UNIVERSIDADE CATÓLICA PORTUGUESA

A Legítima Defesa contra um Ciberataque

Beatriz Alves Serrão

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2021

Esta página foi deixada propositadamente em branco.

UNIVERSIDADE CATÓLICA PORTUGUESA

A Legítima Defesa contra um Ciberataque

Beatriz Alves Serrão

Orientador: Prof. Dra. Maria Isabel Tavares

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2021

Dedicatória

À minha família e aos meus professores

“When considering the range of responses available to states facing harmful cyber operations, it is necessary to begin by determining when those operations rise to the level of an "armed attack" under thejus ad bellum, for an armed attack is the conditio sine qua non of the right to engage in self-defense.”

Michael N. Schmitt, Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum, 8 Harv. Nat'l Sec. J. 239 (2017)

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 à minha orientadora, Professora Doutora Maria Isabel Tavares que, desde o início me acompanhou neste caminho e que sempre me orientou para um trabalho progressivo e disciplinado. Expresso, ainda, o meu profundo agradecimento pela orientação e apoio incondicionais que muito elevaram os meus conhecimentos e, sem dúvida, estimularam o meu desejo de querer, sempre, saber mais e a vontade constante de querer fazer melhor.

Desejo igualmente agradecer à Professora Doutora Cristina Campiglio por todo o apoio, disponibilidade e atenção que sempre me dedicou durante os meses em Itália e que me permitiu desenvolver um trabalho num outro pais que agora também é meu.

Por fim e não por último, quero agradecer ao Professor Doutor Gabriele Della Morte, por todos as horas que dispensou para me poder aconselhar e apoiar neste projeto da dissertação.

À minha família e namorado, em especial à minha mãe, tia e namorado, 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 que, embora distantes fisicamente pelas condições de pandemia que vivemos, apoiaram-me e deram-me força para dar o melhor de mim neste projeto.

O meu profundo e sentido agradecimento a todas as pessoas que contribuíram para a concretização desta dissertação.

Resumo

Atualmente, um dos temas mais debatidos no âmbito do direito internacional concerne à emergente área do ciberespaço, nomeadamente, o recurso ao uso da força em legítima defesa aquando de um ciberataque. Deste modo, a presente dissertação guiar-se-á, em termos estruturais, pelos requisitos subjacentes à legítima defesa lícita perante um ciberataque.

Quanto ao primeiro requisito, são de analisar as condições em que o ciberataque pode ser considerado um ataque armado para efeitos do art. 51º da CNU e, consequentemente, os tipos de legítima defesa lícita, nesse caso, possíveis. Segue-se o esclarecimento dos problemas em redor da qualificação do ciberataque, através da diferenciação de ciberoperação e ciberataque e respetiva imputação do mesmo ao Estado.

O segundo capítulo, por sua vez, dedica-se a escrutinar de que forma a legítima defesa pode ser uma resposta aceitável (e lícita) face a um ciberataque. Para tal, numa primeira fase, são de focar os critérios (ou requisitos) materiais da legítima defesa como resposta a um ciberataque; e numa segunda fase, a natureza que a legítima defesa pode assumir em reação ao mesmo.

Por fim, é de ressalvar o trabalho desenvolvido pelas organizações internacionais no domínio da ciberdefesa, avaliando-se a forma como este trabalho se tem relacionado com debates mais amplos no âmbito do direito internacional.

Em suma, o estudo deste tema permitiu concluir que, no que respeita à construção de normas específicas aplicadas às operações cibernéticas, o direito internacional ainda tem um longo caminho a percorrer.

Esta investigação permitiu ainda concluir que, não obstante ser consensual que a ciberdefesa, enquanto resposta proporcional a um ciberataque, é lícita e permitida, é muito difícil verificar todos os requisitos de uma legítima defesa lícita num contexto cibernético.

Palavras-chave: legítima ciberdefesa, ciberataque, ciberoperação.

Abstract

In regard to International Law, the emerging area of cyberspace is currently one of the most trending topics, especially concerning the use of force in self-defence when a cyberattack occurs. Consequently, this dissertation will abide, in structural terms, by the requirements of the right of self-defence against a cyberattack.

Firstly, the conditions under which a cyberattack may be considered an armed attack must be analysed for the purposes of article 51 of the UN Charter; as well as the following types of a lawful self-defence in the aforementioned context. After that, distinguishing a cyber-operation from a cyberattack, and its respective imputation to a State will allow to highlight the main cyberattack qualification issues.

The second chapter scrutinizes how self-defence can be an acceptable (and lawful) response to a cyberattack. For this purpose, in a first stage, the material criteria (or requirements) of self-defence as a response to a cyberattack are analysed; and, in a second stage, concerning the nature of self-defence as a response to a cyberattack, the same logic is applied.

Finally, international organizations work regarding cyber self-defence will be highlighted, mainly due to its contribution to broader debates within international law. In sum, this dissertation allowed the following conclusion: international law does not establish a specific cyber-operation legal framework; thus, there is a need to resort to traditional international law norms.

Last but not least, this research also allowed to understand that, even though it is very hard to check all the requirements of a lawful self-defence in a cyber context, cyber self-defence is acceptable and lawful as a proportional response to a cyberattack.

Keywords: Cyber self-defence, cyberattack, cyber-operation.

Índice

Listas de siglas e abreviaturas

Art. -Artigo

CCDCOE- The NATO Cooperative Cyber Defence Centre of Excellence

CNU - Carta das Nações Unidas

CS - Conselho de Segurança

N.- Número

NATO - Organização do Tratado do Atlântico Norte

ONU - Organização das Nações Unidas

P./ Pág. - página

PARI - Projeto de Artigos sobre Responsabilidade Internacional, da Comissão de Direito Internacional da Assembleia-Geral das Nações Unidas

TIJ - Tribunal Internacional de Justiça

TPI - Tribunal Penal Internacional

UE - União Europeia

Prefácio

O tema desta dissertação foi pensado durante a parte letiva do Mestrado em Direito Internacional e Europeu. Após a realização de um trabalho de avaliação para a cadeira de Direito internacional Humanitário sobre a ciberguerra e o princípio da distinção, percebi que este tema e temas relacionados com o *"jus in bello*" e *"jus ad bellum*" eram uma área que me interessavam e pela qual podia desenvolver um gosto particular.

Durante a investigação desta dissertação tive a oportunidade e o prazer de fazer um estágio de investigação na Universidade de Pavia, em Itália, que me permitiu conhecer investigadores desta área que me facilitaram diversos materiais para o estudo e aprofundamento do tema.

Ainda durante o desenvolvimento desta dissertação tive duas oportunidades excelentes que me permitiram ter um conhecimento geral e ao mesmo tempo detalhado no direito internacional aplicado às ciberoperações.

A primeira, foi o curso de "Cybersecurity *e Relazioni Internazionale"* no ISPI (Istituto per gli Studi di Politica Internazionale) e, a segunda foi o curso de "*International Law of Cyber Operations",* na CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence).

A realização desta dissertação foi um trabalho longo e com a principal dificuldade de restringir o tema ao máximo pelo obstáculo dos cárteres exigidos.

No entanto, é um tema que me fascina cada vez mais.

Introdução

O ciberespaço é uma dimensão nova na história da humanidade, desde logo pelo simples motivo de que as tecnologias apenas surgiram algumas décadas atrás.

Os primeiros problemas associados ao ciberespaço tiveram lugar na década de 1990, com a chamada guerra entre "colégios" à volta do mundo, sendo que a que mais enfâse teve foi a guerra naval. Foi, na verdade, a partir desta época que o *ciber* começou a ser falado.[1]

Entretanto, em 1998, realizou-se a primeira conferência sobre o ciberespaço, onde se começou a dar importância ao direito na ciberguerra.

Com o 11 de setembro de 2001, o mundo começou a dar os primeiros passos no que respeita ao *ciber* no *Jus ad bellum,* desde logo, na luta contra o terrorismo e, a partir daí surgiram exemplos práticos daquilo que poderia ser considerado uma ciberguerra.

Em 2007, a Estónia tinha conseguido, outra vez, a sua independência, depois de ter sido ocupada pela União Soviética, na altura da II Guerra Mundial. Ora, na cidade de Tallinn existia uma estátua, "O soldado de bronze de Tallinn", que representava a vitória da Rússia contra o nazismo. No entanto, para a Estónia essa estátua era o símbolo da ocupação do seu país pela Rússia e, por esse motivo, a estátua foi transladada do centro da cidade para um cemitério soviético.

Os Russos interpretaram tal ato como uma afronta e derem início a atos de revolta, e motins, ativados pelos meios sociais, protestos, entre outros Foi, neste contexto que surgiram os primeiros ataques cibernéticos contra entidades privadas e governamentais da Estónia. Dos relatos que se leem destes episódios, poderá concluir-se que a Rússia não queria destruir nem causar danos, mas apenas perturbar. Contudo, a verdade é que, durante 10 dias, a Estónia ficou abalada e o caso foi falado em todo o mundo pois, sendo este país um membro da NATO, segundo o art. 5º do Tratado do Atlântico Norte, haveria uma obrigação de defesa coletiva.

Em 2008, foi o *Jus ad bellum* que atuou na linha da frente, com a Geórgia a atacar a Ossétia do Sul. Efetivamente, a Geórgia queria tomar posse da Ossétia do Sul, mas a Rússia já se tinha apoderado da mesma, começando um conflito armado internacional

[1] Hattendorf, John B., "U.S Naval Strategy in the 1990's" (2006). Newport Papers. 27. https://digital-commons.usnwc.ed u/usnwc-newport-papers/27

entre os dois países. Durante esta disputa, nos *websites* da Rússia surgiram listas de alvos e *malware*, pelo que este foi considerado um ciberataque da Rússia contra a Geórgia. As consequências deste ataque não foram tão invasivas como na Estónia, mas também tiveram a sua importância para o crescimento do direito aplicado ao ciberespaço.

A NATO, em 2008, começou a dar os primeiros passos para a aplicação do direito internacional ao ciberespaço, criando o *"NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)",* para resolver os problemas levantados pelo *ciber*. Neste contexto, o Prof. Michael N. Shmitt teve o papel importante de criar um grupo de especialistas de todo o Mundo, que, da perspetiva do Direito Internacional, respondessem e identificassem os problemas do *ciber.*

Outros exemplos importantes para a história do ciberespaço foram os casos do Stuxnet e da SONY. De facto, em 2010, com o caso STUXNET, vieram a ser identificados danos no Estado iraniano, devido a um ataque que teve como objetivo comprometer o funcionamento de, aproximadamente, mil centrifugas. Este ataque teve duas características particulares: a primeira, o facto de ser dirigido a um adversário preciso (a estação nuclear de Natanz); e a segunda, a capacidade de o *software* do vírus Stuxnet duplicar-se nos computadores da central nuclear. Ainda que não tenha sido possível chegar-se a uma conclusão quanto à autoria deste ataque, presume-se que tenha sido fruto da cooperação entre os Estados Unidos e Israel.

A outra grande questão levantada foi quanto à classificação do ataque, isto é, se seria ou não um ciberataque armado e, portanto, uma violação do art. 2º, nº4 da CNU, ou se não chegaria ao limiar deste tipo de ataque. Segundo alguns autores[2], seria, na verdade, um ataque armado, uma vez que provocou danos materiais. No entanto, a dificuldade foi em atribuir a autoria deste ataque a um Estado.

O último caso, menos falado, ocorreu entre novembro e dezembro de 2014, contra a *Sony Pictures Entertainament*[3], na modalidade de *spearp hising.* A particularidade deste caso é o facto de que, muito provavelmente, a respetiva autoria terá sido da Coreia do Norte, pois, no ano anterior, este país havia ameaçado a Sony de que o faria caso não cancelasse o filme "*The Interview".*

---

[2] Ralph Langner, What STUXNET is All About, 10 de maio de 2011. Em linha: http://www.langner.com/en/2011/01/10/what-stuxnet-is-all-about/.

[3] Andrew Griffin, Sony hack: who are the Guardians of Peace, and is North Korea really behind the attack? "The Independent", 17 de dezembro de 2014. Em linha: http://www.independent.co.uk/life-style/gadgets-and-tech/news/sony-hack-who-are-the-guardians-of-peace-and-is-north-korea-really-behind-the-attack-9931282.html.

O primeiro ataque recorreu, inicialmente, ao *spearphising* e, consequentemente, causou danos aos computadores da empresa. Já o ataque seguinte consistiu no aparecimento dos filmes online, sem que tivesse sido a Sony a disponibilizá-los. Por fim, foram divulgados dados pessoais, contratos e salários dos trabalhadores da empresa. Existiram outras peculiaridades neste caso, mas aquela que mais chama a atenção é o facto de que os Estados Unidos defenderam a Sony e tentaram reagir contra a Coreia do Norte[4].

Nos três casos, não está presente a legítima defesa como estratégia de resposta aos ataques. O Irão, embora tenha considerado o ataque como uma ação hostil, não se preocupou em invocar o direito à legítima defesa, tendo optando por uma estratégia simétrica à que sofreu. Na Estónia, apesar das alegações iniciais de que o ataque sofrido era um caso de terrorismo de Estado[5], a reação resultou principalmente numa ação penal (na verdade, contra pessoas desconhecidas) com resultados inconclusivos, assim como, a longo prazo, numa maior cooperação com os aliados da NATO. Finalmente, no caso do ataque da Sony, os Estados Unidos recorreram a uma associação de abordagens estratégicas e legais, reagindo contra a Coreia do Norte tanto com retaliações como com sanções específicas.

Um dos problemas que os estudiosos do Direito Internacional encontram na aplicação do Direito Internacional ao ciberespaço é a ausência de uma prática estabelecida: a não existência de referência a casos de ciberataque e de reação relativa, argumentando-se, a este nível, que a discussão jurídica permanecerá exclusivamente teórica, impedindo, por isso, o estabelecimento de um costume.

Desde 2013 a 2016 foi criado o Manual de Tallin 2.0, que procura responder aos problemas que o *ciber* levanta, de várias perspetivas, como a jurisdição, as imunidades, as responsabilidades estaduais, as contramedidas, o direito aéreo, o direito do espaço, o direito do mar, o direito internacional das telecomunicações, os direitos humanos, entre outros. Os EUA e a Holanda tiveram um papel importante no desenvolvimento desta matéria, antes de mais por terem sido dos primeiros a criar um centro de comandos de ciberdefesa.

[4] Michael Cieply, Brooks Barnes, Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm, "The New York Times", 30 dec. 2014. http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html

[5] Declaração do Ministro dos Negócios Estrangeiros da República da Estónia (Governo da República da Estónia, 1 de Maio de 2007) https://valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia

Posto isto, é percetível que a dimensão cibernética seja algo muito recente e, por isso, com muitas falhas e dúvidas. Assim, apenas recorrendo ao direito consuetudinário poderão vir a ser resolvidas.

Nesta dissertação de mestrado discutiremos um destes problemas. De facto, sempre que são lançados ciberataques contra infraestruturas cibernéticas públicas de um Estado, levanta-se a discussão de saber qual será a resposta adequada para tal ataque. É exatamente sobre este tema em particular que refletiremos ao longo do presente trabalho.

O direito internacional estabelece uma tipologia clara de opções de resposta – a legítima defesa, o consentimento, as contramedidas, as represálias, a força maior, o perigo extremo e o Estado de necessidade. Tais respostas *per se* seriam ilícitas. No entanto, consoante a natureza e as consequências da operação cibernética a que respondem, podem vir a ser consideradas lícitas.

Quando estamos perante um ciberataque equiparado a um ataque armado, portanto, um ataque que viola o art. 2º, nº4 da CNU, tal como supramencionado, o Estado que é vítima tem quatro possibilidades de resposta. Desde logo, duas respostas que não implicam o uso da força são o recurso ao conselho de segurança das Nações Unidas, previsto no art. 35º, nº1 da CNU, e o recurso aos tribunais internacionais, por violação do art. 2º, nº4 da CNU. Já a legítima defesa individual ou coletiva é uma das possibilidades com recurso à força.

Na presente dissertação trataremos, apenas, a legítima defesa individual como resposta a um ciberataque. Note-se que a legítima defesa só é possível (causa de exclusão de responsabilidade internacional e, por isso, lícita) como resposta a um ataque armado típico ou, pelo menos, como resposta à forma mais grave do uso da força.[6] Do mesmo modo, a legítima ciberdefesa só é permitida à luz do art. 51º da Carta se se apresentar como resposta a um ciberataque armado ou convencional.

Parece ser aceite, quer no Manual de Tallinn quer por uma analogia às normas do direito internacional, que uma resposta *ciber* em legítima defesa a um ciberataque preenche um dos requisitos da legítima defesa: a proporcionalidade. O problema surge quando, em confronto com um ciberataque, estamos perante uma legítima defesa convencional ou vice-versa.

[6] Veja-se, Azeredo Lopes, José Alberto (março 2020), capítulo I - "Uso da força e Direito Internacional", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, p. 121-123

Esta dissertação tem, pois, como objetivo analisar os requisitos que permitem a legítima defesa como resposta a um ciberataque e os problemas que daí advêm, pelo que será efetuada uma divisão em capítulos, segundo cada um dos requisitos abaixo identificados.

A legítima defesa só será considerada lícita como resposta a um ciberataque e, portanto, excludente de responsabilidade internacional, na presença dos seguintes requisitos:

1. O ciberataque é um ataque armado;
2. O ciberataque é atribuível ao Estado infrator;
3. O uso da força utilizado em legítima defesa é necessário, proporcional, iminente e imediato.

Capítulo I: Ciberataque ao nível de ataque armado

O preâmbulo da Carta das Nações Unidas[7] apresenta, desde logo, algumas das aspirações pelas quais o direito internacional foi criado.

Ora, o art. 2º, nº 4 da Carta das Nações Unidas expressa um dos principais princípios do Direito Internacional: o princípio proibitivo do uso da força. A regra proibitiva do uso da força é evocada como direito costumeiro, mas é de reconhecimento geral que é uma norma imperativa de direito internacional geral[8].

A interpretação do princípio do art. 2º, nº4 da CNU só faz sentido se interpretado à luz dos objetivos da mesma. No entanto, aquilo que se pretende neste princípio é restringir, tanto quanto possível, o recurso à força de um Estado contra a comunidade internacional[9]. No entanto, esta proibição, absoluta e geral, prevê exceções a este princípio, nomeadamente o art. 42º da CNU, com o sistema de segurança coletiva, e o art. 51º, com o exercício da legítima Defesa pelos Estados. Para além destas duas exceções ao uso da força, autores como José Manuel Pureza, consideram que podem ser aceites outras exceções que não estão expressamente consagradas na CNU, que podem ser admissíveis no espírito da mesma, pelo seu caracter *jus cogens.*[10] A exceção analisada neste trabalho é a que, por norma, é mais vezes invocada pelos Estados: o exercício de legítima defesa, previsto no art. 51º, do Capítulo VII da Carta das Nações Unidas.

Os Estados nem sempre estiveram de acordo quanto à LD, nem que esta viesse a ser regulada pelo DI, por um lado porque a sua legalidade era questionável como resposta ao uso da força e, por outro lado, porque não era necessária a sua tipificação, sendo que não estariam definidos os limites dessa legítima defesa.[11]

---

[7] A Carta das Nações Unidas de 1945 é o tratado fundamental das Nações Unidas, uma organização intergovernamental.[1] A Carta da ONU articulou um compromisso de defender os direitos humanos dos cidadãos e delineou um amplo conjunto de princípios relacionados à obtenção de "padrões de vida mais altos", abordando "problemas econômicos, sociais, de saúde e afins" e "respeito universal e observância direitos humanos e liberdades fundamentais para todos, sem distinção de raça, sexo, idioma ou religião".[2] Como carta constitutiva, é um tratado constituinte e todos os membros estão vinculados a seus artigos. Além disso, o Artigo 103 da Carta afirma que as obrigações para com as Nações Unidas prevalecem sobre todas as outras obrigações do tratado.

[8] Azeredo Lopes, José Alberto (março 2020), capítulo I - "Uso da força e Direito Internacional", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, p. 27

[9] Idem, p. 13.

[10] Exceções como: o direito à autodeterminação dos povos, na forma de guerras de secessão e de libertação dos povos colonizados, e a proteção dos direitos humanos, na forma de intervenções armadas humanitárias. Cf., p. ex., PUREZA, pp. 83-92.

[11] BADR, GAMAL MOURSI, The Exculpatory Effect of Self-Defense in State Responsibility, Georgia Journal of International and Comparative Law, Issue 1, Vol. 10, 1980. Em linha:

Como é do conhecimento geral, o direito de legítima defesa foi consagrado na Carta, mas não significa, como anteriormente referido, que o mesmo constituiu aos Estados o direito de exercer a legítima defesa. Aliás, o direito de legítima defesa resulta do direito internacional consuetudinário[12] e com a CNU adquiriu o estatuto de instituto autónomo de direito internacional, consagrando-se como uma das causas de exclusão da ilicitude em sede de responsabilidade dos Estados[13]. No entanto, para não dar azo a manifestações ilegítimas de força por parte dos Estados, o conceito de legítima defesa adquiriu um significado mais restrito[14].

Antes da sua consagração na CNU, o exercício de legítima defesa era associado a uma resposta ao uso da força, constituindo, na sua maioria, uma manifestação ilegítima da última. O art. 51º estabelece o conceito mais restrito de LD[15], na medida em que a LD será licita apenas "*no caso de ocorrer um ataque armado*". Quer isto dizer que um Estado não poderá invocar a LD exceto em resposta a um ataque armado, podendo incorrer numa violação de uma obrigação internacional.

Posto isto, passou a ser nítido que o Estado não podia reagir de imediato em LD contra ameaças de uso da força, nem contra formas de uso da força dirigidas contra si, que ficassem aquém de um ataque armado. Não obstante, caso ocorra uma rutura da paz (ameaça à paz e segurança internacionais) que não atinja o limiar de ataque armado e para que o Estado ofendido não fique desprotegido, poderá reagir de forma pacífica[16] ou poderá apelar ao CS[17]. No entanto, se um Estado decide recorrer unilateralmente à força,

---

http://digitalcommons.law.uga.edu/gjicl/vol10/iss1/2 , pp. 3-4

[12] Cf. Azeredo Lopes, José Alberto (março 2020), capítulo I - "Uso da força e Direito Internacional", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, p. 81- 82

[13] BADR, GAMAL MOURSI, The Exculpatory Effect of Self-Defense in State Responsibility, Georgia Journal of International and Comparative Law, Issue 1, Vol. 10, 1980. Em linha: http://digitalcommons.law.uga.edu/gjicl/vol10/iss1/2 , p. 5.

[14] É ainda importante deixar claro que a Carta não regula todos os pormenores da LD, sendo que no caso *Nicarágua,* o Tribunal Internacional de Justiça especificou a não objeção à interpretação em simultâneo do art. 51º da CNU e do direito consuetudinário. Para além disso, deixou clara a questão de que uma norma *jus cogens* nunca pode ser posta em causa por uma norma convencional. Ver: Azeredo Lopes, José Alberto (março 2020), capítulo I - "Uso da força e Direito Internacional", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, p. 82

[15] A definição de LD adveio do caso Caroline, http://www.grocjusz.edu.pl/Materials/jp_sem_20191128_B.pdf " The Caroline Incident: Facts and Legal Claims"

[16] Cf. art. 33º da CNU.

[17] Nos termos do art. 35(1) ou 37(1) CNU, para que este exerça as competências que lhe estão cometidas no art. 34. Posteriormente, nos termos do art. 39, o CS, se determinar a existência de uma ameaça à paz, rutura da paz ou ato de agressão, poderá proferir recomendações (artigos 36, 37 ou 38), ou decidir aplicar as medidas sancionatórias do art. 41, ou, enfim, autorizar o uso da força militar contra o agressor, nos termos do art. 42 da CNU

o ónus da prova é do próprio Estado, tendo este que demonstrar que foi vítima de um ataque armado.

Em suma, para o exercício lícito de uma legítima defesa unilateral, prevista no disposto do art. 51º da CNU, é necessária a existência de um ataque armado. Temos, por isso, de definir o conceito de ataque armado, que das questões mais debatidas no DI.

1. Definição de ataque armado no Direito Internacional

Nem o art. 51º nem a doutrina ou a jurisprudência facultam a definição clara e precisa de ataque armado. Contudo, o facto de o conceito estar consagrado na Carta e relacionar-se com o princípio proibitivo do uso da força mostra que um ataque armado tem que demonstrar o uso mais grave de força física pelas forças armadas de um Estado.

Para se poder identificar um ataque armado tem de se compreender, em primeiro lugar, o que é um ato de agressão, através de exemplos em várias escalas.

Em plena Guerra Fria, a Assembleia Geral adota a Resolução 3314 de 1974, sendo que com o seu art.3º, meramente exemplificativo, enumera alguns exemplos daquilo que possam ser considerados atos de agressão. Contudo, a Resolução não resolve o problema aqui tratado, ou seja, não distingue a mera agressão armada de ataque armado.

Certo é que as hipóteses previstas na definição de agressão já foram ultrapassadas pela realidade, tendo em consideração os atores não estaduais (por exemplo, os terroristas). Nas palavras do Professor Doutor Azeredo Lopes, existe como uma escala imaginária de formas da força, onde as ameaças vinham em primeiro lugar e de seguida as "hipóteses que ficassem aquém" do uso da força e, por fim, teríamos o conceito mais grave de uso da força (ataque armado).[18]

Podemos, assim, concluir que o conceito de força está inserido no de ataque armado e, que desta forma, a mera ameaça fica fora do alcance da LD antecipatória. Em suma, o art. 51º da CNU é claro quanto ao facto de a legítima defesa individual ou coletiva apenas ser permitida na resposta a um ataque armado (legítima defesa reativa).

Outro problema que se levanta quanto ao conceito de ataque armado é a de este poder ser conduzido por entidades não estaduais, como acima foi referido.

[18] Azeredo Lopes, José Alberto (março 2020), capítulo I - "Uso da força e Direito Internacional", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, p. 83

O TJI com alusão ao art.3º da Resolução 3314, no Acórdão, Nicarágua consagrou uma conceção restritiva, afirmando-se que a agressão armada conduzida por autores não estaduais apenas podia ser considerada "ataque armado" se fosse imputada ou atribuída a um Estado.[19] Neste seguimento, para que essa agressão armada pudesse ser atribuída a um Estado, este teria que exercer o controlo efetivo sobre as operações militares ou paramilitares em questão, sendo insuficiente o apoio logístico.[20] No fundo, para que o Estado ofendido pudesse reagir em sede de LD, as agressões tinham de ser atribuídas a um Estado ofensor. Esta atribuição, segundo o caso Nicarágua, dependia do difícil teste do controlo efetivo. Levanta-se então, a questão de saber se a LD se destina à resposta de ataques de atores não estaduais, como as organizações terroristas.

Quando é um Estado que envia um grupo armado a realizar atos de força armada com gravidade equivalente a um ataque armado, não há dúvida que a LD é aplicável.[21] Contudo, hoje em dia, alguns autores fazem uma interpretação mais criativa do art. 51º da CNU, considerando que o mesmo permite o recurso à LD no caso de ocorrer um ataque armado por parte de um Estado. [22] Por outro lado, e especialmente depois do 11 de setembro, passou a considerar-se a hipótese de prever a LD em situações de ataques por entes não estaduais, se esse ataque for em grande escala.[23]

Em suma e, tal como o Prof. Dr. Azeredo Lopes referiu, os autores da Carta, tentaram "tanto quanto possível" restringir a possibilidade de legítima defesa, através do conceito mais restrito de uso da força e não com qualquer uso da força.[24]

Em concordância, o TIJ confirmou esta posição no caso Nicarágua, onde afirmou que um Estado pode usar a sua força contra outro Estado, com a justificação de que o mesmo praticou um ato ilícito, desde que se trate de um ataque armado.[25]

---

[19] Azeredo Lopes, José Alberto (março 2020), capítulo I - "Uso da força e Direito Internacional", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, p.84

[20] CF. TAMS, CHRISTIAN J., The Use of Force against Terrorists, EJIL, Vol. 20, No. 2, 2009, p. 360

[21] CF caso Nicarágua, em que TIJ não reconheceu o direito de LD ao Estado ofendido, pelo facto de o ataque sofrido não ter sido atribuído a um Estado, por considerar que a assistência aos rebeldes na forma de fornecimento de armas ou de apoio logístico, não ser atribuída a um Estado no teste do controlo efetivo, apesar de esta forma de assistência poder constituir ameaça ou uso da força, ou intervenção nos assuntos doutro Estado.

[22] TAMS, CHRISTIAN J., The Use of Force against Terrorists, EJIL, Vol. 20, No. 2, 2009, p. 369

[23] No entanto, a questão da LD contra entes não estaduais ainda tem um longo caminho de descoberta.

[24] Cf. Azeredo Lopes, José Alberto (março 2020), capítulo I - "Uso da força e Direito Internacional", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, p. 85

[25] Caso das Atividades armadas no território do Congo (República democrática do Congo c. Uganda)

2. Ciberataque como ataque armado

Até ao momento, ficou assente que, no que respeita ao uso da força num contexto cibernético e, tendo em consideração aquilo que declaram as regras 68 e 69 do Manual de Tallinn, uma operação cibernética que constitua ameaça ou uso da força é ilícita.[26]

Na regra 68, está presente a ameaça ao uso da força que, tal como o uso da força, é ilícita. Uma ameaça em forma de operação cibernética pode assumir duas formas. A primeira concerne numa operação cibernética que sirva para comunicar uma ameaça ao uso da força, podendo ser ou não cibernética. A segunda forma concretiza-se numa ameaça conhecida através de qualquer meio, seja este cibernético ou não, para levar a cabo operações cibernéticas qualificadas, como uso da força.

A ameaça tem de ser explícita ou implicitamente transmitida, pois uma ação que ameace a segurança de um Estado, mas não foi transmitida, não pode ser qualificada como uso da força. Por exemplo, um Estado que comece a ter a capacidade de conduzir operações cibernéticas contra outro Estado não constitui uma ameaça. Isto apenas sucede se esse estado comunicar que adquiriu capacidades cibernéticas para atacar o outro Estado, e que vai fazê-lo.

Um problema que se levanta no contexto cibernético é o de saber se um Estado que não tem capacidade para realizar uma operação cibernética pode violar a regra da "não ameaça do uso da força". Por outras palavras, se um Estado que não tem capacidade para realizar operações cibernéticas contra outro Estado, ao efetuar a ameaça de que vai realizar operações cibernéticas contra o mesmo, está a violar a "não ameaça do uso da força".

No entanto, é extremamente difícil para um Estado avaliar a capacidade cibernética de outro, porque não existe uma relação direta do tamanho território, da população ou da capacidade económica e militar de um Estado com a sua capacidade cibernética. Isso significa que um Estado terá dificuldade em avaliar a capacidade cibernética de outro Estado para poder cumprir a sua ameaça de usar a força por meios cibernéticos. Por outro lado, é possível um Estado que tenha capacidade cibernética e capacidade para ameaçar ciberneticamente outro Estado, mas não tem intenção de o fazer.

[26] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 68

Na regra 69 do Manual de Tallinn está presente a proibição do uso da força. Uma operação cibernética constitui uso da força se ocorrer contra a integridade territorial ou independência territorial de um Estado, como preceituado no art. 2º da CNU. No ponto 4 da regra 69 do Manual de Tallinn, o grupo internacional de peritos constata que "[u]ma ação qualificada como uso da força não precisa ser conduzida pelas forças armadas de um Estado.*"* Isto significa que uma operação cibernética que se qualificaria como uso da força, se conduzida pelas forças armadas, seria igualmente qualificada como uso da força se levada a cabo por entidades de um Estado ou por entidades privadas.[27]

Para auxiliar a definição de ciberataque como ataque armado, a regra 69 do Manual vem determinar que uma operação cibernética constitui uso da força quando a sua "*escala e efeitos"*, ou seja, os seus danos, sejam comparáveis à de uma operação não cibernética que constituía uma violação à proibição do uso da força. De forma a facilitar a determinação de ataques cibernéticos como ataques armados, Michael Schmitt desenvolveu, no ponto 9 da regra 69 do Manual de Tallinn, oito requisitos:[28]

1) "*A gravidade".* Este é o critério que tem maior peso na caracterização de uma ciberoperação como ciberataque, dado que os ataques armados que ameaçam danos físicos e destruição serão assim considerados como atos que violam a proibição do uso da força. Assim, uma operação cibernética que resulte em dano, destruição ou morte é considerada como uso da força;

2) "*A iminência*". Um ataque rápido e sem grandes avisos e que as consequências se manifestem mais rapidamente fará com que seja mais difícil aos Estados conseguirem uma resolução pacífica do conflito, pelo que passa a ser mais fácil caracterizar como ataque armado uma operação cibernética que tenha consequências imediatas. Este requisito da iminência do ataque, para além de ajudar a caracterizar o ciberataque como ataque armado, permite, também, enquadrar a legítima defesa como resposta a esse ataque, pois o direito ao uso da força em legítima defesa como surge se um ciberataque ocorrer. Para além disto, o grau da iminência do ataque vai permitir esclarecer que tipo de legítima defesa antecipatória será considerada possível como resposta a esse ataque.

A legítima defesa convencional, isto é, em resposta um ataque armado convencional, tem como objetivo *repelir* esse ataque armado, mas apenas pode fazê-lo imediatamente após o início do mesmo, isto é, a partir do momento em que esse ataque for iminente.

---

[27] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 69, parág. 4.
[28] Idem

O princípio da prioridade na legítima defesa nasce aquando da ocorrência de um ataque armado. Tal como a Maria Isabel Tavares afirma, uma interpretação rigorosa do art. 51º da CNU, "conduz à evidência de que o surgimento do direito de legítima defesa depende da prévia existência de um ataque armado"[29] sendo, por isso, a legítima defesa uma exceção ao princípio da proibição do uso da força. No entanto, no contexto *ciber,* este requisito não é assim tão ténue, na medida em que um ciberataque pode ser executado em milésimos de segundos.

O princípio de que os Estados não precisam de esperar pelo lançamento efetivo de um ataque armado, mas poderem agir em legítima defesa antecipatória preventiva, é bem aceite no direito internacional, ainda que não se tenha claro qual o momento preciso em que o ataque armado se torna iminente. Nas operações convencionais, tradicionalmente, a norma era entendida nos termos de uma proximidade temporal ao ataque armado, mas o mesmo faz pouco sentido no contexto de ciberataques ou ciberoperações, que podem ser executadas em segundos, sem pré-aviso e com um efeito devastador. O Manual de Tallinn identifica claramente este quesito como sendo o ponto em que uma falha em agir pode tornar um Estado incapaz de se defender quando o ataque realmente ocorre, uma vez que iminência de um ciberataque é muito difícil de antecipar, quer se trate de uma ciberoperação artificial ou de *malware* de verdade.

No entanto, afirma-se que esta iminência, no contexto cibernético, não é assim tão difícil, quanto se possa pensar, de determinar[30], ou seja, a perceção de quando/ e se o ataque será iniciado, passa por um critério de razoabilidade, com base numa avaliação dos factos conhecidos pelo Estado vítima. Concretamente, no caso de ciberataques, o caracter iminente depende da intensidade do ataque, do objetivo do atacante, da imediatez da reação requerida para prevenir o ataque e da velocidade que o dano pode vir a ser sofrido através de redes informáticas, pelo que a iminência do ataque no seu conjunto não depende única e exclusivamente do fator tempo, mas também de outras circunstâncias que envolvem cada caso concreto.

3) "*Caráter direto*". Tem de existir um nexo causal entre as consequências e a conduta, ou seja, quanto maior for o nexo causal entre a operação cibernética e os efeitos, maior será a probabilidade de esta ser considerada como uso da força (ataque armado);

[29] Tavares, Maria Isabel (2015) - "Guerra e Responsabilidade" – A intervenção militar no Iraque em 2003, Publicações Universidade Católica Porto, pp. 138-139.
[30] Azeredo Lopes, José Alberto (março 2020), capítulo I - "Uso da força e Direito Internacional", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, pág.89

4) "*Carácter invasivo".* Este critério refere-se ao grau de intromissão das operações cibernéticas de um Estado noutro Estado, ou seja, torna-se mais fácil perceber se estamos perante um ciberataque se as operações cibernéticas se imiscuem no Estado-alvo ou nos seus sistemas cibernéticos, contrariando os interesses desse Estado. Por exemplo,

> "a intrusão em um sistema militar que foi credenciado no Nível de Garantia de Avaliação 7 (EAL7) dos Critérios Comuns[31] é mais invasiva do que meramente explorar vulnerabilidades de um sistema não credenciado abertamente acessível em uma universidade civil ou pequena empresa."[32];

5) "*A Quantificação dos Efeitos*". Enquanto os efeitos/ consequências de um ataque armado tradicional são fáceis de mensurar, num ciberataque o mesmo já não é tão fácil, pelo que, se esses efeitos/consequências forem mensuráveis tornar-se-á mais fácil qualificar essa operação cibernética como ciberataque;

6) "*Carácter Militar".* Tal como o próprio nome indica, este critério considera o grau de intrusão de uma operação cibernética no sistema militar de um Estado. Isto significa que um nexo causal entre a operação cibernética e as operações militares aumenta a probabilidade de as primeiras se caracterizarem pelo uso da força. No entanto, é importante esclarecer que um ciberataque não é exclusivamente conduzido por forças militares, nem apenas contra objetivos militares.

7) "*A legalidade (Presumptive Legítimacy)*": na maior parte das vezes, o uso da força, no direito internacional, é ilegítimo, a não ser que seja um ato permitido, na ausência de tratados expressos ou de uma proibição expressa de direito consuetudinário. Por exemplo, a propaganda, a espionagem ou mera pressão económica *per se* não são proibidas, logo tudo aquilo que caiba neste âmbito será mais difícil de ser considerado uso da força;

8) *"O envolvimento do Estado (State Involvement)".* O grau de envolvimento do Estado numa operação cibernética é reconhecido através de uma continuidade de operações realizadas por esse Estado. Operações cibernéticas conduzidas pelo Estado de maneira periférica podem ser duvidosas quanto ao envolvimento do mesmo nesse

---

[31] Os *Common Criteria* (CC) constituem um padrão internacional (ISO/IEC 15408) para segurança de computadores. Este padrão é voltado para a segurança lógica das aplicações e para o desenvolvimento de aplicações seguras. Ele define um método para avaliação da segurança de ambientes de desenvolvimento de sistemas. Constituem um quadro em que os utilizadores de sistemas computacionais podem especificar seus requisitos funcionais de segurança e garantia. Dessa forma os fornecedores podem, então, implementar e/ou fazer alegações sobre os atributos de segurança de seus produtos, enquanto que os laboratórios de teste podem avaliar os produtos para determinar se eles realmente cumprem as reivindicações. Por outras palavras, os *Common Criteria* fornecem uma garantia de que o processo de especificação, implementação e avaliação de um produto de segurança computacional foi conduzido de uma maneira rigorosa e padronizada. https://pt.wikipedia.org/wiki/Common_Criteria

[32] Cf. parág. 9, al. d) da regra 69 do Manual de Tallinn.

ciberataque, pelo que é importante encontrar o nexo de proximidade entre o Estado e as ciberoperações. No entanto, este critério, no plano da qualificação do ciberataque armado, parece ser o mesmo critério da atribuição do ciberataque armado ao Estado para imputação da responsabilidade internacional prevista no Manual de Tallinn[33]. O grupo de peritos do Manual tentou fazer esta distinção, embora com bastante dificuldade, pois, por um lado, o critério do envolvimento do Estado na operação cibernética pretende ajudar a definir um ciberataque como armado, na medida em que se um Estado já está em conflito e já executou algumas ciberoperações contra o Estado vítima, é mais fácil encontrar este nexo entre o Estado e a ciberoperação e, por isso, qualificá-la como ciberataque armado. Por outro lado, o requisito da atribuição serve para atribuir responsabilidade internacional ao Estado, tal como será explanado no próximo capítulo.

Por fim, a regra 69 do Manual de Tallinn consolida ainda, mesmo que tal não fosse necessário, que uma ciberoperação pode ser considerada como uso da força, ou seja, como ciberataque, se os danos sofridos forem iguais aos prejuízos causados por ataques tradicionais.

2.1. Legítima defesa antecipatória

Antes de mais, esta doutrina da legítima defesa antecipatória vem ignorar, tal como supramencionado, o disposto no art. 51º da CNU. Tal como na legítima defesa tradicional, no contexto *ciber* a ideia de que não é necessário esperar pelo início do ciberataque para que se possa responder em legítima defesa é bem aceite pelos internacionalistas. Aliás, neste contexto, tem ainda mais sentido a possibilidade de uma legítima defesa antecipatória, sendo que a ocorrência de uma resposta imediata a um ciberataque é quase impossível de alcançar, e em certos casos, mesmo impossível.

No entanto, a legítima defesa antecipatória tem de ser tratada com precaução. Desde logo, porque uma legítima defesa efetuada demasiado antes do ataque pode ser considerada o próprio ataque e, no contexto de um ciberataque, o problema é ainda mais difícil, pois conseguir perceber quando é que o mesmo será lançado não é fácil e, muito menos se não se souber de onde provém e quais as suas consequências.

[33] Cf. Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 69, parag. 9, regra 71, parag. 16 a 18 e regras 15 a 18

A legítima defesa antecipatória pode ser preemptiva (uma ameaça de um futuro ataque) ou preventiva (um ataque que está prestes a ocorrer), sendo que a primeira é considerada ilegal e a segunda legal.[34]

O Manual Tallinn tomou a posição, também prevista no Direito internacional para conflitos internacional tradicionais, de que a legítima ciberdefesa não se podia limitar apenas aos casos em que um ciberataque tivesse ocorrido ou em que já tivesse sido lançado, porque o mesmo seria de tal forma rápido que quando houvesse resposta em legítima defesa, esta seria reativa e, não antecipatória e as consequências do ataque podiam ser irreversíveis. Outro exemplo de um problema que este requisito levanta no contexto ciber é o facto de que, muitas vezes, os danos causados por um ciberataque, ou até mesmo pela ciberoperação, só surgem depois do ataque, ou seja, o ciberataque é efetuado em segundos, mas os danos só se vêm a verificar depois.

Neste seguimento de ideias, levanta-se ainda outra questão quanto à reação do Estado vítima: o Estado vítima pode ser alvo de um ciberataque, que ainda não pode ser qualificado como ataque armado, porque os seus efeitos ainda não se produziram. No entanto, poderá este Estado vítima responder ao ciberataque mesmo que este ainda não seja considerado ataque armado? A dificuldade reside em conseguir perceber se esse ataque vai ter os mesmos efeitos previstos do que um ataque armado, pois, no contexto ciber, todas estas hipóteses são muito relativas.

Quanto a esta questão, Michael N. Shmitt introduziu três fatores que permitem determinar se o Estado vítima dessa ciberoperação pode ou não vir a responder em legítima defesa antecipatória. O primeiro fator (1) é perceber se o ciberataque faz parte de uma ciberoperação maior, ou seja, se já existe um conflito armado e que, portanto, desencadeará em ataque armado. O segundo (2) fator passa por perceber se o ciberataque é irreversível, ou seja, se a decisão do Estado em atacar e, portanto, antes de ser iminente e ser considerado um ataque armado, pode ser parada. O terceiro (3) e último fator está relacionado com o fator anterior, pois o Estado vítima está a atuar antes do ciberataque armado, mas no último momento em que podia reagir. Assim, se estes fatores se cumprirem, o requisito da imediatez fica preenchido.

[34] Em inglês, e dependendo dos autores, estes dois conceitos são tratados com significados opostos ao significado português, pelo que, nesta dissertação, o significado adotado será o português.

O Manual de Tallinn vem, pois, afirmar que o direito de usar a força em legítima defesa surge quando um ciberataque ocorre ou é iminente,[35] sendo que a maioria dos peritos do Manual defende a legalidade da legítima defesa antecipatória. Além disso, o Grupo Internacional de Peritos adota os fatores de Schmitt "da última janela de oportunidade" viável e argumenta que tal janela pode ocorrer pouco antes, mas por vezes muito antes do ataque em questão.[36]

Parece relevante fazer a distinção entre os dois tipos de legítima defesa antecipatória, dado que, no contexto *ciber,* ainda não se chegou a um consenso maioritário. Assim, uma legítima defesa preemptiva seria aquela em que a resposta em legítima defesa ocorreria, mas em que o ciberataque ainda não seria iminente. Este tipo de legítima defesa é proibido, nos termos da CNU, mas o governo dos EUA foi bastante claro relativamente a este respeito, afirmando que se deve adaptar o conceito de iminente ao contexto cibernético.[37] Já a ONU não apoia esta doutrina, defendendo que apenas o Conselho de Segurança das Nações Unidas deve e pode agir de forma preemptiva.

3. Problema da intensidade e da imputação do ciberataque

Analisando o supra exposto, concluímos que uma operação cibernética é diferente de uma operação cibernética que seja considerada como ataque armado. Além disso, concluímos que uma operação cibernética ilícita, mas que não atinja o limiar de ataque armado, "não dá" direito a legítima defesa. No entanto, e segundo alguns autores, como o Prof. Azeredo Lopes [38], é possível verificar uma legítima defesa contra Estados sem que haja o requisito "essencial" da legítima defesa, ou seja, sem que haja ataque armado. Nesta situação, entende-se que o conceito de ataque armado, "ou, talvez melhor, d[o] de

[35] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 73.
[36] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 73, para. 2.
[37] Gill, T. D., & Ducheine, P. A. L. (2013). Anticipatory Self-Defense in the Cyber Context. International Law Studies (Naval War College), 89, 438-471. http://www.heinonline.org/HOL/Page?handle=hein.intyb/ilsusnwc0089&collection=intyb&index=intyb/ilsusnwc456&id=456
[38] Azeredo Lopes, José Alberto (março 2020), capítulo I - "Uso da força e Direito Internacional", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, pág. 120

legítima defesa"[39] deverá ser alargado também aos ataques "assimiláveis", que pela sua natureza, são consideráveis relevantes para a segurança dos cidadãos dos Estados[40].

Posto isto, cabe agora, esclarecer dois pontos importantes para que se possa caracterizar um ciberataque como armado:

1) A intensidade do ataque, ou seja, a compreensão da diferença entre ciberoperação e ciberataque;
2) A imputação desse ciberataque a um Estado, nos termos do art. 2º, nº4 da CNU.

3.1. A intensidade do ciberataque

Neste seguimento[41] e, como suprarreferido, percebe-se que o conceito de ataque armado está intrinsecamente ligado ao de agressão e uso da força. Aliás, agressão encontra-se referida na Carta aquando das competências do Conselho de Segurança, sendo 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"[42]. Esta definição de "agressão" prevista na Resolução 3314 da Assembleia Geral das Nações Unidas, é indispensável para percebermos a extensão de um "ataque armado", visto que tem sido a usada pelo TIJ.

---

[39] Idem

[40] Um exemplo de um ataque que legitimou a legítima defesa do Estado, foi o atentado do 11 de setembro, referido pelo Prof. Azeredo Lopes em: Azeredo Lopes, José Alberto (março 2020), capítulo I - "Uso da força e Direito Internacional", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, pág. 118

[41] Definido o conceito de "ataque armado" no contexto do direito internacional, tornou-se mais fácil definir o conceito de "ciberataque" no contexto cibernético. Deixe-se claro que, ao longo desta dissertação, qualquer referência ao conceito de ciberataque deve ser entendida como ciberataque armado.

[42] Resolução 3314 da Assembleia Geral das Nações Unidas sobre definição de agressão, artigo1, disponível em: http://hrlibrary.umn.edu/instree/GAres3314.html . Pode 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. art.3

O grupo de peritos do Manual de Tallinn teve em consideração os casos das atividades militares do Nicarágua, da República Democrática do Congo/Uganda e, ainda, das Plataformas de petróleo Irão/Estados Unidos da América, sendo que o TIJ define ataque armado a partir da definição de agressão[43]. Já o Tribunal Penal Internacional para a antiga Jugoslávia definiu, na sua jurisprudência, que um ataque armado "existe sempre que se recorre às forças armadas entre os Estados ou em que há violência armada prolongada entre as autoridades governamentais e grupos armados organizados ou entre esses grupos no interior de um Estado" [44].

No contexto *ciber*, tal como já se verificou, um ciberataque constitui o uso da força se a sua "escala e efeitos"[45] - entenda-se, danos- forem comparáveis aos de um ataque armado no contexto tradicional e, portanto, uma violação do princípio da proibição do uso da força.[46] Segundo o Manual de Tallinn, as operações cibernéticas que não pretendam infligir dano e apenas tenham como objetivo fragilizar um governo ou uma economia não se qualificam como uso da força.

Todavia, para que uma operação cibernética se qualifique como ciberataque não necessita obrigatoriamente de infligir um dano físico. A título de exemplo, o roubo de informação sensível ou o bloqueio de um porto, embora não cause danos físicos, cairá sobre a denominação de uso da força. Quer isto dizer que, para se considerar que uma ciberoperação atinge o limiar de ataque armado, isto é, seja considerada uso da força, portanto, ilícita, devem ser levados em consideração os danos infligidos e os elementos qualitativos da operação cibernética em específico. Neste seguimento, aquilo que o Manual de Tallinn pretende é identificar os ciberataques armados, fazendo uma analogia aos ataques armados cinéticos ou não cinéticos, mas que a comunidade internacional descreveria como uso da força.[47]

Para resumir, todos os ciberataques que atingem o limiar de ataque armado - considerando a escala e os efeitos, de acordo com a regra 71 do Manual de Tallinn - e que sejam conduzidos ou atribuíveis a um Estado são considerados "uso da força".[48]

---

[43] "a forma mais gravosa do uso da força".
[44] 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.
[45] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 69.
[46] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 68.
[47] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 69, parág. 9
[48] Opinião dos Estados Unidos, Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 69, parág. 7.

Por sua vez, o grupo de peritos do Manual de Tallinn veio afirmar que a distinção entre os dois conceitos, ciberoperações que não são uso da força e ciberataques, levanta um quesito ainda mais importante no que concerne às ciberoperações que não são ciberataques, mas que são uso da força, pois atos "que ferem ou matam pessoas ou danificam fisicamente ou destroem objetos são usos da força"[49]. Paralelamente, estes peritos defendem que, no caso de existirem dúvidas quanto à natureza da ciberoperação, os Estados que observam as ciberoperações e os que são alvo delas ambicionarão considerá-las uso da força e, por isso, a violação de uma obrigação internacional.[50]

3.2. A imputação / atribuição do ciberataque

Um requisito importante para se determinar se uma ciberoperação pode ser qualificada como ciberataque é a questão de saber quem originou[51] o ataque, isto é, quem é o responsável pelo ciberataque.

Antes de mais, é importante perceber a duplicidade deste requisito, desde logo porque a atribuição de operações cibernéticas a um Estado facilita a qualificação dessa ciberoperação como ataque armado (o envolvimento do Estado) e, por outro lado, permite imputar a responsabilidade, por violações de obrigações jurídico-internacionais, a esse Estado.[52]

Segundo o art. 14º do Manual de Tallinn, um Estado que tem responsabilidade internacional "por um ato cibernético que é imputável ao Estado e que constitui uma violação de uma obrigação jurídica internacional"[53], tal como ocorre no contexto convencional e é sustentada pelo projeto de artigos de responsabilidade internacional do Estados por atos internacionalmente ilícitos de 2001.

Da mesma forma que no contexto tradicional, no contexto cibernético um ato internacionalmente ilícito corresponde a um ato ou uma omissão que viole uma obrigação

[49] Veja-se regra 71 do Manual de Tallinn.
[50] Esta foi uma ideia inicialmente proposta em Michael N. Schmitt, Computer Network and the Use of Force in International Law: Thoughts on a Normative Framework, 37 Colum. J. Transnat'l L. 885, 914 (1999).
[51] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 71, parág. 16.
[52] Tavares, Maria Isabel (março 2020), "Responsabilidade Internacional dos Estados Por Factos Internacionalmente Ilícitos" Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, pág. 632.
[53] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 14

jurídica internacional. Pelo que, um Estado não tem responsabilidade internacional se não violar uma obrigação jurídica internacional.

O art. 15º do Manual de Tallinn, vem afirmar que para efeitos de responsabilidade internacional 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

Posto isto, surge agora a questão de percebermos se os atos cibernéticos praticados por atores não estatais[54] podem ou não constituir um ciberataque e, por isso, permitir o recurso à legítima defesa. No caso Nicarágua, o Tribunal Internacional de Justiça veio declarar que um ataque armado pode ser entendido como não apenas incluindo a ação das forças de um Estado, mas também recorrendo à ação de forças de grupos e de indivíduos privados ou bandos armados[55], desde que o comportamento destes indivíduos possa ser assacado a um Estado.

No contexto cibernético, o Manual, apoiando-se no art.8º do Projeto de Artigos[56], afirma que um Estado é responsável por um ciberataque, se este for imputável ao Estado e constituir uma violação de uma obrigação internacional.[57] O grupo de Peritos do Manual de Tallinn reconhece ainda que uma conduta violadora de direito internacional, conduzida por órgãos estatais e não estatais, quando estão no exercício de autoridade governamental, é imputável a esse Estado.[58] A título de exemplo, as ações de empresas privadas que são autorizadas pelo governo a conduzir operações ofensivas de redes cibernéticas contra outro Estado, ou empresas privadas que se envolvem na recolha de informações cibernéticas de um Estado, podem ser atribuídas ao Estado autorizador.[59]

No direito internacional "tradicional", os atos também podem ser atribuídos a um Estado se o indivíduo ou grupo em exercício estiver a agir sob controlo direto e eficaz do

[54] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 17

[55] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 71, parag. 18.

[56]Projeto de Artigos de Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilícitos, art. 8º: "*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*".

[57] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 14.

[58] Projeto de Artigos de Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilícitos, art 4 e 5.

[59] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 15, para. 8. Ver regra 17.

Estado[60], tal como supramencionado. Os critérios de controlo efetivo devem, de acordo com o comentário ao Projeto de Artigos, ser interpretado extensivamente, ou seja, algum nível de controlo já é suficiente para atribuir os atos a um Estado. No entanto, o TIJ declarou, no caso Nicarágua, que mesmo o controlo global necessita de provas para ser um controlo eficaz, não bastando um grau elevado de dependência para ser atribuído o ato ao Estado. Já o Tribunal Penal Internacional para a ex-Jugoslávia (doravante TPIJ), no caso Tadic, apresentou um limiar inferior de controlo global, distinguindo se o conflito era ou não internacional. Mais tarde, o TIJ abordou os diferentes tipos de controlo no caso de genocídio na Bósnia, concluindo que, para efeitos de atribuição, ao abrigo do Projeto de Artigos de Responsabilidade, o controlo efetivo era o tipo e controlo exato para atribuir essa responsabilidade ao Estado.

No contexto cibernético, também há lugar ao teste do controlo global e efetivo e instruções específicas. Quanto ao controlo efetivo, é importante distingui-lo das iniciativas de cidadãos privados. Os hacktivistas lançam mão de inúmeras operações cibernéticas que não podem ser imputáveis a um Estado, a não ser que este tenha emitido instruções específicas ou dirigido ou controlado uma determinada operação. Tal como num contexto tradicional, num ataque cibernético, o auxílio dos meios de ataque para uso rebelde não será suficiente para provar controlo do grupo. Já o fornecimento de informação específica de cibervulnerabilidades será suficiente para despoletar responsabilidade internacional.

No comentário ao Projeto de Artigos de Responsabilidade Internacional, a Comissão de Direito Internacional veio afirmar que os termos "instruções", "direção" e, "controlo" devem ser entendidos e interpretados em separado. No entanto, os tribunais têm entendido que esses conceitos devem ser interpretados em conjunto, pois transmitem a mesma ideia de exercício de autoridade sobre a atividade de uma ciberoperação.[61]

Parece ainda importante esclarecer que as "instruções específicas" referidas na regra 17 do Manual de Tallinn e na regra 15, têm significados diferentes. Isto é, por um lado, a regra 15 refere-se às condutas praticadas por entidades que foram legalmente habilitadas pelo Estado e, por outro lado, a regra 17, a condutas praticadas por atores não estatais que auxiliam o Estado, como, por exemplo, quando um Estado instiga indivíduos ou grupos

[60] Um limiar que foi estabelecido no caso Nicarágua, ver regra 17 do Manual de Tallinn. Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press

[61] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 17, parág. 5 e International Law Commision, (2001),

a agir em seu nome. Deste modo, se um ator não estatal operar sobre o controlo efetivo de um Estado envolvendo-se em ciberoperações *ultra vires,* deve-se investigar se os atos *ultras vires* são "incidentais" à missão, pois o grupo internacional de peritos do Manual de Tallinn entende que se estas operações *ultras vires* forem "estranhas" à missão, não podem ser imputadas ao Estado.[62]

Cabe, ainda dentro desta responsabilidade perceber que segundo o art.7º do Projeto de Artigos, "[a] conduta de um órgão de um Estado ou de uma pessoa ou entidade habilitada a exercer elementos da autoridade governamental será considerada um ato do Estado", mesmo que esse Estado não tem autorizado essa conduta, mas deve existir um dever de diligência, previsto também no art.6º do Manual de Tallinn, onde o Estado não pode deixar que ciberataques sejam lançados através das suas infraestruturas.

É fácil percebermos que levar a cabo uma operação cibernética através de um computador ligado à rede não é complicado, de tal forma que esta pode 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.[63] Por outro lado, no que respeita ao controlo global nas operações cibernéticas, a opinião é a mesma da adotada no contexto convencional, "com enfâse para o carácter problemático da identificação dos atores envolvidos nas atividades."[64]

É fulcral não aligeirar o critério da imputação de uma conduta ilícita a um Estado, na medida em que este é de tal forma proeminente para efeitos de legítima defesa, que é o tema principal da presente dissertação. Posto isto, passa-se a analisar o facto de a operação cibernética poder parecer ter origem em infraestruturas estatais.

Quando a operação cibernética parece ter sido conduzida numa infraestrutura governamental. Ainda que, este pressuposto possa ser suficiente para admitir que esse ato seja imputável ao Estado, conforme o art. 6º do Manual de Tallinn. Do ponto de vista de que as operações cibernéticas são 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. O entendimento, no contexto cibernético, é que o facto de

[62] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra17, parág. 13.

[63] 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 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.

[64] Cf comentário à regra 31, Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press

uma ciberoperação ter sido executada através de infraestruturas governamentais de um Estado poderá ser uma indicação do envolvimento do Estado.

Desde logo, o que acontece quando uma ciberoperação é lançada através do território ou, através das infraestruturas governamentais de um Estado, mas sem que seja uma ciberoperação controlada ou conduzida por esse Estado, mas sim por exemplo por grupos terroristas.[65]

Neste caso, devemos ter em consideração o princípio da diligência devida ou princípio da obrigação de prevenção, ou seja, o Estado a partir do qual é lançado o ataque ou, simplesmente o seu território foi utilizado para lançar o ataque, tem a obrigação de impedir esse ataque e impedir que sejam violados direitos que, venham a produzir consequências irremediáveis.

Além disso, é consensual que atos ilícitos internacionais podem ser imputados ao Estado se este os reconhece e adota como seus, tal como no caso dos reféns de Terrão, pois o reconhecimento e adoção são requisitos cumulativos que precisam de constituir mais que um mero apoio.[66]

No entanto, como supramencionado, as características do ciberespaço são particulares, dado que a mera passagem de dados através da infraestrutura localizada num Estado é difícil de detetar e pode, na maioria dos casos acontecer sem que seja permitido ao Estado reconhecê-la no seu território, violando o princípio da diligência devida.

No *ciber*, todos estes pressupostos são apenas suposições pois na realidade se se for a identificar de onde é que o ciberataque ocorreu, poder-se-á identificar o Estado. Estado esse que, por sua vez, podia ter previsto que a partir do seu território estaria a ser lançado um ciberataque, mas claro, que tudo isto são meros segundos e, portanto, quase impossíveis de se detetar.

Uma operação cibernética que cause danos severos, quer a nível económico ou, por exemplo, pela interrupção significativa das funções sociais, pode ser caracterizada como ataque armado, ainda que não cause morte, ferimentos, danos ou destruição. No presente,

---

[65] [65] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 6

[66] No caso Teerão, estudantes iranianos fizeram reféns 52 diplomatas americanos, o que levou a embaixada a solicitar assistência da polícia, mas a ajuda não chegou e não foram tomadas medidas contra os estudantes, ainda lhes sendo dada aprovação pelo Estado. Portanto, o TIJ considerou os estudantes como agentes do Estado iraniano, sendo o Irão responsável pela violação de um ato ilícito internacional.Case concerning United States Diplomatic and Consular staff in Teheran

a atribuição é considerada "um luxo indisponível no ciber ataque", isto porque, "é possível prever, na maioria dos casos, que a atribuição do ataque será impossível".[67]

Em suma, a atribuição da autoria dos ciberataques é difícil, devido a três obstáculos. Em primeiro lugar, dada a existência de métodos sofisticados anónimos para esconder a entidade do atacante. Em segundo lugar, perante a possibilidade de um ciberataque ser lançado através de computadores que podem estar em qualquer parte do mundo, incluindo um país diferente do país que realmente ataca. Em terceiro lugar, tendo por base o problema de que os ciberataques ocorrem em muito poucos segundos em contraposição ao tempo que se leva para poder atribuir a autoria de um ciberataque.[68] O Manual de Tallinn dá como exemplo desta complexidade de atribuição o facto de 85000 computadores em todo o mundo serem utilizados para realizar ataques.

Existe ainda o problema da obtenção de provas e a questão relativa às normas de avaliação das mesmas.

Capítulo II: O uso da força utilizado em legítima defesa cibernética

1. Necessidade, imediatez e proporcionalidade no *jus ad bellum*

Como se apurou no capítulo anterior, esta ideia é extraída do artigo 51º da Carta das Nações Unidas, que prevê que "Nada na apresente Carta prejudicará o direito inerente à legítima defesa individual ou coletiva defesa se ocorrer um ataque armado contra um membro das Nações Unidas" [69] É consensual que o direito de legítima defesa é também de carácter consuetudinário[70], mas os seus pressupostos não estão todos "descritos ou referidos na Carta da Nações Unidas"[71].

Posto isto, parece ser consensual que este direito se estende aos ataques armados conduzidos por meios cibernéticos, uma ilação fundamentada pelo Tribunal Internacional de Justiça (TIJ) de que a legítima defesa se aplica a "qualquer uso da força,

[67] Talbot Jensen, E., (2002), *Computer Attacks on Critical National Infrastructure: A Use of Force invoking the Right of Self-defense*, Stanford Journal of International Law, p. 232 .
[68] Tsagourias, N., (2012), *Cyber attacks, self-defence and the problem of attribution*, Journal of Conflict and Security Law, Oxford University Press, p. 5.
[69] Ver art.51º da Carta das Nações Unidas
[70] 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; e Caso Caroline de 1837
[71] Azeredo Lopes, José Alberto (março 2020), capítulo I - "Uso da força e Direito Internacional", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, pág. 95

independentemente das armas utilizadas"[72], e por declarações de Estados e organizações internacionais[73].

Assim, quando um Estado é alvo de operações cibernéticas nocivas que alçam o nível de um ataque armado, "pode responder com operações cibernéticas que de outra forma constituiriam usos proibidos da força em violação do artigo 2º, nº4 da Carta das Nações Unidas e da sua contraparte de direito internacional consuetudinário"[74].

Assumindo que uma ciberoperação ultrapassa o limiar do ataque armado, o Estado vítima do ataque tem direito a responder em legítima defesa.

Ora, essa legitima defesa tem condições ou requisitos para que possa ser exercida. Estes requisitos, da proporcionalidade, necessidade e imediatez servem para determinar se a reposta em legítima defesa a um ataque cibernético não viola o princípio proibitivo do uso da força, previsto no art.2º, nº4, da CNU.

A legítima defesa, desde logo, deve ser uma resposta necessária[75] ao ciberataque, isto é, adequada e exclusivamente necessária para repelir o ciberataque, se a resposta em legítima defesa "não for adequada, nunca poderá ser considerada necessária ou proporcional"[76].

Este requisito da necessidade exige que as medidas que não implicam o uso da força, sejam insuficientes para repelir com sucesso o ciberataque e, desta forma, a solução para parar ou derrotar o ciberataque iminente ou que já esteja em andamento, é o uso da força, incluindo o ciberataque (regra 69). Significa que, o mecanismo para analisar o requisito da necessidade, no contexto cibernético, é a existência, ou a falta, de recursos alternativos que não se elevem ao nível de ataque armado, pois, se for possível repelir o ciberataque armado de forma passiva, uma resposta em "legítima defesa" que alcance o nível de ataque armado é inadmissível.[77]

---

[72] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra **71,** parag. 4.
[73] Ver, Hill, Steven (2020) - 'NATO and the International Law of Cyber Defence' in Nicholas Tsgourias and Russell Buchan, eds., Research Handbook on International Law and Cyberspace, 2ª edição
[74] Cf. article Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum, Michael N. Schmitt, pag. 244
[75] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 72
[76] Azeredo Lopes, José Alberto (março 2020), capítulo I - "Uso da força e Direito Internacional", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, pág. 95
[77] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 72, parág. 3

A necessidade como condição para o exercício de legítima defesa comporta, ainda, um critério de razoabilidade (relacionado com o requisito da imediatez), na medida em que, um Estado vítima de um ciberataque que já tenha terminado e, portanto, não esteja em curso e o Estado agressor já tenham encerrado os seus ataques, não pode responder em legitima defesa, por esta ter deixado de ser necessária.[78]

Já, o requisito da imediatez, intrinsecamente ligado ao requisito da necessidade, comporta a ideia de que uma resposta em legítima defesa imediata é uma resposta no momento imediatamente a seguir ao ciberataque. Contudo, no contexto cibernético o momento em que o ciberataque ocorre podem ser milésimos de segundos e, poder-se-á alegar que uma reposta em legítima defesa pode não ser imediata.

A imediatez da resposta em legítima defesa é calculada por um critério de razoabilidade, este período entre o ataque e a resposta, é o período necessário para que o Estado vítima possa identificar o Estado agressor e consiga preparar uma resposta.[79]

Outra questão que se levanta é o facto da legítima defesa poder continuar mesmo que o Estado já tenha terminado o ataque cibernético.[80]

Naquilo que respeita ao critério da imediatez da legitima defesa, é importante esclarecer que o critério da razoabilidade é analisado tendo em conta as circunstâncias da época, isto porque, num contexto cibernético "todos os segundos" são importantes para o caso.

Por fim, importa levantar duas outras questões relativas a este critério. A primeira relativa ao facto de que, em alguns casos saber se o ciberataque já ocorreu ou está ocorrendo é praticamente impossível, pelo que, torna-se impossível a sua defesa. Nestes casos, os danos e as consequências causadas só vêm a ser verificados muito depois do ataque. Como exemplo disto, o caso de um *worm* como o *Sutxnet*.[81]

---

[78] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 72, parág. 4

[79] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 73, parág.12

[80] o Manual de Tallinn dá como exemplo, um ciberataque que tenha começado com uma série de ciberoperações e, a resposta a essas ciberoperações (em legítima defesa) não tem, necessariamente, que cessar com o termine das ciberoperações, pois, pode ser razoável concluir que essas ciberoperações ainda não terminaram e que ainda poderão ser lançadas outras.

[81] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 73, parág.14

A outra questão levanta e relevada pelo Prof. Azeredo Lopes[82] é a questão de saber o que sucede na hipótese de o Estado vítima, tentar de boa fé resolver (pacificamente) o conflito, mas o Estado agressor não abdica do uso da força e, portanto, o Estado vítima pode ter "perdido" o seu direito à legitima defesa, por causa do requisito da imediatez. Nestes casos, o Estado vítima deve comunicar ao Conselho de Segurança, mas não perder o seu direito à legítima defesa, porque no fundo "tentou" resolver o conflito de boa fé.

A última condição para o exercício da legítima defesa é a proporcionalidade da mesma, que se refere quanto à questão da quantidade de força, incluindo o uso da força, que é permitida e considerada necessária para cessar o ciberataque.

Os peritos do Manual de Tallinn, vieram referir que este critério limita "a escala, o objetivo, a duração e a intensidade da resposta em legítima defesa"[83] àquela que é realmente necessária para fazer cessar ou repelir o ciberataque. Certo é, que o nível de força usada para repelir o ciberataque depende do contexto e no caso em concreto, pois mais força pode ser necessária ou menos força poderá ser suficiente para cessar ou repelir o ciberataque.

Outra questão é perceber se o Estado vítima de um ciberataque não for suficientemente avançado tecnologicamente para responder proporcionalmente ao ciberataque poderá responder em sede de legítima defesa convencional. Por exemplo, quando um Estado ataca ciberneticamente as infraestruturas militares de outro Estado que não tem meios para responder ciberneticamente, será que pode enviar forças militares para o Estado atacante e, dessa forma, atacar militarmente o Estado atacante? Será a resposta considerada proporcional ao ataque? Todas estas questões são de difícil resposta, mas de grande magnitude, para que se possa aplicar corretamente o direito internacional ao ciberespaço. Assim, os princípios da proporcionalidade e da necessidade considerados no contexto de ciberataques têm vindo a ser alvo de muitas discussões entre os investigadores da área do Direito.

Se não for possível alcançar uma solução razoável de um conflito através de meios pacíficos, a legítima defesa contra ciberataques satisfará o requisito da necessidade, do mesmo modo que a legítima defesa será proporcional se o Estado vítima limitar as suas

[82] Azeredo Lopes, José Alberto (março 2020), capítulo I - "Uso da força e Direito Internacional", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, pág. 98

[83] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press, regra 72, parág. 6

ações à quantidade de força necessária para parar um ciberataque em curso ou para dissuadir um futuro ciberataque.

Os princípios da necessidade e da proporcionalidade são de difícil cumprimento, mesmo num contexto convencional, quanto mais num contexto *ciber*, que apresenta novos e duros desafios ao direito internacional. Este é um pensamento que vem sido confirmado pelos autores que discordam da aplicabilidade do *Jus ad bellum* aos ciberataques. Este segmento da comunidade jurídica de direito internacional considera que as dificuldades provêm da complexidade dos ciberataques e, consequentemente, da quantidade de tempo que seria necessária para se poder atribuir a autoria de um ciberataque. Exemplos disto são os casos recentes da Estónia ou do Irão (supra elencados), onde os ataques tiveram origem em locais diferentes, até hoje, desconhecidos.

Na realidade, esta é outra das grandes preocupações desta matéria, pois sem se determinar de onde o ataque surgiu, a ciberdefesa torna-se impossível.

2. Necessidade e Proporcionalidade no *ius in bello*

Neste plano, do *ius in bello*, os princípios da necessidade e proporcionalidade militar são distintos dos requisitos da proporcionalidade e necessidade adotados no plano do *ius ad bellum*.

Estes princípios, da necessidade e proporcionalidade, referem-se às regras que as partes devem adotar num contexto de guerra, ou seja, as regras para a condução das hostilidades, mas não são aplicados "isoladamente"[84], mas em conjunto com os princípios militares da precaução e da distinção.

De maneira sucinta, pois não é este o cerne deste trabalho, a ideia de necessidade militar abrange o poder militar que é utilizado contra alvos selecionados e essenciais (princípio da distinção, humanidade e proporcionalidade) para o sucesso das ações, com o objetivo de vencer o conflito.[85] Já o princípio da proporcionalidade, no direito que rege os conflitos armados, é caracterizado, nas palavras de Isabel Tavares, pela: "ponderação

[84] Tavares, Maria Isabel (março 2020), capítulo II - "Direito Internacional Humanitário", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, pág.247.
[85] Tavares, Maria Isabel (março 2020), capítulo II - "Direito Internacional Humanitário", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto,, pág. 249.

constante entre a vantagem militar esperada e os danos colaterais que se preveem como prováveis (destruição de bens civis, ferimentos, ou morte de civis).*"*[86]

Estes princípios, servem para conduzir as hostilidades e restringir a forma e métodos de combate, durante os conflitos armados que se aplicam, também, aos conflitos armados internacionais cibernéticos.

Outra questão importante é perceber o que são danos no contexto *ciber*. Esta é uma questão que não será abordada na presente dissertação, mas que permite perceber que danos no contexto *ciber* são diferentes de outros no contexto convencional. Importa ainda realçar que danos *ciber* podem desencadear danos colaterais, diretos ou indiretos não cibernéticos, podendo ou não deixar de ser proporcionais.

Quando um ataque tem a forma de "*DoS Attack"*[87] contra um objetivo militar que interfere com os serviços de correio eletrónico civil, esta interferência não precisa de ser considerada quando se avalia se os danos causados pelo ataque são excessivos em relação ao ganho militar pretendido com o ataque. No entanto, no contexto da definição de um ataque, a privação de funcionalidade é qualificada como dano, tal como a perda da funcionalidade de infraestruturas civis. Neste caso, para o princípio da proporcionalidade são considerados danos colaterais.

Quer os efeitos diretos como os indiretos podem ser qualificados como danos colaterais, sendo esta uma consideração importante tendo em conta a natureza das operações cibernéticas.[88] Assim, não se deve considerar apenas e só os danos causados a objetos civis ou ferimentos a civis, mas também quaisquer danos ou lesões a objetos ou indivíduos que dependam das infraestruturas afetadas ou que indiretamente seriam afetados pelo ataque. Neste contexto, Michael N. Shmitt dá o exemplo de uma interferência num sistema de comunicação de uma grande área metropolitana, que poderia resultar na perturbação dos serviços de emergência, causando danos a civis previsíveis.

No que diz respeito ao cálculo da proporcionalidade de um ciberataque, é importante salientar que os danos colaterais a ser considerados são aqueles que seriam,

---

[86] Tavares, Maria Isabel (março 2020), capítulo II - "Direito Internacional Humanitário", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto,. 254

[87] Segundo a Conferência: Advances in Computing, Networking and Security, 2013 TEQIP II National Conference sobre "DoS and DDoS Attacks: Impact, Analysis and Countermeasures"
Dezembro 2013, estes ataques são caracterizados por impedir que utilizadores legítimos tenham acesso a determinado serviço.

[88] Schmitt, M. N., (2013), Cyber Activities and the Law of Countermeasures, in Peacetime Regime for State Activities in Cyberspace, Ed. Katharina Ziolkowski, International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn

razoavelmente, previstos pelos indivíduos envolvidos no mesmo, no momento em que fizeram a sua determinação de proporcionalidade.

O mesmo critério de razoabilidade é aplicado quanto à vantagem militar prevista de um ataque. Noutras palavras, "o cumprimento da regra da proporcionalidade é apreciado *ex ante*, e não *post factum"*[89].

A vantagem militar é importante para o critério da proporcionalidade, porque cria um equilíbrio entre os danos ou ferimentos e a vantagem militar para o Estado, ou seja, o facto de um ciberataque ou um ataque convencional resultar em danos colaterais excessivos em relação a um eventual ataque militar não torna o ataque ilícito, desde que razoável nas circunstâncias do caso concreto.

Finalmente, deve ser advertido que o DIH não define expressamente o termo "excessivo", pelo que, tem vindo a ser sugerido que danos colaterais extensos são, necessariamente, excessivos. Por um lado, se um ciberataque causar apenas danos ou ferimentos ligeiros, mas acumular pouca vantagem militar, pode violar a regra da proporcionalidade. Por outro lado, um ciberataque pode causar danos ou ferimentos significativos, mas não violar a regra da proporcionalidade, desde que alcance uma vantagem militar grande.[90] Posto isto, poder-se-á, com muitas restrições, concluir que um Estado vítima de um ciberataque pode responder em legítima defesa através de um outro ciberataque, se este lhe for proporcional.

Já, no que concerne ao princípio da distinção, também muito importante, neste plano do *ius in bello*.

Este princípio vem distinguir aquilo que é militar num conflito armado, ou seja, quais são os objetivos que podem ser intersetados (objetivos militares), dos objetivos que não podem (objetivos civis). Esta distinção é importante, na medida em que os alvos civis gozam de imunidades de ataques, isto significa que os alvos civis não podem ser alvo de direto de ataque e, em consequência disso, os civis também não podem "pegar em armas" durante um conflito, caso contrário, poderão ser julgados por crimes.[91]

---

[89] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press

[90] Comentário de 1987 - Protocolo Adicional às Conveções de Genebra de 12 de Agosto de 1949 Relativo à Proteção das Vítimas dos Conflitos Armados Internacionais (Protocolo I), 8 Junho 1977, https://ihldatabases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=F906C75AE929B32DC12563CD0043434F

[91] Nomeadamente pelos crimes internacionais previstos no Estatuto de Roma do Tribunal Penal Internacional

Em suma, percebemos que os critérios da necessidade e da proporcionalidade nos dois planos (do *ius ad bellum* e no *ius in bello*), embora sejam diferentes, podem trazer uma certa aproximação que poderá ser confusa, mas que é certamente diferente.

3. A natureza da legítima defesa contra ciberataques

No decurso da história do ciberespaço, a legítima ciberdefesa tem sido a resposta utilizada no confronto com o uso da força no ciber equivalente a um ataque armado, ou seja, um ciberataque.

No entanto, existe a possibilidade de os Estados reagirem em ciberdefesa, sem que haja um ataque armado cibernético, quando a esta afirmação, temos o exemplo dos atentados do 11 de setembro de 2001, onde os Estados Unidos consideraram que podiam reagir contra os ataques em legítima defesa, quer fosse ou não um ataque armado típico.

A verdade é que o desenvolvimento da tecnologia militar põe em risco esta presunção de que a um ciberataque apenas se pode responder com uma legítima defesa cibernética.

Mas e, se for lançado um ataque armado tradicional, poderá o Estado vítima responder em legítima defesa cibernética? E se, por outro lado, for lançado um ciberataque, poderá o Estado vítima responder em legítima defesa tradicional? O grupo de peritos do Manual de Tallinn responde a estas questões de forma positiva, pois consideram que o direito inerente de legítima defesa se aplica tanto a ataques armados tradicionais como a ciberataques, não havendo necessidade de que o ataque em legítima defesa tenha a mesma natureza.[92]

Não obstante as armas nucleares serem de natureza cinética, ao contrário da natureza não cinética dos ciber ataques, o raciocínio do TIJ no seu parecer consultivo sobre armas nucleares é relevante, uma vez que tanto a guerra nuclear como a guerra cibernética envolvem tecnologia militar não tradicional. Neste sentido, o TIJ veio afirmar que o uso de armas nucleares em legítima defesa não está excluído do catálogo de hipóteses, podendo ser lícito ao abrigo do direito internacional, dado que o uso da força será proporcional e satisfará os requisitos do DIH.[93] Ora, da mesma forma que o TIJ concluiu para a questão das armas nucleares, poder-se-á argumentar que, no caso de um cibe

[92] Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press regra 71, parág. 4 e regra 71 parág. 6.
[93] *Legality of the Threat or Use of Nuclear Weapons,* Advisory Opinion of 8 July 1996, I.C.J. Reports 1996, para. 42.

ataque, a resposta em legítima defesa pode ser cibernética, desde que, proporcional e de acordo com o DIH.

Autores como, por exemplo, Larry May, vieram questionar se na legítima defesa como resposta a um ciber ataque deve ser sempre permitido envolver a morte ou ferimento de pessoas[94], se se tratar uma legítima defesa proporcional. Este raciocínio é fácil de ser abalado, pelo simples motivo de que não seria proporcional o ferimento ou morte de pessoas como resposta à destruição de bens, mesmo que em grande escala e abrangente. Deste modo, os peritos do Manual de Tallinn concluíram que a legítima defesa pode constituir uma natureza cinética ou cibernética, desde que seja proporcional ao ataque.

Capítulo III: A Ciberdefesa no século XXI

Nos dias de hoje, falar em ciberdefesa já é mais comum e menos estranho do que no início do século, quando os conceitos de segurança e defesa não eram associados ao ciberespaço. Na verdade, foi após o 11 de setembro de 2001 que as ameaças não tradicionais começaram a ser tratadas com outra prioridade, de maneira a serem incluídas nas estratégias de defesa dos próprios Estados.

Com os diversos acontecimentos da história do ciberespaço, como os ciberataques da Estónia e da Geórgia, demonstrou-se a necessidade de desenvolver novos mecanismos de ciberdefesa, contra este tipo de ameaças. Assim, o ciberespaço, reconhecido já como um domínio operacional, permitiu aos Estados desenvolver programas de estratégias de ciberdefesa nacional. No entanto, ainda nem todos os Estados têm capacidades cibernéticas ofensivas. Daqui se percebe que a cooperação internacional desempenha um papel importante no combate às ciberameaças e aos possíveis ciberataques.

O papel das Organizações Internacionais é o de coordenação, discussão e o desenvolvimento de propostas e estratégias para a criação de estruturas, instituições e definição de políticas, enquanto o trabalho dos Estados, em concreto, passa pela ciberdefesa. As funções das OI variam,

> Desde o estabelecer de normas ou princípios que previnam o uso malicioso de ciber-tecnologias, à correção ou alteração dos acordos existentes no âmbito dos quais são definidos, entre outros, o conceito de conflito armado e a respetiva

[94] May, L., (2015), *The Nature of War and the Idea of "Cyberwar"*, in *Cyberwar, Law and Ethics for Virtual Conflicts*, Eds. Ohlin, J. D., Govern, K., Finkelstein, C., Oxford University Press, pp. 6-9.

> aplicação da lei. Podem ainda promover a prevenção e preparação dos Estados para recuperarem de um ciberataque.[95]

Diversos Estados já expressaram os seus pontos de vista sobre a legítima defesa como resposta a um ciberataque. Efetivamente os Estados Unidos, o Reino Unido e a Rússia mostraram-se favoráveis à possibilidade de responder a ciber ataques utilizando a força. Porém, não é razoável exigir que, à data de hoje, todos os países se tenham expressado sobre esta matéria. Por outro lado, parece ser razoável que apenas os Estados afetados ou com maior poder e influência nestas questões dominam a matéria. Portanto, neste caso dos ciberataques, apenas aqueles países que se desenvolveram militarmente em âmbitos informáticos facilitarão o desenvolvimento do direito consuetudinário nestas matérias.

Tanto a NATO como a UE [96]têm trabalhado para uma fortificação deste tema. O problema, desde logo, é a falta de recursos militares cibernéticos dos países e, portanto, da desigualdade que um conflito internacional cibernético poderá causar. Não obstante estas dificuldades, até ao momento foram criadas, dentro destas organizações internacionais, diversas instituições, e até mesmo organismos dentro do governo de alguns países da UE, para se possa estudar e desenvolver esta matéria da legítima defesa no ciberespaço.

Outro problema que não permite chegar a um consenso e incrementar novas normas neste âmbito é a falta de exemplos práticos, pelo que a grande maioria dos incidentes cibernéticos não chegam ao limiar de ataque armado. Por isso, os advogados internacionais da NATO tiveram que pensar num quadro jurídico para responder a operações cibernéticas ou ciberoperações em tempos de paz.

Deste modo, a NATO desenvolveu recentemente um guia que estabelece instrumentos para responder a atividades cibernéticas maliciosas. No entanto, o mesmo não é publico, o que impossibilita a sua avaliação e credibilização.[97] Esta organização desenvolveu ainda um fórum, onde se pode coordenar múltiplas respostas a esta questão,

---

[95] UNIDIR (2013) -The Cyber Index: International Security Trends and Realities, Genebra: UNIDIR, Disponível em http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf, consultado em fevereiro de 2021

[96] Ver as "Conclusões do Conselho sobre a implementação da Declaração Conjunta do Presidente do Conselho Europeu, do Presidente da Comissão Europeia e do Secretário-Geral da Organização do Tratado do Atlântico Norte": https://data.consilium.europa.eu/doc/document/ST-15283-2016-INIT/pt/pdf

[97] Hill, Steven (2020) - 'NATO and the International Law of Cyber Defence' in Nicholas Tsgourias and Russell Buchan, eds., Research Handbook on International Law and Cyberspace, 2ª edição, p.13.

de forma a perceber qual é a opinião dos Estados envolvidos, tentando, desta forma, chegar a uma possível resolução do problema, o que, contudo, parece utópico.

Este fórum foi criado, também, com o objetivo de, no caso de um incidente cibernético, os Estados solicitarem a assistência da NATO para resolver o conflito. Já no caso de um incidente grave, uma opção seria "solicitar consulta" ao abrigo do artigo 4º do Tratado do Atlântico Norte, onde se prevê que "as Partes consultar-se-ão em conjunto sempre que, na opinião de qualquer delas, a integridade territorial, a independência política ou a segurança de qualquer uma das Partes esteja ameaçada". Certo é que este artigo apenas foi chamado em um par de situações que nada tinham a ver com a ciberatividade.

A verdade é que a NATO veio afirmar que não é necessário utilizar o Artigo 4º para que possa tomar medidas para lidar com um determinado incidente. Todavia, uma atuação da NATO face às futuras respostas a ciberoperações "abaixo do limiar de ataque armado" pode dar asas a outros problemas do direito internacional. Uma das questões é se os Estados estarão dispostos a considerar esta organização como um meio eficaz para conduzir uma legítima defesa coletiva ou contramedidas.

Na perspetiva de Steven Hill "a evolução da política cibernética da NATO ao longo de mais de duas décadas tem sido um excelente exemplo de adaptação da Aliança a novas ameaças."[98] Neste sentido, importa perceber que novos desafios pode a NATO esperar da futura política da Ciberdefesa.

O futuro da política de ciberdefesa da NATO continuará a ser moldado à medida que novas ameaças e, talvez, um verdadeiro ciberataque, surjam. Deste modo, a NATO procura reforçar ainda mais a ciberdefesa dos seus aliados em coletivo e de cada um na individualidade, dissuadindo as atividades cibernéticas dirigidas contra si e os seus aliados, e sendo capaz de responder a futuros incidentes.

A NATO prevê ainda, com o avanço tecnológico e a continua preparação cibernética militar dos países, que o futuro ambiente de ameaça cibernética seja mais intenso e problemático, parecendo certa de que os Estados Aliados continuarão a respeitar o direito internacional e que o problema serão os outros autores do sistema internacional, tanto estatais como não estatais.

[98] Hill, Steven (2020) - 'NATO and the International Law of Cyber Defence' in Nicholas Tsgourias and Russell Buchan, eds., Research Handbook on International Law and Cyberspace, 2ª edição, p. 14.

A NATO acentua, ainda a necessidade de os Estados Aliados continuarem o seu diálogo legal em curso sobre estas questões, como por exemplo o limiar de ataque armado e de ciberataque, prevendo e discutindo possíveis formas ou técnicas de resposta.

Por fim, e porque não podia deixar de ser referido, Portugal, desde 2014, assumiu no âmbito da UE e da NATO a liderança de um projeto *Smart Defence* da NATO e depois a *Disciplina de Ciberdefesa* da União Europeia (em coliderança com a França). Já em 2018, na Cimeira de Bruxelas, a NATO aprovou a transferência, para Oeiras, da Escola de Comunicações e Sistema de Informação da NATO, sediada anteriormente em Itália, como um estímulo essencial, para que Portugal assuma uma posição destacada na vanguarda do ensino e da formação nos domínios da ciberdefesa.[99]

Atualmente, no Centro de Ciberdefesa Nacional estão em curso várias iniciativas e projetos, dos quais um plano de *dinamização da capacidade de ciberdefesa*, "que visa o aumento da capacidade de ciberdefesa nacional, ao nível dos recursos humanos e dos meios, e tem um prazo de implementação de três anos (2019 a 2021)."[100]

[99] Cf. site da Defesa Nacional - Centro de Ciberdefesa:
https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/projetos/Paginas/default.aspx
[100] Defesa Nacional, República Portuguesa:
https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/centro/Paginas/default.aspx

Conclusão

Durante a investigação da presente dissertação foi possível chegar a algumas conclusões.

A melhor forma para se compreender legalmente o termo de ciberataque é através da análise da definição estabelecida no Manual de Tallinn, onde se afirma que uma ciberoperação, seja ela ofensiva ou defensiva, mas em que sejam previsivelmente causadas lesões ou mortes de pessoas, ou danos graves ou destruição de objetos, é considerada um ciberataque.

Certo é que está definição não é concludente e deve ser aperfeiçoada, mas a verdade é que nem a definição de ataque armado no direito internacional é pacífica. Ora, um ciberataque poderia atingir o limiar de ataque armado com *escala e efeitos* graves, pelo que, dessa forma, o direito inerente à legítima defesa seria desencadeado. No entanto, a legítima defesa tem vários requisitos que têm de se verificar para que o Estado vítima possa fazer uso da mesma, não bastando a verificação de um ciberataque como um ataque armado.

Outro requisito que, também está intrinsecamente ligado à definição de ciberataque é a exigência de atribuir um ciberataque a um Estado. Quanto a este requisito, concluímos que existem ainda demasiadas dificuldades técnicas que não permitem uma atribuição clara e sem lacunas. Além disso, existe uma enorme falta de consenso em relação a estas questões, que podem constituir um problema durante quaisquer tentativas de negociação.

Para além destes requisitos, existem ainda, as condições para o exercício de legítima defesa: a necessidade, proporcionalidade e imediatez, que vieram mostrar que, a *escala e os efeitos* de um ciberataque sejam equiparados a um ataque armado para efeitos do art. 51º da CNU e, portanto, desencadeiem o direito à legítima defesa individual do Estado vítima, estes requisitos serão difíceis de cumprir no contexto cibernético.

Por fim, com o estudo deste tema percebemos que a falta de consenso em todas estas questões impede o desenvolvimento do direito internacional no contexto do ciberespaço. Talvez só quando um caso real de ciberataque seja considerado como tal, o direito internacional comece a tomar novas medidas.

No seu conjunto, parece que a CLI (*Cyber Law International*), a ONU e a NATO têm feito esforços para clarificar e fazer evoluir o direito internacional na ciberdefesa, a

fim de responder sem grandes ambiguidades se os ciberataques podem desencadear o direito à autodefesa ao abrigo da Carta das Nações.

Bibliografia

Doutrina

Andrew Griffin, Sony hack: who are the Guardians of Peace, and is North Korea really behind the attack? "The Independent", 17 de dezembro de 2014. Em linha: http://www.independent.co.uk/life-style/gadgets-and-tech/news/sony-hack-who-are-the-guardians-of-peace-and-is-north-korea-really-behind-the-attack-9931282.html.

Arimatsu, L., (2012), *A treaty for governing cyber-weapons: Potential benefits and practical limitations,* 4th International Conference on Cyber Conflict (CYCON), Eds. Czosseck, C., Ottis, R., Ziolkowski, K., NATO CCD COE Publications, Tallinn.

Azeredo Lopes, José Alberto (março 2020), capítulo I - "Uso da força e Direito Internacional", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, pág. 8- 211

BADR, GAMAL MOURSI (1980) The Exculpatory Effect of Self-Defense in State Responsibility, Georgia Journal of International and Comparative Law, Issue 1, Vol. 10. http://digitalcommons.law.uga.edu/gjicl/vol10/iss1/2

Comentário de 1987 - Protocolo Adicional às Conveções de Genebra de 12 de Agosto de 1949 Relativo à Proteção das Vítimas dos Conflitos Armados Internacionais (Protocolo I),8Junho1977, ICRC, https://ihldatabases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=F906C75AE929B32DC12563CD0043434F

Conforti, Benedetto, 2014, X edizione, diritto internazionale, Editoriale Scientifica, Napoli

Corn, Gary (fev. 2020) - Punching on the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses https://www.justsecurity.org/68622/punching-on-the-edges-of-the-grey-zone-iranian-cyber-threats-and-state-cyber-responses/

Corn, Gary (s.d) - Covert Deception, Strategic Fraud, and the Rule of Prohibited Intervention, A Hoover Institution Essay

Corn, Gary (set. 2020) – Cyber Operations and the imperfect art of "translating" the law of war to new technologies, network Cyber

Cyber and International Law in the 21st Century, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century, consultado em fevereiro de 2021

Cyber Attacks and the Roles the Military Can Play to Support the National Cyber Security Efforts: https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/v42n3%204%20Cyber%20Attacks%20and%20the%20Roles%20the%20Military%20can%20play.pdf, consultado em fevereiro de 2021

Della Morte, Gabriele, (2019) Big Data e Protezione Internazionale Dei Diritti Umani, Regole e Conflitti, Editoriale Scientifica, Napoli

Dinstein, Y., (2002), *Computer Network Attacks and Self-Defense*, International Law Studies Series US Naval War College

Falliere, N., Murchu O. L., Chien, E., (2011), *W32 Stuxnet Dossier*, Symantech, version 1.4, available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf., consultado em novembro de 2020

Finlay, Lorraine e Payne, Christian, (2019) – "the attribution problem and cyber armed attacks", Symposium on cyber attribution

Forrest, Craig J.S. (2007)- The Doctrine of Military Necessity and the Protection of Cultural property During armed conflicts, California Western International Law Journal, Volume 37, number 2

Gill, T. D., & Ducheine, P. A. L. (2013). Anticipatory Self-Defense in the Cyber Context. International Law Studies (Naval War College), 89, 438-471. http://www.heinonline.org/HOL/Page?handle=hein.intyb/ilsusnwc0089&collection=intyb&index=intyb/ilsusnwc456&id=456

Harrison Dinnis, H, (2012), *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge.

Hattendorf, John B., "U.S Naval Strategy in the 1990's" (2006). Newport Papers. 27. https://digital-commons.usnwc.edu/usnwc-newport-papers/27

Hill, Steven (2020) - 'NATO and the International Law of Cyber Defence' in Nicholas Tsgourias and Russell Buchan, eds., Research Handbook on International Law and Cyberspace, 2ª edição: http://www.ispionline.it/sites/default/files/pubblicazioni/commentarymelemoro.pdf., consultado em janeiro de 2021

International Law Applied to Operations in Cyberspace: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf, consultado em fevereiro de 2021

International Law Commision, (2001), Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, disponível em: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001 .pdf;

Jensen, Eric Talbot e Watts, Sean (s.d.)- Due Diligence and the US Defend Forward Cyber Strategy, A Hoover Institution Essay

Letter to the parliament on the international legal order in cyberspace, https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace, consultado em fevereiro de 2021

Locatelli, Andrea (October 2013) - The Offence/Defence Balance in Cyberspace, ISPI Analysis No. 203

May, L., (2015), *The Nature of War and the Idea of "Cyberwar"*, in *Cyberwar, Law and Ethics for Virtual Conflicts*, Eds. Ohlin, J. D., Govern, K., Finkelstein, C., Oxford University Press, pp. 6-9.

Mele Stefano, Francesco N. Moro, (25 setembro 2015) - Cyber security: un fronte sempre più caldo, ISPI Commentary,

Michael Cieply, Brooks Barnes, Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm, "The New York Times", 30 dez. 2014 http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisanceswiftly-grew-into-a-firestorm-.html

Ortega Carcelén, Martín, (2014), Derecho Global, Derecho Internacional Público en la Era Global, tecnos editora, pág. 40-58

Ralph Langner, What STUXNET is All About, 10 de maio de 2011. Em linha: http://www.langner.com/en/2011/01/10/what-stuxnet-is-all-about/.

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

Schmitt Michael, (1999) - Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, "Columbia Journal of Transnational Law", Vol. 37, pp. 885-937.

Schmitt Michael, (2003) - Preemptive Strategies in International Law, "Michigan Journal of International Law", Vol. 24, pp. 513-548.

Schmitt Michael, (2008) - Responding to Transnational Terrorism Under the Jus Ad Bellum: A Normative Framework, "Naval Law Review", Vol. 56, pp. 1-42.

Schmitt Michael, (2014) - The Law of Cyberwarfare: Quo Vadis?, "Stanford Law & Policy Review", Vol, 25, No. 2, pp. 269-300.

Schmitt, M. N., (2013), *Cyber Activities and the Law of Countermeasures*, in *Peacetime Regime for State Activities in Cyberspace*, Ed. Katharina Ziolkowski, International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn

Schmitt, Michael N. (2012) – " Attack"as term of art in international law: the cyber operations context, 4ª Conferência Internacional de ciber Conflitos, US Naval War College

Schmitt, Michael N. (2017) - "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", s.l., Cambridge University Press

Schmitt, Michael N. (2017) - Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum, HeinOnline

Talbot Jensen, E., (2002), Computer Attacks on Critical National Infrastructure: A Use of Force invoking the Right of Self-defense, Stanford Journal of International Law

Tams, Christian J. (2009)- The Use of Force against Terrorists, EJIL, Vol. 20, No. 2, p. 359-397

Tavares, Maria Isabel (2015) - "Guerra e Responsabilidade" – A intervenção militar no Iraque em 2003, Publicações Universidade Católica Porto, pp. 138-139.

Tavares, Maria Isabel (março 2020), "Responsabilidade Internacional dos Estados Por Factos Internacionalmente Ilícitos" Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, p.631- 732

Tavares, Maria Isabel (março 2020), capítulo II - "Direito Internacional Humanitário", Azeredo Lopes, José Alberto (Coord.) - Regimes Jurídicos Internacionais, Volume I, Universidade Católica Editora Porto, p.213- 279

Trapp, K. N., (2007), *Back to basics: necessity, proportionality, and the right of self-defence against non-state terrorist actors*, International and Comparative Law Quarterly

Tsagourias, N., (2012), Cyber attacks, self-defence and the problem of attribution, Journal of Conflict and Security Law, Oxford University Press

UNIDIR (2013) -The Cyber Index: International Security Trends and Realities, Genebra: UNIDIR, Disponível em:http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf, consultado em fevereiro de 2021

Legislação, Jurisprudência e Documentos Oficiais

Carta das Nações Unidas, 1945

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

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, I.C.J. Reports 1996.

Projeto de Artigos de Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilícitos (2001)

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

Protocolo Adicional às Conveções de Genebra de 12 de Agosto de 1949 Relativo à Proteção das Vítimas dos Conflitos Armados Internacionais (Protocolo I)

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

República da Estónia - Declaração do Ministro dos Negócios Estrangeiros (Governo da República da Estónia, 1 de Maio de 2007) https://valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia

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

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)" disponível em: www.fd.unl.pt/docentes_docs/ma/TMA_MA_4615.doc;

The Corfu Channel Case, Reports of Judgments, Advisory Opinion and Orders, 9 de Abril de 1949