprovisions, thus uniting the civilised nations of the world in a common renun-ciation of war as na instrument of their national policy;”

As Iligantes Partes Contratantes concordam que a solução ou solução de todas as controvérsias ou conflitos de qualquer natureza ou origem, que possam surgir entre elas, nunca deverá ser buscada, exceto por meios pacíficos.¹²⁹

Tornou-se claro que, ainda que valoroso, os esforços do Pacto foram ineficazes, não só conflitos locais envolvendo os próprios signatários em seus domínios coloniais e adjacentes foram observados nos anos seguintes, como menos de uma década após a assinatura do Documentos, a Europa veria a ascensão do Nazi-fascismo e sua campanha de agressão.

O mundo saído dos horrores da guerra e da completa decadência das relações internacionais, viu-se na necessidade de reconfigurar a lógica na qual os Estados engajariam em suas relações e disputas internacionais, era necessário limitar ao máxima qualquer possibilidade de uma nova grande guerra, para tanto, as Nações Unidas foram criadas, sob égide do princípio do primado do direito. Sob essa perspectiva, a Carta das Nações Unidas concebe que as relações devem ser guiadas pela legalidade, juridicidade e pela segurança em escala global, essa mesma lógica deverá guiar os conflitos, que a priori, devem ser resolvidos pelos meios diplomáticos.

(...) a Carta cria mecanismos fadados a resolver crises emergentes a qualquer preço, garantindo uma segurança provisória e circunstancial, mas também os cria destinados a resolver conflitos em definitivo, aqui sempre mediante a aplicação do direito, a garantia do primado do direito, a realização de justiça que se busca à luz do direito.¹³⁰

As limitações concernentes ao uso da força são claras no cenário internacional, partem de um princípio de reciprocidade, ou seja, o uso da força só é aplicável se e somente se, uma agressão for desferida contra um Estado. No entendimento da ONU, o direito à legítima defesa constitui um direito inerente à soberania dos Estados, diferente do que o Tratado de Briand-Kellogg pressupôs, a Carta da ONU não buscou alienar dos Estados o emprego da força mediante a guerra, enquanto uma prerrogativa de sua soberania:

Artigo 51

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, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais.¹³¹

¹²⁹ *Ibidem*. p. 5-6. Tradução livre de: “ARTICLE 1. The High Contracting Parties solemnly declare in the names of their respective peoples that They condemn recourse to war for the solution of international contro-versies, and renounce it as na instrument of national policy in their relations with one another. ARTICLE 2. The Iligh Contracting Parties agree that the settlement or solution of all disputes or con-flicts of whatever nature or of whatever origin they may be, which may arise among them, shall never be sought except by pacific means.”

¹³⁰ REZEK, Francisco. Preâmbulo. In: BRANT, Leonardo Nemer Caldeira (Org). Comentário à Carta das Nações Unidas. Belo Horizonte: Centro de Direito Internacional, 2008. p. 31

¹³¹ ONU. Carta das Nações Unidas. p. 32. Disponível em: < <https://brasil.un.org/sites/default/files/2022-05/Carta-ONU.pdf>>. Acessado em: 01 de fevereiro de 2022.

Contudo, a busca pela paz é um primado da ordem erigida pela ONU, desta feita, as menções quanto a busca pela paz, do emprego de ações que fomentem e mantenham a paz, bem como as limitações dispostas para o emprego da força, são claros no documento, de modo que, o emprego da força é concebível somente se forem esgotadas todas as demais respostas pacíficas à solução de um conflito, para tanto, incumbiu-se ao Conselho de Segurança da ONU, o juízo de admissibilidade do uso da força em casos particulares:

Artigo 41

O Conselho de Segurança decidirá sobre as medidas que, sem envolver o emprego de forças armadas, deverão ser tomadas para tornar efetivas suas decisões e poderá convidar os membros das Nações Unidas a aplicarem tais medidas. Estas poderão incluir a interrupção completa ou parcial das relações econômicas, dos meios de comunicação ferroviários, marítimos, aéreos, postais, telegráficos, radiofônicos, ou de outra qualquer espécie e o rompimento das relações diplomáticas.

Artigo 42

No caso de o Conselho de Segurança considerar que as medidas previstas no artigo 41 seriam ou demonstraram que são inadequadas, poderá levar a efeito, por meio de forças aéreas, navais ou terrestres, a ação que julgar necessária para manter ou restabelecer a paz e a segurança internacionais. Tal ação poderá compreender demonstrações, bloqueios e outras operações, por parte das forças aéreas, navais ou terrestres dos membros das Nações Unidas.¹³²

Ainda nessa linha, entenderam os plenipotenciários garantir ao Conselho os meios e as ações que poderiam ser invocadas, a fim de garantir a manutenção da paz internacional e resolução dos conflitos que ensejarem o uso da força.

Artigo 43

1. Todos os membros das Nações Unidas, a fim de contribuir para a manutenção da paz e da segurança internacionais, se comprometem a proporcionar ao Conselho de Segurança, a seu pedido e de conformidade com o acordo ou acordos especiais, forças armadas, assistência e facilidades, inclusive direitos de passagem, necessários à manutenção da paz e da segurança internacionais.
2. Tal acordo ou tais acordos determinarão o número e tipo das forças, seu grau de preparação e sua localização geral, bem como a natureza das facilidades e da assistência a serem proporcionadas.
3. O acordo ou acordos serão negociados o mais cedo possível, por iniciativa do Conselho de Segurança. Serão concluídos entre o Conselho de Segurança e membros da Organização ou entre o Conselho de Segurança e grupos de membros e submetidos à ratificação, pelos Estados signatários, de conformidade com seus respectivos processos constitucionais.¹³³

Em regra geral, o Uso da Força está atrelado a um princípio basilar e indissociável à aplicação do mesmo, a ideia da *Legítima Defesa*. Como disposto acima, para que um Estado tenha o direito de empregar o uso da força, é necessário que esse Estado invoque o seu direito à legítima defesa, podendo ainda, em casos excepcionais, invocar a legítima defesa de terceiros, caso haja entendimento de que há ameaça à paz internacional ou a própria territorialidade.

Artigo 2

A Organização e seus membros, para a realização dos propósitos mencionados no artigo 1, agirão de acordo com os seguintes Princípios:
[...]

¹³² *Ibidem*. p. 27.

¹³³ *Ibidem*. p. 28.

3. Todos os membros deverão resolver suas controvérsias internacionais por meios pacíficos, de modo que não sejam ameaçadas a paz, a segurança e a justiça internacionais.

4. Todos os membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a independência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas.

[...]

7. Nenhum dispositivo da presente Carta autorizará as Nações Unidas a intervirem em assuntos que dependam essencialmente da jurisdição de qualquer Estado ou obrigará os membros a submeterem tais assuntos a uma solução, nos termos da presente Carta; este princípio, porém, não prejudicará a aplicação das medidas coercitivas constantes do Capítulo VII.¹³⁴

Ainda que a Carta preveja e garanta regras claras à manutenção da paz e dos limites e possibilidades pelos quais os Estados podem engajar na resolução de conflitos, o já mencionado artigo 51 do documento nos traz um problema relevante à temática “Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva no caso de ocorrer um **ataque armado [...]**”¹³⁵ (grifo nosso). O texto deixa claro a limitação quanto ao uso da força à um ataque armado.

A restrição no conceito “ataque armado” acaba por, como já mencionamos inúmeras vezes, garantir um campo de oportunidade visto que demanda interpretação analógica inserir um ataque cibernético no bojo de um ataque armado, ainda que este se traduza em danos reais análogos a um ataque cinético. Para tanto, a própria norma precisa ser trazida à luz da interpretação, neste caso, aqui cabe somente um exercício, visto que a comunidade internacional ainda não se debruçou sobre caso concreto de operação cibernética.

Contudo, os Protocolos adicionais da Convenção de Genebra nos dão, resguardadas as limitações, uma capacidade de interpretação e de aplicação analógica expansiva à possibilidade de entendermos certas operações cibernéticas enquanto “ataques armados”:

SEÇÃO I

Métodos e Meios de Guerra

Artigo 35 – Regras fundamentais

1. Em qualquer conflito armado, o direito de as Partes em conflito escolherem os métodos ou os meios de guerra não é ilimitado.

2. É proibido utilizar armas, projéteis e materiais, assim como métodos de guerra de natureza a causar danos supérfluos ou sofrimento desnecessário.

3. É proibido utilizar métodos ou meios de guerra concebidos para causar, ou que se possa presumir que irão causar, danos extensos, duradouros e graves ao meio ambiente natural.

Artigo 36 — Armas novas

Durante o estudo, preparação ou aquisição de uma nova arma, de novos meios ou de um novo método de guerra, uma Alta Parte contratante tem a obrigação de determinar se sua utilização seria proibida, em algumas ou em todas as circunstâncias, pelas disposições do presente Protocolo ou por qualquer outra regra de direito internacional aplicável a essa Alta Parte contratante.

Artigo 37 — Proibição de perfídia

¹³⁴ *Ibidem.* p. 5-7.

¹³⁵ *Ibidem.* p. 32.

1. É proibido matar, ferir ou capturar um adversário recorrendo à perfídia. Constituem perfídia os atos que apelem à boa-fé de um adversário, com a intenção de enganá-lo, fazendo-o crer que tem o direito de receber ou a obrigação de assegurar a proteção prevista pelas regras de direito internacional aplicáveis nos conflitos armados. São exemplo de perfídia os seguintes atos:

- a) simular intenção de negociar a coberto da bandeira de trégua, ou simular a rendição;
- b) simular uma incapacidade causada por ferimentos ou enfermidade;
- c) simular o estatuto de civil ou de não combatente;
- d) simular o estatuto protegido utilizando sinais, emblemas ou uniformes das Nações unidas, de Estados neutros ou de outros Estados não Partes em conflito.

2. Os artificios de guerra não são proibidos. Constituem artificios de guerra os atos que têm por fim induzir um adversário a erro ou fazer com que cometa imprudências, mas que não violem nenhuma regra do direito internacional aplicável aos conflitos armados e que, não apelando à boa-fé do adversário no que diz respeito à proteção prevista por aquele direito, não são perfídias. Os atos seguintes são exemplos de artificios de guerra: uso de camuflagem, engodos, operações simuladas e falsas informações.¹³⁶

Inegável que o artigo 36 possui aplicação no ideário das operações cibernéticas. Aqui, não há de se falar em reconhecer o computador ou a internet como uma arma em potencial, não, contudo, um *botnet* nos moldes do Stuxnet, foi concebido e utilizado enquanto armamento. Ainda nessa linha, um ataque DDoS como o perpetrado contra a Estônia, tem implicações que poderiam resultar em uma ação análoga a de um ataque armado.

Um vírus de computador pode ser produzido para causar danos potencialmente mais destrutivos que os de um ataque cinético com armas de fogo em um ambiente controlado, os ataques realizados nas centrífugas iranianas por vírus, se endereçados para outros sistemas dentro da usina nuclear, poderiam desencadear uma explosão. Caso uma operação cibernética venha a danificar os sistemas de alimentação dos gasodutos que alimentam a Europa, em pleno inverno, poderíamos ver uma catástrofe em perdas de vidas no curto prazo. O que esses cenários nos apresentam é a potencialidade da “(...) preparação ou aquisição de uma nova arma, de novos meios ou de um novo método de guerra(...)”¹³⁷, dentro da lógica das operações cibernéticas.

Ainda que pareça ser uma aplicação fática, do ponto de vista do Direito Internacional, a mesma não encontra guarida, razão pela qual, ações como as do grupo de especialistas que formularam o Manual de Tallinn continuam a serem propostas.

A realidade do período em que a Carta fora produzida somente poderia conceber a ideia de uma guerra cibernética em ficções científicas, os primeiros computadores haviam sido empregados a pouco tempo e o imaginário de uma guerra ou de um conflito não cinético era inimaginável. Porém essa limitação textual gera repercussões consideráveis à análise da lógica

¹³⁶ GENEBRA. Os Protocolos Adicionais às Convenções de Genebra de 12 de Agosto de 1949. Comitê Internacional da Cruz Vermelha. CICV. Genebra, Suíça. p. 31-32. Disponível em: <<https://www.icrc.org/pt/publication/os-protocolos-adicionais-convencoes-de-genebra-de-12-de-agosto-de-1949>>. Acessado em: 22 de fevereiro de 2022

¹³⁷ *Ibidem*. p. 31

vigente. O emprego da força por meios cinéticos é de fácil identificação, seus atores e alvos são visíveis, suas implicações são imediatas e inegáveis.

Todavia, não podemos dizer o mesmo dos ataques perpetrados por meios cibernéticos. Operações que façam uso dos meios digitais, que tenham como alvo o ciberespaço ou alvos reais, são de difícil identificação, são operações de um Estado contra outro Estado? Há de se falar em dano, em uma operação cibernética? Qual a extensão desse dano, se ele só pode ser mensurável no decorrer do tempo?

Essas são questões que muito interessaram os especialistas envolvidos na elaboração dos Manuais de Tallinn, visto que, em matéria de Direito Internacional, a normativa criou uma lacuna de oportunidade para as operações cibernéticas, primeiro, pela limitação da terminologia “armado”, o que acaba por limitar o entendimento de que qualquer operação só poderá ser considerada um ataque, se tiver sido realizada mediante um ataque cinético.

Ressalta-se, contudo, que os Estados não se abstêm de discussões quanto a evolução das proibições relativas ao emprego de armas no campo de batalha, ao passo que as armas avançam, também evoluem as discussões quanto suas proibições e limitações¹³⁸, resta ainda incerto onde poderíamos enquadrar as armas digitais.

Contudo, como bem infere Ana Flávia Veloso, é preciso analisar o caso concreto para se chegar a uma definição exata se determinado ataque poderia ou não ser interpretado como o uso de força e, ainda nessa linha, se poderíamos analogicamente atribuir o status de “ataque armado”, ainda que a autora não tenha se referido diretamente ao emprego de métodos no espaço cibernético, a regra é válida ao mesmo, tendo sido esse o prisma analítico utilizado na formulação de Tallinn, interpretação analógica com base em casos concretos:

Uma fórmula universal do ato agressor referido no artigo 51 ainda não foi reconhecida. Não obstante, as situações elencadas na definição da Assembléia Geral são suscetíveis, segundo suas circunstâncias e proporções, de ser assim caracterizadas. Portanto, a qualificação de um ato como ataque armado será determinada à luz de cada caso concreto.¹³⁹

Ainda nessa linha a Convenção de Viena anteviu a possibilidade de interpretação de tratados, não somente atrelada ao caso concreto, como também a demais textos normativos:

ARTIGO 31

Regra geral de interpretação

1. Um tratado deve ser interpretado de boa-fé, segundo o sentido comum atribuído aos termos do tratado em seu contexto e à luz de seu objeto e finalidade.

¹³⁸ A esse respeito ver o artigo “Armas” do Comitê Internacional da Cruz Vermelha, disponível em: < <https://www.icrc.org/pt/doc/war-and-law/weapons/overview-weapons.htm> > acessado em: 20 de fevereiro de 2022.

¹³⁹ VELOSO, Ana Flávia. Ação relativa a ameaças à paz, ruptura da paz e atos de agressão: artigo 51. In BRANT, Leonardo Nemer Caldeira (Org.). Comentário à Carta das Nações Unidas. Belo Horizonte: Centro de Direito Internacional, 2008. p. 782.

2. Para os fins de interpretação de um tratado, o contexto compreende, além do texto, seu preâmbulo e anexos:

a) qualquer acordo relativo ao tratado e feito entre todas as partes por ocasião da conclusão do tratado;

b) qualquer instrumento estabelecido por uma ou várias partes por ocasião da conclusão do tratado e aceito pelas outras partes como instrumento relativo ao tratado.

3. Será levado em consideração, juntamente com o contexto:

a) qualquer acordo posterior entre as partes relativo à interpretação do tratado ou à aplicação de suas disposições;

b) qualquer prática seguida posteriormente na aplicação do tratado pela qual se estabeleça o acordo das partes relativo à sua interpretação;

c) qualquer regra pertinente de direito internacional aplicável às relações entre as partes.

4. Um termo será entendido em sentido especial se estiver estabelecido que essa era a intenção das partes.¹⁴⁰

Ainda que essa possibilidade interpretativa tenha ensejado por parte de muitos Estados entendimentos extensivos a vários conceitos, dentre eles o da possibilidade de enquadramento de coerção política e econômica, enquanto violação da soberania e, conseqüentemente violação da proibição à intervenção, muitos exploraram ainda a possibilidade de aplicação a própria lógica da proibição do uso de força.

[...] Mais uma vez, embora a Declaração não resolva definitivamente o alcance do termo “força”, seu teor geral e os diversos contextos em que surge a coerção armada, econômica e política, sugerem que embora a coerção econômica e política possa constituir ameaças à estabilidade internacional e, portanto, são impedidos pelo princípio da não intervenção (discutido *infra*), o conceito de uso da força é geralmente entendido como força armada.

A análise anterior mostra que a proibição da ameaça ou uso da força inclui coerção armada, mas não econômica ou política. No entanto, não demonstra que as fronteiras da “força” coincidam precisamente com a força armada, ou seja, força física ou cinética aplicada por armamento convencional. Esta realidade só recentemente provou ser de importância aplicativa. Até o advento das operações de informação, a maior parte da coerção podia ser facilmente categorizada em uma das várias boces, pois existiam poucas opções coercitivas que não pudessem ser classificadas como de natureza política, econômica ou armada. Como havia pouca necessidade de olhar além desses gêneros, o discurso sobre a legalidade da coerção estatal, como ilustrado acima, tendia a girar em torno deles. Se o ato em questão se enquadrar no quadro das forças armadas, violou a prescrição que proíbe o uso da força; se não, as questões de legalidade tinham que ser resolvidas procurando em outro lugar.¹⁴¹

¹⁴⁰ BRASIL. Convenção de Viena. Viena 21 de março de 1986. p. 24. Disponível em: < https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=701DBCD1773F1FB1F2C5DA2890871FFD.proposicoesWeb2?codteor=1427770&filename=MSC+589/2015 >. Acessado em: 29 de fevereiro de 2022.

¹⁴¹ SCHMITT. Michael N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework (1999). Columbia Journal of Transnational Law, Vol. 37, 1998-99. p. 907-907. pp. 885-938. Tradução livre de: “[...] Again, while the Declaration does not definitively resolve the reach of the term “force,” its general tenor, and the varying contexts in which armed, economic, and political coercion arise, suggest that although economic and political coercion may constitute threats to international stability and therefore are precluded by the principle of non-intervention (discussed *infra*), the concept of the use of force is generally understood to mean armed force. The foregoing analysis shows that the prohibition of the threat or use of force includes armed, but not economic or political coercion. However, it does not demonstrate that the borders of “force” precisely coincide with armed force, i.e., physical or kinetic force Applied by conventional weaponry. This reality has Only recently proven of applicative import. Until the advent of information operations, most coercion could be handily categorized into one of several boces, for few coercive options existed that could not be typed as political, economic or armed in nature. Because there was little need to look beyond these genera, discourse about the lawfulness of State coercion, as Illustrated *supra*, tended to revolve around them. If the act in question fell

Neste sentido, o entendimento exarado pela Corte Internacional de Justiça no caso *Nicarágua vs Estados Unidos*, nos traz dois grandes pontos de atenção, o primeiro diz respeito ao entendimento dos limites da intervenção e o segundo da própria aplicação do uso da força, sobre o último, a Corte acaba por gerar um problema extensivo ao campo das operações cibernéticas.

Acerca do Uso da Força, a Corte interpretou a existência de gradações do mesmo, sendo somente as mais gravosas, constitutivas de um ataque armada, sendo as demais somente ameaças de uso de força ou ações que antevêm um possível uso de força:

191. Em relação a certos aspectos particulares do princípio em questão, será necessário distinguir as formas mais graves de uso da força (as que constituem um ataque armado) de outras formas menos graves. Ao determinar a norma jurídica que se aplica a estas últimas formas, a Corte pode novamente recorrer às formulações contidas na Declaração sobre Princípios de Direito Internacional sobre Relações Amistosas e Cooperação entre os Estados, de acordo com a Carta das Nações Unidas (Assembleia Geral resolução 2625 (XXV), referida acima). Como já observado, a adoção deste texto pelos Estados oferece uma indicação de sua opiniojuris quanto ao direito internacional consuetudinário sobre a questão. Ao lado de algumas descrições que podem se referir à agressão, este texto inclui outras que se referem apenas a formas menos graves de uso da força. Em particular, de acordo com esta resolução: “Todo Estado tem o dever de abster-se da ameaça ou uso da força para violar as fronteiras internacionais existentes de outro Estado ou como meio de resolver disputas internacionais, incluindo disputas territoriais e problemas relativos às fronteiras dos Estados.

Os Estados têm o dever de abster-se de atos de represália que envolvam o uso da força.

Todo Estado tem o dever de abster-se de qualquer ação coerciva que prive os povos referidos na elaboração do princípio da igualdade de direitos e autodeterminação desse direito à autodeterminação e liberdade e independência.

Todo Estado tem o dever de se abster de organizar ou incentivar a organização de forças irregulares ou bandos armados, inclusive mercenários, para incursão no território de outro Estado.

Todo Estado tem o dever de se abster de organizar, instigar, assistir ou participar em atos de guerra civil ou atos terroristas em outro Estado ou consentir em atividades organizadas em seu território dirigidas à prática de tais atos, quando os atos referidos no presente parágrafo envolvem uma ameaça ou uso da força.”¹⁴²

within the armed force box, it violated the prescription banning the use of force; if not, questions of legality had to be resolved by looking elsewhere.”

¹⁴² INTERNATIONAL COURT OF JUSTICE. Case Concerning Military and Paramilitary Activities in and Against Nicaragua. Merits. Judgment of 27 June 1986. Disponível em: <https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf> >. p. 91. Tradução livre de: “191. As regards certain particular aspects of the principle in question, it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms. In determining the legal rule which applies to these latter forms, the Court can again draw on the formulations contained in the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (General Assembly resolution 2625 (XXV), referred to above). As already observed, the adoption by States of this text affords an indication of their opiniojuris as to customary international law on the question. Alongside certain descriptions which may refer to aggression, this text includes others which refer only to less grave forms of the use of force. In particular, according to this resolution: “Every State has the duty to refrain from the threat or use of force to violate the existing international boundaries of another State or as a means of solving international disputes, including territorial disputes and problems concerning frontiers of States. States have a duty to refrain from acts of reprisal involving the use of force. Every State has the duty to refrain from any forcible action which deprives peoples referred to in the elaboration of the principle of equal rights and self-determination of that right to self-determination and freedom and independence. Every State has the duty to

Este é um ponto extremamente problemático se formos aplicá-lo à lógica de operações cibernéticas, primeiro porque a concepção de um ataque cibernético ser análogo a um ataque armado é um exercício analógico e hipotético, sem embasamento legal. Ainda que a Corte não tenha assentado em um caso de ataque cibernético, a interpretação dada no julgado supracitado é temerária, ainda que tomemos por base as demais normativas anteriormente levantadas acerca da concepção do ideário de armas.

Contudo, ainda que o julgado crie a distinção, ele não isenta a responsabilidade dos Estados na aplicação do uso mais “brando” do uso da força, pelo contrário, entende que o mesmo estaria no bojo dos princípios invioláveis da Carta das Nações Unidas, sendo, invariavelmente, uso da força e quebra da não intervenção, para tanto, é passível de resposta em sede de legítima defesa, ressalvadas as suas particularidades, como da proporcionalidade:

205. Apesar da multiplicidade de declarações de Estados que aceitam o princípio de não intervenção, permanecem duas questões: primeiro, qual é o conteúdo exato do princípio assim aceito e, segundo, se a prática está suficientemente em conformidade com ele para que seja uma regra de direito internacional consuetudinário? No que diz respeito ao primeiro problema - o do conteúdo do princípio da não intervenção - o Tribunal definirá apenas os aspectos do princípio que parecem ser relevantes para a resolução do litígio. Dentro deste respeito, observa que, em vista das formulações geralmente aceitas, o princípio proíbe todos os Estados ou grupos de Estados de intervir direta ou indiretamente nos assuntos internos ou externos de outros Estados. Uma intervenção proibida deve, portanto, ser aquela relacionada a assuntos em que cada Estado é permitido, pelo princípio da soberania do Estado, decidir livremente. Uma delas é a escolha de um sistema político, econômico, social e cultural e a formulação da política externa. A intervenção é injusta quando utiliza métodos de coerção em relação a tais escolhas, que devem permanecer livres. O elemento de coerção, que define, e de fato constitui a própria essência de uma intervenção proibida, é particularmente evidente no caso de uma intervenção que usa a força, seja na forma direta de ação militar, seja na forma indireta de apoio a ações subversivas ou atividades armadas terroristas dentro de outro Estado. Conforme observado acima (parágrafo 191). A resolução 2625 (XXV) da Assembleia Geral equipara a assistência deste tipo ao uso da força pelo Estado que presta assistência quando os atos cometidos em outro Estado "envolvem uma ameaça ou uso da força". Essas formas de ação são, portanto, ilícitas à luz tanto do princípio do não uso da força quanto do princípio da não intervenção. Tendo em vista a natureza das denúncias da Nicarágua contra os Estados Unidos, e aquelas expressas pelos Estados Unidos em relação à conduta da Nicarágua em relação a El Salvador, são principalmente atos de intervenção desse tipo que a Corte se ocupa no presente caso.¹⁴³

refrain from organizing or encouraging the organization of irregular forces or armed bands, including mercenaries, for incursion into the territory of another State. Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.”

¹⁴³ *Ibidem*. p. 97 – 98. Tradução livre de: “205. Notwithstanding the multiplicity of declarations by States accepting the principle of non-intervention, there remain two questions: first, what is the exact content of the principle so accepted, and secondly, is the practice sufficiently in conformity with it for this to be a rule of customary international law? As regards the first problem -that of the content of the principle of non-intervention - the Court will define only those aspects of the principle which appear to be relevant to the resolution of the dispute. In this respect it notes that, in view of the generally accepted formulations, the principle forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty.

Por sua vez, o entendimento da Corte Internacional de Justiça neste caso, no concernente ao financiamento, treinamento e suporte físico material de determinado grupo e, ou, de Estado contra outro Estado, seria passível de responsabilização do Estado financiador. Contudo, aqui a Corte aplica seu entendimento de gradação do uso da força, para tanto, a concepção dos pretores internacionais foi de que o financiamento realizado pelos Estados Unidos ao grupo paramilitar (Contras), que compunham a oposição ao regime vigente da Nicarágua, compreendeu clara violação à soberania do Estado, sendo um ato de intervenção, rompendo assim, o princípio da não intervenção, contudo, o ato por não ter feito uso de aparato militar direto e emprego de forças armadas, não poderia ser visto a luz do uso da força:

228.[...] Quanto à alegação de que as atividades dos Estados Unidos em relação aos contras constituem uma violação do princípio consuetudinário do direito internacional do não uso da força. A Corte considera que, sob reserva da questão de saber se a ação dos Estados Unidos pode ser justificada como exercício do direito de legítima defesa, os Estados Unidos cometeram uma violação *prima facie* desse princípio por sua assistência aos contras na Nicarágua. por "organizar ou incentivar a organização de forças irregulares ou bandos armados... para incursão no território de outro Estado". e "participar de atos de guerra civil... em outro Estado", nos termos da resolução 2625 (XXV) da Assembléia Geral. De acordo com essa resolução, a participação deste tipo é contrária ao princípio da proibição do uso da força quando os atos de conflito civil referidos "envolvem uma ameaça ou uso da força". Na opinião da Corte, embora se possa dizer que o armamento e o treinamento dos contras certamente envolvem a ameaça ou o uso da força contra a Nicarágua, isso não é necessariamente assim em relação a toda a assistência prestada pelo governo dos Estados Unidos. Em particular, a Corte considera que a mera entrega de recursos aos contras, enquanto indubitavelmente um ato de intervenção nos assuntos internos da Nicarágua, como será explicado a seguir, não constitui em si um uso da força.¹⁴⁴

to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State. As noted above (paragraph 191). General Assembly resolution 2625 (XXV) equates assistance of this kind with the use of force by the assisting State when the acts committed in another State "involve a threat or use of force". These forms of action are therefore wrongful in the light of both the principle of non-use of force, and that of non-intervention. In view of the nature of Nicaragua's complaints against the United States, and those expressed by the United States in regard to Nicaragua's conduct towards El Salvador, it is primarily acts of intervention of this kind with which the Court is concerned in the present case."

¹⁴⁴ *Ibidem*. p. 108 – 109. Tradução livre de: "228.[...] As to the claim that United States activities in relation to the contras constitute a breach of the customary international law principle of the non-use of force. the Court finds that, subject to the question whether the action of the United States might be justified as an exercise of the right of self-defence, the United States has committed a *prima facie* violation of that principle by its assistance to the contras in Nicaragua. by "organizing or encouraging the organization of irregular forces or armed bands . . . for incursion into the territory of another State". and "participating in acts of civil strife . . . in another State", in the terms of General Assembly resolution 2625 (XXV). According to that resolution, participation of this kind is contrary to the principle of the prohibition of the use of force when the acts of civil strife referred to "involve a threat or use of force". In the view of the Court, while the arming and training of the contras can certainly be said to involve the threat or use of force against Nicaragua, this is not necessarily so in respect of all the assistance given by the United States Government. In particular, the Court considers that the mere supply of funds to the contras, while undoubtedly an act of intervention in the internal affairs of Nicaragua, as will be explained below, does not in itself amount to a use of force."

Nessa mesma linha, a Corte ainda reforçou o entendimento de violação do princípio de não intervenção, ainda que afastando a ideia do uso da força:

242. A Corte, portanto, considera que o apoio prestado pelos Estados Unidos, até o final de setembro de 1984, às atividades militares e paramilitares dos contras na Nicarágua, mediante apoio financeiro, treinamento, fornecimento de armas, inteligência e apoio logístico, constitui uma clara violação do princípio da não intervenção. [...] ¹⁴⁵

O que esses pontos demonstram é a problemática existente na aplicação do conceito de uso da força em situações que não partam à princípio de um ataque armado. O Problema torna-se ainda mais aparente se formos tratar de operações cibernéticas, contudo, como já vimos anteriormente neste estudo, essas lacunas se apresentam como verdadeiros campos de oportunidade aos Estados que possuem a capacidade ou o interesse de fazer uso dessas ferramentas.

Nesta mesma medida, ficou claro que o caso Nicarágua vs Estados Unidos constitui ponto primordial para o entendimento dessa lógica de “campo de oportunidade”, visto que a interpretação da Corte em diferenciar escalas de uso da força, implicando que formas brandas não ensejariam a aplicação da legítima defesa, podemos ver um paralelo com operações recentes como as apresentadas no capítulo anterior, sob a nomenclatura de guerra híbridas ou guerras omnidimensionais.

Nessa mesma linha inserem-se as operações cibernéticas, campos que não encontram guarida de forma geral no entendimento de um ataque armado, ainda que, como veremos no próximo capítulo, analogicamente podem ser enquadrados como tal, segundo especialistas.

O paradigma de um ataque cibernético é amplo, seus objetivos e consequentes resultados são variados, ainda que inicialmente a interpretação dada no caso Nicarágua soe problemática quanto ao nivelamento do uso da força, a natureza de uma operação cibernética é, necessariamente, mensurável sob um prisma de intensidade, podendo compreender tanto a derrubada de um simples sistema de informação, até o apagão de uma rede elétrica, com a incorrência de perda de vidas.

[...] O ataque à rede de computadores desafia o paradigma predominante, pois suas consequências não podem ser facilmente colocadas em uma área específica ao longo do continuum de ameaça dos valores da comunidade. O dilema está no fato de a CNA abranger o espectro da consequencialidade. Seus efeitos variam livremente de mera inconveniência (por exemplo, desligar uma rede acadêmica temporariamente) a destruição física (por exemplo, como criar um fenômeno de martelar em oleodutos

¹⁴⁵ *Ibidem*. p. 114. Tradução livre de: “242. The Court therefore finds that the support given by the United States, up to the end of September 1984, to the military and paramilitary activities of the contras in Nicaragua, by financial support, training, supply of weapons, intelligence and logistic support, constitutes a clear breach of the principle of non-intervention.[...]”

para fazê-los explodir) até a morte (por exemplo, desligar a energia de um hospital sem geradores de reserva).¹⁴⁶

Como poderia um Estado, responder a uma agressão digital? Primeiramente, seria necessário analisar o caso concreto da presumida agressão, qual a extensão dos seus danos? A agressão teve repercussões no mundo real ou se ateve ao ciberespaço? A operação gerou efeitos análogos aos de um ataque cinético? Essas são questões que, à primeira vista, podem parecer simples, contudo, a complexidade da temática está exatamente em conseguir responde-las, esse é o desafio que recai sobre os Estado, em matéria de uma possível guerra cibernética, visto que, a depender das respostas, o direito ao uso da força restaria dúbio.

Como exposto, não parecem restar dúvidas quanto quais operações e ataques cibernéticos recairiam sob o prisma do princípio do uso da força e, conseqüentemente, ensejariam o direito à legítima defesa por parte do estado vitimado, para tanto, a jurisprudência, bem como o julgado previamente mencionado restou claro quanto este entendimento:

Uma categoria restrita de ataque à rede de computadores é facilmente tratada. A CNA especificamente destinada a causar danos físicos diretos a bens tangíveis ou ferimentos ou morte a seres humanos é razoavelmente caracterizada como uso de força armada e, portanto, enquadrada na proibição. Assim, nos exemplos acima, a destruição do gasoduto e o corte de energia para o hospital são exemplos de CNA que o ator sabe que pode, e pretende, causar diretamente destruição e ferimentos graves. [...]¹⁴⁷

Aqui, o real problema são as operações que não recairiam necessariamente na compreensão análoga a um ataque armado, ou a um uso da força elevado que ensejaria o direito à legítima defesa, qual seria o limite em matéria de um ataque cibernético, no que tange a distinção entre um uso da força brando e um elevado?

[...] A coerção armada não é definida pelo emprego ou liberação de energia cinética, mas sim pela natureza dos resultados diretos causados, especificamente danos físicos e lesões humanas.¹⁴⁸ [...] (grifo nosso)

Sob a afirmação do Professor Schmitt supracitada, um dos responsáveis pela produção do Manual de Tallinn, a grande diferença entre um uso da força elevado, ou uma coerção

¹⁴⁶ SCHMITT. Michael N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework (1999). Columbia Journal of Transnational Law, Vol. 37, 1998-99. p. 912. pp. 885-938. Tradução Livre de: “[...] Computer network attack challenges the prevailing paradigm, for its consequences cannot easily be placed in a particular area along the community values threat continuum. The dilemma lies in the fact that CNA spans the spectrum of consequentiality. Its effects freely range from mere inconvenience (e.g., shutting down na academic network temporarily) to physical destruction (e.g., as in creating a hammering phenomenon in oil pipelines so as to cause them to burst) to death (e.g., shutting down power to a hospital with no back-up generators).”

¹⁴⁷ *Ibidem*. p. 913. Tradução Livre de: “One narrow category of computer network attack is easily dealt with. CNA specifically intended to directly cause physical damage to tangible property or injury or death to human beings is reasonably characterized as a use of armed force and, therefore, encompassed in the prohibition. Thus, in examples above, the pipeline destruction and the shutting of power to the hospital are examples of CNA which the actor knows can, and intends to, directly cause destruction and serious injury. [...]”

¹⁴⁸ *Ibidem*. p. 913. Tradução livre de: “[...] Armed coercion is not defined by whether or not kinetic energy is employed or released, but rather by the nature of the direct results caused, specifically physical damage and human injury.”

armada, que seria análoga a um ataque armado e um uso da força brando seria, necessariamente, a natureza e o resultado do ataque ou operação. Não restando dúvidas quanto a capacidade responsiva nos casos análogos ao de um ataque armado, nos resta discutir a capacidade responsiva relativa às operações não análogas a ataques armados.

A Relevância da temática assenta-se em duas questões, a primeira, como identificar tal ataque, a segunda, quais os limites do Estado vitimado em responder a esses ataques, particularmente no que tange o princípio da proporcionalidade.

2.2 – O PROBLEMA DA CAPACIDADE RESPONSIVA EM MATÉRIA DE LEGÍTIMA DEFESA SOB A NOVA LÓGICA DA GUERRA

Visto que nos deparamos com a problemática da conceitualização do Uso da Força no ciberespaço, é preciso tecer algumas considerações sobre essa matéria sob a luz da legítima defesa, visto que não há de se falar em responsividade sem tangenciar sobre o conceito de legítima defesa.

Ainda que a busca pelas limitações do uso da força tenha assumido a tônica do mundo pós-guerra, os plenipotenciários não excluíram a possibilidade de seu emprego na circunstância de um ato defensivo, ou seja, entendeu-se como legítimo e legal o emprego do uso da força se, e somente se, nos casos de legítima defesa:

Artigo 51

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, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. [...] ¹⁴⁹

Como já extensivamente trabalhado na seção anterior, aqui temos problemas diversos, dentre eles, semânticos, da ordem de conceitualização do termo “ataque armado”, contudo, esse problema é elevado a um outro patamar quando passamos a analisá-lo sob a ótica da nova lógica da guerra; primeiro por esta lançar mão de meios e métodos, a priori, não diretos e não cinéticos, em outras palavras, o conceito “armado”, não se faz presente em um primeiro momento; segundo, quando tratamos de operações cibernéticas, essencialmente não estamos falando de um “ataque armado”, mas sim de uma operação que pode, analogicamente, ser compreendida como tal, isso se formos tomar por base uma análise extensiva do conceito, como pretende Tallinn.

A Carta das Nações Unidas não esclarece com precisão o que se enquadra no conceito de ataque armado. Pelo contrário, no decorrer de seu texto faz menção à “força armada” (preâmbulo), “atos de agressão” (artigo 1, item 1; artigo 39), “controvérsias internacionais” (art. 1, item 3), “ameaça ou uso da força”, “emprego de forças armadas” (artigo 41, artigo 43, item 1), “demonstrações, bloqueios e outras operações, por parte das forças aéreas, navais ou terrestres” (artigo 42), “emprego de força” (artigo 44), “ação coercitiva internacional” (artigo 45), “ataque armado” (artigo 51). ¹⁵⁰

Para tanto, o problema foi objeto de discussão pela ONU, ensejando a formulação da Resolução 3.314 de 1974, em uma tentativa de se definir ou, ao menos tangenciar o conceito de ataque armado, agressão, dentre outros. Aqui, parece fortuito destacar que as discussões acerca da matéria não se limitaram à respectiva Resolução, uma tentativa de melhor enquadrar

¹⁴⁹ ONU. Carta das Nações Unidas. p. 32. Disponível em: < <https://brasil.un.org/sites/default/files/2022-05/Carta-ONU.pdf> >. Acessado em: 01 de fevereiro de 2022.

¹⁵⁰ SILVA. Carla Ribeiro Volpini; ROSA. Patricia Rodrigues. O Uso da Força em Direito Internacional – Legítima Defesa Preemptiva. p. 8. Disponível em: < <http://www.publicadireito.com.br/artigos/?cod=a08c938c1e7c76d8> > Acessado em: 05 de dezembro de 2021.

o conceito de agressão já fora objeto de debate pela Organização, contudo, como avaliado à época, a natureza da guerra moderna (aqui é imperioso destacar que estamos trabalhando em 1945), tornava impossível definir o termo “agressão”:

Na Conferência das Nações Unidas sobre Organização Internacional, realizada em São Francisco de 25 de abril a 26 de junho de 1945, várias delegações propuseram que o termo “agressão”, contido na seção B do Capítulo VIII das Propostas de Dumbarton Oaks (que mais tarde se tornou o Capítulo VII da Carta), ser definida ou explicada, mas a maioria do Comitê III/3, trabalhando com essas questões, achava que uma definição preliminar do termo ia além do escopo da Carta e que as modernas técnicas de guerra davam qualquer definição de “agressão” impossível (ver Relatório do Sr. Paul-Boncour, Relator, sobre o Capítulo VIII, Seção B, Doc. 881 (inglês) III/3/46, 10 de junho de 1945, Conferência das Nações Unidas sobre Organização Internacional, Vol. 12, p. . 505).¹⁵¹

Se em 1945 a percepção era de que a “nova” lógica da guerra tornara impossível definir os conceitos de agressão, em face das operações realizadas durante a Segunda Guerra e o novo dogmatismo do conflito que se avizinhava, sob o manto da Guerra Fria, na atualidade, em que discutimos conceitos como “Guerras Híbridas”, “Guerras Omnidimensionais”, “Guerras Cibernéticas”, dentre outros modelos, os desafios presentes de definição tornam-se ainda mais titânicos. No bojo da supracitada Resolução, alguns pontos merecem atenção:

Artigo 1

Agressão é o uso de força armada por um Estado contra a soberania, integridade territorial ou independência política de outro Estado, ou de qualquer outra forma inconsistente com a Carta das Nações Unidas, conforme estabelecido nesta Definição.
[...]

Artigo 3

Qualquer dos seguintes actos, independentemente de declaração de guerra, qualifica-se, sob reserva e de acordo com o disposto no artigo 2.º, como acto de agressão:

a) A invasão ou ataque pelas forças armadas de um Estado do território de outro Estado, ou qualquer ocupação militar, ainda que temporária, resultante de tal invasão ou ataque, ou qualquer anexação pelo uso da força do território de outro Estado ou parte dele;

b) Bombardeio pelas forças armadas de um Estado contra o território de outro Estado **ou o uso de qualquer arma por um Estado contra o território de outro Estado**;

[...]

d) Um ataque das forças armadas de um Estado às forças terrestres, marítimas ou aéreas, ou às frotas marítimas e aéreas de outro Estado;

[...]

f) A acção de um Estado ao permitir que o seu território, que colocou à disposição de outro Estado, seja utilizado por esse outro Estado para perpetrar um acto de agressão contra um terceiro Estado;

g) O envio, por ou em nome de um Estado, de bandos, grupos, irregulares ou mercenários armados que pratiquem atos de força armada contra outro Estado de tal

¹⁵¹ UNITED NATIONS. Definition of Aggression General Assembly Resolution 3314 (XXIX). United Nations Audiovisual Library of International Law. 2008. p. 1. Disponível em: < https://legal.un.org/avl/pdf/ha/da/da_ph_e.pdf > Acessado em: 05 de dezembro de 2021. Tradução livre de: “At the United Nations Conference on International Organization, held in San Francisco from 25 April to 26 June 1945, several delegations proposed that the term “aggression”, contained in section B of Chapter VIII of the Dumbarton Oaks Proposals (which later became Chapter VII of the Charter), be defined or explained, but the majority of Committee III/3, working with these issues, thought that a preliminary definition of the term went beyond the scope of the Charter and that the modern techniques of warfare rendered any definition of “aggression” impossible (see Report of Mr. Paul-Boncour, Rapporteur, on Chapter VIII, Section B, Doc. 881 (English) III/3/46, 10 June 1945, United Nations Conference on International Organization, Vol. 12,p. 505).”

gravidade que correspondam aos atos acima listados, ou seu envolvimento substancial neles.¹⁵² (grifo nosso)

Mais uma vez fica aparente o problema da inserção do termo “força armada”, contudo, a Resolução tratou do tema sob o aspecto de força armada também enquanto instituição estatal, do contrário não distinguiria expressamente forças armadas de grupos armadas, na mesma linha, não buscaria expressar na resolução ações contra instituições típicas de forças armadas nacionalmente constituídas (a exemplo de exército, aeronáutica e marinha, como disposto no item “d”).

Se formos tomar por base o conceito de forças armadas trazido pela Resolução, poderíamos interpretar a restritividade de operações cibernéticas, contanto que possam ser análogas a ataques armados e contanto que partam de organizações pertencentes às forças armadas. Contudo, resta pouca dúvida que uma operação cibernética, no contexto de um ataque partindo de uma divisão ou de infraestrutura militar, se enquadrem enquanto uma violação, podendo recair em quebra do princípio da não intervenção (em casos brandos), ou no emprego do uso da força, sendo o problema o reconhecimento e a responsabilização pelo ataque.

Contudo, a resolução nos abre dois grandes campos de análise sob a ótica da nova lógica da guerra, particularmente, sobre a possibilidade de enquadrarmos operações cibernéticas, enquanto atos de agressão, o primeiro é disposto no Artigo 3 (b), “(...) uso de qualquer arma por um Estado contra o território de outro Estado”¹⁵³. Como mencionado na cessão anterior, a Convenção de Genebra avançou quanto a ideia do emprego de armas e sua consequente evolução, não sendo mais um conceito estanque, estando muito mais vinculado ao emprego do artifício do que do objeto em si¹⁵⁴.

¹⁵² UNITED NATIONS. Resolution 3314 (XXIX). Definition of Aggression. General Assembly – Twenty-ninth Session. 2319th plenary meeting. 14 December 1974. p. 143. Disponível em: < [https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/3314\(XXIX\)](https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/3314(XXIX)) > Acessado em: 12 de fevereiro de 2022. Disponível em: “Article 1 Aggression is the use of armed force by a State Against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition.[...] Article 3 Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provisions of article 2, qualify as an act of aggression: a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or parte thereof; b) Bombardment by the armed forces of a State Against the territory of another State or the use of **any weapons by a State against the territory of another State;** [...] d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State; e)[...] f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State; The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.”

¹⁵³ *Ibidem*. p. 143

¹⁵⁴ A esse respeito ver Os Protocolos Adicionais às Convenções de Genebra de 12 de Agosto de 1949.

Por essa razão, *softwares* e outros instrumentos e mecanismos digitais podem e em alguns casos, devem ser vistos enquanto armas e, em muitos casos (dentre os quais já tratados neste trabalho), possivelmente desenvolvidos por Estados enquanto ferramentas contra outros Estados ou organizações, passivelmente recaindo sob o manto do Artigo 3 (b).

Nessa mesma linha, o item (g) nos proporciona um outro campo de observação sobre as operações cibernéticas e as Guerras Híbridas. A ideia do emprego de forças não convencionais, ou seja, mercenários, grupos insurgentes, dentre outros em operações que amontem a um ataque armado enquanto um ato de agressão, delimita o escopo enquanto operações cibernéticas e de insurgência poderiam ser interpretadas. Aqui, mais uma vez, esbarramos no termo “ataque armado”, ainda que a utilização de nacionais terceiros, em operações cibernéticas de desestabilização de rede, de danos controlados à infraestrutura crítica, dentre outros, bem como o fomento a insurgentes, possam não caracterizar uma equivalência a um ataque armado desde a decisão da Corte no caso Nicarágua vs Estados Unidos, a Resolução impôs um marco.

Por fim, outro ponto que merece menção é o item (f), a proibição e o reconhecimento de utilização de um Estado terceiro enquanto “base operacional” para a prática de um ato de agressão, ganha nova roupagem se formos levar em consideração a natureza das operações cibernéticas que, não somente podem ser realizadas de qualquer parte do mundo que permitam o uso de equipamentos digitais, como também podem fazer uso de infraestrutura de rede de um país terceiro enquanto base de operações. Em suma, um país ou grupo, poderia fazer uso da rede de computadores de outro país (com seu consentimento ou não) para lançar uma operação ou um ataque cibernético, um exemplo disso foi o próprio ataque à Estônia.

Ainda nessa linha, grupos operacionais ou células terroristas ou insurgentes, a mando de um país, poderiam realizar ataques do país em que se encontram a um outro, como também já apresentado anteriormente. Para tanto, a limitação da possibilidade de uso de outros Estados enquanto verdadeiras bases de operação é tema extremamente pertinente ao tema da nova lógica da guerra e o emprego de seus novos aparatos. O tema também foi objeto no Julgado do Canal de Corfu “(...) e a obrigação de todo Estado de não permitir conscientemente que seu território seja usado para atos contrários aos direitos de outros Estados”¹⁵⁵. Sobre a interpretação do mencionado item ao julgado podemos trazer o seguinte excerto:

Este dispositivo compreenderia duas situações básicas: 1) quando um Estado permite o uso de seu território para que um outro Estado pratique diretamente um ato de agressão contra um terceiro Estado através de suas forças armadas (isto é, um ataque

¹⁵⁵ ICJ, International Court of Justice. Reports of Judgments, Advisory Opinions and Orders The Corfu Channel Case (Merits). Judgment of April 9th, 1949 p. 22. Disponível em: < <https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf> >. Acessado em: 12 de janeiro de 2022. Tradução livre de: and every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States

armado ou invasão); e 2) quando um Estado permite que um outro Estado use o seu território para, indiretamente, através de grupos armados, de irregulares, cometer ato de agressão contra um terceiro Estado. No primeiro caso, o ataque armado pode envolver forças terrestres (exército) que transitem pelo território do outro Estado, ou forças navais que transitem pelo seu mar territorial, ou até mesmo um ataque aéreo através do espaço aéreo daquele Estado. Em qualquer caso, a redação do dispositivo deixa claro que tanto o Estado que pratica o ataque armado como aquele que permite o uso de seu território são agressores. O segundo caso é menos claro, mas poderia dizer-se que o Estado que permite o uso de seu território por grupos armados estaria praticando um ato de agressão nos termos desse item, ao passo que o Estado que enviasse ou apoiasse tal grupo estaria cometendo um ato de agressão nos termos do item g seguinte.¹⁵⁶

Delineadas as questões, resta compreender a inserção da legítima defesa sob a ótica da nova lógica da guerra. Ainda que a questão do ataque armado permaneça, ao menos sob a ótica da norma, a complexidade da questão leva-nos a necessidade de analisar caso a caso, não por outra razão, questões como o Julgado da Nicarágua vs Estados Unidos, ainda que à primeira vista pareçam destoantes, revelam a necessidade de uma análise pontual, o mesmo deve ser observado em possíveis operações cibernéticas. Desta feita, ainda que as lacunas existentes constituam campos de oportunidade, as mesmas são passíveis de uma interpretação que enseja o emprego da legítima defesa:

O que se percebe é que a extensão do termo “ataque armado” deve ser restrita, por se tratar a legítima defesa de prerrogativa que abre aos Estados a possibilidade de perpetrarem ação armada unilateral, comprometendo a paz e segurança internacionais. Acontece que a doutrina e jurisprudência vêm entendendo que a qualificação de um ato como “ataque armado” deve ser feita diante de cada caso concreto, o que nos coloca diante de uma instabilidade jurídica.¹⁵⁷

A resposta a um ataque cibernético apresenta algumas particularidades, dentre elas, a da aplicação do princípio da proporcionalidade, a legítima defesa no Direito Internacional possui conceitos semelhantes ao da legítima defesa em matéria de Direito interno, resguardadas as particularidades, dentre elas, a da referida proporcionalidade:

A licitude do uso da força em legítima defesa depende da obediência de algumas condições, sob pena de se configurar como um novo ataque unilateral e, portanto, ser caracterizado como ilegítima. As condições a que se submete a legítima defesa no plano internacional são as mesmas que fundamentam a alegação de legítima defesa no plano interno dos países.

O que se verifica no plano interno é que a legítima defesa é um ato que se permite tendo em vista uma situação excepcional: ataque efetivo ou iminente contra a integridade física de alguém, que se legitima a fim de suprir uma carência temporária da autoridade pública: prestação de segurança. O poder público, posteriormente, analisa a alegação de legítima defesa, depois de cessada a agressão (por intermédio do Ministério Público).¹⁵⁸

¹⁵⁶ I.M. Lobo de Souza. O conceito de agressão armada no Direito Internacional. Revista de Informação Legislativa. a. 33n. 129 jan./mar. 1996. Senado Federal, Brasília. 1996. p. 154. Disponível em: < <https://www2.senado.leg.br/bdsf/bitstream/handle/id/176388/000506405.pdf?sequence=1&isAllowed=y> > Acessado em: 06 de novembro de 2021.

¹⁵⁷ SILVA. Carla Ribeiro Volpini; ROSA. Patricia Rodrigues. O Uso da Força em Direito Internacional – Legítima Defesa Preemptiva. p. 8. Disponível em: < <http://www.publicadireito.com.br/artigos/?cod=a08c938c1e7c76d8> > Acessado em: 05 de dezembro de 2021. p. 11

¹⁵⁸ *Ibidem*. p. 11 – 12.

Vejamos sob a seguinte ótica, ainda que um Estado se veja ameaçado por um outro Estado com, por exemplo, o deslocamento de exércitos para suas fronteiras, o Estado ameaçado não teria direito de iniciar um ataque, alegando defesa preventiva (ainda que a temática mereça reflexões), contudo, caso esse Estado que iniciou a mobilização, invada suas fronteiras ou dê claros indícios de uma iminente invasão, o Estado ameaçado terá direito de se defender. Aqui é que entra o princípio da proporcionalidade, visto que, o ataque em resposta a agressão, não poderá exceder a própria agressão:

A legítima defesa deve obedecer ao critério da proporcionalidade em relação ao ato agressor. Trata-se de uma resposta ao risco grave, atual ou iminente. O objetivo da legítima defesa é limitado a pôr termo a uma ação agressora inicial. Em nenhuma hipótese a reação defensiva deverá exceder o ato que a autorizou. O artigo 51 não autoriza, por exemplo, uma ocupação militar prolongada e a anexação de um território pertencente ao agressor. Os meios e a extensão da defesa não podem ser desproporcionais à gravidade do ataque¹⁵⁹

Em termos gerais, não poderá um Estado violado em sua parcialidade, violar a integralidade de seu agressor como resposta a agressão, tão pouco poderá o Estado anexá-lo, eliminá-lo, ou cometer qualquer outro ato que não seja uma resposta proporcional, em matéria de extensão e capacidade no emprego bélico.

É exatamente por essa razão, que a resposta a um ataque cibernética ganha um nível de complexidade, como então um Estado responderia a um ataque no ciberespaço? Inicialmente parece óbvio que essa resposta deveria se dar somente no confinamento do mesmo espaço, contudo, há de se falar em proporcionalidade no espaço digital? Um ataque à infraestrutura digital de um país extremamente dependente de sua rede tem repercussões completamente distintas de um ataque a uma nação que ainda não se encontra plenamente integrada ou dependente da rede de computadores:

A escolha das armas pelo Estado atacante é imaterial. Conforme salientado pela Corte Internacional de Justiça, no seu Parecer de 1996, sobre a legalidade da Ameaça ou uso de Armas Nucleares, o art. 51 não se refere a armas específicas; ele se aplica a qualquer ataque armado, independentemente da arma empregada. Em outras palavras, um ataque armado pode ser realizado de forma convencional ou não convencional, de forma primitiva ou sofisticada. No despertar do terceiro milênio, o que desponta no horizonte é um “ataque em rede pelo computador”. Se tal agressão causasse fatalidades (resultando por exemplo no fechamento de sistemas computadorizados que controlam as redes de abastecimento de água e represas, causando a inundação de regiões habitadas), esse fato seria qualificado como um ataque armado¹⁶⁰

Isso ficou claro com os ataques a Estônia, a interdependência do país levou a um dano considerável a infraestrutura crítica do país, como já apresentado anteriormente, outro exemplo

¹⁵⁹ VELOSO, Ana Flávia. Ação relativa a ameaças à paz, ruptura da paz e atos de agressão: artigo 51. In BRANT, Leonardo Nemer Caldeira (Org.). Comentário à Carta das Nações Unidas. Belo Horizonte: Centro de Direito Internacional, 2008. p. 779.

¹⁶⁰ DINSTEIN, Yoram. Guerra, Agressão e Legítima Defesa. São Paulo: Manole, 2004. p. 255.

claro foram os ataques supostamente realizados pela Rússia à infraestrutura crítica da Ucrânia, na recente invasão ao país¹⁶¹. Em contrapartida, a suposta resposta ucraniana em matéria de operação cibernética teve pouco ou nenhum dano a infraestrutura russa, limitando-se somente a retirada de páginas oficiais russas da internet ou o *defacing*¹⁶² de outras¹⁶³.

Contudo, as operações cibernéticas no solo ucraniano não tiveram início no limiar das receitas incursões militares, ainda em 2014, com a manifestação de independência dos territórios de Donbass, uma série de ataques cibernéticos foram diagnosticados por especialistas:

Em maio de 2014, logo após a declaração de independência dos territórios de Donbass em relação ao governo de Kiev, a CyberBerkut, composta por membros das forças policiais ucranianas, grupo 'separatista' dessa região, assumiu a autoria dos ataques cibernéticos que atingiram os serviços de telefonia celular dos membros do Parlamento ucraniano. Os ciber ataques dificultaram a comunicação e o processo decisório a respeito da invasão russa ao território da Crimeia.

Os ataques ocasionaram a queda de diversos websites do governo, incluindo o do gabinete presidencial. O grupo obteve acesso a documentos confidenciais e disponibilizou-os, periodicamente, em sua página na rede.

[...]

De acordo com o relatório do F-Secure Labs (2014), uma variação denominada BlackEnergy2 da mesma família dos malwares utilizados em ciberataques contra a Geórgia (2008) foi utilizada contra alvos políticos do governo ucraniano.¹⁶⁴

Aqui vemos um problema com a proporcionalidade, se formos limitá-la ao espaço de atuação dos ataques, por essa mesma razão, o Manual de Tallinn trouxe algumas considerações, as quais traremos à baila na próxima seção.

Outra questão são os danos causados pelo bloqueio ou indisponibilidade de informações, ações estatais podem ser afetadas, seja pela sua descontinuidade, seja pela sua desestruturação, contudo, esses são danos limitados ao mundo cibernético, ainda que suas repercussões no mundo real sejam tangíveis, o que se tem de dano direto é quantificado somente nos softwares e, em raros casos, nos hardwares, esses assumindo um outro grau de complexidade.

¹⁶¹ A esse respeito ver: PAGLIUSI, Paulo Sergio. Guerra Cibernética Russo-Ucraniana – Lições para o Brasil e o Mundo. Crypto ID. 21 de março de 2022. Disponível em: < <https://cryptoid.com.br/ciberseguranca-seguranca-da-informacao/defesa/guerra-cibernetica-russo-ucraniana-licoes-para-o-brasil-e-o-mundo/>> Acessado em: 12 de abril de 2022.

¹⁶² A esse respeito ver: RODRIGUES, João Guerreiro. Por dentro do exército de hackers voluntários que quer salvar a Ucrânia. Quem são e o que fazem. CNN Portugal. 22 de março de 2022. Disponível em: < <https://cnnportugal.iol.pt/guerra/russia/por-dentro-do-exercito-de-hackers-voluntarios-que-quer-salvar-a-ucrania-quem-sao-e-o-que-fazem/20220322/62339f9a0cf2c7ea0f1ff93b>>. Acessado em> 24 de março de 2022

¹⁶³ A esse respeito ver: REUTERS, G1. Site oficial do Kremlin está fora do ar em meio à guerra na Ucrânia. G1 Globo. 26 de fevereiro de 2022. Disponível em: < <https://g1.globo.com/tecnologia/noticia/2022/02/26/site-oficial-do-kremlin-esta-fora-do-ar-em-meio-a-guerra-na-ucrania.ghtml>>. Acessado em: 24 de março de 2022.

¹⁶⁴ CASALUNGA, Fernando Henrique. Guerra Híbrida Cibernética: Uma Análise do Conflito Rússia-Ucrânia (2014-2016) Sob a Perspectiva da Tecnologia da Informação. ENABED, 10 Encontro Nacional da Associação Brasileira de Estudos de Defesa. 2018. p. 12. Disponível em: < https://www.enabed2018.abedef.org/resources/anais/8/1534467151_ARQUIVO_casalungafh_guerra_hibrida_cibernetica_uma_analise.pdf>. Acessado em: 14 de janeiro de 2022

Um ataque cibernético pode causar danos no mundo real, para além dos danos colaterais, da indisponibilidade ou bloqueio de um sistema, isso pode ocorrer como um objetivo direto do ataque, como visto no caso do *Stuxnet*, onde o objetivo principal era atrasar o programa nuclear iraniano, o vírus tinha como alvo as centrífugas, desse modo, o vírus levava a uma mudança na velocidade das centrífugas, o que, em alguns casos, causava danos físicos nas instalações, para além dos danos as máquinas infectadas.

Antes que possamos analisar essa questão mais a fundo, façamos um outro exercício, suponhamos que o ataque à Estônia, que teve como um dos alvos, sua infraestrutura crítica, tivesse ocorrido em intensidade e violência consideravelmente maiores, sob essa ótica, suponhamos que esse ataque tivesse atingido o setor energético estoniano, desabilitando a rede de fornecimento elétrico, advindo deste fato e, estendendo nossa suposição para que esse dano perdurasse por tempo suficiente, reatores e baterias auxiliares sessariam, deste fato, poderíamos começar a ver falecimentos em hospitais, com a completa inoperabilidade de respiradores.

Aqui temos dois problemas os quais nos deteremos neste momento, o primeiro diz respeito a ataques que façam uso da infraestrutura de rede (ciberespaço), para causar efeitos e danos no espaço real, sendo este, o objetivo precípua, o segundo, por sua vez, referencia ataques realizados no ciberespaço, mas que causem danos ao espaço físico, de forma colateral, não sendo este, o alvo principal ou primário, visto que o objetivo é danificar ou desativar o *software*.

Mister salientar alguns conceitos básicos para se compreender critérios passíveis de aplicação de responsividade no campo da legítima defesa que, poderiam ser empregados em caso de um ataque cibernético, tais critérios foram problematizados pelo Professor Schmitt, na necessidade de se analisar uma reposta, baseada em casos concretos:

- 1) Gravidade: Ataques armados ameaçam danos físicos ou destruição de propriedade em um grau muito maior do que outras formas de coerção. O bem-estar físico geralmente ocupa o ápice da hierarquia humana de necessidades.
- 2) Imediatismo: as consequências negativas da coerção armada, ou sua ameaça, geralmente ocorrem com grande imediatismo, enquanto as de outras formas de coerção se desenvolvem mais lentamente. Assim, a oportunidade para o Estado alvo ou a comunidade internacional buscar acomodações pacíficas é prejudicada no primeiro caso.
- 3) Objetividade: as consequências da coação armada estão mais diretamente ligadas ao *actus reus* do que em outras formas de coerção, que muitas vezes dependem de inúmeros fatores contributivos para operar. Assim, a proibição da força exclui com maior certeza consequências negativas.
- 4) Invasão: na coerção armada, o ato que causa o dano geralmente atravessa o estado alvo, enquanto na guerra econômica os atos geralmente ocorrem além das fronteiras do alvo. Como resultado, embora os atos armados e econômicos possam ter consequências aproximadamente semelhantes, o primeiro representa uma maior intrusão nos direitos do Estado alvo e, portanto, é mais provável que perturbe a estabilidade internacional.
- 5) Mensurabilidade: enquanto as consequências da coerção armada são geralmente fáceis de determinar (por exemplo, um certo nível de destruição), as consequências negativas reais de outras formas de coerção são mais difíceis de medir. Este fato torna

a adequação da condenação da comunidade, e o grau de veemência nela contido, menos suspeito no caso da força armada.

6) Legitimidade Presuntiva: na maioria dos casos, seja no direito interno ou internacional, a aplicação da violência é considerada ilegítima na ausência de algumas exceções específicas, como legítima defesa. A abordagem cognitiva é proibitiva. Em contraste, a maioria das outras formas de coerção – novamente nas esferas doméstica e internacional – são presumivelmente lícitas, na ausência de proibição em contrário. A abordagem cognitiva é permissiva. Assim, as consequências da coerção armada são presumivelmente inadmissíveis, enquanto as de outros atos coercitivos não são (como uma regra muito generalizada).¹⁶⁵

Cumpra esclarecer que os critérios são atinentes ao emprego da força, ou seja, uso de coerção armada, ficando clara a distinção trazida por outras formas de coerção, aqui, a severidade e natureza do ataque ou operação cibernética ditariam a interpretação quanto a sua natureza, seria passível de ser visto como uma coerção armada ou estaria alinhada a outra forma de coerção? Aqui importante destacar que não se exclui a ilicitude do ato, somente seu grau, cabendo, ainda, resposta de alguma natureza.

Sob a ótica da legítima defesa, pesam três grandes problemas quando tratamos de operações cibernéticas, sendo estes o da necessidade, proporcionalidade e os critérios de identificação quanto a autoria da agressão. Sobre o primeiro, está ligado a necessidade militar, o enfoque das respostas deve se ater a objetivos militares e somente a ações que objetivem o cessar das hostilidades, a proporcionalidade está vinculada a ideia de que as respostas devem ser proporcionais aos ataques, para além disso, os ataques não devem exceder as vantagens militares percebidas¹⁶⁶.

¹⁶⁵ SCHMITT, Michael N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework (1999). Columbia Journal of Transnational Law, Vol. 37, 1998-99. p. 915. pp. 885-938 p. Tradução livre de: “1) *Severity*: Armed attacks threaten physical Injury or destruction of property to a Much greater degree than other forms of coercion. Physical well-being usually occupies the apex of the human hierarchy of need. 2) *Immediacy*: the negative consequences of armed coercion, or threat thereof, usually occurs with great immediacy, while those of other forms of coercion develop more slowly. Thus, the opportunity for the target state or the international community to seek peaceful accommodations is hampered in the former case. 3) *Directness*: the consequences of armed coercion are more directly tied to the *actus reus* than in other forms of coercion, which often depend on numerous contributory factors to operate. Thus, the prohibition on force precludes negative consequences with greater certainty. 4) *Invasiveness*: in armed coercion, the act causing the harm usually crosses into the target state, whereas in economic warfare the acts generally occur beyond the target’s borders. As a result, even though armed and economic acts may have roughly similar consequences, the former represents a greater intrusion on the rights of the target state and, therefore, is more likely to disrupt international stability. 5) *Measurability*: while the consequences of armed coercion are usually easy to ascertain (e.g., a certain level of destruction), the actual negative consequences of other forms of coercion are harder to measure. This fact renders the appropriateness of community condemnation, and the degree of vehemence contained therein, less suspect in the case of armed force. 6) *Presumptive Legitimacy*: in most cases, whether under domestic or international law, the application of violence is deemed illegitimate absent some specific exceptions such as self-defense. The cognitive approach is prohibitory. By contrast, most other forms of coercion – again in the domestic and international sphere – are presumptively lawful, absent a prohibition to the contrary. The cognitive approach is permissive. Thus, the consequences of armed coercion are presumptively impermissible, whereas those of other coercive acts are not (as a very generalized rule).”

¹⁶⁶ A respeito dos princípios supracitados ver: CICV. Glossário de Direito Internacional Humanitário (DIH) Para Profissionais da Mídia e; CANÇADO TRINDADE, Antônio Augusto. Princípios do Direito Internacional Contemporâneo. 2. Ed. Ver. Atual. Brasília: FUNAG. 2017.

Em matéria de legítima defesa, um ataque cibernético só poderia ser passível de resposta se fosse possível identificar seu operador e, se esse operador fosse um agente estatal e, ou, diretamente vinculado ou a mando de um Estado, seria necessário ainda que esta operação pudesse ser interpretada de forma análoga a uma operação armada.

A questão da identificação posa como uma dificuldade normativa e técnica, a natureza da rede mundial de computadores é exatamente de sua interconectividade, ainda que os sistemas digitais possuam uma espécie de “DNA”, ou registro “único”, na forma de IPs, a tecnologia permite mascarar esses mesmos registros, ou até mesmo assumir uma nova “identidade”, um agente de país “A” pode mascarar sua máquina para parecer de país “B” e atacar “C”, ou ainda, poderia o agente do país “A”, invadir e utilizar a infraestrutura de rede do país “B” para atacar “C”. Como então imputar a real autoria?

Outra questão delicada é a atribuição de autoria, a identificação da origem de um ataque e a caracterização da intenção hostil, especialmente importantes e complexas levando em conta os ataques remotos e anônimos, a constante invenção de novas técnicas e a possibilidade de utilizar estruturas e atores inocentes, pois a regra da legítima defesa não autoriza atos de defesa ativa além das fronteiras se a provocação não puder ser atribuída a outro país, assim como protege pessoas e bens civis.

Um sistema normativo que exige a determinação da autoria e a caracterização da intenção hostil do ataque cibernético – requisitos passíveis de manipulação quando não se tornam inviáveis - para então autorizar o exercício da legítima defesa, é incompatível com a realidade cibernética e ineficiente para lidar com protagonistas que atuam sem as restrições impostas pela legalidade. O diálogo das fontes jurídicas e técnicas deverá ajudar a comunidade internacional a definir as cautelas necessárias.¹⁶⁷

Ainda nessa linha, a nova lógica da guerra nos apresenta problemas de natureza imaterial no campo das operações. Imaterial, no sentido de que as operações, sejam elas cibernéticas ou não, tendem a assumir características típicas da guerra híbrida ou da guerra omnidimensional, são operações que visam ganhar o suporte da população civil do país alvo, são operações de desestabilização, são operações que, muitas vezes, são identificadas somente quando seus resultados já podem ser sentidos, como, por exemplo, na eclosão de uma guerra civil.

Aqui, outro problema se apresenta no quesito de capacidade responsiva, como poderia um Estado responder a uma campanha de desestabilização, que faz uso de meios digitais? Sem sombra de dúvidas, esse Estado pode se defender sob um ponto de vista interno, seja por intermédio de contrainteligência, seja por intermédio de propaganda e identificação dos meios pelos quais as operações estejam sendo realizadas, contudo, como poderia esse Estado, ao identificar a nação beligerante, responder a essa agressão? Há um inegável ataque à soberania

¹⁶⁷ SALDAN, Eliane. Os Desafios Jurídicos da Guerra no Espaço Cibernético. Dissertação de Mestrado. Instituto Brasiliense de Direito Público – IDP. Brasília. 2012. p. 86 – 87. Disponível em: < https://repositorio.idp.edu.br/bitstream/123456789/1223/1/Disserta%C3%A7%C3%A3o_Eliane%20Saldan.pdf >. Acessado em: 24 de fevereiro de 2022.

do Estado, especialmente se essas campanhas de desestabilização ou de propaganda e de fomento a insurgentes, interfira diretamente em eleições ou na própria organização social do Estado.

A soberania, direito imprescindível do Estado-Nação de autodeterminar-se no campo interno e nas suas relações internacionais era, tradicionalmente, resguardada por determinados cuidados preventivos, particularmente nas áreas de informações e proteção territorial. A invasão territorial inevitável pela informação de todo tipo e rapidez dos transportes modernos, encurtando drasticamente as distancias, vem obrigando os Estados a rever os antigos critérios de atenção na preservação preventiva de suas respectivas soberanias. Os tradicionais meios de proteção territorial dos Estados soberanos mostram-se, hoje, incapazes de impedir esta invasão de imagens sonoras e visuais, difundindo ideias, propaganda e operações financeiras de empresas multinacionais.¹⁶⁸

Difícilmente nesse caso poderemos falar em proporcionalidade, do contrário teríamos um cenário semelhante ao da Guerra Fria, com constantes violações das normativas, é importante ressaltar que a legítima defesa não é aplicável somente a uma agressão cinética, mas sim a uma violação comprovada a sua integridade, seja física (territorial), seja política (organizacional, social e econômica), sendo a violação do princípio da Não Intervenção Nos Assuntos Internos dos Estado¹⁶⁹, passível de resposta sob a lógica da legítima defesa ressalvadas as observações já dispostas, como da violabilidade dos princípios basilares à aplicação da Legítima Defesa, bem como entendimento da Corte Internacional de Justiça.

Contudo, o problema permanece, como responder a esse tipo de agressão? A violação da soberania e da integridade de um Estado, por meios digitais, sob a nova lógica da guerra, sem a utilização de um aparato militar e, ou, de meios cinéticos, pode ser avaliado sob os auspícios do princípio da proporcionalidade? Se sim, o que seria “proporcional”, nos casos em que esses “ataques” ou operações, não causem danos cinéticos ou análogos a danos cinéticos?

A legítima defesa contra ataques cibernéticos pode dar-se de três formas: forma física, eletrônica ou através de meios cibernéticos. Física na medida em que podem ser atacadas através de meios físicos, infraestruturas do atacante bem como os seus servidores. De forma eletrônica, dar-se-á através do uso de energia eletromagnética com o objetivo de impedir ou reduzir o uso efetivo do espectro eletromagnético do oponente. Por último, a legítima defesa por uso de meios cibernéticos, poderá ser passiva ou ativa. Enquanto as medidas passivas não envolvem poder coercivo, a defesa ativa é coerciva.¹⁷⁰

Alguns desses questionamentos foram alvo de estudos por especialistas de vários Estados, o que levou a formulação do Manual de Tallinn, ponto que será objeto de estudo no

¹⁶⁸CARDOSO, Paulo Roberto. *Diatética Cultural: Estado, soberania e defesa cultural*. Belo Horizonte: Universidade Federal de Minas Gerais, 2016, p. 47-48. (Tese, Doutorado em Direito).

¹⁶⁹ A esse respeito ver: SILVA, Alexandre Pereira da. Os Princípios das relações internacionais e os 25 anos da Constituição Federal. Revista de Informação Legislativa. Ano 50. Número 200. out/dez 2013. Senado Federal. Brasília. Disponível em: < https://www12.senado.leg.br/ril/edicoes/50/200/ril_v50_n200_p15.pdf >. Acessado em: 17 de dezembro de 2021.

¹⁷⁰ p. 36. Disponível em: < https://repositorio.ul.pt/bitstream/10451/37376/1/ulfd136516_tese.pdf >. Acessado em: 22 de dezembro de 2021.

próximo capítulo, contudo, a questão da legítima defesa na forma tratada pelo Manual merece atenção.

Regra 71 – Autodefesa contra-ataque armado

Um Estado que seja alvo de uma operação cibernética que atinja o nível de um ataque armado pode exercer seu direito inerente de autodefesa. Se uma operação cibernética constitui um ataque armado depende de sua escala e efeitos.

[....]

2. O Grupo Internacional de Peritos observou que os termos "ataque armado" e "agressão" devem ser distinguidos. Esta Regra trata da legítima defesa, para a qual a condição precedente é um ataque armado. A agressão, por outro lado, é uma das situações em que o Conselho de Segurança da ONU pode empregar seus poderes sob o Capítulo VII da Carta da ONU (Regra 76). Embora um ato de agressão possa constituir um ataque armado, nem sempre pode fazê-lo.

[...]

4. O direito de empregar a força em legítima defesa se estende além dos ataques armados cinéticos àqueles que são perpetrados exclusivamente por meio de operações cibernéticas. O Grupo Internacional de Especialistas concluiu por unanimidade que algumas operações cibernéticas podem ser suficientemente graves para justificar classificá-las como um "ataque armado" na acepção da Carta. Essa conclusão está de acordo com a insistência da Corte Internacional de Justiça em seu parecer consultivo sobre Armas Nucleares de que a escolha do meio de ataque é irrelevante para a questão de saber se uma operação se qualifica como um ataque armado.¹⁷¹

Ainda que o Manual tenha buscado respostas para muitos dos questionamentos, muitas questões vitais ficaram sem resposta definitiva por parte do grupo de especialistas:

9. Os Peritos observaram que a lei não é clara quanto ao ponto preciso em que os efeitos de uma operação cibernética qualificam essa operação como um ataque armado. Na sentença da Nicarágua, a Corte Internacional de Justiça distinguiu entre um ataque armado e um "mero incidente de fronteira". Essa distinção tem sido criticada por vários comentaristas que adotam a visão de que apenas ações inconsequentes devem ser excluídas. A este respeito, a Corte Internacional de Justiça indicou posteriormente que um ataque a uma única plataforma ou instalação militar pode ser qualificado como um ataque armado.

10. Um caso que ilustra a natureza instável do limite de ataque armado é o da operação Stuxnet de 2010. À luz dos danos que a operação causou às centrífugas iranianas, alguns membros do Grupo Internacional de Peritos consideraram que ela atingiu o limiar de ataque armado (a menos que justificável com base em legítima defesa antecipada (Regra 73)). Outros Peritos foram de opinião contrária, embora, conforme discutido na Regra 68, todos os membros considerassem isso um uso da força.

11. Uma questão importante é se um Estado pode exercer o direito de autodefesa em resposta a uma série de incidentes cibernéticos que individualmente caem abaixo do limiar de um ataque armado. Em outras palavras, eles podem constituir um ataque armado quando agregados? O Grupo Internacional de Peritos concordou que o fator

¹⁷¹ SCHMITT, Michael N. (Ed). NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations. 2 Ed. ISBN 978-1-316-63037-2. New York, NY: Cambridge University Press, 2017. p. 339-340. Tradução livre de: "Rule 71 – Self-defence against armed attack A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects. [...] 2. The International Group of Experts noted that the terms 'armed attack' and 'aggression' must be distinguished. This Rule deals with self-defence, for which the condition precedent is an armed attack. Aggression, by contrast, is one of the situations in which the UN Security Council may employ its powers under Chapter VII of the UN Charter (Rule 76). Although an act of aggression can constitute an armed attack, it may not always do so. [...] 4. The right to employ force in self-defence extends beyond kinetic armed attacks to those that are perpetrated solely through cyber operations. The International Group of Experts unanimously concluded that some cyber operations may be sufficiently grave to warrant classifying them as an 'armed attack' within the meaning of the Charter. This conclusion is in accord with the International Court of Justice's insistence in its Nuclear Weapons advisory opinion that the choice of means of attack is immaterial to the issue of whether an operation qualifies as an armed attack."

determinante é se o mesmo originador (ou originadores agindo em conjunto) realizou incidentes de menor escala que estão relacionados e que, em conjunto, atendem à escala e aos efeitos necessários. Se houver provas convincentes de que este é o caso, há motivos para tratar os incidentes como um ataque armado composto.¹⁷²

A exemplificação trazida pelo parágrafo 10 acerca da operação do Stuxnet demonstra quão problemática é a manutenção da lacuna existente atualmente, não estamos tratando nesse caso particular de um exercício especulativo e sim de uma operação real que teve consequências reais, consequências que, em grande medida, permaneceram sem resposta por parte do Estado vitimado.

Por fim, Schmitt apresenta alguns cenários de possíveis respostas, na circunstância de um ataque cibernético ocorrer:

- 1) Se o ataque à rede informática equivaler ao uso da força armada, o Conselho de Segurança pode caracterizá-lo como acto de agressão ou ruptura da paz e autorizar a resposta contundente nos termos do artigo 42.º da Carta. Para constituir um ataque armado, o CNA deve ter como objetivo causar diretamente danos físicos a objetos tangíveis ou ferimentos a seres humanos.
- 2) Se a CNA não constituir um ataque armado, o Conselho de Segurança pode, no entanto, considerá-la uma ameaça à paz (ausência de violência interestatal) e autorizar o uso da força para evitar a subsequente ruptura da paz. A CNA não precisa significar um uso da força antes que o Conselho possa determinar que ela ameaça a paz.
- 3) Os Estados, agindo individual ou colectivamente, podem responder a uma CNA de ataque armado com recurso à força, nos termos do artigo 51.º e do direito inerente de legítima defesa.
- 4) Os Estados, agindo individual ou coletivamente, podem responder a uma CNA que não constitua ataque armado, mas que seja parte integrante de uma operação destinada a culminar em ataque armado quando:
 - a) Os atos em legítima defesa ocorrerem durante a última janela de oportunidade disponível para combater eficazmente o ataque; e
 - b) O CNA é um passo irrevogável em um ataque iminente (de curto prazo) e provavelmente inevitável.¹⁷³

¹⁷² *Ibidem*. p. 341-342. Tradução livre de: “9. The Experts noted that the law is unclear as to the precise point at which the effects of a cyber operation qualify that operation as an armed attack. In the Nicaragua judgment, the International Court of Justice distinguished between an armed attack and a ‘mere frontier incident’. This distinction has been criticised by numerous commentators who adopt the view that only inconsequential actions should be excluded. In this regard, the International Court of Justice has subsequently indicated that an attack on a single military platform or installation might qualify as an armed attack. 10. A case illustrating the unsettled nature of the armed attack threshold is that of the 2010 Stuxnet operation. In light of the damage the operation caused to Iranian centrifuges, some members of the International Group of Experts were of the view that it reached the armed attack threshold (unless justifiable on the basis of anticipatory selfdefence (Rule 73)). Other Experts took the contrary view, although, as discussed in Rule 68, all members considered it a use of force. 11. An important issue is whether a State may exercise the right of self-defence in response to a series of cyber incidents that individually fall below the threshold of an armed attack. In other words, can they constitute an armed attack when aggregated? The International Group of Experts agreed that the determinative factor is whether the same originator (or originators acting in concert) has carried out smaller-scale incidents that are related and that taken together meet the requisite scale and effects. If there is convincing evidence that this is the case, there are grounds for treating the incident as a composite armed attack.”

¹⁷³ SCHMITT. Michael N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework (1999). Columbia Journal of Transnational Law, Vol. 37, 1998-99. p. 936. pp. 885-938 p. Tradução livre de: “If the computer network attack amounts to a use of armed force, then the Security Council may characterize it as an act of aggression or breach of peace and authorize of forceful response under article 42 of the Charter. To constitute an armed attack, the CNA must be intended to directly cause physical damage to tangible objects or injury to human beings. 1) If the CNA does not constitute an armed attack, the Security Council may nevertheless find it to threaten the peace (the absence of Inter-state violence) and authorize the use of force to prevent the subsequent breach of peace. The CNA need not amount to a use of force before the Council may

É interessante observar que o artigo em questão foi produzido em 1998-1999, anos antes da produção do primeiro Manual de Tallinn, ainda assim, muitas das questões que viriam a ser objeto do estudo já foram objeto de análise, contudo, muito do trabalho ainda compreende o campo especulativo, partindo de concepções e exercícios de suposição, sem que, contudo, qualquer demérito à temática. Contudo, aqui vale a distinção dos excertos trazidos no supracitado artigo, para as passagens retiradas do Manual de Tallinn, a evolução do estudo especulativo para a análise de casos de operações cibernéticas concretas em conjunto ao exercício de especulação, a fim de gerar um estudo analógico da temática.

Questões que escoam do mero campo especulativo e encontram guarida no mundo real assumiram considerável relevância aos estudos do Manual de Tallinn, documento que, ainda que não possua força normativa, teceu ricos e valorosos comentários acerca da temática do Direito Humanitário aplicável às operações cibernéticas, comentários esses que nos ateremos (ainda que em escopo reduzido) no próximo capítulo e que entendemos viabilizar aplicação fática.

determine that it threatens peace. 2) States, acting individually or collectively, may respond to a CNA amounting to armed attack with the use of force pursuant to article 51 and the inherent right of self-defense. 3) States, acting individually or collectively, may respond to a CNA not amounting to armed attack, but which is an integral part of an operation intended to culminate in armed attack when: a) The acts in self-defence occur during the last possible window of opportunity available to effectively counter the attack; and b) The CNA is an irrevocable step in an imminent (near-term) and probably unavoidable attack.”

CAPÍTULO III – TALLINN E UM NOVO MARCO NORMATIVO

Neste capítulo pretendemos tecer algumas considerações acerca do Manual de Tallinn, desde sua aplicação e intento, até suas possíveis interpretações e extensões aplicativas, para tanto e, tendo em vista a extensão do Manual (aqui focaremos o estudo na versão 2.0), dividimos o Capítulo em 2 (duas) sessões, que entendemos atender aos objetivos da pesquisa.

Primeiramente nos atemos ao problema da soberania, apresentando os aspectos clássicos da ideia, até a interpretação extensiva trazida pelo Manual, quanto a aplicação da aplicação da soberania do espaço digital. Este é um ponto de extrema relevância se levarmos em consideração que a ideia do uso da força só pode ser entendida se aplicada em teor de violação da soberania do Estado violado.

Contudo, por tratarmos de novas teorias de guerra bem como da aplicação das mesmas nas novas lógicas de conflito, não parecia nos bastar o conceito clássico de soberania para responder aos novos problemas impostos. Este parece ter sido o mesmo questionamento recorrente dentre o grupo de especialistas responsáveis por Tallinn, visto que seus estudos levaram a importantes concepções no campo da soberania e de suas possíveis violações.

Em outro momento, trazemos um estudo analógico da possibilidade de interpretação e aplicação do Manual de Tallinn enquanto *Rule of Engagement*, apresentando a roupagem deste tipo de documento, bem como sua aplicabilidade e, ponderando quanto a aplicabilidade do Manual enquanto uma espécie de “doutrina” para os ROE, aplicados a nova lógica da guerra.

Importante compreender que, ainda que Tallinn não possa ser considerado um instrumento propriamente jurídico, a sua utilização na produção de ROE poderia garantir legitimidade, inclusive no ponto de vista punitivo, quanto aos agentes que o descumprissem. Não obstante, foi possível observar que muitos ROE compreendem questões ligadas a operações digitais, sem, contudo, a profundidade que o próprio Manual de Tallinn apresenta.

O presente capítulo buscou debruçar-se sobre os excertos do Manual de Tallinn 2.0, edição que sucedam o Manual de Tallinn de 2013. A versão 2.0 buscou expandir a temática da legislação internacional aplicável à guerra cibernética também para os tempos de paz, compreendendo um monumental volume de normas e comentários acerca das normas possivelmente aplicáveis a situações que envolvem operações cibernéticas.

A primeira versão surgiu após os ataques realizados contra a Estônia, mais precisamente à sua capital Tallinn, o que levou a OTAN a iniciar um trabalho que, em última instância levou a formulação do Manual pelo grupo de especialistas:

Os ataques também aceleraram o estabelecimento do Centro de Excelência Cooperativa de Defesa Cibernética da OTAN (NATO CCD COE) em Tallinn. A

Estônia tem a honra de sediar e contribuir para este grupo de reflexão e instituição de treinamento de classe mundial que é um parceiro valioso para a OTAN, os Aliados e a comunidade internacional. Entre as primeiras atividades do CCD COE da OTAN foi encomendar um grande estudo sobre guerra cibernética realizado por um grupo internacional de especialistas jurídicos. Os especialistas examinaram como o direito internacional rege o uso da força cibernética pelos Estados e o emprego de operações cibernéticas durante um conflito armado. O Manual de Tallinn resultante tornou-se um guia para governos de todo o mundo à medida que avaliam a aplicação do direito internacional em tais situações.¹⁷⁴

Em face do sucesso e da dimensão da publicação, o Centro de Excelência de Cooperação em Defesa Cibernética da OTAN deu início aos preparativos para a versão 2.0 que encapsularia a produção da primeira versão, somada as questões que governariam atividades e operações cibernéticas e sua legislação afeta em matéria internacional aos tempos de paz:

Após a publicação do Manual de Tallinn em 2013, o CCD COE da OTAN lançou um esforço de pesquisa para expandir o Manual para abranger a lei internacional que rege as atividades cibernéticas que ocorrem em tempos de paz. O resultado é de longe uma das análises mais abrangentes do direito internacional aplicável às operações cibernéticas. A publicação que você está segurando cobre tópicos que vão desde a lei espacial e jurisdição até direito internacional dos direitos humanos, bem como uma análise do direito de conflito do primeiro Manual de Tallinn.¹⁷⁵

Sob esse prisma, buscamos traçar abordagens quanta a natureza do manual, sua aplicação, limitação e possibilidade interpretativa e analógica, mister destacar que, em momento algum, o Manual de Tallinn pretendeu esgotar a temática relativa à norma internacional aplicável às operações cibernéticas, tão pouco intuiu ser um tratado ou documento legal, contudo, não se esquivou de seu possível norte aplicável:

[...] A criação do segundo Manual de Tallinn não foi restringida pela política e o livro servirá como um roteiro para os governos que buscam maior clareza sobre seus direitos e obrigações no ciberespaço. O livro também será útil para a comunidade internacional enquanto luta com a complexidade de identificar normas cibernéticas existentes e promulgar novas.¹⁷⁶

¹⁷⁴ SCHMITT, Michael N. (Ed). NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations. 2 Ed. ISBN 978-1-316-63037-2. New York, NY: Cambridge University Press, 2017. Prefácio p. 23. Tradução livre de: “The attacks also sped up the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in Tallinn. Estonia is honoured to host and contribute to this world-class think tank and training institution that is a valued partner for NATO, Allies, and the international community. Among the NATO CCD COE’s first activities was to commission a major study on cyber warfare conducted by an international group of legal experts. The experts examined how international law governs the use of cyber force by States and the employment of cyber operations during an armed conflict. The resulting Tallinn Manual has become a guidebook for governments around the world as they assess the application of international law in such situations.”

¹⁷⁵ *Ibidem*. p. 23. Tradução livre de: “Upon publication of the Tallinn Manual in 2013, the NATO CCD COE launched a follow-on research effort to expand the Manual to encompass the international law governing cyber activities occurring in peacetime. The outcome is by far one of the most comprehensive analyses of international law applicable to cyber operations. The publication you are holding covers topics ranging from space law and jurisdiction to international human rights law, as well as an analysis of conflict law from the first Tallinn Manual.”

¹⁷⁶ *Ibidem*. p. 24. Tradução livre de: “[...] The creation of the second Tallinn Manual has been unconstrained by politics and the book will serve as a road-map for governments as they seek greater clarity regarding their rights and obligations in cyberspace. The book will also be useful to the international community while struggling with the complexity of identifying extant cyber norms and promulgating new ones.”

3.1 – O PROBLEMA DA SOBERANIA NO CIBERESPAÇO E A PROPOSTA EM TALLINN

O conceito de soberania, a despeito da evolução histórica, em grande parte permaneceu estático quanto a seu entendimento, sendo o questionamento quanto a suas limitações, restrito ao campo da política, contudo, a ideia do Estado Soberano pareceu revolucionária no momento de sua concepção, principalmente por garantir aos Estados à época, a argumentação necessária à legitimação de suas existências, igualmente, nações opositoras argumentavam que suas soberanias extrapolavam suas limitações geográficas, em muitos casos.

Aqui, é preciso fazer uma distinção quanto a própria ideia de soberania, ainda que pareça ser algo claro, devemos analisar essa lógica sob ótica das novas tecnologias e dos novos espaços de poder, é inquestionável que a soberania territorial, em matéria geográfica é pouco questionável, sendo clara, bem definida e, juridicamente, inquestionável. Tanto de um ponto de vista interno, quanto externo, a soberania é exercida através da força, do poder coercitivo, no primeiro caso através da justiça e do poder punitivo do Estado e, no segundo, através do aparato militar, diplomático e político, sendo este segundo, o que nos interessa nesse trabalho.

Contudo, as novas tecnologias e os novos meios de comunicação e interação extrapolam as limitações do espaço físico, muitas vezes se confundindo com este. Aqui estamos falando, particularmente, do espaço digital. A internet criou uma nova fronteira de interação humana, onde as relações são travadas, de maneira plena, não sendo essas relações, limitadas somente aos particulares. Hoje, muitas das interações interestatais, sejam elas econômicas, comerciais, políticas e sociais, são travadas de forma digital.

Ainda que esse “admirável mundo novo”¹⁷⁷ soe de forma utópica, muitos questionamentos acerca destes novos espaços permeiam o debate, especialmente acerca dos limites “territoriais” dos espaços digitais.

Como o campo virtual deve ser visto? De forma análoga ao espaço físico? Ciberespaço é uma extensão do espaço físico ou é uma dimensão própria, dotada de regras próprias? Qual a extensão de nossas normas e suas aplicações aos espaços digitais? esses são questionamentos necessários e que ocuparam o grupo de especialistas ligados a formação do Manual de Tallinn.

A relevância desta discussão está no cerne do problema do limite do próprio emprego da legítima defesa e das operações cibernéticas, só há de se falar em legítima defesa em matéria

¹⁷⁷ Aqui o termo foi inserido entre aspas, de forma a referenciar a obra Aldous Huxley, “Admirável mundo novo”, ficção distópica que apresenta uma sociedade futurística, altamente dependente da tecnologia, ao ponto de criar uma espécie de escravidão sistêmica, é uma distopia mascarada por uma realidade que se apresenta como utópica. A esse respeito ver. HUXLEY, Aldous Leonard. **Admirável mundo novo**. Brasil, Biblioteca Azul, 2014.

internacional se houver uma violação à soberania do Estado vítima, desta feita, para que haja a violação do espaço soberano de um Estado, através das redes virtuais, seria necessário que esse ataque violasse ou se estendesse ao espaço físico. Em outras palavras, seria preciso que uma operação cibernética causasse danos físicos, contudo, como vimos anteriormente, nem todos os ataques têm repercussão no espaço físico.

Para esses casos específicos, seria necessário modificar o entendimento secular, da própria soberania, o que pareceu o mais apropriado para o grupo de especialistas, estendendo a ideia de soberania para o espaço digital, concebendo este como uma extensão do espaço físico de cada Estado e de seus servidores:

Regra 1 – Soberania (princípio geral)

O princípio da soberania do Estado aplica-se no ciberespaço

Regra 2 – Soberania Internacional

Um estado goza de autoridade soberana em relação à infraestrutura cibernética, pessoas e atividades cibernéticas localizadas em seu território, sujeitas às suas obrigações legais internacionais

Regra 4 - Violação de soberania

Um Estado não deve realizar operações cibernéticas que violem a soberania de outro Estado.¹⁷⁸

Segundo o Manual, os Estados detêm soberania sobre toda e qualquer infraestrutura cibernética que esteja localizada em sua territorialidade e, em alguns casos, sobre estruturas que não estejam localizadas em sua circunscrição, caso exerçam jurisdição sobre essas. Cumpre destacar que essa mesma soberania e jurisdição vem acompanhada de prerrogativas e obrigações, inerentes em matéria de Direito Internacional à soberania estatal:

1. [...] Em particular, os Estados gozam de soberania sobre qualquer infraestrutura cibernética localizada em seu território e atividades associadas a essa infraestrutura cibernética. Embora a territorialidade esteja no cerne do princípio de soberania, em certas circunstâncias, os Estados também podem exercer prerrogativas soberanas, como jurisdição sobre infraestrutura cibernética e atividades no exterior, bem como sobre certas pessoas envolvidas nessas atividades (Regras 10-11). Por fim, a natureza territorial da soberania também impõe restrições às operações cibernéticas de outros Estados direcionadas à infraestrutura cibernética localizada em território soberano (ver discussão adicional na Regra 4).

[...]

3. Vários princípios e regras do direito internacional convencional e consuetudinário derivam do princípio geral da soberania. Exemplos incluem aqueles relacionados à jurisdição (Capítulo 3), incluindo a obrigação de respeitar certas imunidades de outros Estados (Regra 5), e o princípio da devida diligência (Regra 6).¹⁷⁹

¹⁷⁸ SCHMITT, Michael N. (Ed). NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations. 2 Ed. ISBN 978-1-316-63037-2. New York, NY: Cambridge University Press, 2017. p. 11-17. Tradução livre de: “Rule 1 – Sovereignty (general principle) The principle of State sovereignty applies in cyberspace Rule 2 – International sovereignty A state enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations Rule 4 – Violation of sovereignty A State must not conduct cyber operations that violate the sovereignty of another State.”

¹⁷⁹ *Ibidem*. p. 11-12. Tradução livre de: “1. [...] In particular, States enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure. Although territoriality lies at the heart of the principle of sovereignty, in certain circumstances, States may also exercise sovereign prerogatives such as jurisdiction over cyber infrastructure and activities abroad, as well as over certain persons engaged in those

Sob essa perspectiva, o grupo de especialistas dividiu a soberania no espaço digital em 03 (três), camadas, uma ligada ao espaço físico, representada pelos *hardwares*, outra composta pelo espaço lógico, compreendida pelas aplicações, dados e operações que garantem a interconectividade dos aparelhos e da infraestrutura de rede para a transferência de dados e uma terceira camada, compreendida pelo tecido social, composta pelos indivíduos que utilizam a infraestrutura de rede, usuários *latu senso*.

4. Para os fins deste Manual, as camadas física, lógica e social do ciberespaço estão englobadas no princípio da soberania. A camada física compreende os componentes físicos da rede (ou seja, hardware e outras infraestruturas, como cabos, roteadores, servidores e computadores). A camada lógica consiste nas conexões que existem entre os dispositivos de rede. Inclui aplicativos, dados e protocolos que permitem a troca de dados na camada física. A camada social engloba indivíduos e grupos envolvidos em atividades cibernéticas.¹⁸⁰

Ainda nessa linha, o manual concebeu que toda e qualquer operação cibernética que tenha como objetivo, intervir nas ações e, ou, organizações internas de um país, é ilegítima, sendo uma violação direta à soberania do Estado afetado, desta feita, uma operação cibernética não necessita de ter repercussões bélicas somente, qualquer ação que afeta as relações comerciais ou políticas de um Estado, que façam uso de infraestrutura digital, ainda assim seriam consideradas violações da soberania do Estado, passíveis de resposta à luz do Direito à Legítima Defesa.

Regra 66 – Intervenção dos Estados

Um Estado não pode intervir, inclusive por meios cibernéticos, nos assuntos internos ou externos de outro Estado.

1. O ciberespaço oferece aos Estados oportunidades de intervenção nos assuntos internos ou externos de outros Estados, em particular devido ao aumento da conectividade global e à crescente dependência dos Estados da tecnologia da informação. Esta Regra proíbe a intervenção coercitiva, inclusive por meios cibernéticos, por um Estado nos assuntos internos ou externos de outro. Baseia-se no princípio da soberania do direito internacional, especificamente aquele aspecto do princípio que prevê a igualdade soberana dos Estados (Regras 1-3). O Grupo Internacional de Peritos concordou que a proibição de intervenção é uma norma do direito internacional consuetudinário. De fato, os Estados expressam ou recorrem regularmente ao princípio. Além disso, a Corte Internacional de Justiça, organizações internacionais e a Comissão de Direito Internacional reconhecem o status costumeiro da proibição.

2. Esta Regra trata de situações em que um Estado intervém por meios cibernéticos nos "assuntos internos ou externos" (conforme discutido abaixo) de outro Estado, por exemplo, usando operações cibernéticas para alterar remotamente cédulas eletrônicas

activities (Rules 10–11). Finally, the territorial nature of sovereignty also places restrictions on other States' cyber operations directed at cyber infrastructure located in sovereign territory (see further discussion in Rule 4). [...] 3. A number of principles and rules of conventional and customary international law derive from the general principle of sovereignty. Examples include those relating to jurisdiction (Chapter 3), including the obligation to respect certain immunities of other States (Rule 5), and the principle of due diligence (Rule 6)."

¹⁸⁰ *Ibidem*. p. 12. Tradução livre de: "4. For the purposes of this Manual, the physical, logical, and social layers of cyberspace are encompassed in the principle of sovereignty. The physical layer comprises the physical network components (i.e., hardware and other infrastructure, such as cables, routers, servers, and computers). The logical layer consists of the connections that exist between network devices. It includes applications, data, and protocols that allow the exchange of data across the physical layer. The social layer encompasses individuals and groups engaged in cyber activities."

e, assim, manipular uma eleição. Também abrange situações em que um Estado intervém por meios não cibernéticos em atividades cibernéticas relacionadas aos assuntos internos ou externos de outro Estado. Por exemplo, esta Regra proibiria o uso por um Estado de meios não cibernéticos coercitivos para obrigar outro Estado a adotar uma legislação doméstica específica relacionada à responsabilidade do provedor de serviços de Internet ou a se abster de se tornar Parte de um tratado multilateral que trata de desarmamento cibernético ou direitos humanos online (sobre direitos humanos, ver também Capítulo 6)¹⁸¹

Aqui algumas questões merecem atenção, a primeira diz respeito aos próprios exemplos utilizados pelo Manual, como a interferência em eleições, fato que tem sido objeto de questionamentos nos últimos pleitos, não somente nacionais, como internacionais, a esse respeito podemos mencionar a possível interferência russa nas eleições americana que elegeram Donal Trump:

O governo russo interferiu nas eleições presidenciais de 2016 de forma abrangente e sistemática. Evidências de operações do governo russo começaram a surgir em meados de 2016. Em junho, o Comitê Nacional Democrata e sua equipe de resposta cibernética anunciaram publicamente que hackers russos haviam comprometido sua rede de computadores. Os lançamentos de materiais hackeados — hacks que os relatórios públicos logo atribuíram ao governo russo — começaram no mesmo mês. Lançamentos adicionais seguiram em julho através da organização WikiLeaks, com outros lançamentos em outubro e novembro.

No final de julho de 2016, logo após a primeira divulgação de documentos roubados pelo WikiLeaks, um governo estrangeiro entrou em contato com o FBI sobre um encontro em maio de 2016 com o conselheiro de política externa da campanha Trump, George Papadopoulos. Papadopoulos havia sugerido a um representante desse governo estrangeiro que a Campanha de Trump havia recebido indicações do governo russo de que poderia ajudar a Campanha por meio da divulgação anônima de informações prejudiciais à candidata presidencial democrata Hillary Clinton. Essa informação levou o FBI em 31 de julho de 2016 a abrir uma investigação sobre se indivíduos associados à Campanha Trump estavam coordenando com o governo russo suas atividades de interferência.¹⁸²

¹⁸¹ *Ibidem*. p. 312-313. Tradução livre de: “Rule 66 – Intervention by States A State may not intervene, including by cyber means, in the internal or external affairs of another State. 1. Cyberspace presents States with opportunities for intervention in other States’ internal or external affairs, in particular due to increasing global connectivity and the growing reliance of States on information technology. This Rule prohibits coercive intervention, including by cyber means, by one State into the internal or external affairs of another. It is based on the international law principle of sovereignty, specifically that aspect of the principle that provides for the sovereign equality of States (Rules 1–3). The International Group of Experts agreed that the prohibition of intervention is a norm of customary international law. Indeed, States regularly express or resort to the principle. Moreover, the International Court of Justice, international organisations, and the International Law Commission recognise the prohibition’s customary status. 2. This Rule addresses situations in which a State intervenes by cyber means in the ‘internal or external affairs’ (as discussed below) of another State, for example, by using cyber operations to remotely alter electronic ballots and thereby manipulate an election. It also encompasses situations in which a State intervenes by non-cyber means in cyber activities related to the internal or external affairs of another State. For instance, this Rule would prohibit the use by one State of non-cyber coercive means to compel another State to adopt particular domestic legislation related to Internet service provider liability or to refrain from becoming Party to a multilateral treaty dealing with cyber disarmament or human rights online (on human rights, see also Chapter 6)”

¹⁸² U.S. Department of Justice. Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volume I of II. Washington D.C. March 2019. p. 1. Tradução livre de: “The Russian government interfered in the 2016 presidential election in sweeping and systematic fashion. Evidence of Russian government operations began to surface in mid-2016. In June, the Democratic National Committee and its cyber response team publicly announced that Russian hackers had compromised its computer network. Releases of hacked materials—hacks that public reporting soon attributed to the Russian government—began that same month. Additional releases followed in July through the organization WikiLeaks, with further releases in October and November. In late July 2016, soon after WikiLeaks’s first release of stolen documents, a foreign government contacted the FBI

Ainda que o documento tenha concluído a existência de indícios de interferência nas eleições, a participação do candidato supostamente favorecido, não pode ser confirmada, contudo, ainda que não tenhamos uma resposta objetiva sobre esse fato, a possibilidade de influenciar decisões íntimas de um Estado mediante ações cibernéticas é um fenômeno não mais restrito às distopias:

Como decidimos não fazer um julgamento tradicional do “Ministério Público”, não tiramos conclusões definitivas sobre a conduta do presidente. As evidências que obtivemos sobre as ações e intenções do presidente apresentam questões difíceis que precisariam ser resolvidas se estivéssemos fazendo um julgamento tradicional do Ministério Público. Ao mesmo tempo, se tivéssemos confiança após uma investigação minuciosa dos fatos que o Presidente claramente não cometeu obstrução de justiça, nós o afirmariamos. Com base nos fatos e nas normas legais aplicáveis, não podemos chegar a esse julgamento. Assim, embora este relatório não conclua que o Presidente cometeu um crime, também não o exonera.¹⁸³

Uma distinção importante trazida pelo manual nessa questão, diz respeito à extensão da coerção, primeiramente, os especialistas entendem que para que uma operação possa ser interpretada como uma quebra no princípio da não intervenção, seria necessário que o Estado interveniente atuasse de modo a violar a soberania de terceiros a fim de mudar um resultado, de atingir um objetivo que violasse decisões íntimas de Estado. Contudo, ainda que uma operação não seja caracterizada como violação do princípio da não intervenção, não significa que ela não seja uma violação à soberania do país violado, essa distinção somente diz respeito à capacidade e possibilidade responsiva.

19. Os Peritos concordaram que a mera coerção não é suficiente para estabelecer uma violação da proibição de intervenção. A maioria dos Especialistas foi de opinião que o esforço coercitivo deve ser projetado para influenciar os resultados ou a conduta em relação a um assunto reservado a um Estado-alvo. Por exemplo, uma campanha cibernética maliciosa de um Estado dirigida contra a infraestrutura cibernética de propriedade de um determinado grupo étnico em um Estado vizinho pode violar a soberania deste último, mas não equivalerá a uma intervenção proibida, pois não se destina a influenciar qualquer resultado ou decisão do Estado alvo. No entanto, se a campanha cibernética for projetada para coagir o Estado a adotar uma posição específica em uma controvérsia étnica interna em andamento, ela se qualificará. Alguns Especialistas entenderam que para ser coercitivo basta que um ato tenha o efeito de privar o Estado do controle da matéria em questão. Assim, no primeiro exemplo acima há, por essa visão, uma intervenção porque o Estado é privado pela

about a May 2016 encounter with Trump Campaign foreign policy advisor George Papadopoulos. Papadopoulos had suggested to a representative of that foreign government that the Trump Campaign had received indications from the Russian government that it could assist the Campaign through the anonymous release of information damaging to Democratic presidential candidate Hillary Clinton. That information prompted the FBI on July 31, 2016, to open an investigation into whether individuals associated with the Trump Campaign were coordinating with the Russian government in its interference activities.”

¹⁸³ *Ibidem*. p. 182. Tradução livre de: “Because we determined not to make a traditional prosecutorial judgment, we did not draw ultimate conclusions about the President’s conduct. The evidence we obtained about the President’s actions and intent presents difficult issues that would need to be resolved if we were making a traditional prosecutorial judgment. At the same time, if we had confidence after a thorough investigation of the facts that the President clearly did not commit obstruction of justice, we would so state. Based on the facts and the applicable legal standards, we are unable to reach that judgment. Accordingly, while this report does not conclude that the President committed a crime, it also does not exonerate him.”

campanha cibernética de seu direito soberano de controlar seus assuntos interétnicos sem interferência externa.

20. O Grupo Internacional de Peritos concordou que, para serem coercitivos para os fins desta Regra, os atos em questão não precisam ser de natureza física. Considere o caso do Estado A que lança operações DDoS direcionadas e altamente disruptivas contra o Estado B na tentativa de obrigar o Estado B a retirar o reconhecimento do Estado C. operações não resultem em consequências físicas não diminui sua caracterização como uma intervenção proibida. Em contrapartida, uma operação cibernética que não busca qualquer mudança de conduta carece do elemento coercitivo necessário.

21. Além disso, a coerção deve ser distinguida da persuasão, crítica, diplomacia pública, propaganda (ver também discussão na Regra 4), retribuição, mera maldade e similares no sentido de que, ao contrário da coerção, tais atividades envolvem meramente influenciar (como distinto de factualmente convincente) as ações voluntárias do Estado alvo, ou não buscar nenhuma ação por parte do Estado alvo [...] A chave é que o ato coercitivo deve ter o potencial de obrigar o Estado alvo a se envolver em uma ação que de outra forma não tomaria (ou abster-se-ia de tomar uma ação que de outra forma tomaria).¹⁸⁴

Sob esse prisma, não há dúvidas de que qualquer campanha digital que tenha por objetivo mudar o resultado de uma eleição, não só é uma violação à soberania de um Estado, como também uma quebra do princípio da não intervenção.

A soberania, ainda que um direito dos Estados, vem carregada de obrigações para estes, especialmente na interpretação do Manual, visto que, o Estado goza de autoridade soberana sobre o espaço digital, bem como da infraestrutura digital localizada em sua territorialidade, desta feita, qualquer operação que afete seus sistemas operacionais seria passível de resposta, bem como qualquer operação que faça uso de sua infraestrutura digital para afetar terceiros.

Regra 6 – Due diligence (princípio geral) Um Estado deve exercer a devida diligência para não permitir que seu território, ou território ou infraestrutura cibernética sob seu

¹⁸⁴ *Ibidem*. p. 318-319. Tradução livre de: “19. The Experts agreed that mere coercion does not suffice to establish a breach of the prohibition of intervention. The majority of Experts was of the view that the coercive effort must be designed to influence outcomes in, or conduct with respect to, a matter reserved to a target State. For example, a State’s malicious cyber campaign directed Against cyber infrastructure owned by a particular ethnic group in a neighbouring State might violate the latter’s sovereignty, but will not amount to prohibited intervention as it is not intended to influence any outcome in, or decision of, the target State. However, if the cyber campaign is designed to coerce the State to adopt a particular position in an ongoing internal ethnic controversy, it will so qualify. A few Experts took the position that to be coercive it is enough that an act has the effect of depriving the State of control over the matter in question. Thus, in the first example above there is, by this view, an intervention because the State is deprived by the cyber campaign of its sovereign right to control its inter-ethnic affairs without outside interference. 20. The International Group of Experts agreed that to be coercive for the purposes of this Rule, the acts concerned need not be physical in nature. Consider the case of State A that launches targeted and highly disruptive DDoS operations against State B in an attempt to compel State B to withdraw recognition of State C. The fact that the cyber operations result in no physical consequences does not detract from their characterisation as a prohibited intervention. By way of contrast, a cyber operation that does not seek any change of conduct lacks the requisite coercive element. 21. Furthermore, coercion must be distinguished from persuasion, criticism, public diplomacy, propaganda (see also discussion in Rule 4), retribution, mere maliciousness, and the like in the sense that, unlike coercion, such activities merely involve either influencing (as distinct from factually compelling) the voluntary actions of the target State, or seek no action on the part of the target State at all [...] The key is that the coercive act must have the potential for compelling the target State to engage in an action that it would otherwise not take (or refrain from taking an action it would otherwise take).”

controle governamental, seja usado para operações cibernéticas que afetem os direitos de, e produzam consequências adversas graves para outros Estados.¹⁸⁵

Ainda nessa linha, o Manual dispõe:

Regra 7 – Cumprimento do princípio de *due diligence* O princípio de *due diligence* exige que um Estado tome todas as medidas que sejam viáveis nas circunstâncias para pôr fim a operações cibernéticas que afetem um direito e produzam graves consequências adversas para outros Estados.¹⁸⁶

Quanto aos comentários trazidos, destacam-se as ideias das obrigações trazidas pelo princípio do *due diligence*, ainda que poucas distinções existam em relação à aplicação do princípio a ações fora do ciberespaço.

2. Um dictum na decisão do caso Canal de Corfu do Tribunal Internacional de Justiça, que observa que "é obrigação de cada Estado não permitir conscientemente que seu território seja usado para atos contrários aos direitos de outros Estados", estabelece a definição contemporânea geralmente reconhecida do princípio da devida diligência. Uma obrigação decorrente da noção de soberania, exige que um Estado "proteja dentro de [seu] território os direitos de outros Estados".

[...]

4. Os Peritos observaram ainda que o princípio da devida diligência há muito se reflete na jurisprudência; é um princípio geral que foi particularizado em regimes especializados de direito internacional. Uma vez que as novas tecnologias estão sujeitas ao direito internacional pré-existente, sem uma exclusão legal, eles concluíram que o princípio da devida diligência se aplica no contexto cibernético.¹⁸⁷

Algumas questões novas, próprias do meio digital merecem atenção, dentre elas, a responsabilidade de um Estado terceiro de exercer *due diligence*, caso seja constada uma operação em curso, em que sua infraestrutura esteja sendo utilizada como passagem de dados maliciosos.

13. O Grupo Internacional de Peritos discutiu a questão de saber se um Estado através do qual os dados transitam apenas, por exemplo, através de um cabo de fibra óptica, assume a obrigação de *due diligence*. Os Peritos diferenciaram essa situação daquela em que uma infraestrutura cibernética específica é instalada no território de um Estado para fins maliciosos, como a que compreende uma botnet. Eles concordaram que, como uma questão estrita de lei, o 'Estado de trânsito' assume a obrigação de devida diligência e deve agir de acordo com a Regra 7 quando (1) possuir conhecimento (sobre conhecimento real e construtivo, veja abaixo) de uma operação infratora que atinge o limite necessário de dano e (2) pode tomar medidas viáveis para efetivamente acabar com ele.¹⁸⁸

¹⁸⁵ *Ibidem*. p. 30. Tradução livre de: "Rule 6 – Due diligence (general principle) A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States."

¹⁸⁶ *Ibidem*. p. 43. Tradução livre de: "Rule 7 – Compliance with the due diligence principle the principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States."

¹⁸⁷ *Ibidem*. p. 31. Tradução livre de: "2. A dictum in the International Court of Justice's Corfu Channel judgment, which observes that 'it is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of Other States', sets forth the generally recognised contemporary definition of the due diligence principle. An obligation deriving from the notion of sovereignty, it requires a State 'to protect within [its] territory the rights of other States'. [...] 4. The Experts further observed that the due diligence principle has long been reflected in jurisprudence; it is a general principle that has been particularised in specialised regimes of international law. Since new technologies are subject to pre-existing international law absent a legal exclusion therefrom, they concluded that the due diligence principle applies in the cyber context."

¹⁸⁸ *Ibidem*. p. 33. Tradução livre de: "13. The International Group of Experts discussed the issue of whether a State through which data only transits, for instance through a fibre optic cable, shoulders the due diligence obligation. The Experts differentiated this situation from that in which specific cyber infrastructure is set up on a State's

É particularmente interessante quando avaliada a questão à luz da lógica clássica dos conflitos armados, se pensarmos que os bits (dados), que estão passando pelo Estado terceiro, podem ser interpretados como soldados ou agentes de um Estado em mobilização para atacar outro, veremos a interpretação trazida pelo manual, ainda que de forma meramente ilustrativa, visto que os dados em curso, não necessariamente terão os mesmos efeitos (cinéticos) de um exército em movimento.

Neste caso, o Manual merece atenção, especialmente tendo em vista as novas teorias das guerras e dos conflitos. Como trabalhado anteriormente, os conflitos não mais se achem ao campo de batalha físico, Nye já havia discriminado a ideia de uma dualidade de poder através do *hard power* e do *soft power* nas relações internacionais, o que a rede de computadores possibilitou, foi a “*weaponization*”¹⁸⁹, dos sistemas digitais para operações de desestabilização, desestruturação e aplicação do *soft power*.

Korybko ao apresentar sua teoria das revoluções coloridas e das Guerras Híbridas, demonstra como as redes sociais foram utilizadas como arma de desestabilização estatal e de fomento a revoluções, no objeto de estudo de sua obra, a Primavera Árabe. Ainda que a propaganda não seja uma novidade, nem que sua aplicação para esses fins seja inovadora, o fomento e a formalização de uma verdadeira infraestrutura digital revolucionária é. Por essa razão, a lógica de violação de soberania precisaria estar em consonância com os novos campos de oportunidade operados nos novos conflitos, em particular, as redes.

Antevendo problemas como os mencionados, o Manual de Tallinn definiu entendimento quanto a violação da soberania, ainda que tema controverso em matéria de violações cibernéticas, para tanto, os comentários trazidos pelo grupo de especialistas merecem atenção.

Regra 4 – Violação de soberania

Um Estado não deve realizar operações cibernéticas que violem a soberania de outro Estado.

1. Conforme observado nas Regras 2 e 3, os Estados gozam de soberania interna e externa, respectivamente. As operações cibernéticas que impeçam ou desrespeitem o exercício de suas prerrogativas soberanas por outro Estado constituem uma violação dessa soberania e são proibidas pelo direito internacional. É claro que em certas situações o direito internacional permite ou prevê exceções à obrigação de respeitar a soberania de outro Estado. Os exemplos paradigmáticos são quando uma ação que violaria a soberania deste último é autorizada pelo Conselho de Segurança (Regra 76) ou é praticada no exercício do direito de legítima defesa (Regra 71).¹⁹⁰

territory for malicious purposes, such as that comprising a botnet. They agreed that, as a strict matter of law, the ‘transit State’ shoulders the due diligence obligation and must act pursuant to Rule 7 when it (1) possesses knowledge (on actual and constructive knowledge, see below) of an offending operation that reaches the requisite threshold of harm and (2) can take feasible measures to effectively terminate it.”

¹⁸⁹ Weaponization é um neologismo inglês, que pode ser entendido como “armar” ou, mais especificamente, transformar algo que naturalmente não teria uma natureza de armamento em uma arma.

¹⁹⁰ SCHMITT, Michael N. (Ed). NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations. 2 Ed. ISBN 978-1-316-63037-2. New York, NY: Cambridge University Press, 2017. p. 17. Tradução livre de: “Rule 4 – Violation of sovereignty A State must not

Para tanto, foi preciso definir o que compreenderia essa lógica de soberania no concernente ao ciberespaço. Aqui, entendeu-se que a infraestrutura cibernética localizada no espaço territorial de um Estado, compreende sua soberania, independente deste ser de propriedade pública ou privada. Isso é relevante quando levamos em consideração as obrigações inerentes ao princípio da *due diligence*, ou seja, caso a infraestrutura cibernética privada de um país seja alvo de um ataque, ainda que essa infraestrutura não tenha qualquer finalidade estatal, o Estado sede desta infraestrutura sofreu uma agressão à sua soberania e poderia responder.

5. Conforme discutido na Regra 2, o princípio da soberania abrange a infraestrutura cibernética localizada no território de um Estado, independentemente de ser uma infraestrutura cibernética governamental ou privada. Por exemplo, se um Estado realiza operações cibernéticas que causam danos à infraestrutura cibernética de uma empresa privada localizada em outro Estado, como infraestrutura crítica de propriedade privada, as ações do primeiro equivalem a uma violação da soberania do segundo Estado. Isso ocorre mesmo que não haja efeito em nenhuma infraestrutura, ativos ou atividades cibernéticas do governo.¹⁹¹

Este é um ponto relevante quando levamos em consideração que uma parte significativa das infraestruturas digitais de Governos ou de sistemas utilizados cotidianamente pela população, estão hospedados em servidores privados, muitas vezes em países distintos dos em que os serviços são prestados, com isso, um ataque que inviabilize ou interrompa os mesmos poderia ensejar não somente uma violação ao país alvo do ataque à infraestrutura, como também do país que venha a ter serviços essenciais afetados de forma drástica, mais uma vez, ensejando à aplicação do princípio de *due diligence*.

4.[...] O Grupo Internacional de Peritos concordou que contramedidas (Regra 20) também podem estar disponíveis contra outro Estado com base no fato de que ele não cumpriu sua obrigação de devida diligência com relação às ações de atores não estatais que operam a partir de seu território (Capítulo 2).¹⁹²

É inegável que caminhamos a passos largos para uma digitalização da própria vida humana, desde as relações mais básicas, como a interação e as relações interpessoais, seja pelas

conduct cyber operations that violate the sovereignty of another State. 1. As noted in Rules 2 and 3, States enjoy internal and external sovereignty, respectively. Cyber operations that prevent or disregard another State's exercise of its sovereign prerogatives constitute a violation of such sovereignty and are prohibited by international law. Of course, in certain situations international law permits or envisages exceptions to the obligation to respect another State's sovereignty. The paradigmatic examples are when an action that would otherwise violate the latter's sovereignty is authorised by the Security Council (Rule 76) or is engaged in pursuant to the exercise of the right of selfdefence (Rule 71)."

¹⁹¹ *Ibidem*. p. 18. Tradução livre de: "5. As discussed in Rule 2, the principle of sovereignty encompasses cyber infrastructure located in a State's territory irrespective of whether it is government or private cyber infrastructure. For instance, if one State conducts cyber operations that cause damage to the cyber infrastructure of a private company located in another State, such as privately owned critical infrastructure, the former's actions amount to a violation of the second State's sovereignty. This is so even though there is no effect on any government cyber infrastructure, assets, or activities."

¹⁹² *Ibidem*. p. 18. Tradução livre de: "4.[...] The International Group of Experts agreed that countermeasures (Rule 20) may also be available against another State on the basis that it has failed to comply with its due diligence obligation with respect to the actions of non-State actors operating from its territory (Chapter 2).

organizações estatais, com a virtualização de documentos e de operações cotidianas das burocracias de Estado. A medida em que a realidade passa por essa dualidade, do físico e do virtual, torna-se derradeira a necessidade de expansão do conceito de soberania ao espaço digital, não somente para proteger o Estado, mas igualmente para garantir direitos básicos aos cidadãos.

Para tanto, o Manual interpretou a norma internacional como aplicável ao espaço digital, manifestando-se de forma hialina, quanto a proibição da intervenção, bem como quanto a proibição do uso da força, inclusive por meios cibernéticos que violem a soberania de um Estado:

11. Quanto à primeira base, os Peritos a analisaram em três níveis distintos: (1) dano físico; (2) perda de funcionalidade; e (3) violação da integridade territorial abaixo do limite de perda de funcionalidade. Em primeiro lugar, a maioria dos Peritos concordou que as operações cibernéticas constituem uma violação da soberania no caso de resultarem em danos físicos ou lesões, como no caso de malware que provoca o mau funcionamento dos elementos de refrigeração dos equipamentos, levando ao superaquecimento que resulta em componentes derretendo. Na medida em que a presença física não consensual no território de outro Estado para realizar operações cibernéticas configura uma violação da soberania, os Peritos concordaram que a causação de consequências físicas por meios remotos naquele território também constitui uma violação da soberania. Ambas as conclusões são consistentes com o objeto e finalidade do princípio da soberania, que protege claramente a integridade territorial contra a violação física. Os Peritos observaram que tais operações também podem constituir uma intervenção proibida (Regra 66), um uso ilegal da força (Regra 68) ou um ataque armado (Regra 71).

[...]

13.[...] Houve total concordância de que uma operação cibernética que exija reparo ou substituição de componentes físicos da infraestrutura cibernética equivale a uma violação porque tais consequências são semelhantes a danos físicos ou ferimentos. A título de exemplo, e assumindo a atribuição a um Estado, o vírus Shamoon que exigiu a reparação ou substituição de milhares de discos rígidos da petrolífera saudita Saudi Aramco em 2012 qualificou-se como uma violação da soberania desse Estado. Os Peritos concordaram ainda que a perda de funcionalidade de equipamentos ou outros itens físicos que dependem da infraestrutura visada para operar constitui uma perda de funcionalidade. Alguns dos Especialistas sugeriram que uma operação cibernética que exija a reinstalação (embora não seja mera reinicialização) do sistema operacional ou outros dados dos quais a infraestrutura cibernética alvo depende para realizar sua finalidade pretendida se qualifica como uma operação que resulta em perda de funcionalidade.[...] ¹⁹³

¹⁹³ SCHMITT, Michael N. (Ed). NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations. 2 Ed. ISBN 978-1-316-63037-2. New York, NY: Cambridge University Press, 2017. p. 20-21. Tradução livre de: “11. As to the first base, the Experts analysed it on three distinct levels: (1) physical damage; (2) loss of functionality; and (3) infringement upon territorial integrity falling below the threshold of loss of functionality. First, most of the Experts agreed that cyber operations constitute a violation of sovereignty in the event they result in physical damage or injury, as in the case of malware that causes the malfunctioning of the cooling elements of equipment, thereby leading to overheating that results in components melting down. To the extent that non-consensual physical presence on another State’s territory to conduct cyber operations amounts to a violation of sovereignty, the Experts concurred that the causation of physical consequences by remote means on that territory likewise constitutes a violation of sovereignty. Both conclusions are consistent with the object and purpose of the principle of sovereignty, which clearly protects territorial integrity against physical violation. The Experts noted that such operations may also constitute prohibited intervention (Rule 66), an unlawful use of force (Rule 68), or an armed attack (Rule 71). [...] 13.[...] There was full agreement that a cyber operation necessitating repair or replacement of physical components of

O Manual apresentou uma nova interpretação da extensão da soberania, ainda que não possua qualquer capacidade legítima de determinar esse entendimento, o fato de um grupo de especialistas (em grande parte, especialistas no campo do Direito Internacional), de diversas nações, terem esse imaginário quanto a soberania e seus novos limites, demonstra que a preocupação quanto as novas fronteiras de interação humana, tem sim permeado o imaginário do pensamento jurídico.

Aqui é preciso redobrada atenção a problemática trazida por Tallinn, primariamente não há de se falar em qualquer capacidade responsiva ou operacional, sem um entendimento expansivo da soberania para as novas fronteiras, visto que não podemos conceber uma ação estatal em um espaço desprovido da própria legitimidade estatal, aqui, então, vemos a tentativa de garantir legitimidade aos Estados, sob o próprio espaço digital.

19. Embora o Grupo Internacional de Especialistas tenha concordado que uma violação de soberania geralmente exige que a operação cibernética em questão ocorra ou se manifeste de outra forma na infraestrutura cibernética no território soberano do Estado afetado, ficou dividido sobre se uma operação cibernética supostamente viola a soberania por meio de interferência com ou usurpação de uma função inerentemente governamental precisa fazê-lo. A maioria dos Especialistas adotou a posição de que, neste caso específico, a soberania é violada, independentemente de onde a operação cibernética ocorra ou se manifeste. Para eles, o fator determinante é se as atividades interferidas se qualificam como funções inerentemente governamentais. Por exemplo, a Estônia anunciou o estabelecimento das chamadas “embaixadas digitais” que permitem ao Estado fazer backup de dados governamentais críticos em outros Estados (ver também discussão na Regra 39). A interferência nesses dados de uma forma que afete o desempenho pela Estônia de suas funções inerentemente governamentais seria, na opinião da maioria, uma violação desta regra. Reconheceram que a operação cibernética em questão também pode violar a soberania do Estado onde a infraestrutura está localizada, uma vez que ocorre no território soberano deste último.¹⁹⁴

cyber infrastructure amounts to a violation because such consequences are akin to physical damage or injury. As an example, and assuming attribution to a State, the Shamoon virus that required repair or replacement of thousands of Saudi Arabia’s oil company Saudi Aramco’s hard drives in 2012 qualified as a violation of that State’s sovereignty. The Experts further agreed that the loss of functionality of equipment or other physical items that rely on the targeted infrastructure in order to operate constitutes a loss of functionality. Some of the Experts suggested that a cyber operation that necessitates reinstallation (albeit not mere rebooting) of the operating system or other data upon which the targeted cyber infrastructure relies in order to perform its intended purpose qualifies as an operation resulting in loss of functionality.[...]”

¹⁹⁴ *Ibidem*. p. 23. Tradução livre de: “19. Although the International Group of Experts agreed that a violation of sovereignty generally requires that the cyber operation in question occur or otherwise manifest on cyber infrastructure in the sovereign territory of the affected State, it was divided over whether a cyber operation purportedly violating sovereignty through interference with or usurpation of an inherently governmental function need do so. The majority of the Experts adopted the position that in this particular case sovereignty is violated irrespective of where the cyber operation occurs or manifests. For them the determinative factor is whether the activities interfered with qualify as inherently governmental functions. For example, Estonia has announced the establishment of so-called ‘digital embassies’ that allow the State to back up critical governmental data in other States (see also discussion in Rule 39). Interference with such data in a way that affects the performance by Estonia of its inherently governmental functions would, by the majority view, amount to a violation of this Rule. They acknowledged that the cyber operation in question might also violate the sovereignty of the State where the infrastructure is located on the basis that it occurs on the sovereign territory of the latter.”

Para tanto, a ideia de que um Estado pode exercer seu poder de coerção e, em última instância, fazer uso de seu poderio bélico no ciberespaço é revolucionário, é compreender que o espaço vital e a própria territorialidade dos Estados Nacionais foi, não somente digitalizada, como também foi expandida.

Por fim, o entendimento de parte dos especialistas inova na concepção quanto a utilização da propaganda nos meios digitais, como uma possível interferência na soberania de outro Estado:

29. Com relação à propaganda, o Grupo Internacional de Peritos concordou que sua transmissão para outros Estados geralmente não é uma violação da soberania. No entanto, a transmissão de propaganda, dependendo de sua natureza, pode violar outras regras do direito internacional. Por exemplo, a propaganda destinada a incitar distúrbios civis em outro Estado provavelmente violaria a proibição de intervenção (Regra 66). Da mesma forma, a propaganda de um navio em trânsito pelo mar territorial torna a passagem não inocente (Regra 48).¹⁹⁵

Ainda que pareça um pormenor, o supracitado entendimento muito corrobora com a lógica trazida pelos novos teóricos da guerra. Se trouxermos à luz a lógica das revoluções coloridas, bem como das guerras omnidimensionais, teremos a propaganda como um instrumento de guerra, utilizado principalmente para fomentar levantes e movimentos insurgentes.

Atos como estes foram a tônica das Primaveras Árabes, bem como dos movimentos realizados no Brasil em 2013 e 2014, em relação a Copa do Mundo, custo das passagens e dos combustíveis, com a propagação de informações e propaganda insurgente em fóruns, redes sociais e na *deepweb*. Por essa razão, o fato de alguns dos especialistas responsáveis pelo Manual de Tallinn terem concebido essa possibilidade como uma violação da soberania estatal, merece menção, visto que representa uma preocupação concreta no cenário global, mais uma vez, demonstrando que a internet garantiu um novo campo de oportunidade para operações deste porte.

¹⁹⁵ *Ibidem*. p. 26. Tradução livre de: “29. With regard to propaganda, the International Group of Experts agreed that its transmission into other States is generally not a violation of sovereignty. However, the transmission of propaganda, depending on its nature, might violate other rules of international law. For instance, propaganda designed to incite civil unrest in another State would likely violate the prohibition of intervention (Rule 66). Similarly, propaganda by a vessel in transit through the territorial sea renders the passage non-innocent (Rule 48).”

3.2 – TALLINN ENQUANTO “RULE OF ENGAGEMENT” DA GUERRA NO CIBERESPAÇO

O Manual de Tallinn, ainda que seja um documento de peso, não possui força jurídica, em outras palavras, não é um documento normativo ou legal, como apresentado, foi um esforço de especialistas de vários campos, no intuito de discutir os limites e as aplicações do uso da força no ciberespaço. Ainda que o Manual tenha relevância e se estruture nos moldes de um documento legal, o mesmo não foi criado com essa pretensão.

Contudo, Tallinn assume outro importante papel, o de um manual de “Rule of Engagement”, de conflitos a serem travados no campo virtual, em outras palavras, seria um possível manual de “regras de engajamento”.

Regras de Engajamento podem ser entendidas como práticas aceitáveis, veiculadas, esperadas e praticáveis por agentes militares no campo de batalha, para tanto, manuais de regras de engajamento são formulados por exércitos nacionais, para garantir o cumprimento de ações de forma esperada, possibilitando que os agentes militares possam atuar seguindo condutas determinadas por lógicas estratégicas, éticas e legais.

As ROE são emitidas pelas autoridades competentes e auxiliam no delineamento das circunstâncias e limitações nas quais as forças militares podem ser empregadas para atingir seus objetivos. ROE aparecem em uma variedade de formas em doutrinas militares nacionais, incluindo ordens de execução, ordens de implantação, planos operacionais ou diretrizes permanentes. Seja qual for a sua forma, eles autorizam e/ou limitam, entre outras coisas, o uso da força, o posicionamento e a postura das forças e o emprego de certas capacidades específicas. Em algumas nações, as ROE têm o status de orientação às forças militares; em outras nações, ROE são comandos legais.¹⁹⁶

Além das normais internacionais, os manuais apresentam regramentos e ações esperadas na execução das ações pelos militares em face do combate, ainda que não tenha força legal em matéria de direito internacional, os manuais possuem legitimidade militar, sendo seu descumprimento passível de punição. É importante ressaltar a questão da não vinculação legal dos ROE, contudo, nessa mesma linha, é inegável que os documentos estruturam as ações e condutas de seus militares, sob a égide da normativa nacional e internacional:

Os aspectos legais das ROEs podem assim ser resumidos da seguinte forma: As ROEs destinam-se a garantir o cumprimento da lei e da política aplicáveis, mas não constituem uma base legal, nem nacional nem internacionalmente. São, no entanto,

¹⁹⁶ International Institute of Humanitarian Law. Sanremio Handbook on Rules of Engagement. Sanremio, November 2009. Sanremio Italy. p. 1. Tradução livre de: “ROE are issued by competent authorities and assist in the delineation of the circumstances and limitations within which military forces may be employed to achieve their objectives. ROE appear in a variety of forms in national military doctrines, including execute orders, deployment orders, operational plans, or standing directives. Whatever their form, they provide authorisation for and/or limits on, among other things, the use of force, the positioning and posturing of forces, and the employment of certain specific capabilities. In some nations, ROE have the status of guidance to military forces; in other nations, ROE are lawful commands.”

em muitos Estados considerados juridicamente vinculativos, quer como ordens militares, quer através de ordens militares. Assim, para soldados individuais, as violações das ROEs provavelmente resultarão em sanções disciplinares ou penais. Para os Estados, o impacto legal das ROEs é menos claro. Apesar de terem sido criadas por unanimidade entre 28 Estados, as ROEs não devem ser vistas como tratados, mas sim como acordos administrativos internos para a OTAN. Como tal, eles não são uma fonte independente de direito, e sua interpretação está sujeita a regras gerais, como o significado comum do texto real, boa fé e tendo em mente o objeto e a finalidade do documento específico.¹⁹⁷

É preciso compreender que em grande medida, a lei não chega em todos os espaços dos campos de batalha, ainda mais complexo é conceber que soldados em um ambiente caótico como o da guerra e muitas vezes em um país diferente do seu, com suas próprias regras e valores, irão seguir normas internacionais, com pouca ou nenhuma capacidade coercitiva, ao menos à primeira vista.

Por essa razão, a ideia de códigos de conduta, de normas de valores éticos e morais, como as inseridas em regras de combate, apresentam uma possibilidade tangível de vinculação ao cumprimento, não somente do esperado, mas do legal:

A lei é o julgamento da comunidade em geral, mas o impulso para a conduta ética entre os guerreiros deve vir de outros guerreiros. O verdadeiro desafio para os comandantes não é apenas ensinar suas tropas sobre a lei do conflito armado, mas inculcar em suas tropas o ethos do guerreiro profissional – inculcar [sic] um senso permanente de honra. Não basta que os soldados conheçam as regras, ou mesmo as sigam. Sem reservas profundas de caráter e força psicológica, as tropas em situações de alto estresse no campo de batalha podem ser vítimas de impulsos indisciplinados. Honra, não lei, é a chave para a disciplina no campo de batalha.¹⁹⁸

É essa lógica, de um código vinculado à honra do combatente, que distingue este de um assassino ou criminoso comum, visto que, ainda que ambos tenham como arte o assassinato, um o faz a luz de uma série de princípios e preceitos éticos, seu objetivo, ainda que seja o de tirar uma vida, precisa ser imbuído de propósito, de forma, de método e de regra, do contrário o soldado passaria a ser um criminoso comum:

¹⁹⁷ Cooper, Camilla, Rules of Engagement Demystified: A Study of the History, Development and Use of ROEs (November 23, 2014). Military Law and the Law of War Review, 53/1 (2014). Disponível em: < <https://ssrn.com/abstract=2602763> > p. 21, Acessado em: 20 de fevereiro de 2022. Tradução livre de: “The legal aspects of ROEs may thus be summed up as follows: ROEs are intended to ensure compliance with applicable law and policy, but do not in themselves amount to a legal basis, neither nationally nor internationally. They are, however, in many States considered to be legally binding either as military orders or through military orders. Thus for individual soldiers, violations of ROEs are likely to result in disciplinary or penal sanctions. For States, the legal impact of ROEs is less clear. Despite being created by reaching unanimity among 28 States, ROEs should not be seen as treaties, but as internal, administrative agreements for NATO. As such they are not an independent source of law, and their interpretation is subject to general rules such as the ordinary meaning of the actual text, good faith and keeping the object and purpose of the specific document in mind.”.

¹⁹⁸ Bradley, Lt. Gabriel. “Honor, Not Law.” *Armed Forces Journal* (March 2012). Disponível em: < <http://www.armedforcesjournal.com/honor-not-law/>>, Acessado em: 20/02/2022. Tradução livre de: “Law is the judgment of the community at large, but the impetus for ethical conduct among warriors must come from other warriors. The real challenge for commanders is not just to teach their troops about the law of armed conflict but to inculcate in their troops the ethos of the professional warrior — to instill [sic] an abiding sense of honor. It is not enough for soldiers to know the rules, or even to follow them. Without deep reserves of character and psychological strength, troops in high-stress battlefield situations may fall prey to undisciplined impulses. Honor, not law, is the key to battlefield discipline.”.

[...] guerreiros devem aprender a tirar apenas certas vidas de certas maneiras, em certos momentos e por certas razões. Caso contrário, eles se tornam assassinos e serão condenados pelas próprias sociedades que foram criados para servir.¹⁹⁹

A natureza das Regras de Engajamento gera uma dificuldade na obtenção de documentos correntes, é de se esperar que ROEs em curso sejam classificados, do contrário, a própria missão e seus operadores poderiam estar em risco, por esta razão, os exemplos aqui trazidos fazem parte de operações já realizadas ou de treinamentos e jogos de guerra, sem, contudo, que a temporalidade afete qualquer avaliação destes, visto que, de regra geral, esses exemplos serão trazidos de forma exemplificativa.

Durante a Guerra do Vietnã (1955 – 1975), os Estados Unidos lançaram um série de operações contra coalizão do Vietnã do Norte, dentre as quais, mencionaremos a operação *Rolling Thunder*, definido por um massivo emprego de bombardeio aéreo, com o objetivo de dissuadir o inimigo, destruir sua infraestrutura, elevar o moral aliado e interromper as ações de insurgência no Vietnã do Sul, sem a necessidade de emprego de forças terrestres, nesse escopo, a ROE da operação compreendeu as dificuldades logísticas das ações, bem como as formas de operacionalizar o engajamento junto aos inimigos:

[limites geográficos do SEA [Sudeste Asiático], espaço aéreo territorial, mares territoriais e mares e espaço aéreo internacionais; definições de forças amigas, forças hostis, atos hostis, aeronaves hostis, perseguição imediata e embarcações hostis; regras que regem o que poderia ser atacado por aeronaves dos Estados Unidos, em que condições a perseguição imediata poderia ser conduzida, como as declarações de “hostil” deveriam ser tratadas e as condições de autodefesa.

[proibições contraclusas, barragens, usinas hidrelétricas, barcos de pesca, casas flutuantes e embarcações navais em certas áreas; proibições contra greves em determinadas áreas; proibições contra greves em certas áreas definidas, como a zona tampão do Partido Comunista Chinês (ChiCom) ou as áreas restritas de Hanói/Haiphong; condições sob as quais os alvos podem ser atingidos, como requisitos de validação, quando são necessários FACs [Forward Air Controllers], distâncias de estradas motorizadas.²⁰⁰

Como mencionado, a obtenção de ROEs é uma tarefa complexa visto a natureza do documento, contudo, por se tratar de material seminal à operacionalização de ações militares, ROEs costumam ser produzidos para a incursão de treinamentos e jogos militares, esses

¹⁹⁹ French, Shannon E. *The Code of the Warrior*. Lanham, MD: Rowman & Littlefield, 2003 p. 3. Tradução livre de: “[...] warriors must learn to take only certain lives in certain ways, at certain times, and for certain reasons. Otherwise, they become murderers and will find themselves condemned by the very societies they were created to serve.”.

²⁰⁰ US Congress. Project CHECO Report 1969, reprinted in Vol. 131 *US Congressional Report* 1985, p. 5248. Tradução livre de: “[G]eographical limits of SEA [Southeast Asia], territorial airspace, territorial seas, and international seas and airspace; definitions of friendly forces, hostile forces, hostile acts, hostile aircraft, immediate pursuit and hostile vessels; rules governing what could be attacked by United States aircraft, under what conditions immediate pursuit could be conducted, how declarations of a ‘hostile’ should be handled, and the conditions of self-defensepursuit. [P]rohibitions against striking locks, dams, hydropower plants, fishing boats, houseboats, and naval craft in certain areas; prohibitions against strikes in certain areas; prohibitions against strikes in certain defined areas such as the Chinese Communist (ChiCom) buffer zone or the Hanoi/Haiphong restricted areas; conditions under which targets might be struck, such as validation requirements, when FACs [Forward Air Controllers] were required, distances from motorable roads.”.

documentos representam de forma satisfatória a ideia de um ROE utilizado no campo real, exatamente pelo fato de sua criação ser para a finalidade de um treinamento da prática recorrente.

Por essa razão, traremos em seguida exemplificações de ROEs utilizados em exercícios e jogos militares pela OTAN, aqui destaca-se que as práticas adotadas pela OTAN nos interessam particularmente, visto que não somente Tallinn surgiu em razão das operações cibernéticas na Estônia, como a visão da Organização representa práticas atuais e sofisticadas de combate e de interação em conflitos armados. Para tanto, a Organização do Tratado do Atlântico Norte define ROE como:

Regras de Engajamento (ROE) - são diretrizes para as forças militares (incluindo indivíduos) que definem as circunstâncias, condições, grau e maneira em que a força, ou ações que possam ser interpretadas como provocativas, podem ser aplicadas. Os padrões mínimos de conhecimento militar acordados pela OTAN para treinamento nas Regras de Engajamento da OTAN estão contidos no STANAG 2597 e na Publicação de Treinamento Aliado-4, Treinamento nas Regras de Engajamento da OTAN.²⁰¹

A preocupação das OTAN com a formulação de boas práticas para seus agentes militares é corroborada quando o Rule of Engagement, passa a incorporar em seu bojo, tanto as normas condizentes aos conflitos armados (Law of Armed Conflict), quando a preocupação de abarcar igualmente demais normas nacionais e internacionais que possam garantir uma condução mais segura dos agentes militares.

Vale rememorar a ideia da guerra enquanto um conflito contínuo, a lógica de que a manutenção de uma certa estabilidade no campo de batalha, bem como a garantia de suporte ou ao menos a negação de resistência da população do Estado alvo, muitas vezes torna-se fator decisivo para uma vitória ou derrota, seja no fronte, seja em “casa”, como exemplo dos EUA contra o Vietnã do Norte. Essa preocupação pode ser extraída da seguinte passagem:

Regras de Engajamento (ROE), a Lei de Conflitos Armados e a legislação nacional são assuntos inter-relacionados na OTAN. Com exceção da autodefesa, durante o tempo de paz e as operações anteriores ao início de um conflito armado, as ROE fornecem autoridade exclusiva às forças lideradas pela OTAN/OTAN para usar a força. A condução de operações militares é circunscrita pelo direito internacional, incluindo as disposições aplicáveis do direito dos conflitos armados e do direito dos direitos humanos. OTAN ROE, e a sua aplicação, nunca permitem o uso de força que viole o direito internacional aplicável. O padrão da OTAN para treinamento em Regras de Engajamento está contido na Publicação de Treinamento Aliado-4. As forças armadas das nações que participam de operações lideradas pela OTAN/OTAN também devem aderir às suas próprias leis nacionais. Eles não são obrigados a

²⁰¹ North Atlantic Treaty Organization. Statement of Requirement for Developing a Proof of Concept Digital Game for Training in NATO Rules of Engagement and the Law of Armed Conflict. Supreme Allied Commander Transformation. Norfolk, Virginia. United States of America. p. 20. Tradução livre de: “Rules of Engagement (ROE) - are directives to military forces (including individuals) that define the circumstances, conditions, degree, and manner in which force, or actions which might be construed as provocative, may be applied. The NATO agreed upon military minimum standards of knowledge for training in NATO Rules of Engagement is contained in STANAG 2597 and Allied Training Publication-4, Training in NATO Rules of Engagement.”

executar tarefas ou operações que constituam uma violação de suas leis nacionais. Quando as leis nacionais estão em desacordo com o ROE da OTAN incluído no ROE para uma operação, as nações devem informar o NAC/DPC e o Comandante Estratégico sobre quaisquer inconsistências, o mais cedo possível. As nações da OTAN têm a responsabilidade de treinar seus Forças a respeitar e cumprir a lei de conflitos armados, quando aplicável, e por outras convenções e tratados internacionais que possam afetar as operações militares.²⁰²

Isso fica evidente quando entramos na designação da possibilidade de aplicação do uso da força que, como esperado, demanda certa resistividade:

Durante períodos de tensão ou crise, violência, conflito ou hostilidades podem irromper sem equivalendo a um conflito armado.

Geralmente, o ROE da OTAN em tais circunstâncias só permitirá o uso da força em resposta a ameaças. Esforços razoáveis e prudentes devem ser feitos para controlar uma situação sem o uso da força. Quando o tempo e as condições permitirem, as forças hostis em potencial devem ser avisadas e ter a oportunidade de retirar ou cessar as ações ameaçadoras.

No que diz respeito ao cumprimento da missão, o grau de força utilizado não deve ser maior do que o necessário para cumprir os deveres e cumprir os objetivos atribuídos à missão. Qualquer força usada deve ser limitada ao grau, intensidade e duração necessários para atingir o objetivo. As forças lideradas pela OTAN/OTAN geralmente devem evitar ações que possam ser percebidas como provocativas ou agressivas.²⁰³

De forma exemplificativa, o Manual supracitado traz alguns exemplos de informações que poderiam estar dispostas em um ROE, para tanto, trazamos à baila uma relacionada ao uso da força, nesse caso, com interpretação inclusive da própria prática do uso da força para a OTAN, especificamente, do mínimo uso necessário de força:

- O uso de “força mínima” inclui, por definição, a autoridade para usar até e incluindo “força mortal”
- Força Mínima é definida como “força, até e incluindo força letal, limitada ao grau, intensidade e duração necessários para atingir o objetivo”
- Força Mortal é definida como “força com intenção ou probabilidade de causar morte ou lesão grave resultando em morte”

Exemplo:

²⁰² *Ibidem*. p. 21-22. Tradução Livre de: Rules of Engagement (ROE), the Law of Armed Conflict, and national domestic law are interrelated subjects in NATO. With the exception of self-defence, during peacetime and operations prior to commencement of an armed conflict, ROE provide the sole authority to NATO/NATO-led forces to use force. The conduct of military operations is circumscribed by international law, to include the applicable provisions of the law of armed conflict and human rights law. NATO ROE, and the application of them, never permit use of force which violates applicable international law. The NATO standard for training in Rules of Engagement is contained in Allied Training Publication-4. The armed forces of nations participating in NATO/NATO-led operations must also adhere to their own national laws. They are not obliged to execute tasks or operations, which would constitute a breach of their national laws. When national laws are at variance with NATO ROE included in the ROE for an operation, nations must inform the NAC/DPC and the Strategic Commander of any inconsistencies, as early as possible. NATO nations have a responsibility to train their forces to respect and abide by the law of armed conflict, when it is applicable, and by Other international conventions and treaties which may affect military operations.

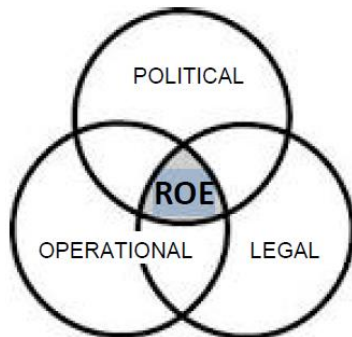
²⁰³ *Ibidem*. p. 96. Tradução livre de: “During periods of tension or crisis, violence, conflict or hostilities may erupt without amounting to an armed conflict. Generally, NATO ROE in such circumstances will only permit the use of force in response to threats. Reasonable and prudent effort should be made to control a situation without the use of force. When time and conditions permit, the potential hostile forces should be warned and given the opportunity to withdraw or cease threatening actions. With respect to mission accomplishment, the degree of force used must be no more than that necessary to carry out duties and accomplish assigned objectives of the mission. Any force used must be limited to the degree, intensity, and duration necessary to achieve the objective. NATO/NATO-led forces generally should avoid action which may be perceived as provocative or aggressive.”

- Regra 333: “É autorizado o uso de força mínima para impedir a tomada de posse ou destruição de torre de rádio”²⁰⁴

É sob a ótica de pesos e contrapesos, de responsabilidade e responsividade que os ROE da OTAN são formulados, com restrito cumprimento dos deveres legais nacionais e internacionais, limitado à lógica de formulação vinculada à operação ou missão, resguardada a garantia da mínima necessidade de aplicação de força, exceto nos casos que a aplicação seja necessária à consecução da missão, resguardadas as situações de aplicação do uso da legítima defesa:

- Exceto para uso da força em autodefesa, a OTAN ROE fornece a única autoridade sobre o uso da força para o cumprimento da missão em todas as operações lideradas pela OTAN/OTAN
- As atuais ROE da OTAN, seja em tempo de paz ou conflito armado, são uma mistura de autorizações e limitações
- MC 362/1 fornece diferentes séries de ROE sobre ações provocativas, uso da força para cumprimento de missão e ataque
- O pessoal deve estar ciente dos principais conceitos e terminologia do MC 362/1 para uso da força em operações lideradas pela OTAN/OTAN:
 - o “força mínima” e “força mortal”
 - o “ataque” no contexto da série 42 da OTAN ROE
 - o “ato hostil (não constituindo ataque real)” e “intenção hostil (não constituindo ataque iminente)”²⁰⁵

Para uma melhor visão do pretendido, o manual da Otan apresenta uma imagem que representa o que deve ser esperado de um documento de Rule of Engagement ideal:



206

Como disposto, o Rule of Engagemente deverá ser a junção e incorporar aspectos das questões política, operacional e legal, não somente deverá incorporar, como deverá

²⁰⁴ *Ibidem.* p. 103. Tradução livre de: “• Use of “minimum force” includes, by definition, the authority to use up to and including “deadly force” • Minimum Force is defined as “force, up to and including deadly force, limited to the degree, intensity, and duration necessary to achieve the objective” • Deadly Force is defined as “force intended or likely to cause death, or serious injury resulting in death” Example: • Rule 333: “Use of minimum force to prevent the taking of possession or destruction of radio tower is authorised””.

²⁰⁵ *Ibidem.* p. 108. Tradução livre de: “• Except for use of force in self-defence, NATO ROE provide the sole authority on use of force for mission accomplishment in all NATO/NATO-led operations • Current NATO ROE, whether in peacetime or armed conflict, are a mixture of authorisations and limitations • MC 362/1 provides different series of ROE on provocative actions, use of force for mission accomplishment and attack • Personnel should be aware of MC 362/1 key concepts and terminology for use of force in NATO/NATO-led operations: o “minimum force” and “deadly force” o “attack” in the context of NATO ROE series 42 o “hostile act (not constituting actual attack)” and “hostile intent (not constituting an imminent attack)””.

²⁰⁶ *Ibidem.* p. 118.

compreender como objetivo precípua à sua finalidade e funcionalidade tais questões. Aqui, ainda que a oportunidade se apresente, essa mesma oportunidade deverá estar restrita aos mecanismos de pesos e contrapesos das três forças que balizaram os ROE, a palavra de ordem nesse caso é a legalidade das condutas, tomadas por base pelo próprio ROE:

Considerações políticas

O ROE desenvolvido deve refletir a orientação política fornecida pelo NAC na Diretiva de Iniciação do NAC (NID) para alcançar um estado final desejado.

Considerações operacionais

O ROE desenvolvido deve permitir o cumprimento da missão levando em consideração fatores-chave, como objetivos da missão e estado final, forças disponíveis, capacidades militares, área de responsabilidade e geografia.

Considerações legais

O ROE desenvolvido deve refletir a autorização do NAC e a estrutura legal aplicável para a operação liderada pela OTAN/OTAN (que pode incluir um mandato do UNSC, consentimento da nação anfitriã, lei de conflito armado, lei internacional de direitos humanos, lei da nação anfitriã, status das forças disposições).²⁰⁷

Como visto, muitas das ações dispostas nos manuais, compreendem condutas esperadas dos militares, é exatamente sob essa ótica, que o Manual de Tallinn, ainda que não possua força normativa internacional, possibilita um novo campo de interpretação pelos agentes militares, especialmente o alto comando das nações, no condizente às operações cibernéticas.

Ao longo deste artigo, será feita referência regular ao Manual de Tallinn. É um documento seminal, pois é a primeira tentativa séria de mostrar como vários aspectos das operações cibernéticas e da guerra cibernética podem ser analisados sob as lentes do LOAC. Além disso, representa uma visão consensual de juristas e advogados militares da Aliança Atlântica sobre questões de uso cibernético da força. Embora não seja obrigatório, é pelo menos o início de uma jornada para explorar como as normas existentes do direito internacional serão aplicadas no ciberespaço. Simplificando, ele conecta os pontos e atua como uma lente para avaliar as ações no ciberespaço permitidas pelo direito internacional. Isso, por sua vez, pode ser usado para formular ROE²⁰⁸

Um dos consideráveis problemas presentes nos conflitos cibernéticos é a distinção entre combatente e civil, um “soldado digital” dificilmente poderia ser identificado por seu uniforme, bits e dados, nesse sentido, são extremamente democráticos, não fazendo distinção entre indivíduos, ao menos no ponto de vista operacional. Por essa razão, civis neste novo paradigma

²⁰⁷ *Ibidem*. p. 118 – 119. Tradução Livre de: “**Political considerations** The ROE developed must reflect the political guidance provided by the NAC in the NAC Initiating Directive (NID) to achieve a desired end state. **Operational considerations** The ROE developed must enable mission accomplishment by taking into account key factors such as mission objectives and end state, available forces, military capabilities, area of responsibility, and geography. **Legal considerations** The ROE developed must reflect the NAC authorisation and the applicable legal framework for the NATO/NATO-led operation (which may include a UNSC mandate, host nation consent, law of armed conflict, international human rights law, host nation law, status of forces provisions).”

²⁰⁸ MACINNIS, D.M. LCdr. Cyber Warfare, The Law of Armed Conflict, ROE And The Sufficiency of International Law. Canadian Forces College. Canada. p. 4. Tradução livre de: “Throughout this paper, regular reference will be made to the *Tallinn Manual*. It is a seminal document in that it is the first serious attempt to show how various aspects of cyber operations and cyber warfare can be analyzed under the lens of LOAC. Furthermore, it represents a consensus view by legal scholars and military lawyers from within the Atlantic Alliance on cyber use of force issues. Although not binding, it is at least the beginning of a journey to explore how the extant norms of international law will apply in cyberspace. Simply put, it connects the dots and acts a lens for assessing actions in cyberspace permissible under international law. This in turn can be used to formulate ROE”

de conflitos, podem ser objetos e objetivos explícitos em matéria de ROE, se compreendida sua participação direta em uma ação cibernética ofensiva, disruptiva ou de insurgência, ainda que altamente questionável, visto a dificuldade de distinção entre um civil que tenha tido sua infraestrutura de rede invadida e utilizada para fins de operações cibernéticas e um insurgente ou soldado digital:

O conceito de distinção da LOAC, que exige que pessoas e objetos civis sejam distinguidos de combatentes e objetos militares, é problemático no ciberespaço. Determinar quem realizou o ataque e quem pode ser o proprietário da infraestrutura é difícil devido à natureza de uso duplo da Internet e à capacidade dos usuários avançados de mascarar suas identidades ou assumir o controle da infraestrutura em um país terceiro para lançar um ataque. Ainda assim, os civis podem ser alvejados se for provado que estão participando diretamente das hostilidades e os civis que exercem uma função de combate contínuo. o

A implicação para a CAF é que os civis que facilitam as operações cibernéticas da CAF podem perder sua imunidade sob o LOAC e se tornar alvos válidos. No entanto, fornece uma base legal para ação contra indivíduos que apoiam o terrorismo organizado ou grupos insurgentes que se envolvem em ataques cibernéticos contra o Canadá e seus aliados.²⁰⁹

Cumprido ressaltar que a aplicação de ROE no campo das operações cibernéticas é uma prática presente, restando problemática quanto a normativa disponível. A esse respeito, o próprio manual de Sanremo dispõe acerca da possibilidade e da relevância da inserção das operações cibernética no rol do ROE:

2.5 Operações do Ciberespaço

a. uma. Introdução

A característica distintiva do ciberespaço é que é um ambiente nocional e além da jurisdição de qualquer nação. As operações de rede de computadores (CNO) são a principal forma de operações no ciberespaço e muitas vezes não são cinéticas, dificultando a determinação do ato hostil e da intenção hostil.

b. Considerações legais

As principais considerações legais ao elaborar ROE para operações no ciberespaço são:

i. As leis civis e criminais domésticas e internacionais e as políticas nacionais variam muito nos aspectos legais da CNO. Além disso, os tratados multilaterais e bilaterais de comunicações têm disposições que afetam a condução das operações de rede de computadores.

ii. Apesar de não cinética, as operações no ciberespaço podem constituir um ato hostil ou intenção hostil. Fatores na determinação de ambos incluem a gravidade, imediatismo, franqueza e efeitos da operação.

c. ROE aplicável

Além das regras obrigatórias estabelecidas no parágrafo 3.d.i do Anexo B, o seguinte ROE deve ser considerado:

- Operações de Rede de Computadores (Série 131)
- Interferência com comunicações por satélite (Série 140)

²⁰⁹ *Ibidem.* p. 8. Tradução livre de: “The LOAC concept of *distinction* which requires civilian persons & objects to be distinguished from combatants & military objects, is problematic within cyberspace. Determining who conducted attack and who may own the infrastructure is difficult because of the dual use nature of the internet and the ability of advanced users to mask their identities or to take-over infrastructure in a third country in order to launch an attack. Still civilians can be targeted if it can be proven that they are directly participating in hostilities and civilians that acting a continuous combat function. The implication for the CAF is that civilians that facilitate CAF cyber operations may lose their immunity under LOAC and become valid targets. However, it does provide a legal basis for action Against individuals supporting organized terror or insurgent groups who engage in cyber attacks against Canada and her allies.”

• Neutralização/Destruição de Satélites (Série 141)²¹⁰

Se visto enquanto um documento operacional militar, o Manual de Tallinn apresenta aplicabilidade, exatamente por enquadrar as possibilidades que comandos militares têm adotado enquanto regras de engajamento de seus manuais. Ainda nessa linha, é importante ressaltar que o Manual não foi construído apartado da realidade, pelo contrário, surgiu exatamente da necessidade de pensar em questões existentes à época e em crescente ocorrência, para tanto, suas acepções não existem no vácuo.

Para tanto, o Manual buscou resguardar certas limitações quanto as operações cibernéticas, limitações que, em alguns casos, poderiam sim compor um ROE, não somente sobre sua análise extensiva da norma existente, como também para própria visão opinativa da aplicação da norma. Ainda que o Manual não possa e não deva ser confundido com um ROE, é de se avaliar a possibilidade de extração de algumas passagens no tocante a definição de uma “conduta esperada” ou “desejada” por um aparato militar:

12. No caso de um ataque armado iniciar um conflito armado (Regras 82–83), o fato de que a resposta se qualifique como legítima defesa não exclui a ilicitude de qualquer lei de violações de conflitos armados que possam ocorrer. Por exemplo, as medidas defensivas podem não incluir a realização de ataques cibernéticos contra civis (Regra 94) ou bens civis (Regra 98). Da mesma forma, o fato de as operações serem conduzidas em legítima defesa não exclui necessariamente a ilicitude da conduta em relação a obrigações de direitos humanos aplicáveis (Regra 35) das quais o Estado não derogou (Regra 38).²¹¹

Outro exemplo que o Manual nos traz que vale reflexão sobre sua possibilidade de transposição a um ROE, diz respeito à proporcionalidade, aqui, o documento em suas considerações acerca da sua “Rule 23 – Proportionality of countermeasures”²¹² delimita o próprio escopo de ação dentro da lógica da proporcionalidade em matéria de responsividade:

²¹⁰ International Institute of Humanitarian Law. Sanremo Handbook on Rules of Engagement. Sanremo, November 2009. Sanremo Italy. p. 15 - 16. Tradução livre de: “2.5 *Cyberspace* Operations a. Introduction The distinctive feature of *cyberspace* is that it is a notional environment and beyond the jurisdiction of any single nation. *Computer network operations (CNO)* are the principle form of operations in *cyberspace* and are often non-kinetic, making the determination of *hostile act* and *hostile intent* difficult. b. Legal Considerations The principal legal considerations when drafting ROE for cyberspace operations are: i. Domestic and international civil and criminal laws and national policies vary widely on the legal aspects of *CNO*. Further, multilateral and bilateral communications treaties have provisions that impact the conduct of *computer network operations*. ii. Despite being non-kinetic, operations in *cyberspace* may constitute a *hostile act* or *hostile intent*. Factors in the determination of both include the severity, immediacy, directness and effects of the operation. c. Applicable ROE In addition to the compulsory rules as set out at paragraph 3.d.i of Annex B, the following ROE should be considered: *Computer Network Operations (Series 131) Interference with Satellite Communications (Series 140) Neutralization/Destruction of Satellites (Series 141)*”.

²¹¹ Tallinn. p. 107. Tradução livre de: “12. In the event an armed attack initiates an armed conflict (Rules 82–83), the fact that the response qualifies as lawful self-defence does not preclude the wrongfulness of any law of armed conflict violations that may occur. For instance, defensive measures may not include conducting cyber attacks against civilians (Rule 94) or civilian objects (Rule 98). Similarly, the fact that operations are conducted in self-defence does not necessarily preclude the wrongfulness of the conduct with respect to applicable human rights obligations (Rule 35) from which the State has not derogated (Rule 38).”

²¹² *Ibidem*. p. 127.

A proporcionalidade no contexto das contramedidas deve ser diferenciada da proporcionalidade *jus ad bellum* (Regra 72), que se refere ao grau de força necessário para que um Estado se defenda efetivamente contra um ataque armado. A proporcionalidade das contramedidas também deve ser distinguida da regra da proporcionalidade na lei de conflitos armados (Regra 113), que avalia o dano esperado a ser causado a civis ou bens civis à luz da vantagem militar prevista de um ataque (Regra 92).²¹³

Ainda que não fosse o objetivo do Manual, passagens como essas apresentam pontos importantes para a construção de um Rule of Engagement em matéria de ações voltadas ao campo cibernético, seja sob a perspectiva de limitação de ações, seja da possibilidade de campos de oportunidade.

Por fim, Tallinn ao definir os “meios e métodos” da guerra cibernética, em igual teor definiu os limites e as extensões responsivas aos mesmos, mesmo que a natureza do Direito Internacional Humanitário, tenha como primado a proporcionalidade, pelo fato da guerra cibernética se tratar de matéria nova, ainda existem muitas dúvidas acerca de suas limitações, restrições e aplicações.

O Manual, dessa forma, garantiu aos corpos militares um rico compêndio que possibilitaria definições em matéria de ROE, dos limites e das possíveis respostas a ataques cibernéticos que tenham como escopo, a guerra cibernética. Não obstante, a própria ideia de dos meios e métodos em que essa nova espécie de guerra seria travada, garante a mesma aplicação análoga aos meios e métodos que as operações cibernéticas poderiam ser travadas em um ROE, seja em uma perspectiva de uso de força (ainda que ilegal), seja em matéria de legítima defesa:

Regra 103 – Definições de meios e métodos de guerra Para os fins deste Manual:
 a) «Meios de guerra cibernética» são as armas cibernéticas e os sistemas cibernéticos associados; e
 (b) “métodos de guerra cibernética” são as táticas, técnicas e procedimentos cibernéticos pelos quais as hostilidades são conduzidas.
 1. Os termos 'meios' e 'métodos' de guerra são termos legais da arte usados no direito do conflito armado. Eles não devem ser confundidos com o termo mais amplo e não legal “operação cibernética” usado ao longo deste Manual. A operação cibernética simplesmente denota uma atividade cibernética específica. As definições estabelecidas nesta Regra são aplicáveis em conflitos armados internacionais e não internacionais.
 2. Para os fins deste Manual, as armas cibernéticas são meios cibernéticos de guerra que são usados, projetados ou destinados a causar ferimentos ou morte de pessoas ou danos ou destruição de objetos, ou seja, que resultem nas consequências necessárias para a qualificação de uma operação cibernética como um ataque (Regra 92). O termo “meios de guerra cibernética” abrange tanto as armas cibernéticas quanto os sistemas de armas cibernéticas. Uma arma é geralmente entendida como aquele aspecto do sistema usado para causar danos ou destruição a objetos ou ferimentos ou morte a

²¹³ *Ibidem*. p. 127. Tradução livre de: “Proportionality in the context of countermeasures must be distinguished from *jus ad bellum* proportionality (Rule 72), which refers to the degree of force required for a State to defend itself effectively against an armed attack. Countermeasures proportionality must also be distinguished from the rule of proportionality in the law of armed conflict (Rule 113), which assesses the harm expected to be caused to civilians or civilian objects in light of an attack’s (Rule 92) anticipated military advantage.”

peças. Meios cibernéticos de guerra, portanto, incluem qualquer dispositivo cibernético, material, instrumento, mecanismo, equipamento ou software usado, projetado ou destinado a ser usado para conduzir um ataque cibernético (Regra 92).
[...]

4. O termo “métodos de guerra” refere-se a como as operações cibernéticas são montadas, diferentemente dos instrumentos usados para conduzi-las. Considere o uso de um botnet para conduzir um ataque de negação de serviço distribuído destrutivo. Neste exemplo, a botnet é o meio de guerra cibernética, enquanto o ataque distribuído de negação de serviço é o método de guerra cibernética.²¹⁴

Em termos gerais, Tallinn não pode ser compreendido como um manual de produção de ROE, como o de Sanremo e da OTAN, apresentados ao longo dessa seção, contudo, Tallinn apresenta um campo de oportunidade para a aplicação extensiva de operações e ações cibernéticas, à lógica clássica do conflito por meios cinéticos, como não podemos ter no Manual um documento normativamente vinculante, podemos vislumbrar nele, ao menos, um documento passível de aplicação analógica para produção de ROEs.

O Próprio Manual de Sanremo já dispõe acerca da inserção de operações cibernéticas no ROE, contudo, a vasta gama de especialistas e documentos utilizados na produção de Tallinn servem como conteúdo assessorio e, de garantia de preservação de direitos à civis, bem como pela garantia de responsabilidade pelos Estados.

²¹⁴ *Ibidem*. p. 452-453. Tradução livre de: “Rule 103 – Definitions of means and methods of warfare For the purposes of this Manual: (a) ‘means of cyber warfare’ are cyber weapons and their associated cyber systems; and (b) ‘methods of cyber warfare’ are the cyber tactics, techniques, and procedures by which hostilities are conducted. 1. The terms ‘means’ and ‘methods’ of warfare are legal terms of art used in the law of armed conflict. They should not be confused with the broader, non-legal term ‘cyber operation’ used throughout this Manual. Cyber operation simply denotes a particular cyber activity. The definitions set forth in this Rule are applicable in both international and noninternational armed conflict. 2. For the purposes of this Manual, cyber weapons are cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack (Rule 92). The term ‘means of cyber warfare’ encompasses both cyber weapons and cyber weapon systems. A weapon is generally understood as that aspect of the system used to cause damage or destruction to objects or injury or death to persons. Cyber means of warfare therefore include any cyber device, materiel, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber attack (Rule 92).[...] 4. The term ‘methods of warfare’ refers to how cyber operations are mounted, as distinct from the instruments used to conduct them. Consider use of a botnet to conduct a destructive distributed denial of service attack. In this example, the botnet is the means of cyber warfare while the distributed denial of service attack is the method of cyber warfare.”

CONSIDERAÇÕES FINAIS

Em face das questões apresentadas, uma questão perdura, O Manual de Tallinn constitui uma superação ou uma limitação normativa? De certo, ele não constitui uma norma de fato, desta feita, questionasse se haveria necessidade ou não da formulação de uma normativa em face da presente realidade e se o Manual seria um texto base viável para tal, ou se a formulação de uma normativa aos moldes do Manual não seria uma limitação, levando os Estados a buscarem novos “campos de oportunidade”.

A este respeito vale relembrar as operações do Stuxnet, que visaram incapacitar o programa nuclear do Irã, caso houvesse norma internacional impeditiva de operações do tipo, as repercussões dos ataques poderiam ser diferentes, especialmente, tendo em vista a capacidade de intervenção política do Conselho de Segurança da ONU, contudo, em razão da inexistência de normativa, foi possível operar a margem da legalidade e, em tese, atrasar ou até mesmo inviabilizar o enriquecimento de urânio, a ponto de sua utilização em armamentos nucleares.

Contudo, o mesmo campo de oportunidade permitiu que ações fossem realizadas em vistas de influenciar o processo eleitoral americano, dentre outros, afetando diretamente a soberania dos Estados.

É exatamente sob esta lógica que poderíamos dividir a questão sob dois ângulos, o primeiro são as operações cibernéticas, análogas às operações cinéticas ou que possam ser operacionalizadas igualmente pelo aparato militar clássico e em outro lado as operações que não constituem operações militares clássicas, que tem por princípio ações político estatais.

Como pudemos observar vivemos em uma nova realidade na lógica do conflito, da guerra e, esse não se limita mais à lógica cinética da guerra clássica. Como demonstrado, tanto pelo trabalho de Azevedo e Mota concernente às Guerras Omnidimensionais, bem como no tocante às Guerras Híbridas, abordadas por Kuribeko, os conflitos agora ocorrem em tempo real e ininterrupto; eles abriram mão da limitação do campo de batalha real e partiram para o campo de guerra virtual (enfoque desta pesquisa) e cultural.

A este respeito, observa-se um cenário de constante violação de soberania, contudo, mediante as lacunas jurídicas e a incapacidade técnica de se rastrear operações virtuais com precisão, seria quase impossível qualquer ação de denuncia e, conseqüente defesa individual e coletiva, legalmente autorizada pela comunidade internacional (ONU), de um Estado parte violado a outro violador.

Este problema foi escancarado em Tallinn, Estônia, com ataques supostamente perpetrados pela Rússia às infraestruturas críticas do Estado, causando danos reais, inclusive à economia e afetação à civis, fato este que, resultou na formulação do Manual de Tallinn.

Dessa forma, torna-se quase que impossível qualquer garantia real de legítima defesa por parte de um Estado vitimado por uma operação cibernética, ao passo que a nova realidade do teatro global, gerou uma verdadeira lacuna jurídica, possibilitando um vasto leque de ações no ciberespaço que de forma analógica se constituiriam enquanto práticas de uso da força e, ou, atos de agressão, com consequências similares às de operações clássicas, típicas de uma guerra cinética.

O uso da força desse modo tem-se dado por novos meios, ainda não compreendidos pela realidade jurídica internacional vigente, garantindo àqueles com capacidade técnica e operacional, atos de agressão indiscriminados, ao passo que os Estados violados não encontram capacidade de resposta legítima, gerando uma escalada internacional de conflitos irregulares, desestabilizadores, baseados na obscuridade da rede digital de computadores.

O uso da força, desse modo, não tem encontrado guarida na forma legal em que foi concebido pela Carta da ONU e pelo Direito Consuetudinário Internacional, dessa forma, o que pode-se observar é uma retomada da aplicação do uso da força do ideário clássico e, esse, não tem ensejado a aplicação do direito à legítima defesa e sim uma contínua aplicação do próprio uso da força em caráter responsivo.

Com isso, apesar do entendimento de que ambos os manuais apresentam um esforço significativo para trabalhar com a questão, o presente trabalho parte da hipótese de que não há substrato suficiente a partir do Direito Consuetudinário Internacional, tão pouco na jurisprudência das Cortes Internacionais para solucionar os problemas da nova realidade supramencionada. Dessa forma, torna-se necessária uma nova lógica jurídica, mediante tratados e esforços da comunidade internacional, que sejam capazes de frear as operações virtuais que têm sido análogas a atos de agressão.

Nessa mesma lógica, a possibilidade de utilização do Manual enquanto um documento de regra de engajamento, especialmente nas ações que sejam operacionais e operacionalizáveis pela organização militar, bem como por ações que tenham resultados e ou aplicações análogas a operações cinéticas, parecem ser uma aplicação interessante para o documento.

O que fica evidente é que a normativa existente não basta, ainda que em caráter interpretativo, para limitar ações e operações que violam toda e qualquer proporcionalidade, não há de se falar em garantia do direito de intervir na soberania de outro Estado, a intervenção

nas ações particulares e inerentes à soberania dos Estados Nacionais precisa ser rechaçada e proibida por norma legal, sob essa questão, Tallinn parece ter sido claro.

Sob essa lógica, parece-nos importante dividir o Manual em dois grandes campos, um ligado as ações que não necessariamente demandariam a formulação de normativa, podendo ser adotadas e, ou, incorporadas pelas organizações militares em seus manuais de regras de engajamento e, em outro grande campo, das questões que necessitam de normativa específica e, ou, atualização da normativa existente para compreender, também, ações e questões no campo digital.

Outra grande contribuição do Manual e que parece ainda permanecer sob pouca relevância por parte dos atores internacionais, foi a extensão dada pelo documento ao conceito de soberania, a ideia incorporada por Tallinn, de que a soberania não mais se limita ao espaço físico, sendo compreendido também pelo espaço digital, estendendo ao Estado soberano direitos e deveres sobre esse mesmo espaço, nos parece ser um conceito revolucionário, uma concepção de fronteira, ainda pouco estudada.

Desta feita, sem esgotar os questionamentos trazidos na problemática do trabalho, bem como ao longo da própria dissertação, entendemos que o Manual foi um documento de extrema relevância, tendo sido objeto de estudo de diversos países, na mesma linha, o documento escancarou uma realidade pouco publicizada a época e que, atualmente, parece ser a regra das ações beligerantes dos Estados Nacionais, não mais a exceção.

Como visto, a própria lógica da guerra evoluiu consideravelmente ao longo dos séculos, ainda que seus objetivos precípuos tenham permanecido os mesmos, na mesma toada, a normativa ligada aos conflitos seja na sua execução seja na sua instituição, acompanhou, ainda que de forma retardatária, sua evolução, sob essa lógica, tendo em vista que estamos sob a égide de uma nova lógica da guerra, composta pela multidimensionalidade, pela confusão entre agente e civil, vítima e algoz, pelas operações cibernéticas e pela guerra híbrida, pelo conflito contínuo, indissociável entre paz e guerra, bem como pela constante intervenção em assuntos privativos das soberania Estatal, parece-nos necessário que a normativa internacional acompanhe as novas mudanças supracitadas.

Se os Estados, em grande medida as superpotências, buscaram novos campos de oportunidade para operar e fazer valer suas vontades de forma beligerante, ainda que nos novos espaços de fronteira, cabe ao Direito, especialmente aquele advindo da superação da barbárie, limitar e reger a presente realidade do ciberespaço.

REFERÊNCIAS

AQUINO, S.T. **Suma teológica**. Tradução de Alexandre Correia. Disponível em: < <https://sumateologica.files.wordpress.com/2017/04/suma-teolc3b3gica.pdf> >.

ALHOFF, Fritz. **Binary bullets: the ethics of cyberwarfare**. Nova York: Oxford University Press, 2016.

AZEVEDO, C.E.F. e MOTA, R.M. **As dimensões do campo de batalha e a guerra omnidimensional**. Coleção Meira Mattos, revista das ciências militares, nº 26, 2º quadrimestre 2012. Rio de Janeiro: ECEME, 2012.

BAEZNER, Marie; ROBIN, Patrice: **Hotspot Analysis: Stuxnet**, October 2017, Center for Security Studies (CSS), ETH Zürich.

BETHLEHEM, Daniel. **Notes and Comments Principles Relevant to the Scope of a State's Right of Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors**. U.N., 2012. Disponível em <<https://www.un.org/law/counsel/Bethlehem%20-%20Self-Defense%20Article.pdf>>.

BLAZATTI, Bruno. **Operações cibernéticas à luz da proibição internacional do uso da força: um estudo sobre o direito à legítima defesa**. Trabalho de Conclusão de Curso (Graduação em Direito) - Faculdade de Direito, Universidade Federal de Minas Gerais. Belo Horizonte, 2015.

BODIN, Jean. **Os seis livros da República**: livro primeiro. Tradução de: José C. O. Morel. São Paulo: Ícone, 2011.

BONAVIDES, Paulo. **Ciência Política**. 10. Ed. São Paulo: Malheiros, 2001.

BRIGAGÃO, Clóvis. **O 11 de Setembro: Novas Ameaças à Paz**. pp. 347-355 in Terrorismo e direito: os impactos do terrorismo na comunidade internacional e no Brasil/ Coordenador, Leonardo Nemer Caldeira Brant. Rio de Janeiro: Forense, 2003.

BRADLEY, Lt. Gabriel. "Honor, Not Law." *Armed Forces Journal* (March 2012). Disponível em: < <http://www.armedforcesjournal.com/honor-not-law/>>

BRASIL. Congresso Nacional. Senado Federal. Comissão de Relações Exteriores e Defesa Nacional. **Rumos da política externa brasileira: temas da agenda internacional, política externa brasileira**. Brasília: Senado Federal, 2012.

BRASIL. Convenção de Viena. Viena 21 de março de 1986. Disponível em: < https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=701DBCD1773F1FB1F2C5DA2890871FFD.proposicoesWeb2?codteor=1427770&filename=MSC+589/2015 >

BUTLER, Rupert. **A Gestapo: a história da polícia secreta de Hitler: 1933-1939**/Ruper Butler; tradução de Emanuel Mendes Rodrigues. São Paulo: Editora Escala, 2008.

BUZAN, Barry. **A evolução dos estudos de segurança internacional/** Barry Buzan, Lene Hansen; tradução Flávio Lira. São Paulo: Editora Unesp, 2012.

CANÇADO TRINDADE, Antônio Augusto. *Princípios do Direito Internacional Contemporâneo*. 2. Ed. Ver. Atual. Brasília: FUNAG. 2017.

CASALUNGA, Fernando Henrique. *Guerra Híbrida Cibernética: Uma Análise do Conflito Rússia-Ucrânia (2014-2016) Sob a Perspectiva da Tecnologia da Informação*. ENABED, 10 Encontro Nacional da Associação Brasileira de Estudos de Defesa. 2018. p. 12. Disponível em: <https://www.enabed2018.abedef.org/resources/anais/8/1534467151_ARQUIVO_casalungaf_h_guerra_hibrida_cibernetica_uma_analise.pdf>.

CARDOSO, Paulo Roberto. *Diatética Cultural: Estado, soberania e defesa cultural*. Belo Horizonte: Universidade Federal de Minas Gerais, 2016. Tese, Doutorado em Direito. Universidade Federal de Minas Gerais – UFMG.

CLAUSEWITZ, Carl Von. **Da Guerra**. São Paulo: Editora WMF Martins Fontes, 2010.

CICV, Armas. 2010. Disponível em: < <https://www.icrc.org/pt/doc/war-and-law/weapons/overview-weapons.htm> >.

CICV, Comitê Internacional da Cruz Vermelha. **Protocolos Adicionais às Convenções de Genebra de 12 de agosto de 1949**. Genebra, Suíça. 2017.

CICV, Comitê Internacional da Cruz Vermelha. **Artigo 3º comum às quatro Convenções de Genebra. 12 de agosto de 1949**. Disponível em < <https://www.icrc.org/pt/doc/resources/documents/treaty/treaty-gc-0-art3-5tdlrm.htm> >.

CLARK, Alan. *Barbarossa: The Russian-German Conflict, 1941-45*. New York: Quill. 1965.

COOPER, Camilla, *Rules of Engagement Demystified: A Study of the History, Development and Use of ROEs (November 23, 2014)*. *Military Law and the Law of War Review*, 53/1 (2014), Disponível em: < <https://ssrn.com/abstract=2602763> >.

DUNANT, Henry. *A Memory of Solferino*. International Committee of the Red Cross. Geneva 1959.

DINSTEIN, Yoram. *Guerra, Agressão e Legítima Defesa*. São Paulo: Manole, 2004.

DIONÍSIO, Cátia S. Gerreiro. *A Responsabilidade Internacional dos Estados e Operações Cibernéticas*. Universidade de Lisboa, Lisboa, 2018. Dissertação de Mestrado Profissionalizante em Direito Internacional e Relações Internacionais da Faculdade de Direito da Universidade de Lisboa. Disponível em: < https://repositorio.ul.pt/bitstream/10451/37376/1/ulfd136516_tese.pdf >.

ESPINER, Tom. *Estonia's Cyberattacks: Lessons learned, a year on*. 1 may, 2008. Disponível em: < <https://www.zdnet.com/article/estonias-cyberattacks-lessons-learned-a-year-on/> >.

FERNANDES, H., 2016. As Novas Guerras: O Desafio da Guerra Híbrida. *Revista de Ciências Militares*, novembro de 2016 IV (2), pp. 13-40. p. 22. Disponível em: < <http://www.iesm.pt/cisdi/index.php/publicacoes/revista-de-ciencias-militares/edicoes> >.

FINK, Bob. *Vietnam – a View from the Walls: a History of the Vietnam Anti-War Movement*. Greenwich Publishing. 1982.

FRENCH, Shannon E. *The Code of the Warrior*. Lanham, MD: Rowman & Littlefield, 2003.

FRIESER, Karl-Heinz. *The Blitzkrieg Legend: The 1940 Campaign in the West [Blitzkrieg-legend: der westfeldzug 1940]* translation. J. T. Greenwood. Annapolis: Naval Institute Press.

GARAMONE, Jim. Petraeus puts protecting people at strategy's center. U.S. Army, American Forces Press Service. August 03, 2010. Disponível em: < https://www.army.mil/article/43205/petraeus_puts_protecting_people_at_strategys_center >.

GENEBRA. Os Protocolos Adicionais às Convenções de Genebra de 12 de Agosto de 1949. Comitê Internacional da Cruz Vermelha. CICV. Genebra, Suíça. Disponível em: < <https://www.icrc.org/pt/publication/os-protocolos-adicionais-convencoes-de-genebra-de-12-de-agosto-de-1949> >.

GLANTZ, David. *Operation Barbarossa: Hitler's Invasion of Russia 1941*. Stroud, Gloucestershire, UK: The History Press. 2012.

GROTIUS, Hugo. *On the Law of War and Peace*. Translated from the original Latin *De Jure Beli ac Pacis* by A.C. Campbell, A.M. Batoche Books. Kitchener. 2001.

GUDERIAN, Heinz. *Panzer Leader*. New York: Da Capo Press. 2001.

HEINL, Robert D. Jr. The Collapse of the Armed Forces. p. 4. *Armed Forces Journal*, 07 june 1971. Disponível em: < <https://msuweb.montclair.edu/~furg/Vietnam/heinl.pdf> >.

HORTA, José Luiz Borges. *História do Estado de Direito*. p. 22 São Paulo: Alameda, 2011.

HUXLEY, Aldous Leonard. **Admirável mundo novo**. Brasil, Biblioteca Azul, 2014.

I.C.J. International Court of Justice. Reports of Judgments, Advisory Opinions and Orders The Corfu Channel Case (Merits). Judgment of April 9th, 1949. Disponível em: < <https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf> >.

I.C.J. International Court of Justice. **Nicaragua v. United States of America, Military and Paramilitary Activities, Judgement of 27 June 1986, Merits**. 1986.

ICRC. **The Potential Human Cost of Cyber Operations**. ICRC Expert Meeting 14-16 November 2018. Geneva. 2018.

JUBILUT, Liliana Lyra. **Os Fundamentos do Direito Internacional Contemporâneo: da Coexistência aos Valores Compartilhados**. Anuário Brasileiro de Direito Internacional 1, 2006, pp 203-219. Disponível em: < <http://www.corteidh.or.cr/tablas/r27213.pdf> >.

KENNEDY, Paul. **Ascensão e queda das grandes potências: transformação econômica e conflito militar de 1500 a 2000**/ Paul Kennedy; tradução de Waltiesir Dutra, 5ª ed. Rio de Janeiro: Campus, 1991.

KORYBKO, Andrew. *Guerras Híbridas das revoluções coloridas aos golpes*. São Paulo: Expressão Popular, 2018.

KURU, Huseyin. Evolution of war and cyber-attacks in the concept of conventional warfare. p. 14. Journal of Learning and Teaching in Digital Age, 2018, 3(1), 12-20.

LAI, Robert. RAHMAN, Syed (Shawon). Analytic of China Cyberattack. The International Journal of Multimedia & Its Application (IJMA) Vol. 4, No. 3, June 2012. Pp 37 – 56.

LARA, Antônio de Sousa, O Terrorismo e a ideologia do ocidente. Edições Almedina, SA. Coimbra. 2007; A nova ordem mundial e os conflitos armados/El nuevo orden mundial y los conflictos armados/Coordenadores Daniel Amin Ferraz e Denise Hauser. Belo Horizonte: Mandamentos, 2002.

LEBEDEV, Anastasiya. The man Who Saved the World Finally Recognized. MosNews. 21 de maio de 2004. Disponível em: <
<https://web.archive.org/web/20110721000030/http://www.worldcitizens.org/petrov2.html> >.

LIND, William S. et al. **The Changing Face of War: Into the Fourth Generation**, Marine Corps Gazette, outubro de 1989, p. 22 e p. 26. Disponível em <
http://www.dnipogo.org/fcs/4th_gen_war_gazette.htm. >.

LIND, William S., **Compreendendo a Guerra de Quarta Geração**, Military Review, Janeiro - Fevereiro 2005, Ed. Brasileira. 2005.

I.M. Lobo de Souza. O conceito de agressão armada no Direito Internacional. Revista de Informação Legislativa. a. 33n. 129 jan./mar. 1996. Senado Federal, Brasília. 1996. Disponível em: <
<https://www2.senado.leg.br/bdsf/bitstream/handle/id/176388/000506405.pdf?sequence=1&isAllowed=y> >.

LOMANS, Marieke. Investigating Titan Rain Cyber Security & Cyber Operations. Master MSS – Class 2015.2017 Disponível em : <
[https://www.academia.edu/32222445/ Investigating Titan Rain Cyber Espionage Cyber Security and Cyber Operations](https://www.academia.edu/32222445/Investigating_Titan_Rain_Cyber_Espionage_Cyber_Security_and_Cyber_Operations) >.

LOPES, Gills; OLIVEIRA de, Carolina Fernanda Jost. Stuxnet e defesa cibernética estadunidense à luz da análise de política externa. Ver. Bra. Est. Def. ano 1, jul./dez., pp 55 – 69.

MACINNIS, D.M. LCdr. Cyber Warfare, The Law of Armed Conflict, ROE And The Sufficiency of International Law. Canadian Forces College. Canada. 2018

MAQUIAVEL. Nicolau, O Príncipe Maquiavel ao Magnífico Lorenzo de Medici. Publicações Eletrônicas, disponível em: <
<http://www.dominiopublico.gov.br/download/texto/cv000052.pdf> >.

MORRIS, Ian. **Guerra: o horror da guerra e seu legado para a humanidade**/ Ian Morris; tradução de Luis Reyes Gil. São Paulo: LeYa, 2015.

MUELLER, Robert S. **Report On The Investigation Into The Russian Interference In The 2016 Presidential Election**. U.S. Departamento f Justice. Washington D.D. 2019. Disponível em < <https://www.justice.gov/storage/report.pdf> >.

NATO. Tallin **Manual on the International Law Applicable to Cyber Warfare**, Cambridge: Cambridge University Press, 2013.

NATO. North Atlantic Treaty Organization. Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. 2014 Disponível em: < https://www.nato.int/cps/en/natohq/official_texts_112964.htm >.

NATO. North Atlantic Treaty Organization. Statement of Requirement for Developing a Proof of Concept Digital Game for Training in NATO Rules of Engagement and the Law of Armed Conflict. Supreme Allied Commander Transformation. Norfolk, Virginia. United States of America. 2018.

NEUFELD, Michael J. **The Rocket and the Reich: Peenemünde and the Coming of the Ballistic Missile Era**. New York: The Free Press. 1995.

NYE, Joseph S. **O paradoxo do poder americano: por que a única superpotência do mundo não pode prosseguir isolada**. Tradução de Luiz Antônio Oliveira de Araújo. São Paulo: Ed. da UNESP, 2002.

OTTIS, Rain. **Analysis of the 2007 Cyber Attacks Against Estonia from the information Warfare Perspective**. Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. Disponível em < <https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/> >.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Carta das Nações Unidas**. <https://www.un.org/en/sections/un-charter/chapter-vii/index.html>.

PAGLIUSI, Paulo Sergio. Guerra Cibernética Russo-Ucraniana – Lições para o Brasil e o Mundo. Crypto ID. 21 de março de 2022. Disponível em: < <https://cryptoid.com.br/ciberseguranca-seguranca-da-informacao/defesa/guerra-cibernetica-russo-ucraniana-licoes-para-o-brasil-e-o-mundo/>>.

PAMMENT, James. Et. Al. Hybrid Threats: 2007 cyber attacks on Estonia. 2019. Disponível em: < <https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86> >

PEREIRA, Antônio Celso Alves. **Soberania e Pós-Modernidade** pp. 619-662, in O Brasil e os novos desafios do direito internacional / Leonardo Nemer Caldeira Brant (coordenador). Rio de Janeiro: Forense, 2004.

RAO, Siddharth Prakash. Stuxnet, A new Cyberwar weapon: Analysis from a technical point of view. Technical Report. May. 2014. Aalto University. 2014.

RECORD, Jeffrey. **The Bush Doctrine and War with Iraq**. 2003.

REUTERS, G1. Site oficial do Kremlin está fora do ar em meio à guerra na Ucrânia. G1 Globo. 26 de fevereiro de 2022. Disponível em: < <https://g1.globo.com/tecnologia/noticia/2022/02/26/site-oficial-do-kremlin-esta-fora-do-ar-em-meio-a-guerra-na-ucrania.ghtml> >.

REZEK, Francisco. Preâmbulo. In: BRANT, Leonardo Nemer Caldeira (Org). Comentário à Carta das Nações Unidas. Belo Horizonte: Centro de Direito Internacional, 2008.

RODRIGUES, João Guerreiro. Por dentro do exército de hackers voluntários que quer salvar a Ucrânia. Quem são e o que fazem. CNN Portugal. 22 de março de 2022. Disponível em: < <https://cnnportugal.iol.pt/guerra/russia/por-dentro-do-exercito-de-hackers-voluntarios-que-quer-salvar-a-ucrania-quem-sao-e-o-que-fazem/20220322/62339f9a0cf2c7ea0f1ff93b> >.

RUSSOMANO, Gilda M C, Meyer. **Direito Internacional Público**. 1. Vol, Rio de Janeiro: Forense. 1989.

SALDAN, Eliane. Os Desafios Jurídicos da Guerra no Espaço Cibernético. Dissertação de Mestrado. Instituto Brasiliense de Direito Público – IDP. Brasília. 2012. Disponível em: < https://repositorio.idp.edu.br/bitstream/123456789/1223/1/Disserta%C3%A7%C3%A3o_Eliane%20Saldan.pdf >.

SANDRONI, Gabriela Araujo. **Prevenção da Guerra no Espaço Cibernético**. Disponível em: < https://www.jurisway.org.br/v2/dhall.asp?id_dh=12381 >.

SANREMO. International Institute of Humanitarian Law. Sanremo Handbook on Rules of Engagement. Sanremo, November 2009. Sanremo Italy.

SAPORITO, Laura e LEWIS James A. **Cyber Incident Attributed to China**. Center for Strategic and International Studies.

SCHMITT, Michael N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework (1999). Columbia Journal of Transnational Law, Vol. 37, 1998-99. pp. 885-938.

SCHMITT, Michael. **International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed**. Harvard International Law Journal Online Vol.54.

SCHMITT, Michael N. (Ed). NATO Cooperative Cyber Defence Centre of Excellence. **Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations**. 2 Ed. New York, NY: Cambridge University Press, 2017.

SETTE CÂMARA, Thiago. Terrorismo na era da internet: O uso de redes sociais pelo Estado Islâmico. Revista Relações Internacionais no Mundo Atual, n. 21, v.1, p. 196-221, 2016.

SHAKARIAN, Paulo. SHAKARIAN, Jana. RUEF, Andrew. Introduction to Cyber-Warfare a Multidisciplinary Approach. Elsevier, Syngress. Waltham, MA. US. 2013.

SILVA, Alexandre Pereira da. Os Princípios das relações internacionais e os 25 anos da Constituição Federal. Revista de Informação Legislativa. Ano 50. Número 200. out/dez 2013.

Senado Federal. Brasília. Disponível em: < https://www12.senado.leg.br/ri/edicoes/50/200/ri/v50_n200_p15.pdf >.

SILVA. Carla Ribeiro Volpini; ROSA. Patricia Rodrigues. O Uso da Força em Direito Internacional – Legítima Defesa Preemptiva. p. 8. Disponível em: < <http://www.publicadireito.com.br/artigos/?cod=a08c938c1e7c76d8> >.

SINGER, Peter W; FRIEDMAN, Allan. **Cybersecurity and cyberwar**: what everyone needs to know. Oxford: Oxford University Press, 2014.

SKJELVER. Danielle Mead, Landsknecht German mercenary pikeman, disponível em: < <https://www.britannica.com/topic/Landsknechte> >.

STEINER, Sylvia Helena, et. al. **O Tribunal Penal Internacional: Comentários ao Estatuto de Roma**. Coordenadores: Sylvia Helena Steiner e Leonardo Nemer Caldeira Brant. Belo Horizonte: Konrad Adenauer Stiftung, CEDIN, Del Rey, 2016.

STEVE Mansfield-Devine, “Estonia: What Doesn’t Kill You Makes You Stronger,” *Network Security* 7 (July 2012): 13. disponível em: < [https://doi.org/10.1016/S1353-4858\(12\)70065-X](https://doi.org/10.1016/S1353-4858(12)70065-X) > Acessado em: 27 de junho de 2021.

TRATADO, INTERNATIONAL TREATY FOR THE RENUNCIATION OF WAR AS NA INSTRUMENT OF NATIONAL POLICY. Paris, agosto, 1928. p. 2-3. Disponível em: < <https://web.archive.org/web/20121016045106/http://www.fco.gov.uk/resources/en/pdf/treaties/TS1/1929/29> >.

TOOZE, Adam. *The Wages of Destruction: The Making and Breaking of the Nazi Economy*, London: Allen Lane. 2006.

U.N, United Nations, **Charter of the United Nations**, UNTS 1945 No.7, 26 June 1945. Disponível em: < <https://www.un.org/en/charter-united-nations/> >.

U.N, United Nations. Resolution 3314 (XXIX). Definition of Aggression. General Assembly – Twenty-ninth Session. 2319th plenary meeting. 14 December 1974. p. 143. Disponível em: < [https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/3314\(XXIX\)](https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/3314(XXIX)) >.

U.N, United Nations. **Responsibility of States for Internationally Wrongful Acts 2001**. United Nations. 2005.

U.N, United Nations. **Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries 2001**. United Nations. 2008.

U.N, United Nations. Definition of Aggression General Assembly Resolution 3314 (XXIX). United Nations Audiovisual Library of International Law. 2008. Disponível em: < https://legal.un.org/avl/pdf/ha/da/da_ph_e.pdf >.

U.S. Congress. Project CHECO Report 1969, reprinted in Vol. 131 *US Congressional Report* 1985.

U.S. Department of the Army. **Army Special Operations Forces Unconventional Warfare Field Manual No. 3-05.130**. Headquarters. Department of the Army, Washington. 2008.

U.S. Joint Chiefs of Staff. **Cyberspace Operations**. Washington 2018. Disponível em: < https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf >.

U.S. **The National Security Strategy of The United States of America**. Washington 2002.

U.S. **Memorandum on Joint Terminology for Cyberspace Operations for Chiefs of the Military Services, Commanders of the Combatant Commands and Directors of the Joint Staff Directorates**. General James E. Cartwright, Vice Chairman of the Joint Chiefs of Staff, Washington D.C. 2011.

U.S. Government Accountability Office, 2010. Hybrid Warfare Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives, 10 de setembro de 2010. United States Government Accountability Office, Washington, DC disponível em: < <https://www.gao.gov/assets/gao-10-1036r.pdf> >.

U.S. Department of Justice. Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volume I of II. Washington D.C. March 2019.

VAIDYA, Tavish. 2001-2013: Survey and Analysis of Major Cyberattacks. Georgetown University. 1 Sep. 2015.

VELOSO, Ana Flávia. **O Terrorismo Internacional e a Legítima Defesa no Direito Internacional: O Artigo 51 da Carta das Nações Unidas** pp. 183-207. In Terrorismo e direito: os impactos do terrorismo na comunidade internacional e no Brasil/ Coordenador, Leonardo Nemer Caldeira Brant. Rio de Janeiro: Forense, 2003.

VELOSO, Ana Flávia. Ação relativa a ameaças à paz, ruptura da paz e atos de agressão: artigo 51. In BRANT, Leonardo Nemer Caldeira (Org.). Comentário à Carta das Nações Unidas. Belo Horizonte: Centro de Direito Internacional, 2008.

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

VOLKVEIS, José Henrique Antunes. Emprego de Obuseiros Autopropulsados, Trabalho de Conclusão de Curso apresentado à Academia Militar das Agulhas Negras. Academia Militar das Agulhas Negras, Resende. 2016. Disponível em: < <https://bdex.eb.mil.br/jspui/bitstream/1/1142/1/TCC%203105%20Antunes.pdf> >.

WALZER, Michael. **Guerras justas e injustas: uma argumentação moral com exemplos históricos**/ Michael Walzer; tradução Waldéa Barcellos. São Paulo: Martins Fontes, 2003.