UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO

A RESPONSABILIDADE INTERNACIONAL DOS ESTADOS E OPERAÇÕES CIBERNÉTICAS

MESTRADO PROFISSIONALIZANTE EM DIREITO INTERNACIONAL E RELAÇÕES INTERNACIONAIS

Autor

CÁTIA S. GUERREIRO DIONÍSIO

Professor Orientador

Professor Doutor Eduardo Vera-Cruz Pinto

2018

Universidade de Lisboa

Faculdade de Direito

Dissertação apresentada como requisito para obtenção de grau de Mestre em Direito, orientado pelo Professor Doutor Eduardo Vera-Cruz.

A RESPONSABILIDADE INTERNACIONAL DOS ESTADOS E OPERAÇÕES CIBERNÉTICAS

CÁTIA S. GUERREIRO DIONÍSIO

Lisboa

2018

Esta página foi deixada propositadamente em branco.

“I think computer viruses should count as life ... I think it says something about human nature that the only form of life we have created so far is purely destructive. We've created life in our own image.”

-Stephen Hawking

Agradecimentos

A presente dissertação de mestrado não poderia chegar a bom porto sem o precioso apoio de várias pessoas.

Em primeiro lugar, não posso deixar de agradecer ao meu orientador, Professor Doutor Eduardo Vera-Cruz. Expresso o meu profundo agradecimento pela orientação e apoio incondicionais que muito elevaram os meus conhecimentos científicos e, sem dúvida, muito estimularam o meu desejo de querer, sempre, saber mais e a vontade constante de querer fazer melhor.

Desejo igualmente agradecer a todos os meus colegas do Mestrado em Direito Internacional e Responsabilidade Internacional, especialmente ao Álvaro Maurício cujo apoio e amizade estiveram presentes em todos os momentos.

À minha família e amigos, em especial aos meus pais, um enorme obrigada por acreditarem sempre em mim e naquilo que faço e por todos os ensinamentos de vida. Espero que esta etapa, que agora termino, possa, de alguma forma, retribuir e compensar todo o carinho, apoio e dedicação que, constantemente, me oferecem. Também aos meus amigos, Ana, Andreia , Bagacina e Flipa, pelas revisões incansáveis ao longo da elaboração desta dissertação.

O meu profundo e sentido agradecimento a todas as pessoas que contribuíram para a concretização desta dissertação, estimulando-me intelectual e emocionalmente.

Lista de Abreviaturas

ARPA - Advanced Research Projects Agency

Art. -(arts.) Artigo(s)

CERN - Conseil Européen pour la Recherche Nucléaire

CERT- Computer Emergency Response Team

CLP - Controladores Lógicos Programáveis

DDoS –Destributed Denial Of Service

DoS – Denial Of Service

HTTP - Hypertext Transfer Protocol

HTML – HyperTextProtocol

IC - Infraestrutura Critica

ICTFY – International Criminal Tribunal for Former Yuguslavia

ICRC – Internacional Committiee of Red Cross

IP – Internet Protocol

IRC - Internet Relay Chat

ILC - International Law Commission

LOAC – Law Of Armed Conflicts

MIT- Massachusetts Institute of Technology

MILNET – Military Network

NSF – National Science Foundation

NSFNET – National Science Foundation Network

ONU – Organização das Nações Unidas

ONG – Organização Não Governamental

OTAN – Organização do Tratado do Atlantico Norte

PEPIC – Programa Europeu de Protecção de Infraestruturas Criticas

PIC – Protecção de Infraestruturas Criticas

TCP – Transmission Control Protocol

TIC – Tecnologias de Informação e Comunicação

TIJ – Tribunal Internacional de Justiça

TJUE – Tribunal de Justiça da União Europeia

TPI – Tribunal Penal Internacional

TPJI – Tribunal Permanente De Justiça Internacional

UE – União Europeia

UN – United Nations

URL – Uniform Resource Locator

SCADA – Supervisory control and data acquisition

USA – United States of America

USDoD – United States Department of Defence

WWW – World Wide Web

Abstract

The aim of this dissertation is to analyse the Responsibility of States in cybernetic activities in the context of armed conflicts. In this analysis, a study was made on the International Law of *Ius ad Bellum* and *Ius in Bello*, making a historical background, exposing the respective sources and finally presenting its fundamental principles. Then, a characterization of armed conflicts was presented, classifying it into international and non-international conflicts.

A cybernetic approach was made for each matter investigated, having the concepts of international armed conflict and non-international armed conflict been discussed. The analysis focused on international conventions and relevant international customs, existing jurisprudence as well as relevant doctrinal studies with particular emphasis on the 2001 Draft of Articles on Resposability of States for Internationally Wrongful Acts and the Tallinn Manual on International Law applicable to Cyber Warfare.

The investigation allowed to conclude that the International Law does not establish specific norms applied to cybernetic operations, reason why there is a need to resort to the Law of non-cyber conflicts. This investigation has revealed, among other things, that, concerning the regime of overall control over an organized entity, this is much more difficult to obtain on a cybernetic level compared to conventional armed groups.

Palavras-chave: International Humanitarian Law, Internatinal Armed Conflict, Non-International Armed Conflict, Ciberwar, Ciber Operations.

Resumo

Constitui objeto da presente dissertação analisar a Responsabilidade dos Estados em atividades cibernéticas no âmbito de conflitos armados. No âmbito deste trabalho foi feito um estudo sobre o Direito Internacional de *Ius ad Bellum* e *Ius in Bello*, fazendo um enquadramento histórico, expondo as respetivas fontes por fim apresentando os seus princípios fundamentais. De seguida foi apresentada uma caracterização dos conflitos armados, classificando-os como internacionais e não internacionais.

Foi feita uma abordagem cibernética para cada universo de estudo, tratando-se os conceitos de conflito armado internacional e de conflito armado não internacional. A investigação incidiu sobre as convenções internacionais e os costumes internacionais pertinentes, a construção jurisprudencial existente e os estudos doutrinários relevantes com especial destaque para o Projeto de Artigos sobre a Responsabilidade dos Estados de 2001 e o Manual de Tallinn sobre o Direito Internacional aplicável à Guerra Cibernética.

A investigação permitiu concluir que o Direito Internacional não estabelece normas específicas aplicadas às operações cibernéticas, pelo que existe uma necessidade de recorrer às normas que regulam os conflitos não cibernéticos. Esta investigação revelou, entre outras coisas, que, no que concerne ao regime de controlo sobre uma entidade organizada, este é muito mais difícil de aferir a nível cibernético comparativamente com os grupos armados convencionais.

Palavras-chave: Direito Internacional Humanitário, Conflito Armado Internacional, Conflito Armado Não Internacional, Ciberguerra, Operações Cibernéticas.

Índice

1.Introdução 9

2.Considerações Históricas 11

2.1 *Ius ad Bellum* e *Ius in Bello* 11

2.2 Conceito e evolução da Internet 16

2.3 Exploração de vulnerabilidades 19

3.Considerações Preliminares 22

3.1 Ciberespaço, o "*sítio*" onde se dá a ciberguerra 22

3.2 As Infraestruturas Críticas: pontos vulneráveis a um ataque cibernético .. 24

4. O Uso da Força 27

4.1 Conceito 27

4.2 Uso da Força em Contexto Cibernético 28

4.2.1 Operações cibernéticas como ataque armado 31

4.3 Exceções ao Uso da Força 34

4.3.1 Legítima defesa 34

4.3.2 Ações Autorizadas ao Conselho de Segurança das Nações Unidas .. 43

4.3.3 O Consentimento 44

5. Conflitos Armados e operações cibernéticas 46

5.1 Conceito de Conflito Armado e a aplicabilidade da Lei dos Conflitos Armados às Operações Cibernéticas 46

5.2 Operações Cibernéticas em/ou como Conflito Armado Internacional 50

5.3 Operações Cibernéticas em/ou como Conflito Armado Não Internacional 51

5.4 Ciberguerra: definição de meios e métodos de guerra 52

5.5 Ciberterrorismo 54

5.5.1 Conceito 54

5.5.2 Ocorrências de ataques terroristas no ciberespaço 58

6 Responsabilidade internacional dos Estados 60
6.1 Conceito 60
6.2 A positivação da Responsabilidade Internacional e o projeto de normas da ILC quanto à responsabilidade dos Estados 61
6.3 O Ato Internacionalmente Ilícito e elementos que o constituem 63
6.4 A violação de uma obrigação Internacional, a ilicitude. 64
6.5 As causas de Exclusão da Ilicitude 65
6.5.1 Represálias 67
6.5.2 O Perigo Extremo (*distress*) 70
6.5.3 Estado de Necessidade 71
6.5.4 Caso Furtuito ou Força maior 73
6.6 A conduta e a sua imputação a um Estado 75
6.7 Responsabilidade dos Estados em Contexto Cibernético 83
7.Conclusão 87
8. Bibliografia 89

1.Introdução

A informatização de todos os serviços é uma inevitável realidade que acompanha a exponencial evolução tecnológica que temos vindo a assistir nas últimas décadas. Esta revolução digital trouxe grandes benesses, tais como a cada vez menor utilização do papel ou a rapidez de acesso à informação a partir de qualquer ponto do globo[1]. Nesse "ciber-local", não há barreiras ou limites que não sejam passíveis de ser ultrapassados, não havendo qualquer delimitação de território no ciberespaço. No entanto, esta rápida ascensão trouxe consigo várias lacunas e vulnerabilidades. São nestas vulnerabilidades que se baseiam as atividades criminosas, sendo muitas as causas que podem levar a atividade ilícita, passando estas pela simples vontade de notoriedade, enriquecimento próprio, espionagem, até à ciberguerra e ciberterrorismo.

Na "Estratégia Internacional para o Ciberespaço" dos Estados Unidos da América lê-se que: "*Todos os Estados têm o direito inerente de legítima defesa e de reconhecer que certos atos hostis realizados no ciberespaço podem obrigar a tomar ações no âmbito dos compromissos que temos com os nossos aliados militares. Reservamo-nos o direito de usar todos os meios necessários: diplomáticos, informacionais, militares e económicos, adequados e consistentes com o direito internacional aplicável, a fim de defender a nossa nação, os nossos aliados, os nossos parceiros e os nossos interesses*"[2].

Do ponto de vista internacional, os Estados utilizam o ciberespaço e as suas lacunas para defender os seus interesses estratégicos.

Consideramos, assim, relevante e oportuno o tema da responsabilidade internacional dos estados em operações cibernéticas, na medida em que constitui uma temática nova e em constante mutação. A abordagem a esta problemática exige um estudo relativamente ao ordenamento jurídico aplicável a estas

[1] *Vide,* VICENTE, Dário Moura, "Direito Internacional Privado, Problemática Internacional da Sociedade da Informação", Almedina, Setembro 2005.
[2] *Vide*, WHITE HOUSE, International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World. 2011, disponível em: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf , consultado pela última vez em 5 de Fevereiro de 2017.

situações. Assim, importa primeiro compreender o *Ius ad Bellum* e o *Ius in Bello*[3], bem como os instrumentos de *Soft Law* que positivam o costume dos Estados, nomeadamente o Projeto de Artigos sobre a Responsabilidade de 2001, inúmeras vezes referido pelo Tribunal Internacional de Justiça, que lhe deu natureza costumeira, e o Manual de Tallinn. Este último um instrumento de *softlaw,* trata do Direito Internacional aplicável à guerra cibernética, que através da opinião de um grupo internacional de peritos independentes, estabelece uma análise das normas já existentes no Direito Internacional Público, estudando a sua aplicabilidade neste novo paradigma de guerra.

A problemática aqui em causa consiste nos efeitos decorrentes de uma *ciber-conduta* ilícita no que concerne à responsabilidade dos Estados. Para tal, será feito um breve enquadramento histórico e algumas considerações preliminares pertinentes. Partiremos posteriormente para uma análise do princípio geral e fundamental da proibição do uso da força, determinando as condutas cibernéticas que entram no espetro desta proibição. É necessário ulteriormente realizar uma abordagem quanto à classificação dos vários tipos de conflitos armados à luz do Direito Internacional Humanitário, enquadrando as operações cibernéticas nos conflitos armados e como um conflito armado *per se*. Por último, é necessário analisar os critérios de responsabilização dos Estados pelos atos e omissões que desrespeitem uma obrigação internacional, bem como os critérios de atribuição duma conduta a um Estado.

Este relatório é constituído por três temas fundamentais. O primeiro diz respeito à proibição do uso da força e às exceções a esta proibição, nomeadamente a legitima defesa, as ações autorizadas pelo Conselho de Segurança das Nações Unidas e o consentimento. Num segundo momento será abordada a classificação dos conflitos armados no plano jurídico. Por fim, o terceiro tema tratará da análise detalhada do regime de responsabilidade dos Estados.

[3] *Vide,* PINTO, Eduardo Vera-Cruz *"*História do Direito Comum da Humanidade. Ius Commune Humanitatis ou Lex Mundi?, *"*AAFDL,1º Volume, 2003.

A metodologia de pesquisa adotada foi documental e bibliográfica, analisando os textos especializados, com destaque para a doutrina e jurisprudência. De ressalvar que devido à complexidade do tema e à constante mutação do universo do ciberespaço, a presente tese não pretende exaurir os temos abordados mas sim trazer reflexões sobre a problemática em questão.

2.Considerações Históricas

2.1 *Ius ad Bellum* e *Ius in Bello*

A ocorrência de guerras dá-se desde a existência da Humanidade em si, mais propriamente, desde a convivência do Homem em sociedade. Um dos primeiros códigos redigidos com normas de guerra foi o Código de Manu[4], que continha as normas sobre o tratamento dos prisioneiros de guerra, comprovando assim que já na altura se legislava sobre a guerra[5].

Também no livro sagrado se pode verificar a existência de normas referentes à guerra, normas estas definidas pelo próprio Deus, no livro de Deuteronómio podeler-se: "*Quando te aproximares duma cidade para combatê-la, apregoar-lhe-ás paz. Se ela te responder em paz, e te abrir as portas, todo o povo que se achar nela será sujeito a trabalhos forçados e te servirá. Se ela, pelo contrário, não fizer paz contigo, mas guerra, (…) passarás ao fio da espada todos*

[4] Redigido entre os séculos II a.C. e II d.C, faz parte de uma coletânea dividido em quatro partes: o Mahabharata, o Ramayana, os Puranas e as Leis Escritas de Manu. Constitui-se na legislação do mundo indiano e estabelece o sistema de castas na sociedade Hindu. As leis de Manu são tidas como a primeira organização geral da sociedade sob a forte motivação religiosa e política. No seu sétimo livro O Código dá relevância às relações externas, ditando regras de diplomacia para os embaixadores do rei e de guerra quando for necessária a utilização de armas. No seu artigo Art. 346º pode ler-se "Por sua própria segurança numa guerra empreendida para defender direitos sagrados e para proteger uma mulher ou um Brâmane, aquele que mata justamente não se torna culpado."

[5] *Vide*, Manusrti - Código de Manu (200 A.C. e 200 D.C.), disponível em file:///C:/Users/Userpl022pc01.CYBER/ Downloads/ CODIGo_%20MANU.pdf consultado pela ultima vez a 10 de Fevereiro de 2017.

os homens que nela houver; porém as mulheres, os pequeninos, os animais e tudo o que houver na cidade, todo o seu despojo, tomarás por presa (…). Assim farás a todas as cidades que estiverem mais longe de ti, que não são das cidades destas nações" [6].

A teoria da Justiça da guerra tem as suas origens no pensamento de Cícero, Santo Agostinho, São Tomás de Aquino e Hugo Grócio. Para Santo Agostinho a guerra é uma extensão do ato de governar, sem que com isto todas as guerras se justifiquem moralmente. Ele distinguia três critérios: a autoridade adequada, a justa causa e a reta intenção. Estabelece ainda como fim último da guerra, o bem comum e a paz[7].

Com o passar do tempo outros critérios foram sendo acrescentados à Teoria da Guerra Justa nomeadamente o critério da oportunidade razoável de sucesso., este assenta numa análise de custo/benefício e da garantia mínima de que a guerra não será em vão. Tal não implica, no entanto, que um poder mais fraco não possa combater por uma causa justa. Um outro critério será o de que a guerra deve ser tida como último recurso, ou seja, devem esgotar-se todas as formas pacíficas de resolução do conflito. Mais tarde, outros requisitos tal como a necessidade e proporcionalidade foram acrescentados à definição de "guerra justa" [8].

No que concerne às normas reguladoras da guerra dever-se-á estabelecer uma diferenciação entre os termos *ius ad bellum* e *ius in bello*[9]. Sendo que o primeiro diz respeito à matéria do Direito Internacional Público que estabelecia as condições necessárias para que se pudesse decretar Estado de Guerra, estabelecendo às partes o que estas poderiam ou não fazer. Em suma, trata-se

[6] Bíblia Sagrada – Antigo Testamento - Deuteronómio : 20 versículo 10–15.
[7] *Vide,* QUINTA, Henrique Nova – "A Guerra Justa ou Justiça da Guerra no Pensamento Português" Instituto de Defesa Nacional "– pp. 170 .
Vide, BARBEYRAC ,Jean , "Natural law and enlightenment classics The Rights of War and Peace book of Hugo Grotius Edited and with an Introduction by Richard Tuck" , Preliminary Discourse, XIII Hugo Grocio, 2005, pp. 255
[8] *Vide*, O Direito à Guerra Justa, Revista Militar , 2451 ,Abril de 2006, disponível em https://www.revistamilitar.pt/artigo/72 acedido pela ultima vez a 09 de Fevereiro de 2017.
[9] *Vide,* GOUVEIA, Jorge Bacelar – "O uso da força no Direito Internacional Público" pp. 155 - Revista Brasileira de Estudos Políticos Belo Horizonte n. 107 2013

aqui dum direito dos Estados poderem recorrer à força no âmbito das relações internacionais. Quanto ao *ius in bello*, este fundamentalmente diz respeito às normas que regulam os conflitos armados, ou seja, é o direito que rege a forma como a guerra é conduzida.

Seria apenas no século XX que se começariam a verificar avanços relevantes no sentido de estabelecer juridicamente a proibição do uso da força. Poder-se-á dizer que estes avanços estão divididos em quatro momentos distintos, sendo estes, a proibição do uso da força na cobrança de dívidas contratuais, a moratória de guerra no âmbito do Pacto da Sociedade das Nações, a renúncia geral ao uso da força no Pacto Briand-Kellog e, por último, a proibição geral do uso da força na Carta das Nações Unidas[10].

A Convenção Drago-Porter[11] de 1907 foi o primeiro instrumento jurídico internacional que visava a proibição da utilização da guerra como meio de resolução de conflitos, no que concerne à recuperação de débitos de um Estado a outro Estado devedor.

O segundo grande passo no que diz respeito à proibição do uso da força foi introduzido com o Pacto da Liga das Nações em 1919, no seu artigo 10º pode-se ler que os Estados Membros da Sociedade das Nações se comprometeriam a "*respeitar e manter contra toda a agressão externa a integridade territorial e a independência política presente de todos os Membros da Sociedade. Em caso de agressão, ameaça ou perigo de agressão, o Conselho resolverá os meios de assegurar a execução desta obrigação*" [12].

Também no artigo 11º se faz menção à declaração ou ameaça de guerra, dizendo-se que " *interessará à Sociedade inteira e esta deverá tomar as medidas apropriadas para salvaguardar eficazmente a paz das Nações. Em semelhante*

[10] *Vide,* GOUVEIA, Jorge Bacelar – "O uso da força(…)" *op.cit*. pp.156.
[11] Adotada na segunda conferência de Hague de 1907. cfr "Convention Respecting the Limitation of the Employment of Force for the Recovery of Contract Debts".
Disponível em https://www.loc.gov/law/help/us-treaties/bevans/m-ust000001-0607.pdf acedida a 10 de Agosto de 2017.
[12] Pacto da Sociedade das Nações - Primeira parte do Tratado de Versalhes, de 28 de junho de 1919, artigo 10º.

caso, o Secretário-geral convocará imediatamente o Conselho a pedido de qualquer Membro da Sociedade"[13].

Em 1928 foi celebrado o Tratado de Renúncia Geral do Uso da Força também conhecido por Pacto de Paris ou Pacto Briand-Kellog, do qual constam três artigos. O tratado condenava explicitamente a guerra como instrumento de política internacional. Nos termos deste tratado *"os povos condenam o recurso à guerra para a solução das controvérsias internacionais, e a ela renunciam como instrumento de política nacional nas suas mútuas relações.*"[14].

Após breves momentos de paz na Europa, os anos que se seguiriam seriam de guerra, sendo que a segunda Guerra Mundial teria a duração de seis anos. Foi sobre esta catástrofe que em 1945 foi ratificada a Carta das Nações Unidas. Depois do insucesso da Liga das Nações, a Organização das Nações Unidas viria a ser a sua filha pródiga, mantendo-se até aos dias de hoje. A Carta das Nações Unidas estabeleceria, de todos os textos acima mencionados, a mais abrangente proibição do uso da força, afirmando no seu artigo 2º nº 4 que "*Os membros deverão abster-se nas suas relações internacionais de recorrer à ameaça ou ao uso da força*" [15]. A própria Carta prevê exceções à utilização da força nas relações internacionais. A primeira exceção diz respeito às intervenções autorizadas pelo Conselho de Segurança da Organização, descrita no capítulo VII do tratado constitutivo. Nesse caso, estando perante uma ameaça à paz internacional, a intervenção dos Estados Membros é possível desde que por meio de autorização prévia e específica do Conselho de Segurança, apenas após o esgotamento dos meios pacíficos[16]. A segunda exceção está presente no artigo 52º da Carta da ONU e trata do direito dos Estados ao uso da legítima defesa[17]. O uso da força como legítima defesa só terá lugar aquando da ocorrência dum ataque armado ou quando este se encontre iminente. A legítima defesa deverá respeitar os princípios

[13] Pacto da Sociedade das Nações (…), *op.cit*. artigo 11.
[14] Artigo 1º do Tratado de Renúncia à Guerra.
[15] Artigo 2°, n° 4 da Carta das Nações Unidas.
[16] Esse é o caso da intervenção da coalizão internacional no conflito na Líbia, em 2011, autorizada pela Resolução 1793 do Conselho de Segurança.
[17] Artigo 52º da Carta das Nações Unidas.

da necessidade, proporcionalidade e emergência. Estes requisitos podem ser verificados pelo Conselho de Segurança, não sendo no entanto necessária a autorização prévia do conselho para fazer uso da figura da legítima defesa. No que concerne a uma terceira exceção, existe no plano doutrinal uma discussão se o consentimento será uma causa de justificação, não ilicitude ou que em nada desrespeite a proibição do uso da força[18]. Para haver convencimento deverá haver uma situação em que um Estado solicite o auxílio militar de outro Estado no seu território. Entendemos aqui que o uso da força, existindo um consentimento prévio, não será considerado contrário à proibição, sendo que não irá contra a soberania de um Estado, presente no artigo 2º nº 7 da Carta, segunfo este "*Nenhuma disposição da presente Carta autorizará as Nações Unidas a intervir em assuntos que dependam essencialmente da jurisdição interna de qualquer Estado, ou obrigará os membros a submeterem tais assuntos a uma solução, nos termos da presente Carta"*[19]. Desta forma, ainda que o consentimento se encontre no projeto de artigos de 2001 da Comissão de Direito Internacional[20] como uma causa de exclusão da ilicitude, não o será. Parece-nos que existindo o consentimento do Estado titular do direito, não haverá lugar a um desrespeito da norma, não cabendo justificar esse ato[21].

A proibição do uso da força bem como as suas exceções serão abordadas com mais detalhe no curso desta dissertação.

[18]Presente no Projeto de artigos da Comissão de Direito Internacional das Nações Unidas sobre a Responsabilidade Internacional dos Estados, no seu artigo 20º- "Um consentimento válido de um Estado à comissão de um determinado ato por outro Estado exclui a ilicitude daquele ato em relação ao primeiro na medida em que o ato permanece dentro dos limites do mencionado consentimento.". O consentimento mencionado pelo Presidente da Rússia Putin como justificativo para a atuação da Rússia no conflito sírio, sendo que o Estado Sírio solicitou o apoio russo para no conflito armado não internacional que mantinham contra o autoproclamado Estado Islâmico.

[19] Artigo 2º da Carta das Nações Unidas.

[20] *Vide,* Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries 2001

[21] *Vide,* BAPTISTA, Eduardo Correia, "Direito Internacional Público" , pp. 485.

2.2 Conceito e evolução da Internet

A ideia do computador moderno[22] foi-nos introduzida por Alan Turing e por John Von Neumann, com o objetivo comum de conceber uma nova máquina de calcular, que para além dos cálculos conseguiria ter processamento lógico de informações. O primeiro computador operacional foi construído por Alan Turing em 1940, aquando da Segunda Guerra Mundial, com o objetivo de decifrar as mensagens da máquina alemã Enigma[23]. A internet só viria a surgir duas décadas mais tarde partilhando com o computador as origens em clima de guerra. Remonta aos anos 60 durante a Guerra Fria, tendo sido desenvolvida pelo Departamento de Defesa Americano, surgindo de uma necessidade de partilhar informação entre vários computadores. Assim, em 1969 a ARPA (sigla em inglês para Advance Research Projects Agency), uma agência do departamento de defesa americano, desenvolveria uma pequena rede compreendida por quatro computadores[24]. Em 1982 a ARPAnet, nome dado à rede desenvolvida pela ARPA, juntou-se a outras redes, com o objetivo de fazer transferência de um maior volume de informação. Esta interligação entre várias redes formou uma rede de redes, ou seja, uma Internet.

Nos anos que se seguiriam, a ARPA viria a desenvolver vários protocolos e modelos que contribuíram para melhorar o funcionamento desta comunicação. Um destes modelos, o modelo de TCP/IP, siglas em inglês para *Transmission Control Protocol/Internet Protocol,* continua a ser utilizado hoje em dia na nossa arquitetura de rede. Sucintamente, o modelo de TCP/IP representa um conjunto de protocolos, que permitem que diversos equipamentos constituintes de uma rede possam estabelecer comunicação. Este modelo é representado com uma

[22] Existe uma larga discussão quanto à origem do primeiro computador, sendo que o computador Z-1 de 1936 de Konrad Zuse é considerado por muitos como o primeiro computador eletromecânico. A ideia de computador programável tal como o conhecemos hoje, com as noções de rapidez, versatilidade e auto-modificação foi planificado por Alan Turing e Von Neumann.
[23] Enigma foi o nome dado a uma máquina para encriptar e desencriptar códigos de guerra, nomeadamente durante a segunda guerra mundial.
[24] *Vide,* POE, T. Marshall, A History of Communications, Cambridge University Press, 2011 – pp. 213.

divisão em vários níveis ou camadas, tendo cada um destes níveis uma função própria. Em cada nível são desenvolvidos serviços para que o trafego de dados possa seguir para os restantes níveis. São cinco as camadas referidas, a física, a de rede, a camada de Protocolo de Internet, mais conhecida pelas siglas IP, a de transporte e, por último, a camada de aplicação. Este protocolo assegura a transferência da informação.

A ideia de transferência de informação através de uma rede de computadores acabou por se efetivar em 1983, quando o departamento de investigação militar americana desenvolveu a sua própria rede privada, a MILNET[25]. Um ano mais tarde viria a ser a Fundação Nacional da Ciência dos Estados Unidos da América (NSF) a criar a rede NSFNET, ligando cinco supercomputadores[26] de diferentes centros de investigação, de forma a que, a informação proveniente de todos os centros pudesse ser de fácil acesso às outras entidades.

Desde a sua criação, a NSFNET continuou em crescente desenvolvimento e entidades públicas de ensino e administração foram sendo acrescentadas à rede. Como se tornaria dispendioso aumentar a rede de supercomputadores, a solução encontrada foi a de criar várias redes de pequena e média dimensão, interligando-as entre si. À interligação de todas estas redes deu-se o nome de *inter-network*, em português uma ligação de várias redes internas.

Em 1988, na Universidade de Oulu na Finlândia o programador finlandês Jarkko Oikarinen começou a trabalhar num sistema que permitisse comunicação entre vários utilizadores através do protocolo de TCP/IP. Este protocolo de comunicação viria a chamar-se-ia Internet *Relay Chat* conhecido pela sigla IRC e sem tradução para português. Os IRC's permitem uma comunicação em tempo real entre utilizadores a nível mundial. As primeiras redes

[25] *Vide*, POE, T. Marshall, A History of (…) – *op.cit*. pp.214

[26] Um supercomputador com altíssima velocidade de processamento e grande capacidade de memória. Tem aplicação em áreas de pesquisa em que seja necessária uma grande capacidade de processamento. Os primeiros supercomputadores foram criados na década de 1960 por Seymour Cray. Atualmente supercomputadores utlizam-se em áreas que necessitem de cálculos complexos nomeadamente na área física quântica, mecânica, meteorologia, e também para simulações físicas, como simulação de aviões, detonação de armas nucleares, fusões nucleares entre outros.

de IRC surgiram na Finlândia começando a expandir-se pelos países escandinavos, sendo que 1989 já existiam mais de quarenta servidores espalhados por todo o mundo[27].

O IRC, tal como foi perspetivado, torna possível ter conversas privadas com um grupo de utilizadores, desde que se encontrem conectados à rede simultaneamente. No entanto, dado que a Internet estava na esfera do domínio público, tais interações entre utilizadores privados só viriam a acontecer em 1991, aquando da privatização da internet. Começando, desta forma, a surgir os primeiros distribuidores privados de serviços de internet, potencializando o seu crescimento e difusão[28].

Ao mesmo tempo Robert Cailliau, publicava uma proposta para o que viria a ser a *World Wide Web*[29]. Esta rede foi concebida com o objetivo de disponibilizar documentos em hipermédia[30], estando estes conectados entre si e sendo executados através da *Internet.* Em 1993, o CERN anunciou que a *World Wide Web* também conhecida por *WWW* , seria livre para todos, sem custo. Nesse mesmo ano a *WWW* começou a utilizar o navegador *Mosaic*[31]. O *Mosaic* é um navegador gráfico e por isso de mais simples utilização. Antes do seu lançamento no mercado não era frequente que o grafismo e texto fossem utilizados em simultâneo nas páginas *web*. A *World Wide Web Consortium* viria a ser oficialmente fundada em Outubro de 1994, após Tim Berners-Lee sair do instituto *CERN*.

A *WWW*, ainda que não sendo o único serviço disponível na Internet, tornou-se rapidamente o mais popular, em grande parte devido aos protocolos que utiliza, nomeadamente o protocolo de transferência de hipertexto conhecido pelas siglas

[27] Durante a Guerra do Golfo IRC foi utlizado para transmitir informação em direto.
[28] Um dos mais famosos chat de IRC chama-se mIRC, desenvolvido por Khaled Mardam-Bey, foi amplamente utilizado na década de 90. Tinha como objetivo principal ser um chat com a possibilidade de os utilizadores de todo o mundo poderem conversar *online*.
[29] Quanto ao seu funcionamento, visualizar uma página *web* ou outro recurso disponibilizado normalmente inicia-se ou ao digitar uma endereço no navegador ou através de uma hiperligação. Desta forma o protocolo em consonância com um outro protocolo (Domain Name Server) transforma o endereço num IP. O navegador estabelece, então, uma conexão TCP-IP com o servidor *web* localizado no endereço IP retornado o sitio pretendido.
[30] Hipermédia é o termo utilizado para designar a interligação de várias mídias.
[31] é conhecido por muitos como o primeiro Navegador *WWW* . Foi desenvolvido no National Center for Supercomputing Applications.

HTTP, um protocolo da camada de Aplicação do modelo de *Open System Interconnection*[32], utilizado para transferência de dados na *WWW*. Na prática, o que acontece é que o protocolo HTTP faz a comunicação entre o cliente e o servidor através de mensagens. O cliente envia uma mensagem com o objetivo de requisitar um recurso e o servidor envia uma mensagem de resposta ao cliente com a solicitação. Normalmente o HTTP usa o porto 80[33] e é utilizado para a obtenção de "*sites*" (sítios), comunicando na linguagem de Marcação de Hipertexto comummente conhecido por HTML.

A maioria dos navegadores *web*[34], mais conhecido por *browsers*, têm a capacidade de ler documentos bem como descarregá-los para o computador do utilizador. Os navegadores web localizam a informação pedida pelo utilizador através de localizadores universais de recursos, mais conhecidos pela sigla em inglês URL (Universal Resource Locators). Os URL's são endereços que possibilitam a localização de qualquer recurso Internet, baseando-se no serviço de Domain Name System[35].

2.3 Exploração de vulnerabilidades

Em 1984 foi introduzida a primeira definição de vírus informático[36], um programa criado com o objetivo de infetar um sistema. Traçando um paralelo com um vírus biológico, a difusão do vírus informático dá-se igualmente através da

[32] O modelo Open System Interconnection, conhecido por modelo OSI é a par do modelo de TCP/IP um modelo de camadas, com objetivo de estabelecer uma padronização, para protocolos de comunicação .
[33] Um porto da rede, é um ponto físico ou logico onde se fazem conexões, ou seja, um canal por onde são enviados dados. Dependendo do tipo de ligações que são pretendidas existem diferentes portos.
[34] Um navegador é um programa ou aplicação que permite aos utilizadores obterem documentos disponíveis num servidor de internet, atualmente entre os navegadores mais utilizados estão o Google Chrome, Mozilla Firefox, Opera, Microsoft Explora entre outros.
[35] O DNS, é um serviço que permite a tradução de um IP num nome, por exemplo ao nome de www.cm-lisboa.pt corresponde o IP 176.124.252.110, desta forma se no broser for colocado o IP referenciado irá ser aberto o website da camara de lisboa. (O IP indicado poderá vir a ser alterado).
[36] Definição introduzida por Frederick B. Cohen.

intrusão num sistema, alterando-o de forma a criar uma réplica de si mesmo dentro desse sistema. A difusão do vírus pode ser através de dispositivos móveis ou da própria rede de comunicações.

A evolução da transmissão de vírus ocorre de forma paralela à evolução da internet. Previamente à existência da rede, a forma de infetar um sistema seria através de componentes amovíveis como as disquetes. Com o surgir de pequenas redes e de interligação dessas redes entre si, deu-se uma paralela evolução do universo do vírus informático, de forma a tirar partido da dimensão da Internet. Com a globalização da rede, a forma mais rápida e eficaz de propagação de *malware*[37] tornou-se a *world wide web* e o correio eletrónico. Por conseguinte, ainda que os utilizadores continuassem durante os anos subsequentes a utilizar dispositivos amovíveis para introduzir vírus, a sua propagação dar-se-ia muito mais rapidamente através da internet.

O primeiro vírus surgiria em 1986, foi apelidado de "*brain*" e tinha como objetivo danificar o *boot*[38] do sistema, ou seja, danificava o setor de inicialização do disco rígido. No mesmo ano, nascem os primeiros sistemas de *firewall*[39], com o fim de intercetar *malware*. Na prática a *firewall* impõe restrições de acesso entre as redes através de políticas de segurança no conjunto de protocolos TCP/IP.

No ano seguinte é-nos introduzido o conceito de antivírus, concebido por Denny Yanuar Ramdhani. Este *software*[40] tinha como finalidade imunizar os sistemas contra o vírus *brain* e, ao contrário das *firewalls*, não interceta o *malware*, o antivírus só será acionado depois de o vírus já se ter estabelecido no sistema.

Desde o virus "*brain*" até aos dias de hoje, houve um aumento exponencial tanto da complexidade dos vírus como do tipo de *malware.* Os ataques de grande

[37] *Malwar*e da aglutinação dos termos *Malicious Software* é um termo utilizado para se referir a uma variedade de formas de *software* malicioso como Vírus, *Worms, Scripts* e outros .O *malware* pode ser enviado previamente para dispositivos, através de meios físicos, por *online* ou ainda através de protocolos como ftp, dentro da mesma rede. Este *malware* pode ser depois acionado à distancia ou ser programado para ser acionado a uma certa data ou até uma ação realizada pelo utilizador.

[38] O termo *boot* é utilizado para descrever o sistema de arranque de um computador.

[39] O termo em inglês, firewall faz alusão a uma parede anti-fogo visto ter como objetivo proteger os sistemas informáticos da disseminação dos acessos maliciosos à rede.

[40] *Sofware* é o termo em inglês utilizado para designar um conjunto de pogramas informáticos ou de processos. O seu funcionamento dá-se sobre um *hardawre*. O *hardware* é o termo utilizado para designar a parte física de um computador.

dimensão, já não se dão apenas à rede global de forma geral, mas sim em específico a instituições estatais, ataques estes que começariam na década de 2000. Em Abril de 2007, a Estónia foi alvo de intensos ataques cibernéticos, em inúmeras instituições estatais, incluindo o parlamento, bancos, ministérios, jornais e estações de rádio. Tal incursão deu-se através de ataques de Negação de Serviço, conhecidos pela sua sigla em inglês *DoS*. Estes ataques caracterizam-se por inúmeras solicitações de serviços, causando impossibilidade de resposta. Através de milhões de solicitações enviadas em simultâneo, um servidor fica sobrecarregado, não conseguindo satisfazer todos os pedidos. Para isto, é necessário uma máquina com grande capacidade de processamento de forma a gerar pedidos suficientes para causar a sobrecarga no processador, ou ter o controlo de várias máquinas com menor poder de processamento que consigam enviar vários pedidos. A esta última forma de *DoS,* que tem por objetivo distribuir os ataques em várias máquinas, dá-se o nome de ataque de Negação de Serviço Distribuído, ou *DDoS*[41].

Em 2008, durante o conflito armado entre a Geórgia e a Rússia, à semelhança do que havia acontecido na Estónia, também as páginas *web* e as redes de telecomunicações do governo da Geórgia sofreriam ataques de *Denial of Service* provocando uma subsequente indisponibilidade de vários serviços durante o conflito.

Em 2009, instalações nucleares iranianas foram alvo de um vírus informático, mais precisamente um *malware*, denominado *stuxnet*, que foi transmitido através de um dispositivo de armazenamento. O *stuxnet* é um *malware* através do qual é possível reprogramar Controladores Lógicos Programáveis (CLP) de sistemas de controlo industriais. Neste caso em concreto os CPL comprometidos foram os da Siemens (SCADA) que era responsável pelo controlo da velocidade de rotação das centrifugadoras de urânio do Irão. O *warm* foi assim capaz de alterar a velocidade das centrifugadoras iranianas, alterando a sua velocidade de rotação e conduzindo a uma inutilização ou até destruição do

[41] *Vide,* LIBICKI, Martin C. “Conquest in Cyberspace - National Security and Information Warfare”, Cambridge University Press pp.80

urânio. Para agravar a situação o *stuxnet* era tão complexo que foi ainda capaz de aceder ao sistema de monitorização, fazendo com que não fossem enviados sinais de anomalia e não fossem assim acionados mecanismos de defesa. Para além das centrais no Irão o vírus atingiu ainda sistemas na Índia, Indonésia, China, Paquistão e Alemanha[42].

3.Considerações Preliminares

3.1 Ciberespaço, o "*sítio*" onde se dá a ciberguerra

Devemos o termo Ciberespaço ao escritor William Gibson[43] definindo-o como uma *"uma alucinação consensual experimentada diariamente por milhares de milhões de utilizadores em todas as nações... Uma representação gráfica de dados extraídos dos bancos de dados de cada computador... Complexidade impensável..."* que na realidade não era habitada fisicamente. Foram nos livros de Gibson que mais tarde se basearam filmes como *The Matrix*, onde a realidade é alterada e simulada e o ciberespaço não passa de uma alucinação. Tal como *The Matrix* também outros livros, filmes e séries de ficção cientifica partiram das ideias de Gibson, como a icónica série *Ficheiros Secretos*.

À parte das histórias de Gibson, que não estão muito longe da definição atual de ciberespaço, consideremos três definições do que é o ciberespaço. Segundo o dicionário de Oxford, é um espaço no qual comunicamos através de computadores ligados em rede. Já David Clark[44], do Instituto de Tecnologia de

[42] *Vide*, ZETTER, Kim, "Contagem Regressiva até Zero Day, Stuxnet e o lançamento da primeira arma digital do mundo, Brassport Livros e Multimidia Lda.,201, 162-165

[43] *Vide*, GIBSON, William "Neuromancer", Harper Collins, 1986, pp. 53.

Noa verdade o termo ciberespaço foi utilizado pela primeira vez no conto Burning Chrome de 1982 mas apenas ficou celebrizado posteriormente no livro Neuromancer.

Massachusetts, considera que o ciberespaço é "*um conjunto de computadores ligados em rede, na qual é eletronicamente armazenada e utilizada informação, onde há lugar à comunicação".* Finalmente, o Departamento de Defesa dos Estados Unidos da América considera que o ciberespaço para além da internet engloba em si também os sistemas de computadores e os seus processadores e controladores. Quanto aos atores, os ataques no ciberespaço podem ter as mais diversas origens, desde cidadãos comuns, sociedades criminosas, organizações terroristas ou Estados[45].

Sobre esta definição de ciberespaço e os atores que nele realizam atividades criminosas, assenta toda uma nova sociedade cibernética cada vez mais dependente de toda e qualquer funcionalidade advinda do ciberespaço.

Como vimos anteriormente, com esta nova realidade surgiram novas formas de explorar as suas vulnerabilidades e urge assim uma necessidade de estreita cooperação e coordenação entre os Estados e organizações internacionais bem como a exigência de que elas desempenhem os seus respetivos papéis de forma complementar e interligada, na prevenção e gestão de crises. Consideramos, portanto, de carácter urgente uma regulação internacional, ou seja, é necessário o estabelecimento de regras e condutas que conduzam os Estados a melhorar o nível de defesa[46].

O facto da tecnologia da informação ter tido e continuar a ter um desenvolvimento desmedido alterou o conceito e o escopo da segurança cibernética. Os últimos dez anos foram de mudanças radicais no paradigma da cibersegurança; os crimes cibernéticos deixaram de ser unidirecionais e apenas

[44]Characterizing, cyberspace: past, present and future. David Clark MIT,CSAIL Version,1.2,of,March,12,,2010 – disponível em: https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf , consultado pela última vez a 30 de Dezembro de 2016.

[45]*Vide,* WHITE HOUSE, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23, 2008, disponivel em https://fas.org/irp/offdocs/nspd/nspd-54.pdf consultado pela ultima vez a 26 de Junho de 2017.pp.3.

[46] CIJIC, Revista Científica Sobre CyberLaw do Centro de Investigação Jurídica do Ciberespaço – CIJIC – Da Faculdade de Direito da Universidade de Lisboa, Edição N.º III-Fevereiro de 2017-pp.109 disponível em: http://www.cijic.org/publicacao/ , consultado pela última vez a 11 de Novembro de 2017.

com fins económicos para passarem a ser multidirecionais com o objetivo de alcançar vários alvos. Desta forma os planos de proteção atuais deixaram de ser eficazes, levantando a questão essencial de equilibrar o desenvolvimento tecnológico e a sua exploração com a política pública e o Direito, ou seja, é necessário estabelecer uma segurança cibernética que tenha em consideração o desenvolvimento tecnológico e que simultaneamente atente à política pública nacional e internacional. Ajustando ainda à cibersegurança o enquadramento legal com o objetivo último de conseguir um equilíbrio entre o desenvolvimento tecnológico, a politica pública e o Direito[47].

Torna-se assim inadiável a formulação de uma Lei que regule a Informática e todo o ciberespaço, que evolua em consonância com o desenvolvimento das tecnologias das redes e das comunicações.

3.2 As Infraestruturas Críticas: pontos vulneráveis a um ataque cibernético

Infraestruturas críticas (IC) são as instalações, redes, sistemas e equipamentos físicos e de tecnologia da informação sobre os quais funcionam serviços essenciais à sociedade, sendo estas infraestruturas indispensáveis para o normal funcionamento desses serviços. Desta forma, qualquer dano neste tipo de infraestrutura teria um enorme impacto negativo no setor para o qual a infraestrutura presta serviços. As IC estão normalmente associadas ao sector da banca, saúde, segurança, social etc., podendo tomar a forma de bancos, hospitais, centrais de abastecimento de água, eletricidade etc. Assim e como descrito acima, qualquer ocorrência que destabilize o normal funcionamento destas estruturas provocaria um enorme dano e prejuízo à população.

Em 2004, a Comissão Europeia adotou uma Comunicação relativa à Proteção de Infraestruturas Críticas (PIC), elaborando um “Programa Europeu de

[47] CIJIC, Revista Científica Sobre CyberLaw (..) *op.cit*,pp.113.

Proteção de Infraestruturas Críticas" (PEPIC). Assim, em 2008 nasce a Diretiva 2008/114/CE[48]. Nela encontramos identificadas as Infraestruturas Críticas Europeias. A diretiva caracteriza as IC como *"… o elemento, sistema ou parte deste situado nos Estados-Membros que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo num Estado Membro, dada a impossibilidade de continuar a assegurar essas funções"*[49]. Os setores elencados nesta diretiva são a Administração, Água, Alimentação, Energia, Espaço, Indústria Nuclear, Indústria Química, Instalações de Pesquisa, Saúde, Sistema Financeiro e Tributário, Tecnologias da Informação e as Comunicações (TIC) e Transportes. As ameaças a estas infraestruturas podem ter diversas origens, no entanto, para fins da diretiva de proteção de IC, são destacadas as ameaçadas de origem terrorista ou ataques intencionais, tanto física como ciberneticamente[50].

A comunidade internacional discute também o conceito de "crítica" no que diz respeito às IC, sendo largamente aceite que uma infraestrutura é considerada crítica quando o seu funcionamento é relevante para a sociedade, visto que uma falha nessa infraestrutura causará uma crise num determinado setor ou vários setores cruciais à vida em sociedade.

Claro está que a definição de "crítica" variará consoante o tempo e espaço. Um serviço importante a nível Nacional poderá não o ser a nível Municipal. No

[48] Directiva 2008/114/CE do Conselho de 8 de Dezembro de 2008 relativa à identificação e designação das infra-estruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção – disponível em: http://www.umic.pt/images/stories/publicacoes5/Directiva%202008%20do%20Conselho%20sobre%20infra-estruturas%20críticas.pdf – , consultado pela última vez a 14 de Março 2017.

[49] Diretiva 2008/114/CE da (..) *op.cit* .Artigo 2º.

[50] *Vide,* HORNO ,Maria Jose Mateo,"Infraestruturas Críticas e Cibersegurança",2016 disponível em http://ingenieriadeseguridad.telefonica.com/not%C3%ADcia/2016/11/07/Infraestruturas-Cr%C3%ADticas-e-Ciberseguran%C3%A7a.html, consultado pela última vez em 10 de Março de 2017.

que diz respeito ao tempo, um serviço é mais ou menos crítico em função das horas, dos dias, ou dos meses[51] .

No que concerne à dependência das IC existe entre elas uma ligação interdependente. Certas IC necessitam que outras providenciem serviços de forma a assegurar o seu funcionamento[52]. Esta interdependência torna-se alarmante visto que a disrupção do serviço de uma IC poderá afetar em larga escala outras IC's, tendo um impacto devastador para a sociedade.

A interdependência de IC pode revestir diferentes formas, de entre as várias classificações existem quatro categorias que são unanimemente aceites, sendo estas[53]:

• Cibernética: Uma IC terá uma interdependência a nível cibernético se o seu estado depende da transferência de dados entre as IC.

• Física: Infraestruturas são interdependentes de forma física quando o seu funcionamento dependente de uma conexão física entre elas.

• Geográfica: Uma IC terá uma interdependência a nível geográfico se a sua operabilidade resultar de uma proximidade geográfica entre elas.

• Lógica: Existe interdependência lógica de IC's se o seu funcionamento se der por meio que não seja físico, cibernético ou geográfico.

[51] Os serviços de restauro a base de dados são feitos durante o período noturno. Se houver uma disrupção do serviço devido a problemas na base de dados este problema poderá ser resolvido durante à noite quando a funcionalidade do serviço não seja tão necessária relativamente ao período diurno.

[52] Por exemplo um hospital dependerá de um provedor de eletricidade.

[53] *Vide*, RINALDI, Steven M; PEERENBOOM, James P.; KELLY, Terrence K., "Identifying, Understanding, and Analyzing Crítical Infrastrucres Interdependecies" pp.14-16 – disponível em http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf, consultado pela última vez a 10 de Março de 2017.

4. O Uso da Força

4.1 Conceito

A Carta das Nações Unidas foi um grande passo evolutivo no controlo do uso da força, no sentido em que foi formalizado como princípio geral e fundamental da ONU. Encontramos este principio no artigo 2° n°4 da Carta, afirmando que "*A Organização e os seus membros, para a realização dos objetivos do artigo 1º deverão agir de acordo com certos princípios nomeadamente, os membros deverão abster-se nas suas relações internacionais de recorrer à ameaça ou ao uso da força, quer seja contra a integridade territorial ou a independência política de um Estado, quer seja de qualquer outro modo incompatível com os objetivos das Nações Unidas"*. Este artigo é de aplicação universal, visto que os Estados não membros da ONU a aceitam como sendo de Direito Consuetudinário[54]. Esta norma insere-se na estrutura global da Carta que assenta sobre o pilar básico da necessidade da paz mundial, como está patente no seu primeiro artigo. O artigo nº1 da Carta estatui como primeiro objetivo a manutenção da paz e segurança internacionais, para alcançar tal fim dever-se-ão *"tomar medidas coletivas eficazes para prevenir e afastar ameaças à paz e reprimir os atos de agressão, ou outra qualquer rutura da paz e chegar, por meios pacíficos, e em conformidade com os princípios da justiça e do Direito Internacional, a um ajustamento ou solução das controvérsias ou situações internacionais que possam levar a uma perturbação da paz".[55].*

De sublinhar que o artigo 2º nº 4 da Carta faz menção não só ao uso da força, mas também à ameaça. Assim sendo, é ilícito qualquer tipo de ameaça ao recurso à força. O artigo 2° nº 4 [56], tornou-se numa norma de *Ius cogens*, isto é, uma norma imperativa que, no dizer do artigo 53° da Convenção de Viena sobre Direito dos Tratados de 1969, *"… é a que for aceite e reconhecida pela*

[54] *Vide*, AKEHURST, MICHAEL, "Introdução ao Direito Internacional", Almedina Coimbra,1985, pp.271.
[55] Carta das Nações Unidas assinada 26 de Julho de 1945, artigo 1º.
[56] *Idem*, artigo 2º.

comunidade internacional dos Estados no seu conjunto como norma à qual nenhuma derrogação é permitida e que só pode ser modificada por uma nova norma de Direito Internacional geral com a mesma natureza"[57] tendo, por isso, uma força acrescida, reconhecida por toda a comunidade internacional.

A proibição do uso da força, visto ser também ela de Direito Costumeiro aplica-se não só aos Estados signatários como também aos demais Estados, no entanto não se aplicará a grupos armados ou indivíduos, a menos que o ato destes seja atribuível a um Estado, cenário no qual o ato seria então do Estado e não do grupo ou indivíduos.

Sendo que a Carta das Nações Unidas não oferece nenhum critério para determinar se um ato pode ser definido como uso da força, o Tribunal Internacional de Justiça no caso *concerning military and paramilitary activities in and against Nicaragua*[58] afirmou que a "escala de efeitos" deve ser considerada para determinar se ações equivalem a um ataque armado. Tem-se que "escala de efeitos" é o termo utilizado para descrever os fatores quantitativos e qualitativos a serem analisados na determinação de quando uma operação cibernética ou não cibernética se qualifica como uso da força[59].

4.2 Uso da Força em Contexto Cibernético

No que concerne ao uso da força em contexto cibernético, as regras 10 e 11 do Manual de Tallinn dizem-nos que é ilícita uma operação cibernética que constitua ameaça ou uso da força[60].

[57] Convenção de Viena sobre o Direito dos Tratados, assinada em 23 de Maio de 1969.

[58] Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) disponivel em: http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf consultado pela última vez a 21-02-2017.

[59] *Vide*, SCHMITT, Michael N*, "*Tallinnn Manual on the International Law Applicable to Cyber Warfare" – Universidade de Cambridge, 2013. regra 11.

[60] A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any state, or that is in other manner inconsistent with the purpose of the United nations, is unlawful." Shmitt, Tallin Manual, regra 10

Na regra 10 encontramos a ameaça ao uso da força, que, como já vimos, não só é ilícito o uso da força propriamente dito mas também a ameaça. Uma operação cibernética em forma de ameaça poder-se-á conduzir de duas formas. A primeira diz respeito a uma operação cibernética que sirva para comunicar uma ameaça ao uso da força, seja esta cibernética ou não. A segunda forma consubstancia-se numa ameaça transmitida por qualquer meio, seja este cibernético ou não, para levar a cabo operações cibernéticas qualificadas como uso da força[61].

Uma ameaça deverá ser explícita ou implicitamente comunicada. Ações que simplesmente ameaçam a segurança do Estado alvo mas que não foram de alguma forma transmitidas, não se qualificam como ameaça ao uso da força. Supondo que o Estado A começa a desenvolver capacidade de conduzir operações cibernéticas maliciosas contra o Estado B, a mera aquisição de tais capacidades, que pode ser usada para conduzir operações, não constitui uma ameaça. Apenas quando o Estado A comunicar que o equipamento adquirido será utilizado contra o Estado B, se poderá considerar tal conduta como uma violação da "não ameaça do uso da força*"*.[62].

No contexto cibernético, mais do que no contexto convencional, põe-se o problema de saber se um Estado que não possui nenhuma capacidade para realizar uma operação, poderá violar a regra da "não ameaça do uso da força". A opinião é a de que, aferir da capacidade cibernética é altamente difícil, pois não haverá uma relação tão direta com o tamanho do território, da população ou da capacidade económica e militar dum Estado com a capacidade cibernética de que um Estado poderá dispor. Tal implica que será mais difícil para um Estado avaliar a capacidade de outro Estado para cumprir a sua ameaça de usar a força por meios cibernéticos. Do mesmo modo, também não pode ser alcançado nenhum consenso sobre um Estado que possua a capacidade de realizar a ameaça, mas que não tenha intenção de o fazer. Nos casos acima descritos acreditamos que deve ser feita uma análise caso a caso.

[61] *Vide*, SCHMITT, Michael N," Tallinn Manual(…)"*op.cit*. regra 10

[62] *Ibedim.*

Quanto ao uso da força propriamente dito, segundo o Manual de Tallinn[63], na sua regra nº 10 relativamente à proibição do uso da força, uma operação cibernética constituirá uso da força se se der contra a integridade territorial ou independência territorial de um Estado, tal como disposto no artigo 2º da Carta. No comentário 4º à regra nº 10 do Manual de Tallinn o grupo internacional de peritos constata que "*Uma ação qualificada como uso da força não precisa ser conduzida pelas forças armadas de um Estado. Por exemplo, uma operação cibernética que se qualificaria como uso da força, se conduzida pelas forças armadas seria igualmente qualificada como uso da força se levado a cabo por entidades de Inteligence de um Estado ou por entidades privadas que contratem com o Estado cuja conduta lhe seja a si imputável*".[64]

Outra regra do manual que apoia a definição de ataque cibernético como ataque armado é a regra nº 11, que determina que uma operação cibernética constitui uso da força quando a sua "escala e efeitos" (danos) seja comparável à de uma operação não cibernética que constituía também esta uma violação à proibição do uso da força. Na regra nº 11 do Manual de Tallinn são abordados seis requisitos, desenvolvidos por Michael Schmitt, de forma a determinar se ataque cibernético pode ser visto como constituindo uma violação à proibição do uso da força. São estes critérios[65]:

1) A gravidade. Dado que os ataques armados ameaçam danos físicos e destruição, serão assim considerados como atos que transgridem a proibição do uso da força. Desta forma uma operação cibernética que resulte em dano, destruição ou morte é muito provável que seja considerada como uso da força. Este critério será o critério que tem maior peso na caracterização de uma operação cibernética como um ataque armado;

2) A eminência. Um ataque cujas consequências se manifestem mais rapidamente, fará com que seja mais difícil aos Estados conseguirem uma

[63] Um documento não vinculativo sobre a aplicabilidade da lei internacional na resolução conflitos cibernéticos.
[64] *Vide*, SCHMITT, Michael N, "Tallinnn Manual(…)" *op.cit*. regra 11.
[65] *Idem,* comentário 9 à regra 11.

resolução pacífica do conflito. Assim será mais fácil caracterizar como ataque armado uma operação cibernética que tenha consequências imediatas;

3) Carácter direto. Este critério pretende traçar uma ligação entre as consequências e conduta, ou seja, quanto maior for o nexo causal entre a operação cibernética e os efeitos, maior será a probabilidade desta ser considerada como uso da força;

4) Carácter invasivo. Este critério tem em consideração o grau de intrusão de uma operação cibernética. Uma operação cibernética que entre dentro de um sistema militar de um Estado será mais provavelmente considerada como uso da força do que uma mera exploração de vulnerabilidades de um sistema de uma Universidade;

5) Quantificação dos Efeitos. Torna-se mais fácil caracterizar um ato como uso da força se as consequências do ato ilícito forem mensuráveis. Assim, quanto mais quantificável e fácil de identificar forem as consequências de uma operação cibernética, mais plausível será de a qualificar como uso da força;

6) Carácter Militar. Havendo um nexo de causalidade entre uma ciberoperação e uma operação militar, será mais facilmente presumível que esta constitua uma violação à proibição do uso da força.

Analisada a definição de uso da força e o enquadramento de operações cibernéticas importa agora saber se estas podem ser vistas como um ataque armado.

4.2.1 Operações cibernéticas como ataque armado

Para definir ataque armado é necessário perceber que este termo está diretamente ligado à agressão e à proibição do uso da força. A agressão, mencionada na Carta no artigo 29º quanto às competências do Conselho de Segurança, é-nos definida como *"o uso da força armada por parte de um Estado contra a soberania, integridade territorial ou independência política de outro*

Estado, ou de qualquer outra forma incompatível com a Carta das Nações Unidas".[66]-[67].

Esta definição presente na Resolução 3314 da Assembleia Geral das Nações Unidas é crucial para definir ataque armado visto que tem sido várias vezes mencionada pelo TIJ. Nos casos das atividades militares do Nicarágua[68] anteriormente mencionado, bem como nos casos da Republica Democrática do Congo/Uganda[69] e das Plataformas de petróleo Irão/Estados Unidos da América[70], o TIJ, a partir da definição de agressão, define ataque armado como "*a forma mais gravosa do uso da força*".

De acordo com a jurisprudência, o Tribunal Penal Internacional para a antiga Jugoslávia declarou que *"um ataque armado existe sempre que se recorre às forças armadas entre os Estados ou em que há violência armada prolongada entre*

[66] Resolução 3314 da Assembleia Geral das Nações Unidas sobre definição de agressão, artigo1º, disponível em: http://hrlibrary.umn.edu/instree/GAres3314.html, acedido a 12 de Março de2017.

[67] Pode-se ler-se ainda no artigo 3º desta resolução os tipos de uso da força que revestem a forma de agressão: "Considerar-se-á ato de agressão qualquer um dos atos a seguir enunciados, tenha ou não havido declaração de guerra, sob reserva das disposições do artigo 2.° e de acordo com elas: a) A invasão ou o ataque do território de um Estado pelas forças armadas de outro Estado, ou qualquer ocupação militar, ainda que temporária, que resulte dessa invasão ou ataque, ou qualquer anexação mediante o uso da força do território ou de parte do território de outro Estado; h) O bombardeamento pelas forças armadas de um Estado, ou o uso de quaisquer armas por um Estado, contra o território de outro Estado; c) O bloqueio dos portos ou da costa de um Estado pelas forças armadas de outro Estado; d) O ataque pelas forças armadas de um Estado contra as forças armadas terrestres, navais ou aéreas, ou a marinha e aviação civis de outro Estado; e) A utilização das forças armadas de um Estado, estacionadas no território de outro com o assentimento do Estado recetor, cm violação das condições previstas no acordo, ou o prolongamento da sua presença no território em questão após o termo do acordo; f) O facto de um Estado aceitar que o seu território, posto à disposição de outro Estado, seja utilizado por este para perpetrar um ato de agressão contra um terceiro Estado; g) O envio por um Estado, ou em seu nome, de bandos ou de grupos armados, de forças irregulares ou de mercenários que pratiquem atos de força armada contra outro Estado de uma gravidade tal que sejam equiparáveis aos atos acima enumerados, ou o facto de participar de uma forma substancial numa tal ação.", artigo, cfr. 3º Resolução 3314 da Assembleia Geral das Nações Unidas(…) *op.cit*. artigo3º.

[68] Case concerning military and paramilitary activities in and against Nicaragua (…) *op cit*

[69] Case concerning armed activities on the territory of the Congo (Democratic Republic of Congo v. Uganda), 19 de Dezembro de 2005, disponível em : http://www.icj-cij.org/docket/files/116/10455.pdf.

[70] Case concerning oil platforms (Islamic Republic of Iran v. United States of America), 6 de Novembro de 2003, disponível em: http://www.icj-cij.org/docket/files/90/9715.pdf.

as autoridades governamentais e grupos armados organizados ou entre esses grupos no interior de um Estado" [71].

Um ataque armado, para que se qualifique como tal, deverá sempre contemplar um elemento transfronteiriço, visto que os atos organizados, conduzidos e dirigidos apenas no território do próprio Estado, leva a aplicabilidade do "uso a força" de acordo com a sua lei interna (desde que em consonância com a lei internacional de direitos humanos e em situações de conflito armado não internacional com a lei dos conflitos armados) [72].

Quanto ao financiamento de grupos que realizem operações cibernéticas, apoiado na decisão do TIJ no caso acima mencionado, que considera que o financiamento de guerrilhas envolvidas em operações contra outro Estado não é considerado o uso de força, então também aqui um mero financiamento a um grupo *hacktivista* que leve a cabo operações cibernéticas contra outro Estado, não será considerado uso da força.

No que concerne a apoio logístico, no caso do Nicarágua o TIJ decidiu que armar e treinar uma força de guerrilha envolvida em operações contra outro Estado seria qualificado como uso da força, como tal, fazendo um paralelo entre treinar forças de guerrilha e fornecer a um grupo de *hacktivistas malware* e/ou formação passíveis de ser utilizados em ataques cibernéticos contra outro Estado, também poderá ser qualificado como uso da força[73].

As operações cibernéticas que não pretendam infligir dano e apenas tenham como objetivo fragilizar um governo ou economia, segundo o Manual de Tallinn, não se qualificam como uso da força. No entanto, para que uma operação cibernética seja considerada como uso da força, não necessita obrigatoriamente de infligir um dano físico. O roubo de Informação sensível ou por exemplo o

[71] Promotor v. Dusko Tadic, Caso No. IT-94-1-AR72, Decisão sobre a Moção de Defesa para a Apelação de Interlocução em relação à Jurisdição, 2 de Outubro de 1995. Apelações do TPI, para70.
[72] *Vide*, SCHMITT, Michael N, "Tallinnn Manual(…) "*op cit.* regra 13
[73]*Ibedim.*

bloqueio de um porto, embora não cause danos físicos, cairá sobre a denominação de uso da força[74].

4.3 Exceções ao Uso da Força

4.3.1 Legítima defesa

a) Conceito de legítima defesa

A figura da legítima defesa tal como a conhecemos hoje surge com a Liga das Nações, sendo um resquício do que havia sido outrora o direito da auto-preservação[75]. Foi ainda durante a Liga das Nações que a legítima defesa apareceu comummente no contexto do uso da força. Trata-se essencialmente de uma reação de um Estado contra o uso da força por parte de outro Estado, tendo como base a proporcionalidade à ameaça. Criou-se então a presunção de que o uso da força no exercício da legítima defesa seria lícito apenas se em reação ao uso prévio da força[76].

Esta causa de exclusão da ilicitude é assim particular, na medida em que viola a norma de *Ius Congens* da Carta das Nações Unidas no que concerne à proibição do uso da força nas relações internacionais[77]. O Artigo 21º do Projeto da Comissão de Direito Internacional das Nações Unidas sobre Responsabilidade

[74] *Vide,* ROSCINI, Marco: "*Ciber Operations* (…)" *op cit.,* pp. 71

[75] Definida por Vattel no livro "*Direito das Gentes vol 3"* como "En traitant du Droit de sfirete, nous avons montre, que la Nature donne aux hommes le droit d'user de force, quand cela est necessaire, pour leur defense et pour la conservation de leurs droits."

[76] *Vide*, BROWNLIE, Ian M.A., D.PHIL.: "*The Use of Force in Self-Defense*" -Lecturer in Law in the University of Nottingham, Reino Unido, 1961– pp183.

[77] Carta das Nações Unidas de 26 de Julho de 1945 – artigo 2º nº 3 e 4 – "3) Os membros da Organização deverão resolver as suas controvérsias internacionais por meios pacíficos, de modo a que a paz e a segurança internacionais, bem como a justiça, não sejam ameaçadas;
4) Os membros deverão abster-se nas suas relações internacionais de recorrer à ameaça ou ao uso da força, quer que seja contra a integridade territorial ou a independência política de um Estado, quer seja de qualquer outro modo incompatível com os objetivos das Nações Unidas."

Internacional dos Estados de 2001, doravante designado por projeto de artigos de 2001, diz-nos que a legítima defesa exclui a ilicitude de um ato, se este estiver em conformidade com a Carta das Nações Unidas. Também a Convenção de Viena[78] no seu artigo 52º nos reporta para a carta das Nações Unidas na medida em que diz ser *"nulo todo o tratado cuja conclusão tenha sido obtida pela ameaça ou pelo emprego da força, em violação dos princípios de direito internacional consignados na Carta das Nações Unidas*."

A Carta faz, no entanto, menção a duas exceções à proibição de usar a força sendo uma destas exceções[79] a legítima defesa. No seu artigo 51º a Carta diz-*nos que:*

> *"Nada na presente Carta prejudica 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 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 momento, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais."*

O Conselho de Segurança nas Resoluções 1368 e 1373, ambas de 2001, afirma e reitera o "*reconhecimento do direito inerente à legítima defesa individual ou coletiva em concordância com a Carta das Nações Unidas"*[80].

Quanto aos pressupostos da legítima defesa, é necessário que a entidade que a pretende invocar tenha sido objeto de um ataque armado por parte duma entidade vinculada pela proibição do uso da força[81]. No entanto, a proibição do

[78] Convenção de Viena sobre o Direito dos Tratados -, 23 de Maio de 1969.

[79] Uma outra exceção à utilização da força é por via de autorização do Conselho de Segurança.

[80] Resolution 1368 (2001) Adopted by the Security Council at its 4370th meeting, on 12 September 2001 e Resolution 1373 (2001) Adopted by the Security Council at its 4385th meeting, on 28 September 2001.

[81] *Vide,* BAPTISTA, Eduardo Correia –"*Direito Internacional Público* "(…) *op.cit*.,pp 427.

uso da força elenca mais do que uma forma de violação com diferente escala de gravidade: o uso ilícito da força, a agressão e o ataque armado. A invocabilidade desta causa de exclusão da ilicitude dependerá apenas da ocorrência de um ataque armado. Segundo jurisprudência do TIJ no caso de 1986 que opôs o Nicarágua aos Estados Unidos da América em *Case concerning military and paramilitary activities in and against Nicaragua*[82], "*Um Estado não tem o direito de ter uma resposta armada em resposta a atos que não sejam um 'ataque armado'."* O ataque armado deverá ser atual ou particularmente grave ou ainda que não tendo ocorrido, existam riscos da eminência desse ataque[83]. Um exemplo de um ataque armando que deu lugar à legítima defesa ainda que não houvesse atualidade foram os ataques ao *World Trade Center* a 11 de Setembro de 2001.

A utilização do termo uso da força surge em contexto de conflito cibernético do mesmo modo que num conflito armado cinético, ou seja, em resposta a um ataque armado. Tal como vimos antes, o artigo 51º da Carta das Nações Unidas trata de referenciar a dependência de um ataque armado para o uso da legítima defesa. Desta forma, haverá aqui lugar a legitima defesa quando um ataque cibernético causou ou está a causar, num período continuo, danos. Estão também aqui abrangidas situações em que um ataque cibernético seja um meio para iniciar um ataque armado.

A legítima defesa contra ataques cibernéticos pode dar-se de três formas: forma física, eletrónica 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 eletrónica, 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.[84]

[82] Case concerning military and paramilitary activities in and against Nicaragua de 1986 disponível em : http://www.icj-cij.org/docket/files/70/6503.pdf.
[83] A questão da legitima defesa preemptiva será analisada mais à frente.
[84] *Vide,* ROSCINI Marco: "*Cyber Operations and the Use of Force in International Law"*, Oxford University Press, Reino Unido. 2014

b) Legítima defesa em conflitos armados não internacionais

Como veremos mais à frente, um conflito armado não-internacional dar-se-á de duas formas: quando grupos armados não-governamentais lutam entre si ou quando grupos armados lutam contra forças governamentais. O nível do conflito deverá exceder a intensidade de meros atos de violência isolados e o grupo armado deverá ter um nível de organização que lhe permita conduzir operações bem preparadas e de longa duração[85].

Definido que está ataque armado, importa saber como poderá um Estado exercer legítima defesa contra um ataque cibernético vindo de um grupo organizado, e se os atos desse grupo podem ser imputados a um Estado, transformando um conflito armando não-internacional num conflito armado internacional. Quanto à controversa questão de saber se a legítima defesa se poderá dar em resposta a uma violação da proibição do uso da força por parte de um grupo armado, o artigo 51º da Carta, apenas faz menção ao facto de que o ataque deverá ter como alvo um Estado, no entanto, em nada se refere à origem desse ataque. Desta forma, parece-nos que poderá haver lugar a legítima defesa em resposta à conduta ilícita de um grupo armado. A prática também parece apontar nesse sentido, dado que a conduta dos Estados Unidos da América contra os ataques do "11 de Setembro" foram consideradas dentro do escopo do direito da legítima defesa[86].

Do ponto de vista cibernético, a legítima defesa está prevista no Manual de Tallinn, a regra 13 diz-nos que um Estado alvo de uma operação cibernética que

[85] Comité Internacional da Cruz Vermelha – violência e o Uso da força – Agosto 2009 pp 26. Disponível em : https://www.icrc.org/por/assets/files/other/icrc_007_0943.pdf ,

[86] Vide, IMPRENSA NATO, "*NATO's Contribution to the Fight Against Terrorism 20 July 2004"*. É invocado o artigo 5º do tratado de Washington de 1949 como justificação para a considerer como ataque armado os atos da Al Qaeda no 11 de Setembro de 2001. O artigo 5º do Tratado de Washington diz:" The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area".

possa ser equiparada a um ataque armado, pode exercer o seu direito à legítima defesa.

c) Legítima defesa preemptiva contra um ataque armado iminente

Ainda que não seja claro no artigo 51º da Carta das Nações Unidas, nem preveja expressamente a ação defensiva em antecipação a um ataque armado, há aqui lugar à análise de diversos fatores.

Em primeiro lugar é importante estabelecer a diferença entre legítima defesa preventiva e legítima defesa preemptiva. A primeira dá-se em resposta a um ataque armado futuro plausível de acontecer mas que no entanto não é certo e não existem provas do seu planeamento. Diferentemente acontece no caso da legítima defesa preemptiva, a qual se dá em resposta a um ataque armado iminente.

No caso Caroline de 1837[87], o Governo dos EUA não aceitou a argumentação do Governo britânico, que defendeu a legitimidade da destruição preventiva deste navio. O secretário-geral do governo britânico Daniel Webster, na sequência deste caso e após um pedido de desculpas ao governo americano, definiu critérios de legítima defesa que admitiam a preempção contra ataque iminente mas não a prevenção. Desde aí, definidos os critérios, é pacífico na doutrina que a legítima defesa preemptiva cabe nos critérios do artigo 51º da Carta.

No que concerne a ações preemptivas contra ataques cibernéticos, estas estão compreendidas na regra 15 do manual de Tallinn – *Imminence and Immediacy – "O direito de usar a força em legítima defesa surge se um ataque cibernético estiver a ocorrer ou seja iminente. A legítima defesa está assim sujeita a um requisito de urgência*". O grupo de peritos seguiu a opinião descrita acima de que, embora o artigo 51º da Carta não preveja expressamente uma ação defensiva antecipada, um Estado não terá de esperar enquanto o inimigo se

[87] Durante um movimento insurreição do Canada contra a Grã-Bretanha um navio americano que estaria a ajudar as forças rebeldes é atacado a 29 de Dezembro de 1837 por tropas britânicas que embarcaram no navio e mataram vários cidadãos norte-americanos.

prepara para atacar. Em vez disso, um Estado pode defender-se de um ataque armado iminente. O grupo de peritos dá ainda um exemplo no comentário 5º, um destes exemplos pressupõe que o serviço de *Intelligence* de um determinado Estado, o Estado A, recebe informações incontrovertíveis de que o Estado B está a preparar um ataque cibernético que destruirá dentro de duas semanas um oleoduto seu. Sabe ainda o Estado A que o ataque se realizará fazendo com que os microcontroladores aumentem a pressão dos tubos do oleoduto provocando explosões[88]. Os serviços de *Intelligence,* não tendo qualquer informação sobre a vulnerabilidade dos microcontroladores e não sabendo como controlar o ataque, detêm, contudo, informações sobre uma reunião que terá lugar com todos os indivíduos envolvidos na operação. Conclui-se que neste exemplo o Estado A teria a necessidade de tomar ações preemptivas contra um ataque que estaria ataque[89]. Desta forma, ataques contra esses indivíduos não seriam ilícitos[90]. Um outro exemplo dado pelo grupo de peritos no Manual de Tallinn é o de um Estado que pretende realizar ataque armado através do uso de *malware*[91] previamente enviado para os dispositivos do Estado alvo. Estamos perante um ataque armado iminente, sendo que se o Estado alvo não intervir perante a situação, não o poderá fazer após o seu sistema ter sofrido uma falha devido ao *malware*.

Fatores como a proximidade temporal entre o ataque e a resposta, ou o período necessário para identificar o atacante, bem como o tempo necessário para preparar uma resposta são altamente relevantes nesta análise.

A situação de legítima defesa não conclui necessariamente com o término da operação cibernética. Se for razoável concluir que as operações cibernéticas adicionais provavelmente terão continuidade, o Estado vítima pode tratar essas operações como uma campanha cibernética continuada, fazendo-se valer do seu direito à legítima defesa, seja este um ataque cinético ou cibernético. Não é razoável, no entanto, qualquer uso adicional da força, seja cinética ou ciberneticamente, podendo esta conduta ser caracterizada como mera retaliação.

[88] Ataque em tudo semelhante ao *Stuxnet*.
[89] Vide, SCHMITT, Michael N, "Tallinn Manual(…)"*op.cit*.regra 15.
[90] *Ibedim.*

Em última análise, o requisito de imediação resume-se a uma prova de razoabilidade à luz das circunstâncias prevalecentes no momento.

Em alguns casos, o ataque cibernético pode não ser aparente por um período indeterminado de tempo. Tal pode acontecer quando a fonte do ataque ainda não foi identificada. O próprio ataque pode até estar a decorrer nos dispositivos e não ser notório, como no caso da utilização de *botnets*[92]. Da mesma forma, poder-se-á dar que, o iniciador do ataque não seja identificado por um largo período de tempo findo o ataque. O exemplo clássico de ambas as situações é utilização de um *malware* como o *stuxnet*[93].

O ataque armado, para permitir uma ação em legítima defesa, deve assim ser atual, tendo iniciado a sua execução ou existirem riscos sérios de estar iminente. Assim, o requisito necessário para aferir da licitude da legítima defesa preemptiva é o requisito da iminência ou não de um ataque armado.

d) Legítima Defesa: Necessidade e Proporcionalidade

A legítima defesa contra ataques cibernéticos tal como a legítima defesa contra ataques físicos contra Estados ou grupos armados, deve atender a critérios de necessidade e proporcionalidade.

A Carta no seu artigo 51º não é explícita quanto a estes critérios, no entanto, no caso sobre *Legality of the Threat or Use Nuclear Weapons*[94]*,* o TIJ declarou que a legítima defesa está sujeita às condições de necessidade e proporcionalidade em concordância com a decisão do caso da Nicarágua[95] . O

[92] Este tipo de ameaça têm este nome por se parecer com um robot, que poderá ser programado para levar a cabo tarefas no computador do utilizador afetado. Uma *botnet* é uma rede de *bots* que interligando computadores controlados remotamente quse sempre infetados com software mal-intencionado. Uma vez criada, a rede de computadores infetados que constituem a *botnet* pode ser ativada sem o conhecimento dos utilizadores dos computadores a fim de lançar um ciberataque em grande escala, o que geralmente tem o potencial de provocar danos graves como, por exemplo, a perturbação de serviços de sistema de importância pública significativa, ou importantes custos financeiros ou a perda de dados pessoais ou informações sensíveis.

[93]O *Stuxnet* actua nos microcontroladores de uma forma continua e não se sabia inicialmente a sua origem.

[94] Case concerning Legality of the Threat or Use of Nuclear Weapons - Advisory Opinion of 8 July 1996 disponível em http://www.icj-cij.org/docket/files/95/7497.pdf.

[95] Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgement, International Court of Justice (ICJ), 27 June 1986, §94

TIJ, não declarando que o uso de armas nucleares desrespeite o princípio da proporcionalidade, alerta para que os Estados que acreditam que o uso de armas nucleares possa ser feito de acordo com o princípio da proporcionalidade, se consciencializem para a própria natureza dessas armas e o risco a elas associados.

O manual de Tallinn prevê na sua regra 14 os princípios da Necessidade e Proporcionalidade em contexto cibernético, dizendo-nos que o uso da força em operações cibernéticas no exercício do direito à legítima defesa deve ser necessário e proporcional[96].

e) Legítima defesa coletiva

A legítima defesa pode ser exercida coletivamente, em bom rigor trata-se de uma defesa de terceiro[97] e está prevista no artigo 51º da Carta das Nações Unidas.

A legítima defesa coletiva habilita um Estado ou Estados a assistir outro ou outros Estados que sejam vítimas de um ataque armado. Este direito está explicitamente estabelecido no artigo 51º da carta quando nos diz que "*Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva*"[98]. Esta norma reflete o direito internacional consuetudinário.

A legítima defesa coletiva só pode ser exercida à luz do direito internacional costumeiro, quando a conduta tiver sido qualificada como sendo um ataque armado[99] e o Estado vitima tiver solicitado o auxílio de um terceiro. Desta forma,

"there is a specific rule whereby self-defence would warrant only measures which are proportionality to the armed attack and necessary to respond to it, a rule well established in customary international law".

[96] Vide, SCHMITT, Michael N, "Tallinn Manual(…)" *op.cit*. regra 14.

[97] Neste sentido alguns autores consideram que a legítima defesa tem um carácter unilateral e assim sendo o direito à legítima defesa seria o direito apenas do Estado vítima. Seguindo esta cadeia de pensamento, alguns reconhecem como definição o direito de defesa de Estado terceiro e não de legítima defesa coletiva. . cfr Kelsen Hanz, The Law of United Nations – A critical Analysis of Its Fundamental Problems, London 1950, pp.792.

[98] Carta das Nações Unidas(…) art.51º.

[99] O TIJ afirmou que : "Whether self-defence be individual or collective, it can only be exercised in response to an "armed attack". In the view of the Court, this is to be understood as meaning not

será lícito a um Estado exercer esta forma de legítima defesa apenas quando o Estado vítima lhe tiver feito um pedido de assistência[100]. O direito de legítima defesa coletivo está sujeito às condições estipuladas no pedido do Estado vítima.

Importa agora averiguar se o pedido de auxílio poderá ou não advir de um tratado prévio, ou seja, se na existência de um tratado em que esteja previsto tal auxílio, um Estado poderá atuar conforme a legítima defesa coletiva sem um pedido prévio de auxílio do Estado lesado. Acredita-se que sim, mas apenas se o Estado lesado não recusar tal auxilio[101].

A legítima defesa coletiva está também sujeita ao princípio da necessidade e proporcionalidade[102].

No plano cibernético, a legítima defesa coletiva pode ser exercida igualmente quando a pedido do Estado que tenha sido vítima de uma operação cibernética tida como um ataque armado[103].

merely action by regular armed forces across an international border, but also the sending by a State of armed bands on to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack had it been carried out by regular armed forces. The Court quotes the definition of aggression annexed to General Assembly resolution 3314 (XXIX) as expressing customary law in this respect." cfr Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), cit. ICJ Summary of the Judgment of 27 June 1986 p.6 – disponível em: www.fd.unl.pt/docentes_docs/ma/TMA_MA_4615.doc , consultado pela última vez a 10 de Outubro de 2017.

[100] O TIJ afirmou que: "the Court finds that in customary international law, whether of a general kind or that particular to the inter-American legal system, there is no rule permitting the exercise of collective self-defence in the absence of a request by the State which is a victim of the alleged attack, this being additional to the requirement that the State in question should have declared itself to have been attacked." Cfr Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) cit. ICJ Summary of the Judgment(..) pp.6.

[101] Vide, BAPTISTA ,Eduardo Correia, "*O Poder Público Bélico em Direito Internacional: O Uso da Força Pelas Nações Unidas em Especial*", Dissertação de Doutoramento em Ciências Jurídico-Políticas na Faculdade de Direito da Universidade de Lisboa, Almedina 2003, p.198-199

[102] O TIJ afirma que: "The general rule prohibiting force established in customary law allows for certain exceptions. The exception of the right of individual or collective self-defence is also, in the view of States, established in customary law, as is apparent for example from the terms of Article 51 of the United Nations Charter, which refers to an "inherent right", and from the declaration in resolution 2625 (XXV). The Parties, who consider the existence of this right to be established as a matter of customary international law, agree in holding that whether the response to an attack is lawful depends on the observance of the criteria of the necessity and the proportionality of the measures taken in self-defence. "Cfr Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) cit. ICJ Summary of the Judgment of 27 June 1986 pp.6 .

[103] *Vide*, SCHMITT, Michael N, "*Tallinn Manual(…)" op.cit.* regra 16.

e) Comunicação Imediata das medidas de Legítima Defesa.

As medidas tomadas no exercício da legítima defesa devem ser comunicadas imediatamente ao Conselho de Segurança.

Este requisito surge-nos no artigo 51º da Carta das Nações Unidas, dizendo-nos que "*As medidas tomadas pelos membros no exercício do direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança*" [104]. Também neste sentido parece apontar a justificação legal da notificação em *Operation Enduring Fredom*[105] relativa aos ataques do "11 de Setembro", a 7 de Outubro de 2001 os Estados Unidos da América e o Reino Unido informaram ao Conselho de Segurança das Nações Unidas que haviam iniciado atividades de uso de força militar em legítima defesa em conformidade com o artigo 51º da Carta das Nações Unidas, que reconhece "*o direito inerente à legítima defesa individual ou coletiva*" e exige que os Estados notifiquem tais ações.

Igualmente na legítima defesa, em resposta a operações cibernéticas devem ser comunicadas ao Conselho de Segurança. Assim faz menção o Manual de Tallinn quando diz que "*Medidas que envolvam operações cibernéticas cometidas por Estados no exercício da legítima defesa consoante o artigo 51º da Carta das Nações Unidas devem ser imediatamente reportadas ao Conselho de Segurança das Nações Unidas*" [106].

4.3.2 Ações Autorizadas ao Conselho de Segurança das Nações Unidas

Uma segunda exceção à proibição do uso da força trata das ações autorizadas ao Conselho de Segurança das Nações Unidas. No seu artigo 42º a Carta autoriza o Conselho de Segurança a usar forças militares pra obter a paz e segurança[107]. No entanto, ainda que a Carta autorize o Conselho a usar a força,

[104] Carta das Nações Unidas *op.cit*. Art.51º.
[105] Operação conduzida em resposta aos ataques conduzidos a 11 de Setembro de 2001 pela al-Qaeda.
[106] *Vide*, SCHMITT, Michael N, "*Tallinn Manual(…)"op.cit.*regra 17.
[107] Carta das Nações Unidas(…) art.42º.

este apenas o pode fazer se as medidas previstas no artigo 4º demonstrarem ser inadequadas. O artigo 41º prevê medidas que não envolvam a utilização de força armada, nomeadamente *"a interrupção completa ou parcial das relações económicas, dos meios de comunicação ferroviários, marítimos, aéreos, postais, telegráficos, radioelétricos, ou de outra qualquer espécie, e o rompimento das relações diplomáticas."*[108].

Estes artigos estão contidos no Capitulo IV da Carta das Nações Unidas sobre ações em caso de ameaça à paz, rutura da paz e ato de agressão. Assim, tanto a aplicação do artigo 41º como a posterior aplicação do artigo 42º dependem da determinação, por parte do Conselho de Segurança, da existência de qualquer ameaça à paz, rutura da paz ou ato de agressão" como descrito no artigo 39º da Carta[109].

4.3.3 O Consentimento

O consentimento dá-se quando um Estado concede a outro a prática de um ato que seria contrário a uma obrigação internacional se não tivesse sido consentido. O consentimento é tratado no Projeto de Artigos sobre a Responsabilidade dos Estados de 2001 como uma causa de exclusão da ilicitude, na medida em que um Estado titular de um direito internacional consente a outro Estado, obrigado por esse direito, a violá-lo. Desta forma, desde que o Estado que viola a obrigação não extravase o consentimento do titular desse direito considera-se que não há ilicitude.

No artigo 20º do projeto de artigos de 2001[110] prevê-se que *"o consentimento válido dum Estado para a prática de um determinado ato por outro Estado exclui a ilicitude daquele ato*", entendendo-se por válido o que não seja contrario às normas de *Ius Cogens*[111].

[108] Carta das Nações Unidas(…) ,*op,cit*.art.51º.
[109] *Idem,* art.39º.
[110] Draft articles on Responsibility of States (..) *op.cit*.art. 20º.
[111] Convenção de Viena sobre o Direito dos Tratados, 23 de Maio de 1969, art.º 53º - Tratados incompatíveis com uma norma imperativa de direito internacional geral (*ius cogens*).

O consentimento foi aqui tratado, seguindo a ótica de organização do projeto de artigos de 2001, como uma causa de exclusão da ilicitude, no entanto não consideramos o consentimento como tal. Existindo um prévio consentimento a uma conduta, não há lugar à justificação dessa conduta, visto o ato em si não conter qualquer ilicitude [112].

Como pressuposto, o consentimento deverá ser prévio à conduta para a qual este é concedido. O consentimento dado depois da conduta violadora de uma obrigação internacional ter sido levada a cabo, não excluirá a ilicitude da conduta. Nesta situação o Estado renuncia essencialmente ao direito de invocar a responsabilidade, no entanto tal não exclui a ilicitude do ato ou omissão[113].

De ressalvar que, se uma conduta levada a cabo por um Estado violar o direito ou interesse de mais de um titular, o consentimento apenas exclui a ilicitude em relação ao Estado que deu o consentimento. Assim sendo, para que o ato esteja dentro da causa de exclusão da ilicitude o consentimento terá de ser dado por todos os titulares a quem seja violado o direito ou interesse[114].

O consentimento está ainda sujeito a normas *Ius Congens,* devendo ser dado em conformidade com as normas imperativas do Direito Internacional.

O consentimento em contexto cibernético encontra-se previsto no Manual de Tallinn, na regra 19[115] consagrando que o consentimento de um Estado a outro na persecução de uma operação cibernética levará a que uma conduta que outrora seria contrária a uma obrigação internacional, o não seja. Por exemplo, um Estado pode permitir que outro Estado controle temporariamente as suas infraestruturas cibernéticas, numa situação em que por exemplo o Estado não tenha capacidade para responder a um certo tipo de ciberataque. Desta forma

"É nulo todo o tratado que, no momento da sua conclusão, seja incompatível com uma norma imperativa de direito internacional geral. Para os efeitos da presente Convenção, uma norma imperativa de direito internacional geral é uma norma aceite e reconhecida pela comunidade internacional dos Estados no seu todo como norma cuja derrogação não é permitida e que só pode ser modificada por uma nova norma de direito internacional geral com a mesma natureza. Disponível em http://www.gddc.pt/siii/docs/rar67-2003.pdf

[112] *Vide,* BAPTISTA, Eduardo Correia. Direito Internacional (…) *op.cit*.pp.485.

[113] *Idem,* pp.486

[114] *Ibedim.*

[115] *Vide*, SCHMITT, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation", rule 19.

o Estado que deu o consentimento não poderá mais tarde alegar que a conduta do segundo Estado violou uma obrigação internacional[116].

Claro está que, o consentimento terá de ser válido e livremente dado, ou seja, não poderá ser o resultado de uma coação. Além disso, a operação cibernética em questão não pode exceder o alcance do consentimento do Estado, ou seja, não vai além da ação ou omissão para a qual o consentimento foi concedido.

5. Conflitos Armados e operações cibernéticas

5.1 Conceito de Conflito Armado e a aplicabilidade da Lei dos Conflitos Armados às Operações Cibernéticas

Para poder definir conflito armado podemo-nos socorrer do artigo 2º comum às Convenções de Genebra de 1949, que estipula:

> *"Além das disposições que devem entrar em vigor desde o tempo de paz, a presente Convenção será aplicada em caso de guerra declarada ou de qualquer outro conflito armado que possa surgir entre duas ou mais das Altas Partes contratantes, mesmo se o estado de guerra não tiver sido reconhecido por uma delas.*
> *A Convenção aplicar-se-á igualmente em todos os casos de ocupação total ou parcial do território de uma Alta Parte contratante, mesmo que esta ocupação não encontre qualquer resistência militar.*
> *Se uma das Potências em conflito não for Parte na presente Convenção, as Potências que nela são partes manter-se-ão, no entanto, ligadas pela referida Convenção nas suas relações recíprocas.*
> *Além disso, elas ficarão ligadas por esta Convenção à referida Potência, se esta aceitar e aplicar as suas disposições."*

Assim, de acordo com as disposições da Carta, estamos na presença de um conflito armado internacional quando este se dá entre as "Altas Partes Contratantes", ou seja, os Estados. Desta forma, verificar-se-á um conflito armado internacional quando um ou mais Estados recorram à força armada contra outro Estado, não sendo tomada em conta a intensidade do conflito, ou seja, não é

[116] *Vide*, SCHMITT, Michael N., Tallinn Manual(…) *op.cit* . regra 19.

necessário haver lugar a um ataque armado, pois uma mera agressão será o bastante para que se considere um conflito como um conflito armado internacional.

A existência de um conflito armado internacional não depende de uma declaração formal de guerra, esta apenas está dependente dos acontecimentos em concreto[117].

É possível ler nos Comentários às Convenções de Genebra de 1949 que se houver lugar à intervenção das forças armadas no decorrer da controvérsia entre dois ou mais Estados, estamos perante um conflito armado[118].

Além dos conflitos armados regulares entre Estados, o Protocolo Adicional I amplia a definição de conflito armado englobando os conflitos armados não internacionais. Estes ainda que possam envolver Estados, se no conflito uma das partes for um grupo armado já estaremos na presença de um conflito armado não internacional.

Segundo o artigo 3º comum às Convenções de Genebra de 1949:

> *"No caso de conflito armado que não apresente um carácter internacional e que ocorra no território de uma das Altas Partes Contratantes, cada uma das Partes no conflito será obrigada, pelo menos, a aplicar as seguintes disposições:*
>
> *1) As pessoas que não tomem parte diretamente nas hostilidades, incluindo os membros das forças armadas que tenham deposto as armas e as pessoas que tenham sido postas fora de combate por doença, ferimentos, detenção ou por qualquer outra causa, serão, em todas as circunstâncias, tratadas com humanidade, sem nenhuma distinção de carácter desfavorável baseada na raça, cor, religião ou crença, sexo, nascimento ou fortuna, ou qualquer outro critério análogo. Para este efeito, são e manter-se-ão proibidas, em qualquer ocasião e lugar, relativamente às pessoas acima mencionadas:*
>
> *a) As ofensas contra a vida e a integridade física, especialmente o homicídio sob todas as formas, mutilações, tratamentos cruéis, torturas e suplícios;*
>
> *b) A tomada de reféns;*

[117] Pode haver um conflito armado internacional mesmo que um dos beligerantes não reconheça o governo da parte adversa.

[118] Em conformidade com " Como o Direito Internacional Humanitário define "conflitos armados"? "Comité Internacional da Cruz Vermelha (CICV) Artigo de opinião, março de 2008 disponível em https://www.icrc.org/por/assets/files/other/rev-definicao-de-conflitos-armados.pdf, consultado pela última vez pela última vez a 07 de Agosto de 2017.

> *c) As ofensas à dignidade das pessoas, especialmente os tratamentos humilhantes e degradantes;*
>
> *d) As condenações proferidas e as execuções efetuadas sem prévio julgamento realizado por um tribunal regularmente constituído, que ofereça todas as garantias judiciais reconhecidas como indispensáveis pelos povos civilizados.*
>
> *2) Os feridos e doentes serão recolhidos e tratados. Um organismo humanitário imparcial, como a Comissão da Cruz Vermelha, poderá oferecer os seus serviços às Partes no conflito. Partes no conflito esforçar-se-ão também por pôr em vigor por meio de acordos especiais todas ou parte das restantes disposições da presente Convenção. A aplicação das disposições precedentes não afetará o estatuto jurídico das Partes no conflito."*

Para além deste artigo, também o artigo 1.º do Protocolo Adicional II às Convenções de Genebra, de 12 de agosto de 1949, relativo à Proteção das Vítimas dos Conflitos Armados Não Internacionais, define o que é um conflito não internacional dizendo-nos que se tratam de conflitos em "*território de uma Alta Parte Contratante, entre as suas forças armadas e forças armadas dissidentes ou grupos armados organizados que, sob a chefia de um comando responsável, exerçam sobre uma parte do seu território um controlo tal que lhes permita levar a cabo operações militares contínuas e organizadas e aplicar o presente Protocolo"*[119].

Também o acórdão *Tadic*[120] avança com uma definição de conflito armado não internacional, sendo esta "*sempre que existir violência entre autoridades governamentais e grupos armados organizados, ou entre grupos armados em território de um Estado"*.

Destas definições podemos retirar algumas conclusões, nomeadamente que de forma a caracterizar uma situação como sendo um conflito armado não internacional não basta uma mera agressão, é necessário que sejam observados dois critérios. O primeiro tem em conta a organização dos grupos armados, que devem ter um "comando responsável" para controlar parte do território. O segundo critério tem em conta a capacidade do grupo de "sustentar operações militares prolongadas". Importa aqui fazer uma breve distinção entre grupo armado e mero bando armado, visto que o primeiro terá ocupação de território e terá uma "cadeia

[119] Artigo 1 do Protocolo Adicional às Convenções de Genebra de 12 de Agosto de 1949 relativo à proteção das vítimas dos Conflitos Armados Não Internacionais (Protocolo II).
[120] ICTFY, The Prosecutor v. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995, para.70.

de comando", já um bando armado será apenas uma "associação" de beligerantes sem uma "cadeia de comando" nem controlo de território. Esta distinção é importante, visto que só será visto como um conflito armado não internacional aquele em que estejam presentes grupos armados ou um grupo armado e Estados. No que concerne à intensidade do conflito, não bastará uma mera agressão como acontece nos conflitos armados internacionais, aqui será necessário estarmos na presença de um ataque armado para que o conflito seja caracterizado como conflito armado não internacional.

Quanto à responsabilidade dos atos de grupos armados, ainda que o grupo armado esteja no seu território, o Estado não tem qualquer responsabilidade pelos seus atos. O Estado apenas poderá ser responsabilizado por não adotar medidas para controlar os grupos ou movimentos de insurreição, de acordo com o comentário ao artigo 10º do projeto de artigps de 2001[121]. A conduta dos membros de um grupo ou bando armando trata-se de uma conduta de natureza particular. Quando estamos perante um movimento organizado com existência de facto, é ainda menos plausível que a sua conduta seja atribuível ao Estado. Este critério parte do facto de que um Estado não reunirá as condições para exercer um controlo das atividades do grupo. Assim, é o grupo armado que responde pelos seus atos.

Dadas estas considerações, uma operação cibernética poder-se-á dar no ceio de um conflito ou em si ser caracterizada como um conflito armado internacional ou não internacional, dependendo da origem e do destinatário do ataque.

Quanto à aplicabilidade da lei dos conflitos armados às operações cibernéticas, a regra 20 do Manual de Tallinn[122] diz-nos que "*As operações cibernéticas executadas no contexto de um conflito armado estão sujeitas à lei dos conflitos armados. A lei de conflitos armados aplica-se às operações cibernéticas, como a outras operações no contexto de um conflito armado*." No entanto, claro está que, uma condição prévia à aplicação da lei dos conflitos

[121] Nesse sentido, comentário da comissão no projeto de artigos sobre responsabilidade internacional- parag2.
[122] *Vide*, SCHMITT, Michael N., Tallinn Manual(…) *op.cit* . regra 20.

armados é a existência de um conflito armado. Os peritos no comentário à regra 20 deram o exemplo do caso das operações cibernéticas na Estónia e na Geórgia. No caso da Estónia, ainda que esta tenha sido alvo de várias operações cibernéticas, estas não se configuram como ataques armados. Desta forma, a lei dos conflitos armados não se aplicou. Já no caso da Geórgia, as operações cibernéticas ocorreram durante o conflito armado internacional entre Geórgia e a Rússia, aplicando-se neste caso em concreto a lei dos conflitos armados. Esta problemática será abordada mais detalhadamente no próximo tópico.

5.2 Operações Cibernéticas em/ou como Conflito Armado Internacional

No que diz respeito a conflitos armados internacionais em contexto cibernético, no artigo 22 do Manual de Tallinn pode ler-se que "*Existe um conflito armado internacional sempre que há hostilidades que podem incluir ou limitar-se a operações cibernéticas, ocorrendo entre dois ou mais estados*." [123].

Desta forma, operações cibernéticas poderão ser caracterizadas como conflitos armados internacionais, havendo uma intrusão ou envio de código malicioso. Quanto à caracterização de ataques cibernéticos como conflitos armados internacionais, há que ter em conta se estes podem ou não ser classificados como ataques armados. Como foi dito anteriormente, a classificação como agressão bastará para despoletar um ataque armado internacional.[124]

No que concerne à caracterização de uma operação cibernética como internacional, aqui aplicar-se-á o mesmo critério que num conflito armado internacional em sentido convencional, ou seja, uma operação cibernética terá carácter internacional se se der entre dois ou mais Estados. O problema está em saber se poderá a operação cibernética ser "armada". Ainda que a lei dos conflitos armados não seja clara, a regra 22 do Manual de Tallinn define operação cibernética como conflito armado através de dois requisitos. O primeiro requisito

[123] *Vide*, SCHMITT, Michael N., Tallinn Manual(…) *op.cit*. regra 22.
[124] *Ibedim.*

obriga o confronto a dar-se entre Estados e a segunda condição diz que as hostilidades deverão atingir o nível de um conflito armado[125].

Assim, uma operação atribuível a um Estado que cause dano a uma infraestrutura estatal de outro Estado poderá bastar para caracterizar uma operação cibernética como conflito armado internacional.

5.3 Operações Cibernéticas em/ou como Conflito Armado Não Internacional

No que diz respeito a conflitos armados não internacionais na esfera das operações cibernéticas, este dar-se-á, tal como nos conflitos armados não internacionais convencionais, quando existe um conflito entre Estados e grupos armados ou entre grupos armados entre si. Este dá-se sempre que exista violência armada, podendo esta incluir ou limitar-se a operações cibernéticas.

Um grupo armado em contexto cibernético sê-lo-á se tiver capacidade para realizar ataques cibernéticos e será organizado se tiver sob uma estrutura de comando estabelecida. No que concerne à organização, os grupos não têm que atingir o nível de uma unidade convencional disciplinada. No entanto, as operações cibernéticas e ataques de computadores por particulares não são suficientes. Mesmo os pequenos grupos de *hackers* é improvável que consigam cumprir o requisito de organização. A conclusão é que quanto à organização de grupo, deverá ser feita uma análise caso a caso. As ciberoperações conduzidas por indivíduos isolados também não se qualificam como conflito armado não internacional, visto não serem levadas a cabo por um grupo armado organizado. No que diz respeito a organizações que estejam apenas no plano virtual, ou seja, grupos organizados exclusivamente na internet, é altamente improvável que preencham os requisitos para serem considerados grupos organizados. A opinião no grupo de peritos no Manual de Tallinn, é a de que, a natureza da organização

[125] *Vide*, SCHMITT, Michael N., Tallinn Manual(…) *op.cit*. regra 22.

deve ser tal que admita a aplicação da LOAC. Ora numa organização virtual, o facto de não haver qualquer tipo de contato físico torna difícil caracterizá-lo como grupo armado organizado. Neste âmbito terá de ser feita uma avaliação às circunstâncias de cada situação concreta[126].

Quanto ao requisito de controlo do território disposto no artigo 1º do Protocolo Adicional às Convenções de Genebra[127] sobre proteção das vítimas dos conflitos armados não internacionais, este não se encontra preenchido, visto que o controlo das operações cibernéticas por si só não é suficiente para ser caracterizado como controlo do território. No entanto esse controlo sobre operações cibernéticas poderá significar um certo controlo de território nomeadamente de instalações que admitam máquinas com um certo poder de processamento[128].

5.4 Ciberguerra: definição de meios e métodos de guerra

A ciberguerra está dentro do que será a guerra da informação. De forma simples a Ciberguerra trata da guerra no ciberespaço. Como já vimos, o ciberespaço é uma realidade virtual concebida a partir de elementos físicos, redes de computadores e componentes de *software*.

A ciberguerra caracteriza-se pela utilização de meios cibernéticos com o objetivo de neutralizar ou interferir nos sistemas de outros Estados ou Grupos Armados. Ao contrário da guerra "tradicional", baseada em território e soberania, no mundo virtual é impossível definir os limites da soberania de cada Estado. Outra grande diferença estre estas duas formas de guerra, jaz no tipo de armas utilizadas, sendo que na ciberguerra não há lugar à utilização de armas de fogo

[126] *Vide*, SCHMITT, Michael N., Tallinn Manual(…) *op.cit*. regra 23.
[127] Artigo 1º do Protocolo Adicional às Convenções de Genebra de 12 de Agosto de 1949 Relativo à Proteção das Vítimas dos Conflitos Armados Internacionais.
[128] *Vide*, SCHMITT, Michael N., Tallinn Manual(…) *op.cit*. regra 23.

mas sim de armas cibernéticas, vírus, *botnets, DoS*[129] entre outros, tendo como objetivo atacar sistemas de infraestruturas ou redes.

A par da diferenciação de métodos e meios de guerra, estabelecida no protocolo adicional às convenções de Genebra, também o Manual de Tallinn estabelece uma diferenciação no que diz respeito aos meios e métodos utilizados no decorrer da ciberguerra. A regra 41 estabelece que um meio de ciberguerra trata de *ciberarmas* e sistemas a estas associadas, enquanto métodos se traduzem nas táticas, técnicas e procedimentos, com base nos quais é desenvolvida a ciberguerra. Desta forma o termo "método de guerra" refere-se aos procedimentos utilizados nas operações cibernéticas, sendo estes diferentes dos instrumentos utilizados para conduzir os ataques. Tenha-se como exemplo um ataque de negação de serviço levado a cabo por uma rede de *bots*. Aqui a rede de *bots* será o meio enquanto o *DoS* será o método[130].

A redação do artigo 36º do protocolo adicional às convenções de Genebra deixa intencionalmente antever a evolução de armas[131], nomeadamente no plano cibernético, com a epigrafe "Armas Novas" o artigo diz-nos que:

> *"Durante o estudo, preparação, aquisição ou adoção de uma nova arma, de novos meios ou de um novo método de guerra, a Alta Parte Contratante tem a obrigação de determinar se o seu emprego seria proibido, em algumas ou em todas a circunstancias, pelas disposições do presente Protocolo ou por qualquer outra regra de direito internacional aplicável a essa Alta Parte Contratante."*[132].

O artigo não especifica, no entanto, de que forma as Altas Partes devem determinar se a utilização da arma ou método irá contra as normas de Direito

[129] Ataque que consiste em "consumir" todos só recursos de um Sistema de forma a tornar o esse sistema indisponível para os seus utilizadores.

[130] *Vide*, SCHMITT, Michael N., Tallinn Manual(…) *op.cit* rule 4.

[131] A previsão do conceito de armas novas já existia previamente ao protocolo adicional às Convenções de Génova, o primeiro instrumento internacional a projetar a evolução das armas foi a Declaração de São Petersburgo de 29 de Novembro/11 de Dezembro 1868. Pode ler-se no seu texto: "The Contracting or Acceding Parties reserve to themselves to come hereafter to an understanding whenever a precise proposition shall be drawn up in view of future improvements which science may effect in the armament of troops, in order to maintain the principles which they have established, and to conciliate the necessities of war with the laws of humanity."

[132] Artigo 36º do Protocolo Adicional às Convenções de Genebra de 12 de Agosto de 1949 Relativo à Proteção das Vítimas dos Conflitos Armados Internacionais.

Internacional. Segundo os comentários[133] tecidos pela Comissão Internacional da Cruz Vermelha o artigo 36º tem implícita a obrigação da Alta parte em estabelecer procedimentos internos com o objetivo de esclarecer a legalidade da arma[134].

Desta forma, e tendo em conta a letra do artigo 36º do protocolo adicional, no que concerne à legalidade dos métodos e meios cibernéticos, aplicar-se-á "*para além do protocolo, outras normas de Direito Internacional aplicáveis*" [135].

5.5 Ciberterrorismo

5.5.1 Conceito

Quanto ao conceito de terrorismo, este trata de uma relação triangular entre o ator que inflige um mal a outrem para exercer pressão sobre um terceiro.

A preocupação com o terrorismo do ponto de vista do Direito Internacional não é recente e em nada se prende com o nascimento do ciberterrorismo[136]. A convenção de Haia de 1970, uma convenção que reprime atos que tenham em vista a captura ilícita de aeronaves, estipula que os Estados punam os sequestros com "penas severas" e que extraditem ou instaurem um processo judicial contra os infratores[137]. Também a Convenção Montreal de 1971 para a Repressão de Atos Ilícitos contra a Segurança da Aviação Civil, exige que as Partes punam as infrações e extraditem ou instaurem um processo judicial contra os infratores[138].

[133] *Vide,* in ICRC, "*A Guide to the Legal Review of New Weapons, Means and Methods of Warfare Measures to Implement Article 36 of Additional Protocol I of 1977"* pp. 5.
[134] Em 2003 na 28º Conferência Internacional da Cruz Vermelha voltou a ser abordado o tema reiterando-se que: "to establish mechanisms and procedures to determine whether the use of weapons, whether held in their inventories or being procured or developed, would conform to the obligations binding on them under international humanitarian law." It also encouraged States "to promote, wherever possible, exchange of information and transparency in relation to these mechanisms, procedures and evaluations."
[135]Artigo 36º do Protocolo Adicional I (…) *op.cit*.
[136] *Vide*, GOUVEIA, Jorge Bacelar, "Manual de Direito Internacional Público" pp.813.
[137] Convenção De Haia para a repressão da tomada ilícita de aeronaves de 16 de Dezembro de 1970.
[138] Convenção de Montreal para a repressão de atos ilícitos contra a segurança da aviação civil de 23 de Fevereiro de 1971.

De entre outras Convenções[139] sobre terrorismo é ainda de relevar a Convenção Internacional para a Repressão de Atentados Terroristas à Bomba, que procura negar o asilo a indivíduos procurados por ataques de bombardeamento terrorista, exigindo aos Estados a instauração dum processo judicial ou a extradição para outro Estado que tenha emitido um pedido para tal.

Os acontecimentos de "11 de setembro de 2001" vieram agitar o paradigma do terrorismo, deixando a comunidade internacional em estado de alerta. Refletindo sobre essas preocupações, a Assembleia Geral das Nações Unidas adotou, em 2002, a Convenção Internacional para a eliminação do financiamento do terrorismo[140].

Em 2006 a Assembleia Geral adotou com unanimidade a Estratégia Antiterrorista Global da ONU. Pode ler-se na estratégia: "*Baseada na convicção fundamental de que o terrorismo, em todas as suas formas, é inaceitável e não pode nunca ser justificado, a Estratégia define uma série de medidas específicas para combater o terrorismo em todas suas vertentes, em nível nacional, regional e internacional*" [141].

[139] Convenção referente às Infrações e a certos outros Atos cometidos a bordo de Aeronaves, aprovada em 1963; Convenção de Nova Iorque sobre prevenção e punição dos delitos contra as pessoas internacionalmente protegidas; Nova Iorque 1973; Convenção de Nova Iorque sobre a tomada de reféns, Nova Iorque 1979; Protocolo para a Repressão de Atos Ilícitos de Violência nos Aeroportos ao Serviço da Aviação Civil, Montreal, 1988; Convenção de Roma sobre a repressão de atos ilícitos contra a segurança de navegação marítima, Roma 1988;Convenção de Montreal sobre a repressão dos atos ilícitos contra a segurança da navegação marítima, Montreal 1991; Convenção de Nova Iorque sobre a repressão dos explosivos plásticos, Nova Iorque, 1991; Convenção de Nova Iorque para eliminação de financiamento do terrorismo, NOVA Iorque 1999.

[140] Resolução da Assembleia da República n.º 51/2002, Convenção Internacional para a Eliminação do Financiamento do Terrorismo, adotada em Nova Iorque em 9 de Dezembro de 1999

[141] Podendo ler-se no plano de ação da estratégia: "The member States resolve: To consistently, unequivocally and strongly condemn terrorism in all its forms and manifestations, committed by whomever, wherever and for whatever purposes, as it constitutes one of the most serious threats to international peace and security. 2) To take urgent action to prevent and combat terrorism in all its forms and manifestations and, in particular: to consider becoming parties without delay to the existing international conventions and protocols against terrorism, and implementing them, and to make every effort to reach an agreement on and conclude a comprehensive convention on international terrorism; b. To implement all General Assembly resolutions on measures to eliminate international terrorism, and relevant General Assembly resolutions on the protection of human rights and fundamental freedoms while countering terrorism; c. To implement all Security Council resolutions related to international terrorism and to cooperate fully with the counter-terrorism subsidiary bodies of the Security Council in the fulfilment of their tasks, recognizing that many States continue to require assistance in implementing these resolutions." Disponível em: www.un.org/counterterrorism/ctitf/en/un-global-counter-terrorism-strategy , consultado pela última vez a 20 do Outubro de 2017.

No que concerne ao ciberespaço, e do ponto de vista conceptual, o termo "terror cibernético" foi-nos introduzido por Barry C. Collin do *Institute for Security and Inteligence* da Califórnia, como a junção dos conceitos ciber e de terrorismo. No entanto, essa definição carecia de uma distinção clara de termos como cibercrime, ativismo cibernético (hacktivismo) e ciber-extremismo. Foi apenas na década de 80, altura em que se começou a dar a *revolução tecnológica,* que se começou a debater a ideia do terrorismo feito no ciberespaço[142].

O Terrorismo cibernético, na sua acessão, consiste no terrorismo dirigido a sistemas de redes ou que utiliza os mesmos sistemas com o propósito de perturbar infraestruturas fundamentais que estes controlem. Estes ataques cibernéticos consistem geralmente em intrusões direcionadas a redes de computadores com o objetivo de roubar ou alterar informação ou danificar o sistema. Estes são conseguidos através de código malicioso, conhecido como vírus ou *worms*, que se difundem pela rede, perturbando o seu normal funcionamento ou ataques de *DoS* que "bombardeiam" redes com comunicações falsas para que deixem de funcionar corretamente.

As motivações por detrás de um ataque podem ser as mais variadas: os atacantes vão desde *hackers* empenhados em provar as suas habilidades, a criminosos que roubam números de cartões de crédito, a redes de extorsão, a serviços de inteligência estrangeiros que pretendem roubar segredos militares e económicos, a terroristas ou exércitos estrangeiros com a finalidade de causar danos a outros países[143]. No caso do ciberterrorismo, os ataques têm como objetivo aterrorizar ou causar o medo a um determinado grupo étnico, religioso ou nação.

No comentário à regra 36 do manual de Tallinn com a epígrafe – *" Ataques de Terror - Os ataques cibernéticos ou ameaça, cujo principal objetivo seja espalhar o terror entre a população civil, são proibidos"*, faz-se a distinção entre ciberterrorismo, *cyber-harassment,* ciber-sabotagem e terrorismo cibernético,

[142]*Vide,* COLLIN, Barry C. *"Future of Cyberterrorism: The Physical and Virtual Worlds Converge",* Crime and Justice International, Vol.13, Issue:2,March 1997 ,pp.16.

[143] Em concordância com Centre of Excellence Defence Against Terrorism, "Responses to Cyber Terrorism" ,IOS Press 2008,pp.37

definindo como ciberterrorismo *"... Os ataques cibernéticos, ou a ameaça de tais ataques, com o objetivo de espalhar o terror entre a população civil ...*".[144] Dos comentários podemos ainda retirar que o objetivo do ciberterrorismo deverá ser aterrorizar um grande número de civis e a mais importante elação é a de que não só o ato de ciberterrorismo mas também a mera ameaça é proibida. No comentário 3 à regra 36 são referidos dois exemplos demonstrativos, o primeiro ilustra violação à regra: *"a ameaça de usar um ataque cibernético para desativar um sistema de distribuição de água de uma cidade, para contaminar água potável e causar morte ou doença violará a Regra*" e um segundo exemplifica uma conduta não violadora da regra: "*um tweet falso (mensagem do Twitter) enviado para causar pânico, indicando falsamente que uma doença altamente contagiosa e mortal se está a espalhar rapidamente por toda a população. Visto que um tweet não constitui um ataque nem uma ameaça, não viola esta Regra*."[145].

Numa breve distinção entre ciberterrorismo e hacktivismo podemos verificar que contrariamente ao ciberterrorismo, o hacktivismo não pretende danificar um sistema para causar terror na sociedade, mas sim expressar uma ideia ou opinião. O hacktivismo tal como conhecido hoje remonta a meados da década de 1990. O objetivo deste tipo de manipulação de serviços online[146] é expressar uma ideia. Tal como os ativistas que se manifestam em praça pública, o objetivo dos hacktivistas é manifestarem-se na *Web*.

O grupo *anonymous*[147] criado em 2003, fez desde aí inúmeros ataques cibernéticos, nomeadamente contra os *websites* da igreja de cientologia, contra à qual "luta" desde que esta interpôs uma ação contra o *youtube.* A ação era sobre violações de direitos de autor, visto estar no *youtube* um vídeo que tinha sido

[144] *Vide*, SCHMITT, Tallinn Manual (…) *op.cit*. regra regra 36.

[145] *Ibedim*.

[146] Segundo o Departamento de Defesa dos Nacional é "normalmente entendido como escrever código fonte, ou até mesmo manipular bits, para promover ideologia política - promovendo expressão política, liberdade de expressão, direitos humanos, ou informação ética".

[147] Rede internacional de entidades ativistas e *hacktivistas.* Fundada em 2003 no 4chan (fórum web onde utilizadores publicam anonimamente as suas ideias). Segundo o grupo: "representa um cérebro global anárquico e digitalizado de utilizadores numa comunidade. Conceito de muitos utilizadores da comunidade on-line e off-line".

produzido pela igreja. Os *anonymous* consideraram este ato como sendo um ato de censura e desde aí fizeram várias incursões ao *website* da instituição[148].

Anos mais tarde durante a primavera Árabe, os *anonymous* tiveram várias incursões por *websites* institucionais, nomeadamente na Tunísia onde levaram a cabo ataques de DdoS contra *websites* governamentais e também no Egito contra o *website* do Partido Nacional Democrático.

Em 2015 o grupo *anonymous* Portugal atacou a infraestrutura da Procuradoria Geral da República, divulgando dados pessoais de magistrados e juristas. Interferiram ainda com os *websites* da Polícia Judiciária e do Conselho Superior da Magistratura (CSM) bem como com a aplicação de gestão processual nos Tribunais Judiciais de Portugal, o portal do *Citius*.

5.5.2 Ocorrências de ataques terroristas no ciberespaço

Na esteira da definição acima, serão mencionados alguns exemplos de atos de ciberterrorismo.

O primeiro ataque conhecido por terroristas contra os sistemas de computadores, assim caracterizado por vários departamentos de inteligência, foi em 1998. Uma organização terrorista enviou para a embaixada do Sri Lanka cerca de oitocentos *e-mails* por dia durante duas semanas. Os *e-mails* apenas diziam *"Nós somos os Tigres Negros da Internet e estamos a fazer isto para interromper as vossas comunicações".*[149]*.*

Na Suécia, em Setembro de 1998, na sequência do agendamento de eleições, deu-se um ataque ao *site* de um partido político, onde foram colocadas hiperligações para *sites* de partidos da oposição bem como para *sites* de pornografia[150]. Ainda em 1998 no México, foi atacada a *homepage* de um *website*

[148] *Vide,* HOLT, Thomas J., SCELL, Bernardette," Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications" , IGI Global, 2011 pp.175.
[149] HOLT, Thomas J., SCELL, Bernardette," Corporate Hacking (…)", *op.cit*.,pp.175.
[150] BOGDANOSKI, Mitko, "Cyber Terrorism – Global Security Threat" International Scientific, Security and Peace Journal, disponível em https://pdfs.semanticscholar.org/151f/8f87a85b616d58c57cc22f67ae29 d662c1fa pdf consultado pela última vez a 15 de Setembro de 2017,pp.61-62

do governo mexicano tendo este ataque o propósito de protestar contra atos corruptos do governo[151].

Na Austrália, em Março de 2001, um funcionário descontente com o horário de trabalho, após várias tentativas conseguiu através de meios cibernéticos escoar um milhão de litros de água de esgoto para o rio[152].

Em 2007 aconteceram os ataques a instituições públicas e privadas na Estónia já referenciados.

Em 2013, vários bancos norte americanos foram atacados, dezenas de *websites* de bancos diminuíram o seu desempenho ou até deixaram de funcionar. Técnicos de cibersegurança afirmam que em vez de explorar computadores individuais, os atacantes criaram redes de computadores em *data centers*[153]. Dizem ainda que as habilidades necessárias para realizar ataques dessa envergadura, fazem acreditar que possa ter sido levado a cabo pelo Irão, provavelmente como represálias por sanções económicas e ataques *online* que haviam sido impostas pelos EUA[154].

Um grupo hacktivista autoproclamado "Exército Eletrónico Sírio" em Junho de 2015 fez *defacement*[155] ao *website* do exército dos Estados Unidos da América, publicando mensagens que criticavam a política dos EUA no Médio Oriente.[156]

[151]GANDHI, Robin, Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political, 2011.
[152] *Vide*, ABRAMS, Marshall D.,"*Malicious Control System Cyber - Security Attack Case Study–Maroochy Water Services,Australia",* Annual Computer Security Applications Conference, *2008.* disponível em: https://www.researchgate.net/publication/224223630_Dimensions_of_Cyber-Attacks_Cultural_Social_Economic_and_Political consultado pela última vez a 15 de Setembro de 2017.
[153] Comummente conhecidos como *data centers*, os centros de processamento de dados são locais onde estão concentrados os sistemas computacionais, como um sistema de telecomunicações ou um sistema de armazenamento de dados.
[154] *Vide*, PERLROTH, Nicole , HARDY, Quentin, "Bank Hacking Was the Work of Iranians, Officials Say", The New York Times, disponível em: http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html consultado pela última vez a 16 de Setembro de 2017.
[155] *Defacement* ou deface são termos utilizados denominar os ataques realizados por *defacers* e *script kiddies* para modificar a página de um *web*site na Internet.
[156] *Vide*, TATUM, Sophia, CNN Politics, *"U.S. Army public website compromised*", 9 de Julho de 2015, disponível em: http://edition.cnn.com/2015/06/08/politics/us-army-syrian-electronic-army-hacked/index.html consultado pela última vez a 16 de Setembro de 2017.

6 Responsabilidade internacional dos Estados

6.1 Conceito

A responsabilidade dos Estados pode hodiernamente considerar-se como um princípio geral do Direito Internacional. O Direito da Responsabilidade, na generalidade diz respeito à ocorrência de certa conduta ilícita e às consequências que desta advêm. No entanto, diferentemente do que acontece no Direito Interno dos Estados, a natureza da responsabilidade Internacional não se baseia somente no dlito mas também em violações de tratados e outras violações de um dever jurídico[157].

Quanto à definição de responsabilidade internacional, no caso das reclamações britânicas relativas à zona espanhola de Marrocos, o TPJI afirmou: "*A responsabilidade é o corolário necessário de um direito. Todos os direitos de carácter internacional implicam responsabilidade internacional. Se a obrigação em causa não for cumprida, a responsabilidade acarreta o dever de reparação"* [158].

A responsabilidade por factos ilícitos trata de uma obrigação imposta ao autor de um ato ilícito, de reparar os prejuízos causados a terceiros pela sua prática.

A responsabilidade internacional tem, ao longo dos anos, sofrido diversas alterações. Até há pouco tempo restringia-se apenas aos Estados, hodiernamente conhece-se também a responsabilidade de organizações internacionais, por ações ou omissões cometidas na prossecução dos seus fins. A responsabilidade alargou-se também às organizações internacionais na medida em que deixou de

[157] *Vide*, BROWNLIE, Ian, "Princípios de Direito Internacional Público", pp.459.

[158] No caso dos bens britanicos em Marocos, pode ler-se: "Les Réclamations britanniques présentent un caractère particulier du fait qu'elles concernent des dommages subis dans un pays de protectorat et de capitulations. Toutefois, avant d'examiner si ces deux circonstances modifient les règles du droit international relatives à la responsabilité d l'État, il y a lieu d'envisager le problème à un point de vue général. (…) La responsabilité est le corollaire necessaire du droit. Tous droits d'ordre international ont pour conséquence une responsabilité internationale. La responsabilité entraîne comme conséquence l'obligation d'accorder une réparation au cas où l'obligation n'aurait pas été remplie. Reste à examiner la nature et l'étendue de la réparation." Cfr. Affaire des biens britanniques au Maroc espagnol (Espagne contre Royaume-Uni) 1 de Maio 1925, pp.641, disponível em http://legal.un.org/riaa/cases/vol_II/615-742.pdf acedido a 05 de Outubro de 2017.

ser apenas uma responsabilidade de Estados perante os outros para englobar também a responsabilidade dos Estados perante organizações internacionais.[159]

Anteriormente a responsabilidade assentava apenas na culpa sendo somente necessário que existisse ilicitude na conduta, ao passo que atualmente será necessário que o autor tenha praticado um ato ou omissão ilícita e que desta conduta ilícita emerjam prejuízos para terceiros. Desta forma, para que exista uma obrigação de reparar, terão de estar preenchidos certos pressupostos, sendo estes: a conduta, a ilicitude, a imputabilidade da conduta e um nexo de causalidade entre os dois últimos[160].

6.2 A positivação da Responsabilidade Internacional e o projeto de normas da ILC quanto à responsabilidade dos Estados

A questão da responsabilidade dos Estados e o interesse em positivá-la na lei internacional é desde o início do século XX uma meta a atingir. Desta forma, em 1948, a Liga das Nações estabeleceu a *International Law Commission* que, de entre outros tópicos tinha a responsabilidade de apresentar relatórios e soluções relativos à responsabilidade dos Estados.

[159] *Vide*, MIRANDA, Jorge, Curso de Direito Internacional Público. 3ª Edição – Principia 2006, pp.334.

[160] *Vide*, BRITO, Wladimir "Direito Internacional Público", Coimbra Editora, 2ª edição, Coimbra 2014, pp500-501.
Vide, MIRANDA, Jorge, Curso de Direito (…) .*op.cit.,* pp.331.
Ian Browlie discorda quanto à imputabilidade, afirmado que "a responsabilidade só surge quando o ato ou omissão alvo de reclamação é imputável a um Estado. A imputabilidade pode parecer uma noção supérflua, uma vez que a questão principal, numa dada situação, é a de saber se houve uma violação de um dever; o conteúdo da "imputabilidade" varia de acordo com o dever concreto, com a natureza da violação, e assim por diante. A imputabilidade implica uma ficção onde esta não existe e sugere a ideia de responsabilidade por ato de outrem onde se não pode aplicar" cfr. Brownlie, Ian Direito Internacional Público , pp.460.

Foi apenas em 1996 que a ILC logrou fazer um primeiro Projeto de Artigos sobre Responsabilidade dos Estados por Atos Ilícitos[161], alterando-o em 2001 para a versão que ainda vigora atualmente.

O projeto sobre a responsabilidade dos Estados é um documento de *softlaw*, o que significa que estando as normas de *softlaw* despidas de obrigatoriedade jurídica, os Estados podem ou não vincular-se ao Projeto de Artigos. No estatuto do TIJ, instrumentos de *soflaw* não constam como fontes de Direito Internacional, embora, como já vimos, o TIJ tenha inúmeras vezes feito menção a este projeto nos seus acórdãos. Algumas das vantagens de utilização de instrumentos de *soft law* são exatamente, a flexibilidade que não têm as normas vinculativas do Direito Internacional e o facto de, ao contrário dos tratados, não acarretar problemas quanto à ratificação.

O internacionalmente conhecido como *Draft of Articles on Responsibility of States for Internationally Wrongful Acts* 2001[162] conta com cinquenta e nove artigos e divide-se em quatro partes. A parte I diz respeito ao ato internacionalmente ilícito de um Estado, contendo os princípios gerais, as normas sobre a atribuição de uma conduta ao Estado, normas de violação de uma obrigação internacional, a responsabilidade de um Estado em conexão com um ato de outro Estado e ainda normas sobre a exclusão da ilicitude. A parte II regula o conteúdo da responsabilidade internacional de um Estado e elenca em si, os princípios gerais, as normas sobre a reparação do prejuízo causado, e artigos respeitantes às violações graves de obrigações decorrentes de normas imperativas de Direito internacional Geral. A parte III diz respeito à implementação da responsabilidade internacional de um Estado, e contém normas relativas à invocação dessa responsabilidade e às contramedidas, impondo os seus limites. Por fim, a parte IV elenca em si as Provisões Gerais.

[161] Draft Articles on State Responsibility With Commentaries Thereto Adopted by the International Law Commission on First Reading,1996 disponível em: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_1996.pdf consultado pela ultima vez a 15 de Outubro de 2017.
[162] Draft articles on Responsibility of States (..) *op.cit*.

6.3 O Ato Internacionalmente Ilícito e elementos que o constituem

O Ato internacionalmente ilícito está contemplado na primeira parte do Projeto de Artigos de 2001[163], refletindo em si o Direito Internacional Costumeiro. É um ato atribuído a um sujeito jurídico-internacional que constitui uma violação do Direito Internacional, na medida em que afeta direitos ou interesses de outros sujeitos. Assim, tais violações geram uma responsabilidade internacional por um ato ilícito, que deve desencadear uma reação no sentido de cessar a violação ou indemnização pelos danos causados.

Segundo o artigo 1º do Projeto de Artigos de 2001 *"todo o ato internacionalmente ilícito de um Estado acarreta responsabilidade internacional."* No seu artigo 2º, uma norma que mais uma vez reflete o Direito Internacional Costumeiro, dá-nos dois elementos constitutivos do ato ilícito, dizendo-nos que há *"um ato internacionalmente ilícito do Estado quando a conduta consiste numa ação ou omissão"*[164] que seja atribuível a um Estado pelo Direito Internacional, sendo que esse ato deverá ainda constituir uma violação de uma obrigação internacional desse mesmo Estado.

Existem aqui dois elementos de naturezas distintas, um elemento subjetivo, no que concerne à atribuição, ou seja, à imputação duma conduta ilícita a um Estado e um segundo elemento, o elemento objetivo da própria violação. O TPIJ, no caso *Phosphates du Maroc Arret*[165] refere-se a uma conduta ilícita e imputável a um Estado, depreendendo-se assim que será necessária uma conduta, que essa conduta seja atribuível a um Estado e ainda que seja ilícita. No caso dos reféns americanos em Teerão, o TIJ entende que deve ser determinada a

[163] Draft articles on Responsibility of States (..) *op.cit*

[164] A omissão vista também como conduta ilícita foi referenciada caso de TIJ do canal de Corfu tendo sido Albânia seria responsável não pelo ato mas pela omissão no aviso a outros Estados sobre colocação de minas nas suas aguas territoriais dizendo o tribunal que "Estas graves omissões implicam a responsabilidade internacional da Albânia. O Tribunal chega, pelas explosões que ocorrem (…) e pelos danos e perda de vidas humanas que delas resultam, que a Albânia tem o dever de pagar uma indeminização ao Reino Unido".

[165] *Vide*, TRIBUNAL PERMANENTE DE JUSTIÇA INTERNACIONAL, "Arrêts Ordonnances et Avis Consultatifs, Fascicule no 74 Phosphates Du Maroc, 14 de Julho de 1938, disponível em: http://www.icj-cij.org/files/permanent-court-of-international-justice/serie_AB/AB_74/01_Phosphates _du_Maroc_Arret.pdf, consultado pela ultima vez a 20 de Outubro de 2017, pp.22.

imputabilidade dos atos ao Estado Iraniano e que se deve ainda ter em consideração se o Irão estaria ou não a violar normas a que estivesse sujeito por força de tratados[166].

Na esfera cibernética, a regra 14 do Manual de Tallinn, que prevê a responsabilidade internacional por atos ilícitos cibernéticos, refere que "*um Estado tem responsabilidade internacional por um ato cibernético contrário a uma obrigação internacional que lhe seja atribuível*" [167]. Também no domínio do ciberespaço, um ato internacionalmente ilícito pode consistir em violações das regras que regem o tempo de paz ou as aplicáveis a conflitos armados.

É particularmente relevante aqui, a responsabilidade em que incorre um Estado por não tomar medidas para controlar atividades cibernéticas ilícitas que ocorram no seu território, visto que é comum grupos de hacktivistas levarem a cabo operações cibernéticas de grande escala.[168]

De salientar que o dano físico ou lesão não é uma condição prévia para a caracterização de uma operação cibernética como um ato internacionalmente ilícito sob a lei da responsabilidade do Estado[169].

6.4 A violação de uma obrigação Internacional, a ilicitude.

O ato imputável a um Estado deve ser contrário ao Direito Internacional, no sentido em que viola uma obrigação decorrente deste direito. O artigo 12º do Projeto de artigos de 2001 diz-nos que existe uma violação de uma obrigação internacional quando "*um ato deste Estado não está em conformidade com o que lhe é referido pela obrigação, seja qual for a origem ou natureza desta obrigação*"[170]. Assim, não definindo a natureza da obrigação, da leitura extensiva

[166] *Vide*, TRIBUNAL INTERNACIONAL DE JUSTIÇA, Case concerning United States Diplomatic and Consular staff in Tehran – Disponível em: http://www.icj-cij.org/files/case-related/64/064-19800524-JUD-01-00-EN.pdf, consultado pela ultima vez em 25 de Outubro de 2017.
[167] *Vide*, SCHMITT, Michael N, "*Tallinn Manual(…)"op.cit.* regra 14.
[168] *Idem,* regra 14 comentario 5.
[169] *Vide*, SCHMITT, Michael N, "*Tallinn Manual(…)"op.cit.* regra 14 comentário 8.
[170] Draft articles on Responsibility of States (..) *op.cit*. artigo 12º.

do artigo entende-se que a obrigação pode ter natureza de costume, tratado, princípios gerais e acórdãos do TIJ ou decisões de órgãos de organizações internacionais.

O artigo 13º acrescenta ainda que um ato de um Estado só viola uma obrigação à qual este esteja vinculado no momento em que ocorre o ato. Daqui depreendemos que a obrigação tem de estar em vigor para o Estado no momento em que foi praticado o ato ilícito[171]. É assim relevante saber qual o Direito temporalmente aplicável para atos que perduram no tempo. Segundo o nº 2 do artigo 14º do Projeto de artigos de 2001, "*a violação de uma obrigação internacional por um ato de um Estado que tenha carácter contínuo estende-se por todo o período em que o evento continue e esteja em desacordo com a obrigação internacional*" [172]. O mesmo critério se aplica aos atos compostos, ou seja, atos ou omissões que no seu conjunto são ilícitos. Assim, segundo o nº 2 do artigo 15º, a violação começa com o primeiro ato de ilicitude e estende-se enquanto essas ações ou omissões contrárias à obrigação internacional forem repetidas[173].

6.5 As causas de Exclusão da Ilicitude

Como vimos anteriormente, um ato internacionalmente ilícito é um ato ou omissão atribuído a um sujeito jurídico-internacional que constitui uma violação do Direito Internacional, na medida em que tais violações afetam direitos ou interesses de outros sujeitos. Tais violações geram uma responsabilidade internacional que deve desencadear uma reação no sentido de cessar a violação ou indemnizar pelos danos causados.

Segundo o artigo 1º do projeto de Artigos de 2001 "todo o ato internacionalmente ilícito de um Estado acarreta responsabilidade

[171] Draft articles on Responsibility of States (..) *op.cit*. artigo 13º.
[172] *Idem*, artigo 14º.
[173] *Idem*., artigo 15º.

internacional"[174]. Ainda que preenchidos todos os pressupostos para que se incorra em responsabilidade internacional, existem situações em que a ilicitude da conduta pode ser justificada. Visto que a prática do ato ilícito pressupõe a vontade livre do sujeito, quando esta não está reunida constata-se a ocorrência de uma situação que, não sendo decorrente da vontade do sujeito, gera a existência de uma causa de exclusão da ilicitude[175]. De ressalvar que mesmo havendo exclusão da ilicitude tal não fará com que a obrigação seja extinta. O TIJ no *Case concerning The Gabcikovo-Nagymaros Project(Hungary/ Slovakia*)[176] de 1997, fez menção a causas da exclusão da ilicitude, referindo que não haverá lugar a extinção da obrigação internacional, mas apenas a causas que justifiquem o não cumprimento dessa obrigação.

Segundo o capitulo V, parte I do projeto de artigos, as causas de exclusão da ilicitude são:

- o consentimento (art.º 20º);
- a legítima defesa (art.º 21º);
- as contramedidas ou represálias (art.º 22º, 49º a 54º);
- a força maior (art.º 23º);
- o perigo extremo (art.º 24º);
- o estado de necessidade (art.º 25º).

Também na segunda versão do Manual de Tallinn, na regra 19 estão elencadas estas figuras de exclusão da ilicitude, enquadrando-as no paradigma cibernético.

A figura da legítima defesa e do consentimento foram abordados no capítulo anterior. Desta forma analisaremos agora as demais causas de exclusão da ilicitude.

[174] Draft articles on Responsibility of States (..) *op.cit*. artigo 1º.
[175] *Vide,* ALMEIDA, Francisco António de Macedo Lucas Ferreira: *Direito Internacional Público* –2º Edição, Coimbra Editora, Coimbra, pp 237
[176] *Vide,* Case concerning the Gabcikovo-Nagymaros Project (Hungaryslovakia)m Judgement of 25 September 1997, disponível em http://www.icj-cij.org/docket/files/92/7375.pdf, consultado pela última vez a 17 de Setembro de 2017.

6.5.1 Represálias

Autores do século XX definiram represálias como atos de coação que, não obstante serem contrários ao direito, tinham como objetivo responder a outros atos, também estes contrários ao Direito[177]. O conceito foi posteriormente substituído, passando as represálias a consistirem em atos de coação, que apesar de serem interditos pela ordem jurídica internacional, consistirão numa ressalva, quando praticados por um Estado em resposta a atos ilícitos realizados por outro Estado, com o objetivo último de os cessar[178].

As represálias, também conhecidas por contramedidas, estão previstas como causa da exclusão da ilicitude no artigo 22º, artigo 49º e seguintes do Projeto de Artigos de 2001[179]-[180].

Na prática estamos perante um importante meio de exclusão da ilicitude, visto que o receio dos Estados em sofrerem represálias impele-os muitas vezes a não violar as obrigações internacionais a que estão vinculados.

Esta figura exclui a ilicitude da conduta que viola uma obrigação internacional se tiver havido uma prévia violação dessa ou de outra obrigação por parte de um outro Estado. Como referido, a represália pode recair sobre a mesma norma que foi violada pelo ato contra o qual se reage, chamando-se represália idêntica, ou em inglês, *in kind,* ou sobre outras normas. Em qualquer destes casos é necessário que a entidade que se quer fazer valer desta figura tenha sido previamente lesada por um ato ilícito da entidade destinatária da represália[181].

Segundo o artigo 49º do Projeto de Artigos de 2001, no que concerne aos limites das represálias, um Estado só pode fazer uso desta figura contra outro Estado que seja responsável por um ato internacionalmente ilícito com o objetivo de levá-lo a cumprir com as suas respetivas obrigações. As represálias estão

[177] *Vide,* ALBUQUERQUE, Ruy "As represlias: estudo de história do direito português (secs. xv e xvi)." Faculdade de Direito, Universidade de Lisboa., 1972 p.75-76, apud Martens G.F. – Eprécis du Droit des Gens Moderne de L'Europe, Guillaumin Paris 1858 pp 185-186.
[178] *Vide,* ALBUQUERQUE, Ruy "As represálias(…) pp.76, apud VENEZIA, V. Jean-Claude. – "La notion de represailles en droit international public ", Imprenta: Paris, A. Pedone, 1894, pp.467.
[179] Draft articles on Responsibility of States (..) *op.cit*. artigo 22º.
[180] Draft articles on Responsibility of States (..) *op.cit*. artigo 49º.
[181] *Vide,* BAPTISTA, Eduardo Correia – "Direito Internacional…" op cit. pp.542

limitadas temporalmente pelas obrigações internacionais e deverão ainda permitir que a obrigação possa vir a ser cumprida novamente.

Não é líquido aferir se a gravidade e danos da represália podem ou não ir além do ato que a originou. Acredita-se que as represálias que excedem os danos provocados pelo ato contra o qual reagem possam ser licitas[182]. No entanto, se estas forem claramente desproporcionais, não respeitarão o requisito da proporcionalidade.[183] Nos casos em que os danos possam ser comparáveis em termos quantitativos, represálias que causem mais do dobro dos danos deverão ser consideradas desproporcionais[184].

Quanto ao princípio da necessidade, segundo o nº 2 do artigo 52º do Projeto de artigos de 2001, é possível ao Estado lesado adotar represálias urgentes que sejam necessárias para acautelar os seus direitos[185].

O Estado lesado antes de se socorrer do instituto das represálias deve notificar o Estado violador de tal intenção para que este possa cessar a violação.

[182] No comentário 3 ao artigo 51 do Projeto sobre responsabilidade dos Estados de 2001, os peritos baseiam-se na decisão arbitrária. Assim parece atestar a opinião do Tribunal Internacional de Justiça no caso que envolvia a França e os Estados Unidos da América Air Service Agreement of 27 March 1946 - No caso em apreço, a França considera as represálias dos Estados Unidos não Justificadas, o tribunal responde que "It is generally agreed that all counter-measures must, in the first instance, have some degree of equivalence with the alleged breach; this is a well known rule. In the course of the present proceedings, both Parties have recognised that the rule applies to this case, and they both have invoked it. It has been observed, generally, that judging the "proportionality" of countermeasures is not an easy task and can at best be accomplished by approximation. In the Tribunal's view, it is essential, in a dispute between States, to take into account not only the injuries suffered by the companies concerned but also the importance of the questions of principle arising from the alleged breach. The Tribunal thinks that it will not suffice, in the present case, to compare the losses suffered by Pan Am on account of the suspension of the projected services with the losses which the French companies would have suffered as a result of the counter-measures; it will also be necessary to take into account the importance of the positions of principle which were taken when the French authorities prohibited changes of gauge in third countries. If the importance of the issue is viewed within the framework of the general air transport policy adopted by the United States Government and implemented by the conclusion of a large number of international agreements with countries other than France, the measures taken by the United States do not appear to be clearly disproportionate when compared to those taken by France. Neither Party has provide the Tribunal with evidence that would be sufficient to affirm or reject the existence of proportionality in these terms, and the Tribunal must be satisfied with a very approximative appreciation " para.83.

[183] Desse modo o TIJ no caso Gabcíkovo-Nagymaros pronunciou-se dizendo "The Court considers that Czechoslovakia, by unilaterally assuming control of a shared resource, and thereby depriving Hungary of its right to an equitable and reasonable share of the natural resources of the Danube—with the continuing effects of the diversion of these waters on the ecology of the riparian area of the Szigetköz—failed to respect the proportionality which is required by international law"

[184] *Vide,* BAPTISTA, Eduardo Correia – "Direito Internacional…" op cit. pp.516.

[185] Draft articles on Responsibility of States (..) *op.cit*. artigo 52ºnº2.

Deve ainda constar da notificação as formas de reparação do prejuízo que adveio dessa violação. Tal é justificado pela alínea b do nº 1 do artigo 52º do Projeto de Artigos de 2001, que estabelece que caso o Estado lesado pretenda levar a cabo represálias, deve notificar o outro Estado dessa decisão, acompanhada da exigência de uma promessa de não repetição, propondo ainda meios pacíficos de resolução da situação[186].

Uma vez que as represálias visam exclusivamente levar a que a entidade violadora volte a cumprir com as suas obrigações internacionais, estas devem cessar assim que o Estado deixe de violar a norma em questão, havendo lugar a uma compensação pelos prejuízos causados.

Existem, no entanto, normas cujo incumprimento parece ser insuscetível de ser justificado pela invocação de represálias. É o caso das normas que impõem obrigações *erga omnes,* visto que o facto da obrigação vincular mais do que um sujeito faria com que fossem prejudicados terceiros. O artigo 49º nos seus números 1 e 2 estabelece que as represálias se devem dirigir ao Estado responsável pelo ato ilícito. No entanto, o parágrafo 5 do comentário ao mesmo artigo admite que a represália possa pontualmente afetar terceiros[187]. Desta forma, parece-nos que em algumas situações as represálias possam recair sobre obrigações *erga omnes*. Outro tipo de normas que parece não dar lugar a represálias, são as normas que integram o *ius cogens.* Visto serem normas imperativas e inderrogáveis, a maioria da doutrina tem a opinião de que na presença destas não haverá lugar a represálias, contudo acreditamos que tal não possa ser aferido com tanta liquidez[188].

[186] Draft articles on Responsibility of States (..) *op.cit*. artigo 52º nº1.

[187] Pode ler-se no comentário ao artigo 49º no seu parágrafo 5 “This does not mean that countermeasures may not incidentally affect the position of third States or indeed other third parties. For example, if the injured State suspends transit rights with the responsible State in accordance with this chapter, other parties, including third States, may be affected thereby. If they have no individual rights in the matter they cannot complain. The same is true if, as a consequence of suspension of a trade agreement, trade with the responsible State is affected and one or more companies lose business or even go bankrupt. Such indirect or collateral effects cannot be entirely avoided.”

[188] *Vide,* BAPTISTA, Eduardo Correia – “Direito Internacional…” op cit. pp.521
Acreditamos que assim não o será, visto que por um lado a justificação de tal restrição jaz no facto das normas de *ius congens* imporem normas erga omnes, as normas erga omnes podem ser passiveis de represálias.

Parece-nos que a forma mais eficaz de proibir represálias será restringindo a sua admissibilidade em matérias específicas.

Para além das mencionadas restrições às represálias, são evidentemente ilícitas as represálias que violem a proibição do uso da força.

No que diz respeito às represálias no plano cibernético, a regra 9 do Manual de Tallinn estabelece que "*Um Estado que sofreu uma violação por um ato internacionalmente ilícito poderá recorrer à figura das represálias incluindo represálias cibernéticas contra o Estado Responsável*"[189].

Tal como as represálias em sentido convencional, também as represálias cibernéticas deverão ainda permitir que a obrigação possa vir a ser cumprida novamente. Assim, devem consistir em medidas que tenham efeitos temporários ou reversíveis. No domínio do espaço cibernético, este requisito implica que as ações que visem interrupções permanentes de sistemas de computação não sejam viáveis. Em alguns casos acredita-se haver exceções a esta regra, suponhamos que um *malware* informático alojado num sistema apenas é suscetível de ser interrompido se todo o sistema computacional for também interrompido permanentemente, acredita-se que nesta situação poderá então haver lugar a uma represália com efeitos irreversíveis[190].

6.5.2 O Perigo Extremo (*distress*)

O perigo extremo é uma figura que visa acautelar os interesses de bens individuais e não os interesses do Estado, desta forma, um ato praticado por um

No que concerne ao argumente de que as represálias poderiam servir como forma de derrogar uma norma de *iuris congentis*, através de uma represália e uma contra-represália também não se afigura bastante visto que ainda que o primeiro acto de represália seja licito, se preenchidos os critérios, as contra represálias são ilícitas.

A razão apontada por Eduardo Correia Baptista e com a qual concordamos, é a de que existe uma repulsa quanto a represálias. Nesse sentido Fernando Peres sobre a licitude das represálias afirma que ainda que não sendo contestável o direito a represálias, estas constituem um prática odiosa, reputando ilicita a sua prática extensiva. *Vide,* in Albuquerque, Ruy "As represálias…) p.76, apud Peres Fernando – "In Materiam de Bello", art. I, disp. I, man 3299.

[189] *Vide*, SCHMITT, Michael N, "*Tallinn Manual(…)"op.cit.* regra 9.

[190] *Ibidem*.

sujeito ou sujeitos que tenha em vista salvar a vida ou prevenir riscos sérios para a saúde[191], será justificado através desta causa de exclusão da ilicitude.

O perigo extremo na sua origem visa reagir contra situações de fenómenos da natureza que colocariam em risco um bem pessoal, assim para o acautelar dar-se-ia a necessidade de violar uma obrigação[192]. Neste momento a prática aponta para que o perigo extremo possa também ser aplicado em reação a atos humanos que coloquem em risco a vida ou integridade física de sujeitos.

Segundo o artigo 24º do projeto de artigos de 2001, esta figura de exclusão da ilicitude não se aplicará quando "*a situação de perigo extremo é devida unicamente, ou em combinação com outros fatores, à conduta do Estado que a invoque*" ou ainda se para acautelar esse bem criar um risco igual ou superior[193].

De um ponto de vista cibernético, a figura do perigo extremo está contemplada na regra 19 do Manual de Tallinn. O Manual diz que a ilicitude de uma conduta cibernética contrária a uma obrigação internacional, será excluída perante uma situação de perigo extremo que atente contra a vida[194].

6.5.3 Estado de Necessidade

O estado de necessidade é uma figura em tudo semelhante ao perigo extremo, residindo a distinção no facto de o estado de necessidade ter em vista os interesses do Estado ou organizações internacionais e não a proteção de interesses individuais.

[191] No caso *Rainbow Warrior Case* (Nova Zelândia/França) de 9 de Julho de 1986 o tribunal teve como entendimento que o perigo extremo poderá não ser só invocado para situação de risco de vida, podendo também ser invocado em situações de sério risco para a integridade física. Cfr Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements, concluded on 9 July 1986 , between the two States and which related to the problems arising from the Rainbow Warrior Affair Decision of 30 April 1990 disponível em http://legal.un.org/riaa/cases/vol_XX/215-284.pdf consultado pela última vez a 9 de Outubro de 2017 pp.253-255
between the two States and which related to the problems arising from the Rainbow Warrior Affair
[192] Um exemplo deste tipo de ocorrências será uma embarcação que perante uma tempestade entra sem autorização no espaço marítimo de outro Estado na procura de refúgio.
[193] Draft articles on Responsibility of States (..) *op.cit*. artigo 24º.
[194] *Vide*, SCHMITT, Michael N, "*Tallinn Manual 2.0(…)"opcit.* regra 19.

A par do perigo extremo, o estado de necessidade não visa reagir contra uma situação em que o Estado contra quem é invocado é o responsável pela situação, mas sim contra um evento natural ou uma situação que ainda que ilícita não é da responsabilidade desse Estado[195]. A letra do artigo 25º do Projeto de Artigos de 2001 está escrita na negativa[196], restringindo a invocação desta figura a apenas duas situações, se for *"o único modo para o Estado preservar um interesse essencial contra um perigo grave iminente*"[197] e o ato não poderá ainda afetar "*gravemente um interesse essencial[198] do Estado ou Estados em relação aos quais exista a obrigação, ou da comunidade internacional como um todo.*"[199]

Ainda que preenchidos estes dois pressupostos, o Estado não poderá invocar estado de necessidade se o Estado que o pretende invocar tiver responsabilidade na ocorrência dessa situação[200].

Em nenhum caso o estado de necessidade poderá ser invocado como causa de justificação se a obrigação internacional em questão exclui a possibilidade de invocar a necessidade.

Na regra 26 o Manual de Tallinn apenas estende os pressupostos do Estado de necessidade às operações cibernéticas, dizendo que um Estado poderá invocar o estado de necessidade contra um perigo iminente, salvaguardado um interesse essencial, seja ou não de natureza cibernética. [201]

---

[195] *Vide,* BAPTISTA, Eduardo Correia – "Direito Internacional…" opcit pp.499.

[196] Também o TIJ no caso Gabcikovo-Nagymaros fez um reparo sobre a forma como está escrito o artigo mencionando que "The Court considers ... that the state of necessity is a ground recognized by customary international law for precluding the wrongfulness of an act not in conformity with an international obligation. It observes moreover that such ground for precluding wrongfulness can only be accepted on an exceptional basis. The International Law Commission was of the same opinion when it explained that it had opted for a negative form of words ..."cfr Gabicíkovo-Nagymaros, 1997, pp. 40– 41

[197] Ainda no caso Gabcikovo-Nagymaros o TIJ considerou que o interesse do Estado agressor "must have been threathened by a grave and imminent peril" cfr Gabicíkovo-Nagymaros, 1997, pp. 40– 41.

[198] O Tribunal Internacional de Justiça no caso Concerning The Gabcikovo-Nagymaros(..) considerou que " the act being challaged must have been the only means of safeguarding that interest" acrescentado ainda que conduta" must have been occasioned by an "essential interest" of the State which is the author of the act conflicting with one of its international obligations".

[199] Draft articles on Responsibility of States (..) *op.cit*. artigo 25º.

[200] Nesse sentido O Tribunal Internacional de Justiça no caso Concerning The Gabcikovo-Nagymaros(..) considerou que " the act being challaged must have been the only means of safeguarding that interest" acrescentado ainda que o ato levado a cabo por estado de necessidade não poderá "seriously impair an essential interest.

[201] *Vide*, SCHMITT, Michael N, "*Tallinn Manual 2.0(…)"op.cit*. regra 26.

Tendo em conta que várias estruturas cibernéticas foram consideradas pela comunidade internacional como infraestruturas críticas, consideramos aqui que uma ameaça a estas infraestruturas poderá ser considerada como um interesse essencial do Estado.

6.5.4 Caso Furtuito ou Força maior

Excluem a imputação de uma conduta a um Estado as figuras de força maior e caso furtuito. Quanto à distinção entre os conceitos, o critério aqui aceite será o de que a força maior poder-se-á classificar como um acontecimento que ainda que previsível será fatal, portanto insuperável, enquanto o caso furtuito será um acontecimento quase impossível de ser previsto. Ainda que terminologicamente exista esta distinção, acreditamos não haver razão para que não se exclua a ilicitude de uma conduta constitutiva de caso furtuito ainda que a lei apenas mencione a figura da força maior, aplicando-se também pela mesma ordem de razão o mesmo critério, ou seja, quando a lei apenas mencione caso furtuito e a conduta caiba no escopo de força maior[202].

São indispensáveis à caracterização de caso furtuito dois elementos, um elemento objetivo, no que concerne à inevitabilidade ou impossibilidade em resistir, e um elemento subjetivo respeitante à ausência de culpa[203].

Diz-nos o artigo 23º do Projeto de Artigos de 2001[204] que:

> 1.*" A ilicitude de um ato de um Estado em desacordo com uma obrigação internacional daquele Estado será excluída se o ato se der em razão de força maior, entendida como a ocorrência de uma força irresistível ou de um acontecimento imprevisível, além do controle do*

[202] *Vide*, PIRES, Manuel," Do Caso Fortuito ou de Força Maior" (dissertação do Curso Complementar de Ciências Jurídicas), 1958
No antigo código civil estipulava o artigo 877 que "não poderá o devedor alegar perda ou deterioração ainda que por força maior ou caso furtuito . Atualmente o artigo que tomou o seu lugar, artigo 616, estipula que: "O adquirente de má fé é responsável pelo valor dos bens que tenha alienado, bem como dos que tenham perecido ou se hajam deteriorado por caso fortuito…." Acreditamos aqui que o legislador ao retirar a figura de "força maior" não pretendia exclui-la mas sim deixar subentendida ainda que apenas se mencione a figura do caso furtuito.
[203] *Vide*, FONSECA, Arnoldo Medeiros, Caso Fortuito e Teoria da Imprevisão, 3ª Edição, Edição Revista Forense, 1958 p.147
[204] Draft articles on Responsibility of States (..) *op.cit*. artigo 23º.

Estado, tornando materialmente impossível, nesta circunstância, a realização da obrigação.

2. O parágrafo 1º não se aplica se:
a)a situação de força maior é devida, por si só ou em combinação com outros fatores, à conduta do Estado que a invoca; ou
b)o Estado assumiu o risco daquela situação ocorrida.

Para que um ato jurídico seja imputado a um Estado não basta a atribuição desses atos, é também condição necessária para a existência de um ato a voluntariedade[205]. Desta forma, não existindo vontade não poderão ser imputados a um Estado atos que, ainda que cabendo dentro dos atos imputáveis do capitulo II do Projeto de Artigos de 2001, sejam consequência de eventos involuntários. Ora um ato jurídico contempla em si o elemento da voluntariedade, sendo que tanto a força maior como o caso furtuito, quer seja um evento humano ou provocado pela natureza, são figuras que contemplam a involuntariedade de um acontecimento, pela falta de vontade não estamos sequer perante um ato jurídico e portanto não suscetível de ser imputado.

O artigo 23º do projeto de artigos de 2001 encontra-se inserido nas causas que excluem a ilicitude, no entanto parte da doutrina afirma que, ao não existir um ato jurídico, por falta de vontade, não se poderá excluir a ilicitude desse ato, não existindo desta forma qualquer necessidade de este ser justificado[206].

A força maior foi mencionada no caso de 1949 do Canal de Corfu, afirmando o TIJ que os Estados "*têm a obrigação de não autorizar atos no seu território que possam ser contrários aos direitos de outros Estados*"[207] acreditamos, no entanto, que se for impossível ao Estado controlar movimentos de beligerantes, estes atos não lhe serão imputáveis.

A força maior está também contemplada no Manual de Tallinn como figura de exclusão da ilicitude. A regra invoca os pressupostos acima mencionados, sendo

[205] *Vide,* BAPTISTA, Eduardo Correia – "Direito Internacional…" op cit . pp..452.
[206] *Idem, pp.*453.
[207] The Corfu Channel Case, International Court of Justice, Abril de 1949, disponível em http://www.icj-cij.org/files/case-related/1/001-19490409-JUD-01-00-EN.pdf acedido a 05 de Outubro.

que se reunidos excluirão a ilicitude de uma operação cibernética contrária a uma obrigação internacional.[208]

6.6 A conduta e a sua imputação a um Estado

A conduta, como contemplada no artigo 2º do projeto de artigos de 2001[209], consistirá numa ação ou omissão. Por conseguinte, quanto à imputação desta ação ou omissão dever-se-á analisar dois pontos essenciais: primeiramente saber quais as normas internacionais que regulam a imputação dos atos ou omissões, sendo de seguida necessário entender que atos ou omissões estão em causa e que requisitos devem ser atendidos e considerados relevantes para apurar responsabilidade.

Quanto à imputação, o princípio governante da responsabilidade do Estado, de acordo com o Direito Internacional, tem sido tradicionalmente o de que a conduta de atores privados, tanto entidades quanto indivíduos, não é atribuível ao Estado, a menos que o Estado tenha delegado direta e explicitamente uma parte das suas tarefas e funções a uma entidade privada[210].

A visão atual para a atribuição de atos ainda requer alguma forma de controlo geral pelo Estado sobre atores privados. A lei sobre a responsabilidade do Estado está baseada no conceito de agência, portanto, para determinar se a responsabilidade pode ser atribuída a um Estado, as principais questões são saber se a pessoa atuou como agente de um determinado Estado e quando é que essa ação se qualifica como uma ação desse Estado. Embora a responsabilidade do Estado seja aparente quando o Estado comete certos atos em resultado direto do exercício de suas funções públicas, a responsabilidade indireta também é possível se o Estado tolerar uma determinada ação ou se for incapaz de a

[208] *Vide*, SCHMITT, Michael N, "*Tallinn Manual 2.0(…)"op.cit*. regra 19.
[209] Draft articles on Responsibility of States (..) *op.cit*. artigo 2º.
[210] *Vide*, BAPTISTA, Eduardo Correia – "Direito Internacional…" op cit. pp.451.

prevenir, traduzindo-se em esforços inadequados por parte do Estado para evitar a ação privada[211].

O capítulo II do projeto sobre responsabilidade dos Estados de 2001 estabelece que será atribuível a um Estado a conduta que:

- é realizada por órgãos de um Estado[212];
- é realizada por pessoas ou entidades que exerçam poderes governamentais[213];
- é realizada por órgãos colocados à disposição de um Estado por outro Estado[214];
- é dirigida ou controlada por um Estado[215];
- é realizada por ausência ou defeito nas autoridades oficiais[216];
- é realizada por um movimento insurrecional [217];
- é reconhecida e adotada por um Estado como se fosse a sua conduta[218].

O TIJ considerou uma norma costumeira o enunciado pela ILC no artigo 4º do projeto sobre responsabilidade dos Estados de 2001, segundo o TIJ *"A conduta de um órgão de um Estado deve ser vista como um ato do Estado. Esta regra tem carácter costumeiro e refletia-se no artigo 6º[219] do Projeto de artigos sobre Responsabilidade dos Estados de 1996"[220]*.

Está estabelecido que os indivíduos que constituem órgãos de pessoas coletivas, não são seus representantes, mas antes as materializam. No entanto,

[211] *Vide,* BRITO, Wladimir "Direito Internacional"*op.cit* pp.510.
[212] Draft articles on Responsibility of States (..) *op.cit*. artigo 4º.
[213] Draft articles on Responsibility of States (..) *op.cit*. artigo 5º.
[214] *Idem*, artigo 6º.
[215] *Idem*, artigo 8º.
[216] *Idem*, artigo 9º.
[217] *Idem*, artigo 10º.
[218] *Idem*, artigo 11º.
[219] Assim no artigo 6º do Pojecto sobre a Responsabildiade dos Estados de 1996 "The conduct of an organ of the State shall be considered as an act of that State under international law, whether that organ belongs to the constituent, legislative, executive, judicial or other power, whether its functions are of an international or an internal character, and whether it holds a superior or a subordinate position in the organization of the State" – Draft Articles on State Responsabilitity (…) op cit. artigo 6º.
[220] Vide,TIJ, Reports of Judgments, Advisory Opinions and Orders Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human RigHTS disponivem em: http://www.icj-cij.org/files/case-related/100/100-19990429-ADV-01-00-EN.pdf aconsultado a 18 de Outubro de 2017 pp.29

apenas são da responsabilidade do Estado os atos praticados pelos seus órgãos quando no exercício das suas funções. Por consequência, quando os atos de um indivíduo sejam praticados para prosseguir fins pessoais não haverá lugar a responsabilidade da pessoa coletiva de que seja órgão, salvaguardando o Estado[221]. Todos os atos praticados no exercício de funções estatais são atos da pessoa coletiva independentemente das funções que ocupem. Existindo uma ressalva para forças armadas, sendo que atos praticados pelos seus membros, ainda que a título pessoal, podem ser considerados atos da pessoa coletiva se utilizarem meios fornecidos pelo Estado ou estiverem ao serviço do seu Estado no estrangeiro[222-223].

Além de entidades que tenham estatuto de órgão à luz do seu Direito interno, são ainda órgãos das referidas pessoas coletivas, os "órgãos de facto". Órgãos de facto são pessoas ou indivíduos que ainda que não sejam órgãos de Direito do Estado atuem como tal, ou seja, que praticam atos no exercício dos poderes estatais, vinculando assim o Estado[224].

O projeto sobre responsabilidade dos Estados de 1996 da Comissão de Direito Internacional definia no seu artigo 8º alínea a) que atos de um indivíduo ou indivíduos seriam considerados como atos do Estado se ficasse estabelecido que um individuo ou grupo de pessoas estivesse a atuar em nome do Estado[225-226]. No entanto, a norma foi retirada do projeto sobre responsabilidade dos Estados

[221] *Vide,* BAPTISTA, Eduardo Correia – "Direito Internacional…" op cit pp.461.
[222] *Ibedim.*
Nesse sentido também BRITO, Wladimir "Direito Internacional"*op.cit* pp.507.
[223] Principio estabelecido na sequência do artigo 3 da convenção IV relativa as leis e costumes de guerra de 18 de outubro de 1907 (artigo da convecção e não do regulamento anexo que esta aprovou. "será responsável por todos os atos cometidos por pessoas que façam parte das forças armadas
[224] Como exemplo temos indivíduos que se encontrem inseridos numa cadeia de comando informal, ou governos *de facto,* ou seja, que sejam considerados e atuem como tal.
[225] Draft articles on Responsibility of States (..),1996. *op.cit*. artigo 8º.
[226] Na letra do artigo pode ler-se "The conduct of a person or group of persons shall also be considered as an act of the State under international law if: (a) it is established that such person or group of persons was in fact acting on behalf of that State" op.cit Draft Areticles 1996 (…) pp 32.

de 2001 sendo que no artigo 8º do novo projeto apenas são mencionadas pessoas ou grupos de pessoas sujeitas a instruções direcção ou controlo de um Estado[227].

Uma outra situação é a do artigo 6º, que diz respeito a órgãos que por meio de um acordo entre Estados sejam colocados sob direção jurídica de outro Estado[228]. Há aqui lugar a um controlo destes órgãos por parte de outro Estado e enquanto esse controlo se mantiver passam a ser seus órgãos. Tal "cedência" de órgãos governamentais poder-se-á dar entre Estados, entre Estados e organizações internacionais, em organizações internacionais entre si e até de Estados a favor de movimentos armados[229].

Mencionando novamente o artigo 8º do projeto de artigos de 2001, este diz-nos que a conduta de uma pessoa ou grupo de pessoas é imputável a um Estado, se essa pessoa ou grupo de pessoas agir sob instrução, direção ou controlo desse mesmo Estado[230]. O critério da direção e controlo encontra-se ainda consagrado no artigo 17º do projeto de artigos de 2001 no que concerne à responsabilidade de um Estado que exerça direção e controlo sobre outro Estado, sendo o Estado que controla, tendo conhecimento, responsabilizado pelos atos internacionalmente ilícitos que o Estado controlado cometer. O Estado que exerce o controlo será ainda responsabilizado pelos atos do Estado controlado caso tais atos fossem ilícitos se cometidos por si[231]. Traçando um paralelo entre os dois artigos, ao contrário do que acontece no artigo 17º, no artigo 8º direção e controlo aparecem como alternativa, na letra do artigo "direção ou controlo". Parece ter sido de forma intencional, com o objetivo de aligeirar a imputação de atos de particulares ao Estado[232].

[227] Pode lêr-se no artigo 8º do projeto de 2001 que "The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct." Draft Articles on Responsibility 2001(…) *op.cit* artigo 8º.
[228] Draft articles on Responsibility of States (..) *op.cit*. artigo 6º.
[229] Deste modo a CLI no art. 6º do Projeto sobre a responsabilidade dos Estados de 2001, estabelece que ; "The conduct of an organ placed at the disposal of a State by another State shall be considered an act of the former state under the international law if the organ acting in the exercise of elements of the governmental authority of the state at whose disposal it's placed. Ora colocar á disposição significa sujeitar à completa direção do outro Estado os efetivos (órgãos)
[230] Draft articles on Responsibility of States (..) *op.cit*. artigo 8º.
[231] *Idem*, artigo 17º.
[232] *Vide,* BAPTISTA, Eduardo Correira " Direito Internacional(…)", *op.cit*., pp.465.

Analisaremos em seguida a forma de 'controlo' necessária para imputar os atos ao Estado. Poderão aqui ser tomados em consideração alguns critérios aplicados, o 'controlo' poderá vestir a forma de instruções específicas ou controlo efetivo e excecionalmente um controlo genérico[233] da pessoa ou grupo. Estes critérios foram acolhidos pela jurisprudência a pensar em grupos armados[234]. No que concerne ao critério do controlo efetivo, como mencionado, a uma entidade devem-lhe ser imputados atos de terceiros quando estes atuem de facto como seus órgãos. Deste modo, uma situação em que haja cadeia de comando efetiva, levará à responsabilização da entidade pelos atos praticados por terceiros. Existindo essa efetiva cadeia de comando os terceiros passam a ser órgãos de facto, responsabilizando os superiores integrados na sua estrutura de poder formal, ainda que as suas ordens tenham sido desobedecidas, ou até que não tivessem qualquer conhecimento dos atos praticados[235].

No caso sobre as atividades militares e paramilitares no Nicarágua, é considerado o teste ao regime do controlo efetivo e controlo genérico. O tribunal

[233] Considerar o controlo genérico uma forma de imputar uma conduta a um Estado pode acarretar consequências graves, visto que, significara que o Estado vítima pode considerar, que, acontecendo uma operação de um grupo armado no seu território , estão reunidos os pressupostos de um ataque armado por parte do Estado ao qual são imputados os atos, como vimos anteriormente ataque armado legitimará uma recção de legítima defesa, o que pode levar a um conflito armado internacional.

[234] O TIJ no caso Concerning United States Dilplomate and Consular Staff in Thehran conclui que ainda que não fosse possivel determinar que os mlitantes aquando da conduta tivessem algum *status* official de agentes ou órgãos do Estado Iraniano a sua conduta "migth be considered as itself directly imputable to Iranian State only if were established that, in fact, on the occasion in question the militants acted on behalf of the State, having been charged by some competent organ of Iranian State to carry put a specific operation " – ICJ reports of judgments, advisory opninion and orders, Case concerning United States Diplomatic and Consular staff in Teheran – Disponível em: http://www.icj-cij.org/files/case-related/64/064-19800524-JUD-01-00-EN.pdf, , consultado pela última em 25 de Outubro de 2017.

No que diz respeito ao Segundo critério no caso das activities militares e paramilitares no Nicaragua o TIJ considerou que: United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the contras, the selection of its military or paramilitary targets, and the planning of the whole of its operation, is still insufficient in itself [...] for the purpose of attributing to the United States the acts committed by the contras in the course of their military or paramilitary operations in Nicaragua. [...] [What has to be proven is that] that State had effective control of the military or paramilitary operation in the course of which the alleged violations were committed. –International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, I.C.J. Reports 1986, para. 115. Disponível em: http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN., consultado pela última vez pela última vez a 15 de Outubro de 2017.

[235] *Vide,* BAPTISTA, Eduardo Correia "Direito Internacional…" *op.cit*. pp.469.

fez uma distinção clara entre dois tipos de grupos, primeiramente os que não estão juridicamente vinculados a um Estado mas que podem atuar em nome deste e outros que, não obstante poderem ser financiados por um Estado, mantêm uma certa independência. O TIJ entendeu que os *CONTRAS*, grupo financiado pelos Estados Unidos da América que lutava a favor da ex-ditadura, ainda que sendo financiado, teria alguma independência desse Estado. Desta forma, não havendo um controlo efetivo dos Estados Unidos da América sobre os *CONTRAS* e não havendo instruções em relação a operações específicas, o TIJ não imputou responsabilidade aos EUA pela conduta do grupo armado[236], entendendo assim que apenas um controlo efetivo poderia responsabilizar um Estado. Assim, ainda que um órgão atue em abuso das suas competências ou de forma contrária às ordens do Estado, tal não é relevante para efeitos de imputabilidade dos seus atos ao Estado.

No caso do pessoal diplomático e consular dos Estados Unidos, o TIJ ainda que não dispondo de elementos suficientes e determinantes para imputar ao Estado Iraniano o comportamento efetivo dos militantes, tal não se traduziu na inimputabilidade desses atos ao Irão. O TIJ considerou que o Irão deveria ter adotado as medidas necessárias para proteger o pessoal diplomático e consular

[236] No que diz respeito ao segundo critério no caso das activities militares e paramitares no Nicaragua o TIJ considerou que: United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the contras, the selection of its military or paramilitary targets, and the planning of the whole of its operation, is still insufficient in itself [...] for the purpose of attributing to the United States the acts committed by the contras in the course of their military or paramilitary operations in Nicaragua. (...) [What has to be proven is that] that State had effective control of the military or paramilitary operation in the course of which the alleged violations were committed. –International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, I.C.J. Reports 1986, para. 115. Disponível em: http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN., consultado pela última vez pela última vez a 15 de Outubro de 2017
Existe uma corrente contraria que se baseia na decisão do Tribunal Penal para a Ex-Juguslavia no caso Tádic, sendo que o Tribunal entendeu que: "The control required by international law may be deemed to exist whem a State has a role in organising, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group [...] regardless of any specific instructions by the controlling State concerning the commission of each of those acts." No entando entendemos que este teste poderá ter sido feito apenas com o objetivo de justificar a caracterização dos crimes como internacionais e a competência do próprio tribunal.

dos Estados Unidos da América, tendo visivelmente falhado no seu dever essencial de prevenção e repressão[237].

O critério do controlo efetivo será aplicado em situações que tratem de imputar atos de uma entidade a outra, sendo estas entidades distintas. Tal critério aplicar-se-á a entidades formalmente independentes como Estados, ou entre estes e organizações internacionais, bem como entre estas e paralelas, como Associações de Estados. O mesmo critério será ainda aplicado a governos "fantoche", situação em que existe um controlo efetivo da entidade ocupante, ou em caso de coerção, sendo que todos os atos praticados pelos órgãos do Estado ocupado, estando este sob controlo de facto, serão imputados à entidade ocupante[238].

No critério das instruções específicas, ainda que tal como no controlo efetivo, a pessoa ou grupo atou sob instrução do Estado[239], não há aqui uma direção ou controlo efetivo, ou seja, ainda que a entidade seja instruída a atuar de uma certa forma, esta não se encontra forçosamente obrigada a executá-la ou a executá-la nos moldes pretendidos. Por conseguinte, há aqui que perceber se o resultado dessa instrução foi o pretendido pelo Estado e, não sendo, a imputação poder-se-á dar na medida do excesso da conduta, sob forma de cumplicidade ou negligência[240].

Segundo o critério do artigo 10º do projeto de artigos de 2001[241] a um Estado ser-lhe-á imputada a conduta ilícita causada por um grupo de insurreição que seja vitorioso e se torne governo. No entanto, caso o movimento de insurgentes tenha fracassado, os seus atos não serão imputáveis ao Estado, sendo responsável apenas pelos atos que os seus agentes possam ter tomado durante o conflito[242]. No entanto, caso o grupo de insurreição fracassado tiver de alguma forma

[237] Case concerning United States Diplomatic and Consular (..) *op.cit*.para 28 disponível em : http://www.icj-cij.org/files/case-related/64/064-19800524-JUD-01-00-EN.pdf , consultado pela última vez de 10 de Outubro de 2017

[238] *Vide,* BAPTISTA, Eduardo Correia "Direito Internacional…" *op.cit*. pp.469.

[239] Exemplo de Estados vassalos, protegidos ou satélites.

[240] Nesta sentida Comissão de Direito Internacional, comentário ao artigo 8 do projeto 2001 pp. 108-109.

[241] Draft articles on Responsibility of States (..) *op.cit*. artigo 10º.

[242] *Vide,* BRITO, Wladimir "Direito Internacional"*op.cit* pp.510.

realizado investimentos que tenham gerado benefícios para o Estado, o Estado deverá responder pelas dívidas que o grupo possa ter contraído nesse investimento[243].

Por último, existe ainda imputabilidade quando há uma assunção por parte do Estado dos atos de indivíduos ou grupos, ou seja, segundo o artigo 11º do projeto de artigos de 2001, "*na medida em que o Estado reconheça e adote a conduta em questão como sua própria*" [244], ou seja, o que acontece é que uma conduta que inicialmente não é imputável a um Estado é-lhe posteriormente atribuída visto que o Estado a aceita como sua[245].

No que diz respeito à responsabilidade de um Estado em conexão com um ato de outro Estado, esta está contemplada no capítulo V do projeto de artigos sobre a responsabilidade dos Estados de 2001. Um Estado será responsabilizado se tiver auxiliado outro Estado na prática de um ato contrário a uma obrigação internacional segundo o artigo 16º do Projeto de Artigos de 2001[246] se:

> *"Auxílio ou assistência na prática de um ato internacionalmente ilícito-*
> *Um Estado que auxilia ou assiste outro Estado a cometer um ato internacionalmente ilícito é internacionalmente responsável por prestar este auxílio ou assistência se:*
> *a)aquele Estado assim o faz conhecendo as circunstâncias do ato internacionalmente ilícito; e*
> *b)o ato fosse internacionalmente ilícito se cometido por aquele Estado."*

Como supramencionado, a um Estado é-lhe imputado um ato quando estejam reunidos critérios de direção e controlo. Assim estipula o artigo 17º do Projeto de Responsabilidade de 2001[247]:

> ***"****Um Estado que dirige e controla outro Estado no cometimento de um ato internacionalmente ilícito é responsável internacionalmente por aquele ato se:*
> *a)aquele Estado assim o faz com o conhecimento das circunstâncias do ato internacionalmente ilícito; e*
> *b)o ato fosse internacionalmente ilícito se cometido pelo Estado que dirige e controla."*

[243] *Vide,* BAPTISTA, Eduardo Correia "Direito Internacional…" *op.cit*. pp.475.
[244] Draft articles on Responsibility of States (..) *op.cit*. artigo 11º.
[245] *Vide,* BRITO, Wladimir "Direito Internacional"*op.cit* pp.511.
[246] Draft articles on Responsibility of States (..) *op.cit*. artigo 16º.
[247] *Idem,* artigo 17º.

Por último um Estado terá ainda responsabilidade se coagir outro Estado à prática de um ato ilícito, ora diz o artigo 18º do Projeto de Artigos de 2001[248] que:

> *Um Estado que coage outro Estado a cometer um ato é internacionalmente responsável se:*
> *a) em não havendo coação, tal ato constituísse um ato internacionalmente ilícito do Estado coagido; e*
> *b)o Estado que coage o faz conhecendo as circunstâncias do ato.*

6.7 Responsabilidade dos Estados em Contexto Cibernético

Segundo o Manual de Tallinn na sua regra 6, um Estado entra em responsabilidade internacional "*quando uma operação cibernética contrária ao Direito Internacional lhe é imputável"*[249], ou seja, tal como em contexto não cibernético, um Estado incorre em responsabilidade quando uma conduta que lhe seja atribuível viola uma obrigação internacional. Esta regra baseia-se no direito internacional consuetudinário da responsabilidade do Estado, que tal como vimos anteriormente, é amplamente refletido nos artigos da comissão internacional sobre a responsabilidade dos Estados de 2001.

Tal como em contexto convencional, também em contexto cibernético um ato internacionalmente ilícito consiste num ato ou omissão que viole o Direito Internacional. Os Estados não incorrem em responsabilidade internacional se praticarem atos que sejam permitidos ou não regulamentados pelo Direito Internacional, assim a título de exemplo um Estado que pratique atos de ciberespionagem não incorrerá em responsabilidade internacional. Segundo o grupo de peritos, o dano não é um requisito para que uma operação cibernética seja considerada internacionalmente ilícita, contudo, se a regra em questão incluir

[248] [248] Draft articles on Responsibility of States (..) *op.cit*., artigo 18º.
[249] *Vide*, SCHMITT, Michael N, "*Tallinn Manual(…)"op.cit*. regra 6.

danos como elemento essencial tal dever-se-a verificar para que estejamos na presença de um ato internacionalmente ilícito[250].

O ato internacionalmente ilícito na forma de operação cibernética deve ainda ser atribuível a um Estado. Todos os atos ou omissões dos órgãos de um Estado são, como já vimos, imputáveis a um Estado, quer órgãos de direito quer órgãos de facto. O grupo de peritos no Manual de Tallinn faz menção no comentário à regra 6, que para efeitos da lei da responsabilidade dos Estados, pessoas ou entidades que, embora não sejam órgãos desse Estado, são especialmente habilitadas pela lei interna para exercer a *"autoridade governamental"*, são equiparadas aos órgãos do Estado[251]. No entanto, só é imputável ao Estado a conduta dessas entidades quando estejam no exercício de funções. Assim, um Estado pode ter legislação que autorize as equipas de resposta de emergência informática[252] a prestar serviços de defesa de redes, sendo-lhe imputados os atos dessa entidade, porquanto não serão imputados atos a um Estado quando a entidade privada esteja a realizar serviços de segurança de informação para empresas privadas.

Como já vimos anteriormente, segundo o artigo 8º do projeto de artigos de 2001 *"a conduta de uma pessoa ou grupo de pessoas deve ser considerada como sendo um ato de um Estado se a pessoa ou grupo de pessoas estiver de facto a agir de acordo com as instruções ou sob a direção ou controlo desse Estado".*[253] Esta norma é particularmente relevante no contexto cibernético, visto que ao contrário do que acontece em sentido convencional, não existem aqui *forças armadas cibernéticas*.

Como analisámos anteriormente, aqui também há lugar aos testes de controlo genérico, controlo efetivo e instruções específicas. No que concerne ao controlo efetivo, acima já analisado, é importante distingui-lo de iniciativas de

[250] *Vide*, SCHMITT, Michael N, "*Tallinn Manual(…)"op.cit.* comentário à regra 6.
[251] Exemplos incluem uma corporação privada que foi processada pela autoridade pelo governo para realizar operações de rede de computadores ofensivas contra outro Estado, bem como uma entidade privada habilitada a recolher informações sobre CiberInteligence
[252] Trata-se de uma entidade de suporto técnico, responsável por resolver incidentes relacionados à segurança em sistemas computacionais, podendo esta entidade ter cariz público ou privado
[253] Draft articles on Responsibility of States (..) *op.cit*. artigo 8º.

cidadãos privados. Hacktivistas levam a cabo inúmeras operações cibernéticas que não podem ser imputáveis a um Estado. Para tal seria necessário que o Estado tivesse emitido instruções específicas ou dirigido ou controlado uma determinada operação. Tal como em contexto convencional, também no plano cibernético, o apoio em meios de ataque cibernético para uso rebelde não será suficiente para provar controlo do grupo. No entanto, o fornecimento de informação específica de ciber-vulnerabilidades será suficiente para despoletar responsabilidade internacional[254].

Dado que uma operação cibernética é relativamente fácil de levar a cabo através de um computador ligado à rede, tal faz com que esta possa ser efetuada em qualquer lugar. Assim, importa clarificar que o local onde se dá uma operação cibernética não afetará a imputação de um ato a um Estado. O grupo de peritos no Manual de Tallinn dá o exemplo de uma situação na qual um grupo no Estado A através de uma *botnet* assume o controlo de dispositivos localizados no Estado B. Sendo que o objetivo do grupo será levar a cabo um ataque de *DoS* nos dispositivos do Estado C e que o grupo tinha atuado com base em instruções recebidas do Estado D. Assim, aqui a conduta será imputável pelo critério das instruções específicas ao Estado D[255].

No que concerne ao controlo genérico em operações cibernéticas, a opinião será a mesma que em contexto convencional acima mencionada, com enfâse para o carácter problemático da identificação dos atores envolvidos nas atividades. É importante não aligeirar o critério da imputação de uma conduta ilícita a um Estado, tal é especialmente relevante para efeitos de legítima defesa.[256]

Quanto ao facto da operação cibernética ter origem ou "parecer" ter origem em infraestruturas Estatais, podemos distinguir duas situações. Primeiramente pode ter sido conduzida numa infraestrutura governamental. No entanto, o facto de uma operação cibernética ter sido levada a cabo numa infraestrutura governamental não é suficiente para que esse ato seja imputável ao Estado, mas

[254] *Vide, SCHMITT, Michael N, "Tallinn Manual(…)"op.cit. regra* 8
[255] *Ibedim.*
[256] *Vide,* ROSCINI, Marco "Cyber Operations and the Use of Force(…)*" op.cit.pp137-139.*

é uma indicação de que o Estado em questão está associado à operação. Do ponto de vista de operações conduzidas no ciberespaço, comparativamente às operações não cibernéticas, a imputação dos atos ao Estado é bem mais complexa e deverá ser feita caso a caso[257]. A regra 7 do Manual de Tallinn diz-nos que o facto de a operação ter decorrido em infraestruturas governamentais poderá apenas ser uma indicação do envolvimento do Estado, mas não será por si só suficiente para imputar a conduta ilícita ao Estado. Sendo que no limite o Estado pode ter responsabilização sob forma de negligência.[258] Uma segunda situação trata das operações que "parecem" ter sido conduzidas a partir de infraestruturas de um Estado, ou seja, situações em que operações cibernéticas são roteadas num Estado terceiro. Tal acontece quando um ataque cibernético levado a cabo por um Estado é encaminhado através de infraestruturas de um outro Estado[259]. Em tal situação, este último não pode ser presumido como associado à operação cibernética. Tal ocorre porque as características do ciberespaço são tais que a mera passagem de dados através da infraestrutura localizada num Estado não pressupõe qualquer envolvimento desse Estado na operação cibernética associada.

No limite, tal como na primeira situação, o Estado poderá ser responsabilizado por não tomar medidas razoáveis para evitar o trânsito do tráfego de informação associado à operação cibernética[260].

---

[257] *Vide*, SCHMITT, "Manual de Tallinn (…)"*op.cit*. regra 7.

[258] *Ibedim.*

Um claro exemplo de um situação deste tipo será o de uma *Botnet* de um Estado ter os seus *Bots* numa infraestrutura cibernética de um outro Estado. Ora um *bot* ao ter o seu comando e controlo no primeiro Estado agira como um robot desse Estado, efetuando as operações que lhes forem dadas a processar.

Um dos ataques mais comuns de uma *botnet* é ataque de *Denial of Service*, ou seja, utilizar o poder de processamento de *botnets* para atacar o servidor de um site através de milhões solicitações enviadas ao mesmo tempo, essencialmente sobrecarregando o servidor com muito tráfego. Em 2007 na Estónia foram levados a cabo uma série de ataques cibernéticos que 'inundaram' sites de organizações estonianas, incluindo o parlamento, bancos, ministérios, jornais e estações de rádio. A maioria dos ataques foram ataque de *Denial of Service* e *Distributed Denial of Service*.

[259] *Vide*, SCHMITT, Michael N, "*Tallinn Manual(…)"op.cit.* regra 8.

[260] *Ibedim.*

7.Conclusão

Hodiernamente a digitalização dos serviços nos mais diversos setores é uma realidade. A demarcada evolução gerou um enorme impacto na sociedade e uma consequente alteração drástica de diversas formas de prosseguir atividades de índole criminosa. Desta forma, com o presente estudo visou-se fazer uma análise do impacto que a revolução tecnológica teve sobre o conceito de guerra. Outrora vista de um prisma maioritariamente cinético, o conceito de guerra encontra no século XXI um novo paradigma, a guerra à distância através de programas, vírus, *warms, bots, DDoS* e outras infindáveis formas de explorar as vulnerabilidades do ciberespaço. Entramos na nova era da guerra, a era da ciberguerra.

Aqui chegados, importa agora responder a algumas questões, nomeadamente no que concerne ao acompanhamento do Direito Internacional Público e do Direito Humanitário deste novo paradigma de guerra. Questões como saber se um ataque cibernético poderá ou não ser considerado um ataque armado ou gerar uma violação ao princípio da proibição do uso da força, legitimando assim a legítima defesa, foram aqui analisadas. De forma a responder a estas questões foi feito um breve enquadramento histórico, com vista a clarificar alguns conceitos tanto da esfera cibernética como da evolução dos conceitos de guerra e da lei e costumes internacionais. Foram ainda estudados conceitos preliminares necessários à análise da temática, nomeadamente compreender o que é o ciberespaço e o que são infraestruturas críticas.

No sentido de responder à questão de saber se uma operação cibernética pode ser vista como uma violação ao princípio da proibição do uso da força, foram vistos conceitos relativos a esta proibição, nomeadamente a sua definição, fontes jurídicas e exceções a este princípio, sendo traçado um paralelo entre o conceito tradicional de força e o novo paradigma de força não cinética. Foram ainda revistos conceitos como agressão e ataque armado à luz das operações cibernéticas, de forma a poder ou não colocá-las dentro destas categorias. Em função desta compreensão prévia foi-nos possível concluir que uma operação cibernética poderá, em função de certos critérios, ser vista como uma violação da

proibição do uso da força, cabendo ainda no conceito de ataque armado e desta forma dar lugar ao uso da legítima defesa.

De seguida foi apresentada uma análise da tipologia de conflitos armados classificando-os e descrevendo o regime jurídico associado a cada um deles. Foi possível classificar os conflitos armados em dois tipos: conflitos armados internacionais e conflitos armados não internacionais.

Ulteriormente foi realizada uma análise do conceito de responsabilidade internacional dos Estados por factos ilícitos, bem como as figuras de exclusão da ilicitude. Primeiramente em contexto convencional e depois em contexto cibernético.

Para obter as necessárias conclusões face à investigação realizada, fizemos a análise de convenções internacionais aplicáveis e os costumes internacionais pertinentes, a construção jurisprudencial existente e os estudos doutrinários relevantes com especial destaque para o Projeto de Artigos sobre a Responsabilidade dos Estados de 2001 e o Manual de Tallinn sobre o Direito Internacional aplicável à Guerra Cibernética.

A investigação permitiu concluir que o Direito Internacional não estabelece normas específicas aplicadas às operações cibernéticas pelo que existe uma necessidade de recorrer ao Direito Comparado. Esta investigação revelou que no que concerne ao regime de controlo sobre uma entidade organizada este é muito mais difícil de aferir a nível cibernético comparativamente com os grupos armados convencionais.

A constante atualização e mutação desta nova realidade de guerra obrigará o Direito Internacional a um constante acompanhamento, acreditamos ser indispensável a formulação de uma *CiberLex* capaz de acompanhar e prever a evolução e sofisticação destes novos atores do ciberespaço.

8. Bibliografia

- ALBUQUERQUE, Ruy “As represálias: estudo de história do direito português (secs. XV e XVI).” Faculdade de Direito, Universidade de Lisboa., 1972.

- ALMEIDA, Francisco António de Macedo Lucas Ferreira, “Direito Internacional Público”–2º Edição, Coimbra Editora, Coimbra, 2003.

- AKEHURST, MICHAEL, “Introdução ao Direito Internacional”, Almedina Coimbra,1985.

- ASSEMBLEIA DA REPUBLICA, Resolução da Assembleia da República n.º 51/2002.

- N.d., BÍBLIA SAGRADA - Sociedade Bíblicas Unidas, 1992.

- BAPTISTA, Eduardo Correira, “O Poder Público Bélico em Direito Internacional: O Uso da Força Pelas Nações Unidas em Especial”, Dissertação de Doutoramento em Ciências Jurídico-políticas na Faculdade de Direito da Universidade de Lisboa, Almedina, 2003.

- _____.“Direito Internacional Público, Volume II - Sujeitos e Responsabilidade”, Almedina 2004.

- BARBEYRAC ,Jean , “Natural law and enlightenment classics The Rights of War and Peace book of Hugo Grotius Edited and with an Introduction by Richard Tuck” , Preliminary Discourse, XIII Hugo Grocio,Liberty Fund Indianopolis, 2005.

- BOGDANOSKI, Mitko, “Cyber Terrorism – Global Security Threat” International Scientific, Security and Peace Journal, disponivel em https://pdfs.semanticscholar.org/151f/8f87a85b6 16d58c57cc22f67ae29 d662c1fa pdf consultado pela ultima vez a 15 de Setembro de 2017.

- BRITO, Wladimir, “Direito Internacional Público”, Coimbra Editora, 2ª edição, Coimbra 2014.

- BROWNLIE, Ian M.A., D.PHIL.: *The Use of Force in Self-Defense*- Lecturer in Law in the University of Nottingham, Reino Unido, 1961.

- N.d.,Código de Manu (200 A.C. e 200 D.C.), disponível em file:///C:/Users/Userpl022pc01.CYBER/Downloads/CODIGo_%20MANU.pdf consultado pela ultima vez a 10 de Fevereiro de 2017.

- CENTRO DE INVESTIGAÇÃO JURIDICA DO CIBERESPAÇO, Revista Científica Sobre CyberLaw do Centro de Investigação Jurídica do Ciberespaço – CIJIC – Da Faculdade de Direito da Universidade de Lisboa, Edição N.º III-Fevereiro de 2017- disponível em: http://www.cijic.org/publicacao/ , consultado pela última vez a 11 de Novembro de 2017.

- COLLIN, Barry C,. *“Future of Cyberterrorism: The Physical and Virtual Worlds Converge”,* Crime and Justice International, Vol.13, Issue:2,March 1997 .

- CENTRE OF EXCELLENCE OF DEFENCE AGAINST TERRORISM, “Responses to Cyber Terrorism” ,IOS Press 2008.

- CENTRO DE INVESTIGAÇÃO JURIDICA DO– CIJIC - Revista Científica Sobre CyberLaw - Da Faculdade de Direito da Universidade de Lisboa, Edição N.ºIII -Fevereiro de 2017- disponiel em: http://www.cijic.org/publicacao/ consultado pela úlrima vez a 11 de Novembro de 2017.

- COMITE INTERNACIONAL DA CRUZ VERMELHA, " Como o Direito Internacional Humanitário define conflitos armados?" Artigo de opinião, março de 2008 disponível em https://www.icrc.org/por/assets/files/other/rev-definicao-de-conflitos-armados.pdf, consultado pela última vez pela última vez a 07 de Agosto de 2017.

- _____. "A Guide to the Legal Review of New Weapons, Means and Methods of Warfare Measures to Implement Article 36 of Additional Protocol of 1977" - Geneva, January 2006. disponivel em: https://www.icrc.org/eng/assets/files/other/icrc_002_0902.pdf consultado pela ultima vez em 25 Setembro de 2017.

- _____. "violência e o Uso da força" , Agosto 2009 pp 26. Disponível em: https://www.icrc.org/por/assets/files/other/icrc_007_0943.pdf consultado pela ultima vez em 15 de Agosto de 2017.

- EUA WHITE HOUSE, "International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World.", 2011, disponível em: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international, consultado pela última vez em 5 de Fevereiro de 2017.

- _____.National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23, 2008, disponivel em https://fas.org/irp/offdocs/nspd/nspd-54.pdf consultado pela ultima vez a 26 de Junho de 2017.

- FONSECA, Arnoldo Medeiros, “Caso Fortuito e Teoria da Imprevisão”, 3ª Edição, Edição Revista Forense, 1958 .

- GANDHI, Robin, Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political, 2011, disponível em: https://www.researchgate.net/publication/224223630_Dimensions_of_Cyber-Attacks_Cultural_Social_Economic_and_Political consultado pela última vez a 15 de Setembro de 2017.

- GIBSON, William “Neuromancer”, Harper Collins, 1986.

- GOUVEIA, Jorge Bacelar, “O uso da força no Direito Internacional Público””, Revista Brasileira de Estudos Políticos, 2013.

- GOUVEIA, Jorge Bacelar, “Manual de Direito Internacional Público”, Coimbra 1º Edição, Coimbra 2009.

- HANZ, Kelsen, “The Law of United Nations – A critical Analysis of Its Fundamental Problems” London, 1950.

- HOLT, Thomas J., SCELL, Bernardette,” Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications” , IGI Global, 2011.

- HORNO,Maria Jose Mateo,“Infraestruturas Críticas e Cibersegurança“, 2016 disponível em http://ingenieriadeseguridad.telefonica.com/not%C3%ADcia/2016/11/07/Infraestruturas-Cr%C3%ADticas-e-Ciberseguran%C3%A7a.html, acedido pela última vez em 10 de Março de 2017

- INTERNATIONAL COURT OF JUSTICE, Case concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda), 19 de Dezembro de 2005, disponivel em : http://www.icj-cij.org/docket/files/116/10455.pdf consultada pela última vez a 17 de Julho de 2017.

- _____.Case concerning United States Diplomatic and Consular staff in Teheran – Disponivel em: http://www.icj-cij.org/files/case-related/64/064-19800524-JUD-01-00-EN.pdf, consultado pela ultima vez em 25 de Outubro de 2017.

- _____.Case concerning Legality of the Threat or Use of Nuclear Weapons - Advisory Opinion of 8 July 1996 disponível em http://www.icj-cij.org/docket/files/95/7497.pdf consultado pela ultima vez em 25 de Outubro de 2017.

- _____.Case concerning Military and paramilitary activities in and against Nicaragua de 1986 disponível em : http://www.icj-cij.org/docket/files/70/6503.pdf consultado pela ultima vez em 18 de Julho de 2017.

- _____.Case concerning Oil platforms (Islamic Republic of Iran v. United States of America), 6 de Novembro de 2003, disponível em: http://www.icj-cij.org/docket/files/90/9715.pdf consultado pela ultima vez em 18 de Julho de 2017.
- _____.Case concerning the Gabcikovo-Nagymaros Project (Hungaryslovakia) Judgement of 25 September 1997, disponível em http://www.icj-cij.org/docket/files/92/7375.pdf, consultado pela ultima vez a 17 de Setembro de 2017

- _____.Reports of Judgments, Advisory Opinions and Orders Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights disponível em: http://www.icj-cij.org/files/case-related/100/100-19990429-ADV-01-00-EN.pdf aconsultado a 18 de Outubro de 2017.

- _____.The Corfu Channel Case, Reports of Judgments, Advisory Opinion and Orders, 9de Abril de 1949, disponivel em http://www.icj-cij.org/files/case-related/1/001-19490409-JUD-01-00-EN.pdf consultado pela última vez a 05 de Outubro.

- _____. “Summary of the Judgment of 27 June 1986 Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)” disponivel em: www.fd.unl.pt/docentes_docs/ma/TMA_MA_4615.doc consultado pela última vez a 10 de Outubro de 2017;

- INTERNATIONAL CRIMINAL TRIBUNAL FOR FORMER YUGOSLAVIA, The Prosecutor v. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995

- INTERNATIONAL LAW COMMISION, Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, 2001, disponivel em: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf, consultado pela última vez a 15 de Outubro de 2017.

- _____. Draft Articles on State Responsibility With Commentaries Thereto Adopted by the International Law Commission on First Reading,1996 disponível em: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_1996.pdf consultado pela ultima vez a 15 de Outubro de 2017.

- JINKS DEREK, “State Responsibility for the Acts of Private Armed Groups”, Chicago Journal of International Law 4, 2003, – disponível em http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1197&context=cjil consultado pela ultima vez em 15 de Setembro de 2017.

- LIBICKI, Martin C. “Conquest in Cyberspace - National Security and Information Warfare”, Cambridge University Press, 2007.

- MIRANDA, Jorge “Curso Direito Internacional Publico”, 3ª Edição – Principia 2006.

- NAÇÕES UNIDAS, Carta das Nações Unidas, São Francisco 1945;

- _____. Convenção de Viena sobre o Direito dos Tratados, 1969;

- _____.Convenção de Haia para a repressão da tomada ilícita de aeronaves de 16 de Dezembro de 1970.

- _____.Convenção Internacional para a Eliminação do Financiamento do Terrorismo, adotada em Nova Iorque em 9 de Dezembro de 1999.

- _____.Convenção de Montreal para a repressão de atos ilícitos contra a segurança da aviação civil de 23 de Fevereiro de 1971.

- _____.Convenção de Montreal sobre a repressão dos atos ilícitos contra a segurança da navegação marítima, Montreal 1991;

- _____.Convenção de Nova Iorque sobre prevenção e punição dos delitos contra as pessoas internacionalmente protegidas; Nova Iorque 1973;

- _____. Convenção de Nova Iorque sobre a tomada de reféns, Nova Iorque 1979; Protocolo para a Repressão de actos Ilícitos de Violência nos Aeroportos ao Serviço da Aviação Civil, Montreal, 1988;

- _____.Convenção de Roma sobre a repressão de actos ilícitos contra a segurança de navegação marítima, Roma 1988;

- _____.Convenção de Nova Iorque sobre a repressão dos explosivos plásticos, Nova Iorque, 1991;

- _____.Convenção de Nova Iorque para eliminação de financiamento do terrorismo, NOVA Iorque 1999.

- _____.Convenção referente às Infrações e a certos outros Atos cometidos a bordo de Aeronaves, aprovada em 1963;

- _____.Convention respecting the Limitation of the Employment of Force for the Recovery of Contract Debts (done 18 October 1907, entered into force 26 January 1910) (1908) 2 AJIL Supp 81 (Drago-Porter Convention).
- _____.Couter-Terrorism Strategy, disponível em https: //obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf , consultado pela última vez em 5 de Fevereiro de 2017.

- _____.Protocolo Adicional às Convenções de Genebra de 12 de Agosto de 1949 relativo à proteção das vítimas dos Conflitos Armados Não Internacionais (Protocolo II).

- _____.Resolução 3314 da Assembleia Geral das Nações Unidas sobre definição de agressão, Nova Iorque, 03 de dezembro de 1973 disponível em: http://hrlibrary.umn.edu/instree/GAres3314.html consultado pela última vez a 28 de Julho de 2017

- _____.Resolução de 1368 (2001) Adotada pelo Conselho de Segurança na seu 4370º reunião, 12 Setembro de 2001;

- _____.Resolução 1373 (2001) Adopted by the Security Council at its 4385th meeting, on 28 September 2001

- _____.Protocolo Adicional às Conveções de Genebra de 12 de Agosto de 1949 Relativo à Protecção das Vítimas dos Conflitos Armados Internacionais.

- PEREIRA, André Gonçalves. QUADROS, Fausto. "Manual de Direito Internacional Publico" – 3ª Edição – Almedina 1999.
- PERLROTH, Nicole , HARDY, Quentin, "Bank Hacking Was the Work of Iranians, Officials Say", The New York Times, disponivel em: http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html consultado pela última vez a 16 de Setembro de 2017.

- PERMANENT COURT OF INTERNATIONAL JUSTICE, Affaire des biens britanniques au Maroc espagnol (Espagne contre RoyaumeUni) 1er mai 1925, disponível em http://legal.un.org/riaa/cases/vol_II/615-742.pdf disponível em http://legal.un.org/riaa/cases/vol_II/615-742.pdf consultado pela ultima vez a 05 de Outubro de 2017

- _____. “Arrêts Ordonnances et Avis Consultatifs, Fascicule no 74 Phosphates Du Maroc, 14 de Julho de 1938, disponível em: http://www.icj-cij.org/files/permanent-court-of-international-justice/serie_AB/AB_74/01_Phosphates _du_Maroc_Arret.pdf, consultado pela ultima vez a 20 de Outubro de 2017

- PERÉZ, Javier , UN Secretary-General ,Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements, concluded on 9 July 1986 , between the two States and which related to the problems arising from the Rainbow Warrior Affair Decision of 30 April 1990 disponível em http://legal.un.org/riaa/cases/vol_XX/215-284.pdf consultado pela ultima vez a 09 de Outubro de 2017

- PIRES, Manuel,” Do Caso Fortuito ou de Força Maior” (dissertação do Curso Complementar de Ciências Jurídicas), 1958.

- PINTO, Eduardo Vera-Cruz, *“*História do Direito Comum da Humanidade. Ius Commune Humanitatis ou Lex Mundi?,*“* AAFDL,1º Volumes, 2003

- POE, T. Marshall, “ A History of Communications”, Cambridge University Press, 2011.

- QUINTA, Henrique Nova – “A Guerra Justa ou Justiça da Guerra no Pensamento Português” Instituto de Defesa Nacional, 1996.

- RINALDI, Steven M; Peerenboom, James P.; Kelly, Terrence K., Odentifying, Understanding, and Analyzing Critical Infrastrucres Interdependecies, 2001 Disponivel em: disponível em http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf consultado pela última vez a 10 de Março de 2017.

- ROSCINI, Marco "*Cyber Operations and the Use of Force in International Law"*, Oxford University Press, Reino Unido 2014.

- SOCIEDADE DAS NAÇÕES, Pacto da Sociedade das Nações - Primeira parte do Tratado de Versalhes, de 28 de junho de 1919.

- SCHMITT, Michael N, *Tallinn Manual on the International Law Applicable to Cyber Warfare* – Universidade de Cambridge Press, 2013.

- SCHMITT, Michael N – "Tallinn Manual on the International Law Applicable to Cyber Warfare", Cambridge University Press, 2013.

- _____. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare" Cambridge University Press, 2017.

- TATUM, Sophia, CNN Politics, *"U.S. Army public website compromised*", 9 de Julho de 2015, disponível em: http://edition.cnn.com/2015/06/08/politics/us-army-syrian-electronic-army-hacked/index.html consultado pela ultima vez a 16 de Setembro de 2017

- N.d. Tratado de Renuncia à Guerra (Pacto de Paris ou Brand-Kellog), Paris, 27 de agosto de 1928

- UNIÃO EUROPEIA, Diretiva 2008/114/CE do Conselho de 8 de Dezembro de 2008 relativa à identificação e designação das infra-estruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção.

- VATTEL, "Direito das Gentes" disponível em https://play.google.com/books/reader?id=OLYWAAAAQAAJ&printsec=frontcover&output=reader&hl=pt_PT&pg=GBS.PA1, XVIII.

- VICENTE, Dário Moura, “Direito Internacional Privado, Problemática Internacional da Sociedade da Informação”, Almedina, Setembro 2005.

- VICENTE, João Paulo Nunes, O Direito à Guerra Justa, Revista Militar, 2451, Abril de 2006, disponível em https://www.revistamilitar.pt/artigo/72 acedido pela ultima vez a 09 de Fevereiro de 2017.

- ZETTER, Kim, “Contagem Regressiva até Zero Day, Stuxnet e o lançamento da primeira arma digital do mundo, Brassport Livros e Multimidia Lda.,2011.