UNIVERSIDADE CATÓLICA PORTUGUESA

A Imputação de Ataques Ciber aos Estados
Estudo de Caso : IT ARMY

Joana Isabel Aragão Pires

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2023

UNIVERSIDADE CATÓLICA PORTUGUESA

A Imputação de Ataques Ciber aos Estados
Estudo de Caso : IT ARMY

Joana Isabel Aragão Pires

Orientadora : Maria Isabel Tavares

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2023

Agradecimentos

A presente dissertação é prol de grande perseverança, esforço e dedicação. E o alcance deste capítulo não teria sido possível sem a colaboração e suporte de algumas pessoas em especial. Por esta razão, quero aproveitar para agradecer :

À minha Orientadora e Professora Maria Isabel Tavares, pelo acompanhamento prestado no âmbito desta dissertação. Por todas as correções e sugestões construtivas que foram fundamentais para todo o processo de investigação.

Aos meus pais, que são os meus pilares e guiam-me sempre pelo caminho certo. São a minha inspiração e motivação constante. Por todo o amor incondicional, paciência e constantes incentivos que me transmitem. Por me darem asas para ir atrás dos meus sonhos. Com vocês, sonhar é fácil e concretizar é possível. Sou-vos eternamente grata!

Às minhas irmãs, que são grandes exemplos para mim. Pelo apoio, força e incentivo sem igual que me dão. Por acreditarem em mim e encorajarem-me desde sempre a dar o meu melhor em tudo que faça.

À minha sobrinha, pelos miminhos e abraços que me enchem o coração. Quando ela crescer, espero que veja em mim um belo e grande exemplo.

À minha avó materna, pelos valores e princípios que me ensinou durante a vida. O meu anjo da guarda, não estando mais presente fisicamente permanecerá eternamente no meu coração. E espero que esteja orgulhosa das minhas conquistas.

Resumo

Este trabalho investiga a temática da imputação de ataques ciber aos Estados. Neste caso analisou-se especificamente o caso do IT ARMY e de que forma será possível imputar os seus ciberataques ao Estado da Ucrânia.

A imputação e a clarificação dos limites da imputação funcional são parâmetros muito importantes nas relações entre Estados. E existem atividades que até recentemente eram executadas somente pelo próprio Estado que hoje são executadas por agentes privados.

Pensa-se que o IT ARMY é uma organização composta por indivíduos de todo o mundo ligados em rede através do Telegram, e pensa-se que essa rede é controlada pelo Ministério da Defesa Ucrâniano, que dispõe os alvos e as ações a serem executadas pelos vários membros deste grupo.

O IT Army é estudado para identificar o que é esta organização, quem faz parte, e de que maneira atuam. De seguida, fez-se um enquadramento da dimensão ciber dos conflitos. Para focar depois na imputação dos ataques. É então que este trabalho desenvolve o processo de imputação funcional bem como os comportamentos de direção e controlo, tão importantes na imputação funcional. Por fim, foram apresentadas perspetivas futuras para uma evolução no processo de imputação funcional no universo ciber.

Palavras-chave: IT ARMY ; Imputação ; Direito Internacional Humanitário ; PARI ; Manual de Tallin ; Controlo Global ; Controlo Efetivo.

Abstract

This work investigates the theme of attributing cyber attacks to States. In this case, the specific analysis was conducted on the IT Army and how it is possible to attribute cyber attacks to the State of Ukraine.

Attribution and clarification of the boundaries of functional attribution are very important parameters in State relations. There are activities that were, until recently, solely performed by the State but are now carried out by private agents.

It is believed that the IT Army is an organization composed of individuals from around the world connected through the Telegram network, and it is thought that this network is controlled by the Ukranian Ministry of Defense, which assigns targets and actions to be carried out by various members of this group.

The IT Army is studied to identify what this organization is, who is involved, and how they operate. Next, the cyber dimension of conflicts is framed, with a focus on attributing cyberattacks. It is at this point that this work develops the process of functional attribution, as well as the behaviors of direction and control, which are crucial in functional attribution. Finally, future perspectives for an evolution in the process of functional attribution in cyber universe were presented.

Keywords: IT Army ; Attribution ; International Humanitarian Law ; PARI ; Tallinn Manual ; Global control ; Effective control.

Lista de Siglas e Abreviaturas

c. - *Contra*

CCDCOE – *Cooperative Cyber Defence Centre of Excellence*

Col. – Coluna

DDoS – Ataque de Navegação de Serviço

Ed. – Editor

NATO/OTAN – Organização do Tratado do Atlântico Norte

N.d. – *No date*, sem data

p./ pp. – página / páginas

Par – Parágrafo

PARI – *Projet d'Articles sur la Responsabilité de l'État pour Fait Internationalement Illicite*

TIJ – Tribunal Internacional de Justiça

TPEJ – Tribunal Penal Especial de Justiça

U.C.L.A – University of California Los Angeles

URSS – União das Repúblicas Socialistas Soviéticas

Vol. – Volume

Índice

1. Introdução

Este documento é o resultado final de mestrado que tem por objetivo estudar o Direito Internacional. Este trabalho vai incidir especificamente sobre o regime jurídico da responsabilidade internacional do Estado por factos internacionalmente ilícitos [1].

O objetivo deste trabalho de final de mestrado é analisar e desenvolver especificamente o problema inicial: é possível imputar os ciberataques perpetrados através do IT Army em específico, ao Estado da Ucrânia? Para chegar a essas conclusões vou usar duas ferramentas essenciais, o *Projet d'Articles sur la Responsabilité de l'État pour Fait Internationalement Illicite* ou PARI, com comentários e o *Manual de Tallinn*. O PARI apresenta-se num documento de 2001, mas editado pelas Nações Unidas e publicado em 2005. Será usado também o *Manual de Tallinn 2.0*, ou seja, em segunda edição [2] .

O instrumento jurídico de estudo aqui enunciado, que se pode traduzir como "Projeto de Artigos sobre a Responsabilidade Internacional do Estado" ou PARI, foi adotado pela *International Law Comission* e por diferentes países em 2001. Este projeto foi classificado por Eichensher como «the most authoritative treatment of state responsability»[3].

O PARI é um conjunto de diretrizes que pretende regular as consequências jurídicas da comissão de um acto internacionalmente ilícito entre Estados. Neste trabalho foram utilizados os Artigos 4, 5 e 8 do PARI, bem como o Artigo 2º.

Tavares em 2020 afirmou que o PARI não foi aceite como uma convenção internacional, mas Portugal tem uma posição altamente favorável a «uma convenção

[1] Tavares, M. I. (2020). Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilícitos Fechar o Círculo. In *Regimes Jurídicos Internacionais* (Vol. 1, p. 632). Universidade Católica Editora Porto. Caso do TIJ, Barcelona Traction, Light and Power Company Limited (Bélgica c. Espanha), Col., 1979, P.33, PAR.36. In *Regimes Jurídicos Internacionais Questões, Casos e Materiais*, (Vol. 2, p. 606). Universidade Católica Editora Porto.

[2] Nations Unies. (2005). *Projet d'Articles Sur La Responsabilité de l'État Pour Fait Internationalement Illicite.* Nations Unies. https://legal.un.org/ilc/texts/instruments/french/draft_articles/9_6_2001.pdf; Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. Cambridge University Press.

[3] Eichensehr, K. E. (2020). The Law and Politics of Cyberattack Attribution. *U.C.L.A. Law Review*, *520*, p.562. Tradução: «O tratamento mais autoritário da responsabilidade do Estado».

sobre esta matéria» [4]. Esta autora mostrou reservas quanto à utilização do PARI como uma convenção internacional [5].

O *Manual de Tallinn* é o manual que o organismo *The Nato Cooperative Cyber Defense Centre of Excellence* desenvolveu (vai na 3ª edição) e vou usar a versão de 2017 (2ª edição), porque é a última edição a estar disponível ao público. Este Manual não tem estatuto jurídico obrigatório [6].

O *Manual de Tallinn* é uma pedra angular no Direito Internacional, porque é a adaptação do Direito Internacional ao ambiente cibernético. Esta adaptação foi um verdadeiro desafio para os Estados. O Direito Internacional não foi desenvolvido com as tecnologias de informação e comunicação do século XXI no seu âmago. Mas, de qualquer forma, Schmitt avisou que algumas nações, como os Estados Unidos da América já defendiam, no início da década de 2010, que o Direito Internacional podia ser adaptado às caraterísticas do ambiente cibernético. Neste trabalho foram utilizadas as Regras 15 e 17 do *Manual de Tallinn* para discutir a imputação funcional e as Regras 71 e 92 para ajudar nos argumentos utilizados.

«I believe that the application of international law to State conduct in the digital domain can serve as a bedrock for peace and security, as it does in all other domains, because technology advances have no bearing on the underlying legal principles» [7]. Esta é a visão de Koenders, à data, Ministro dos Negócios Estrangeiros dos Países Baixos. Em 2017, Koenders teve uma visão clara. O facto de o Direito Internacional ter sido desenvolvido sem as tecnologias da informação e comunicação do século XXI não invalida a utilidade do Direito Internacional também no domínio cibernético. Na

[4] Tavares, M. I. (2020). Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilícitos Fechar o Círculo. In *Regimes Jurídicos Internacionais*, (Vol. 1, p. 634). Universidade Católica Editora Porto. Veja-se um excerto da posição de Portugal, na 71ª Sessão, na Ata do 9º Encontro, 6ª Comissão ocorrido na sexta-feira, 7 Outubro de 2016 às 15h00. In *Regimes Jurídicos Internacionais Questões, Casos e Materiais*, (Vol. 2, pp. 618-619). Universidade Católica Editora Porto.

[5] Tavares, M. I. (2020). Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilícitos Fechar o Círculo. In *Regimes Jurídicos Internacionais*, (Vol. 1, p. 634). Universidade Católica Editora Porto.

[6] The NATO Cooperative Cyber Defense Centre of Excellence (n.d.). *The Tallinn Manual*. CCDCOE. Consultado a 19 de julho de 2023 de https://ccdcoe.org/research/tallinn-manual/

[7] Koenders, B. (2017), Foreword. In M. N. Schmitt (Ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed. p. XXVI). Tradução da autora: «Eu acredito que a aplicação do Direito Internacional à conduta do Estado no domínio digital pode servir como um leito de rocha firme para a paz e a segurança, tal como faz em todos os outros domínios, porque os avanços tecnológicos não têm influência nos princípios legais subjacentes».

realidade, é uma simples questão de desenvolvimento e adaptação, como o *Manual de Tallinn* tem mostrado.

Lopes mostra como evoluíram, ao longo dos tempos, os diferentes conceitos de uso da força, agressão, ataque armado, entre outros. E mostra também que o *Manual de Tallinn* está a gerar bastante consenso na forma como o Direito Internacional pode ser usado no ambiente ciber. Para Lopes, o *Manual de Tallinn* estabelece «uma relação umbilical entre operações ciber e não-ciber» [8].

A imputação funcional é um conceito importante no contexto do Direito Internacional. Este conceito refere-se à atribuição de responsabilidade a um Estado ou entidade por ações ou omissões de um indivíduo ou de um grupo de indivíduos que atua em nome do Estado. Logo, quer a imputação funcional quer a clarificação dos limites da imputação funcional são assuntos muito importantes. A sua importância baseia-se no facto de que se vive num mundo que se move muito mais rapidamente que o planeta gira por si próprio, e existem atividades que até recentemente eram executadas somente pelo próprio Estado que hoje são executadas por agentes privados. Tavares, em 2020, afirmou que o exercício de poderes públicos está a ser contratado fora do próprio Estado, e a utilização das tecnologias de informação e comunicação do século XXI faz com que seja muito mais difícil considerar a conduta de organizações privadas que cumprem funções públicas como agentes do próprio Estado [9].

É do conhecimento comum que a Ucrânia dispõe de uma organização composta por indivíduos de todo o mundo ligados em rede através do Telegram, e pensa-se que essa rede é controlada pelo Ministério da Defesa Ucrâniano. Pensa-se que é o Estado ucraniano que dispõe os alvos e as ações a serem executadas pelos vários membros do grupo denominado como IT Army.

A questão que instiga este trabalho é a seguinte : Serão as operações cibernéticas, executadas por pessoas de todo o mundo, que se pensa serem o IT Army, atribuíveis ao Estado ucrâniano? Esta pergunta gera uma pergunta mais aberta de contextualização: Quais são os problemas de imputação que se podem identificar neste caso específico?

---

[8] Lopes, J. A. (2020). Uso da Força e Direito Internacional Direito em Tempos de Cólera. In *Regimes Jurídicos Internacionais* (Vol. 1, p. 89). Universidade Católica Editora Porto.

[9] Tavares, M.I. (2020). Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilícitos Fechar o Círculo. In *Regimes Jurídicos Internacionais,* (Vol. 1 p. 642). Universidade Católica Editora Porto.

A estrutura deste trabalho divide-se em 5 pontos. Nesta introdução foi feita uma apresentação sobre o conteúdo que constrói este trabalho e sobre algumas das ferramentas que foram usadas. O segundo capítulo explica o que se pensa que se sabe sobre o que é o IT Army.

Foi necessário olhar especificamente para o que se sabe sobre este IT Army para esmiuçar as suas caraterísticas e perceber de que forma é que a atuação destas pessoas ou grupo de pessoas pode ou não ser imputada ao Estado da Ucrânia.

No terceiro capítulo será feita uma contextualização da dimensão ciber dos conflitos armados e como é que essa dimensão está a moldar a guerra nos dias de hoje. Porque é necessário ter em atenção que o IT Army foi formado, em princípio, como resposta aos ciberataques de que estava a ser vítima. Aparentemente, o IT Army formou-se numa altura em que se percebeu que o Estado da Ucrânia não tinha como defender-se dos ciberataques de outra nação [10].

Uma vez conceptualizada a dimensão ciber das guerras modernas, o quarto capítulo desenvolve a dimensão da imputação de ataques cibernéticos aos Estados. Vai-se mostrar isso mesmo através do *Projet d'Articles* e do *Manual de Tallinn* que ajudam a contextualizar a situação. Numa terceira parte deste capítulo explora-se uma outra possibilidade de imputação identificada pelas fontes disponíveis para este trabalho.

No último capítulo apresentam-se as perspetivas futuras sobre esta situação, e as conclusões sobre a pergunta de partida.

[10] Pinho, A. L. (2022). Ciberdefesa, Ciberdissuasão e Poder Nacional no Ciberespaço. *IDN Brief, Julho,* 3.

2. O IT Army

O IT Army possui um *site* onde é referido, na data de consulta (19/07/2023), que este grupo é constituído por voluntários de todo o mundo, que querem ajudar a Ucrânia a resistir à invasão de que o país está a ser alvo. Os editores do *site* afirmam que o IT Army consegue bloquear 800 alvos em simultâneo, utiliza sistemas automáticos para perturbar os serviços de *internet* e *websites* do adversário. O *website* do IT Army foi feito para mostrar como as pessoas se podem juntar ao IT Army. Afiança-se neste *website* que as pessoas que queiram ingressar nas fileiras do IT Army podem utilizar o canal do Telegram. Entre os objetivos reconhecidos do IT Army figuram a danificação de economias agressoras, bloquear serviços vitais de finanças, infraestruturas, e de governo, parar a propaganda de guerra do adversário e espalhar a verdade sobre os motivos das hostilidades. Existe informação no *website* sobre parceiros, mas nenhum dos parceiros identificados é o Estado da Ucrânia, nem se consegue, com acesso à versão inglesa do *site* perceber se este é um orgão do Estado da Ucrânia [11].

Os editores do site da Wikipédia que especificamente se refere ao IT Army, mostram uma lista de operações cibernéticas. Essas operações cibernéticas identificadas são dirigidas a alvos específicos e empregam estratégias como a negação de serviço (DDoS), ou a defaciação de *sites*, por exemplo [12].

Lewis afiança que os hacktivistas do IT Army, com as suas ações simbólicas em prol da Ucrânia também não conseguiram mais que o seu simbolismo, porque essas ciberoperações não tiveram consequências nas forças militares do adversário. Mas a Ucrânia tem muito a ensinar no campo da ciberdefesa. Para este autor, o facto de a Ucrânia ter sido continuamente vítima de ciberoperações bastante violentas, pelo menos desde 2014, colocou este Estado numa posição de se adaptar para resistir ou desistir. Para Lewis, a Ucrânia desenvolveu uma rede eficiente de colaboradores (estaduais e empresariais) que lhe forneceram treino e formação [13].

Para Soesanto, o IT Army da Ucrânia nasceu da ausência de um cibercomando nas forças armadas ucranianas com capacidade para proteger os direitos estaduais do país no ciberespaço. Quando o país foi invadido em 2022, o IT Army foi criado sem qualquer

[11] IT Army of Ukraine. (2023). *IT Army of Ukraine*. IT Army of Ukraine. https://itarmy.com.ua/?lang=en

[12] *IT Army*. (2023, July 18). Wikipedia. https://en.wikipedia.org/wiki/IT_Army_of_Ukraine

[13] Lewis, J. A. (2022). *Cyber War and Ukraine.* https://www.csis.org/analysis/cyber-war-and-ukraine

estrutura e nasceu da necessidade premente de utilizar o ciberespaço como o 5º domínio da guerra que a Ucrânia estava a travar contra o seu adversário [14].

O autor, Soesanto, avisa que construiu o seu relatório com fontes abertas. E neste relatório, o IT Army nasceu da necessidade de defender a nação contra o ataque da guerra no ciberespaço e no espaço físico. E o IT Army não é uma estrutura civil ou militar, local ou internacional, e, para o mesmo autor, não é legal ou ilegal. Para Soesanto, o IT Army tem duas partes. Numa dessas partes colocam-se todos os voluntários que à volta do mundo voluntariam o seu tempo para ajudar a Ucrânia na sua guerra contra o seu adversário. Esta parte da infraestrutura participa em ataques coordenados contra alvos selecionados e primariamente civis. A outra parte da infraestrutura faz parte dos orgãos de inteligência e ciberdefesa do Estado da Ucrânia. As duas parte do IT Army possuem natureza ofensiva. Por outro lado, o IT Army fez florescer um ecosistema que concentra empresas nas tecnologias da informação, pertencentes a donos ucranianos, localizados dentro e fora da Ucrânia, ou ucranianos a trabalhar para empresas ocidentais que estão continuamente a criar novas ferramentas ou novos conhecimentos, por exemplo, para apoiar o esforço de guerra ucrâniano [15].

Soesanto acusa os estados-membros da NATO e da Europa de ignorarem os problemas criados pelo IT Army, e uma das razões que ele aponta para isso é o facto de os estados da Europa e da NATO estarem ideologicamente e politicamente involucrados no conceito de defesa da Ucrânia. Os problemas identificados por Soesanto têm a ver com o Direito Internacional no ciberespaço, o comportamento normativo dos estados, atingir infraestruturas civis, e a ética de conduta de várias empresas situadas fora das fronteiras físicas da Ucrânia [16].

Soesanto considerou que a ideia do IT Army foi de Yegor Aushev, empreendedor ucrâniano na área do ciberespaço. Quando a Rússia invadiu o território ucrâniano, e, entre 24 e 26 de fevereiro de 2022, Mykhailo Federov, o Ministro da Transformação Digital da Ucrânia tinha adotado a ideia, segundo afirmou Soesanto. Na mesma altura Aushev tentou produzir um conjunto de voluntários para trabalhar no ciberespaço. Aushev fez isso com

[14] Soesanto, S. (2022). *The IT Army of Ukraine Structure, Tasking, and Ecosystem*, p. 6. https://doi.org/10.3929/ethz-b-000552293
[15] Soesanto, S. (2022), *The IT Army of Ukraine Structure, Tasking, and Ecosystem*, p. 4.
[16] Soesanto, S. (2022), *The IT Army of Ukraine Structure, Tasking, and Ecosystem*, p. 4.

comunicados em várias redes de comunicação. E em simultâneo, Federov, o ministro, fez o mesmo apelo no Facebook [17].

A intenção de criar um exército de hackers chamou a atenção da imprensa ocidental [18]. Para Soesanto não se pode confiar nos relatórios públicos que colocam o IT Army com cerca de 300 000 membros, porque esses são o número de subscritores do canal do IT Army Telegram. Em junho de 2022 o número de subscritores era de cerca de 260 000. Soesanto afirmou que ninguém sabia ao certo de quantos elementos se compõe o IT Army. Soesanto reclama que nem o próprio IT Army tem essa informação e conhecimento. Apesar de se pensar no canal do Telegram como o meio de comunicação do IT Army, Soesanto afirma que existem muitos outros meios cibernéticos que não são conhecidos [19].

Devido às diferentes coincidências que Soesanto notou e descreveu no relatório que está a ser citado, ele acredita que o IT Army é controlado pelo Estado da Ucrânia, nomeadamente pelos seus departamentos de defesa e informação. No entanto, segundo ele, a imagem pública que passa é a de um conjunto de pessoas que atua independentemente da estrutura militar do Estado. Mas Soesanto duvida desta imagem.

Uma notícia, no *site* de uma agência de notícias ucrâniano, dá conta que, três meses depois do início da guerra Rússia/Ucrânia em 2022, o ministro ucrâniano Fedorov disse que a Ucrânia tinha criado um exército de 300 000 pessoas, nacionais e estrangeiros, peritos em IT e, pelo transcrito na notícia, chamou-lhes «soldados» que se tinham juntado à luta de forma totalmente voluntária [20].

O jornal português Expresso, alegadamente numa entrevista a um membro do IT Army, refere que o IT Army não faz parte das forças armadas ucranianas, mas tem ajudado o país a minimizar os efeitos dos ataques cibernéticos realizados por grupos de hackers adversários [21].

---

[17] Soesanto, S. (2022), *The IT Army of Ukraine Structure, Tasking, and Ecosystem*, p. 4.
[18] Pearson, J. (2022). *Ukraine launches "IT Army" Takes Aim at Rússian Cyberspace*. Reuters. https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-Rússian-cyberspace-2022-02-26/
[19] Soesanto, S.(2022), *The IT Army of Ukraine Structure, Tasking, and Ecosystem*, pp. 7-8.
[20] *Ukraine Creates IT Army of 300,000 specialists - Fedorov*. (2022, May 24). Interfax - Ukraine. https://en.interfax.com.ua/news/general/834508.html
[21] Soares, T. (2023, April 23). Hackers Pró-Rússia Criam "Caos" no Ocidente: A Guerra Cibernética Está Cada Vez Mais Perigosa. *Expresso*. https://expresso.pt/internacional/guerra-na-ucrania/2023-04-23-Hackers-pro-Russia-criam-caos-no-ocidente-a-guerra-cibernetica-esta-cada-vez-mais-perigosa-53e3774a

Por outro lado, o canal de televisão CNN apresentou uma entrevista a um grupo de hackers que supostamente fazem parte do IT Army. Estes peritos em IT não se identificam como piratas, pois não reclamam qualquer compensação financeira, mas vêem-se como hackers éticos. Esta notícia afirmou que o grupo português já teve oito membros, dos quais quatro estavam num grupo que analisava os alvos e reportava a inexistência de danos colaterais e os outros quatro avançavam com a ciberoperação. Utilizam mais o DDoS ou o "Ataque Distribuído de Negação de Serviço", o *defacing* onde danificam a aparência de um *site* e o *web cache poisoning* que serve para desviar o tráfego para servidores falsos. O jornalista informou que através do canal do Telegram as autoridades ucranianas dão instruções aos hackers. Não se leu isso nas palavras do entrevistado, mas sim nas afirmações do próprio jornalista que fez a entrevista [22].

Outra construção sobre o IT Army da Ucrânia discute que o governo da Ucrânia apoia o esforço de guerra no ciberespaço através de financiamento, mas a liderança é primariamente civil. Um dos hackers pertencentes ao IT Army mostrou que não existe organização ou hierarquia nas ações dos hackers, e que muitos se juntam ao esforço por motivos nobres mas sem conhecimentos para poderem ser uma vantagem no ciberespaço, tornando-se mesmo um perigo para os próprios colegas [23].

Recentemente pode haver alguma clarificação. Neste momento e de acordo com esta notícia, a clarificação total é apenas uma possibilidade. O Comité Internacional da Cruz Vermelha mostrou preocupação pela segurança dos voluntários e das famílias dos voluntários no IT Army. Embora nem todas as ações empreendidas pelo IT Army ultrapassem o limiar para o ciberataque, os seus voluntários podem todos sofrer represálias do outro Estado beligerante neste conflito. Para terminar com o status indeterminado do IT Army, e para salvaguardar os voluntários como combatentes com direitos legais pelo lado da Ucrânia, este Estado está a elaborar uma lei que vai colocar os voluntários do IT Army como reservas das Forças Armadas do Estado da Ucrânia [24]. Entretanto não foi possível confirmar esta informação através de outras notícias ou informações obtidas através da *internet*.

---

[22] Rodrigues, J. G. (2023, February 23). *"Atacamos Tudo Menos Hospitais e Serviços Essenciais". Por Dentro do Grupo de Hackers Portugueses que Luta contra a Guerra da Rússia*. CNN.

[23] Kurtzleben, D. (2022, March 27). *Volunteer Hackers from "IT Army" to Help Ukraine Fight Russia*. NPR. https://www.npr.org/2022/03/27/1089072560/volunteer-hackers-form-it-army-to-help-ukraine-fight-russia

[24] Biggerstaff, W. C. (2023). *The Status of Ukraine's "IT Army" under the Law of Armed Conflict*. Lieber Institute West Point. https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/

Buchan e Tsagourias mostram porque é tão importante que os membros do IT Army recebam um estatuto oficial como orgão do Estado da Ucrânia. Como combatentes, os voluntários do IT Army podem participar no conflito armado, usar força letal, e em caso de serem capturados pelo inimigo têm direito ao estatuto de Prisioneiro de Guerra. Enquanto civis podem ser alvos das forças inimigas quando participam de ataques contra o inimigo mas não têm direito ao estatuto de Prisioneiro de Guerra se capturados como civis [25].

O IT Army é neste momento um recurso eficaz na guerra que a Ucrânia trava contra a invasão do seu território, por isso as fontes de informação que se podem utilizar são as fontes abertas na *internet*. Este conjunto de pessoas ainda não foi estudado convenientemente pois que isso iria destroçar a sua operacionalidade no campo de batalha.

Em conclusão, Soesanto diz que o IT Army é uma organização sobre a tutela do poder político ucrâniano, e esta organização é um ator não-estadual. Outros autores mostraram que não se sabe muito sobre o IT Army.

Alegadamente, estas pessoas do IT Army estão espalhadas por todo o mundo e actuam por motivos pessoais (hacktivistas). Nisso, uma entrevista a um hacker do IT Army (notícia do Expresso), pode parecer uma confirmação da independência do estatuto do IT Army [26]. Mas numa cadeia de televisão (CNN) essa independência parece não ser um facto [27]. Por outro lado, os hackers parecem receber instruções de alguém, mas quem é esse alguém, será um agente do Estado ucraniano? Outra notícia refuta a existência de uma organização, pelo menos, uma organização eficiente e alega que a direção das operações, a existir será maioritariamente civil. O hacker duvida mesmo que exista uma organização em que todos respondem a uma hierarquia. De acordo com o entrevistado, essa opinião é mantida porque os hackers voluntários interferem nas operações uns dos outros. Segundo o hacker, os diferentes hackers que estão a tentar trabalhar em conjunto

[25] Buchan, R. & Tsagourias, N. (2022). *Ukranian "IT Army": A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?* Blog of the European Journal of International Law. https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/

[26] Soares, T. (2023, April 23). Hackers Pró-Rússia Criam "Caos" no Ocidente: A Guerra Cibernética Está Cada Vez Mais Perigosa. *Expresso*. https://expresso.pt/internacional/guerra-na-ucrania/2023-04-23-Hackers-pro-Russia-criam-caos-no.Ocidente-a-guerra-cibernetica-esta-cada-vez-mais-perigosa-53e3774a

[27] Rodrigues, J. G. (2023, February 23). *"Atacamos Tudo Menos Hospitais e Serviços Essenciais". Por Dentro do Grupo de Hackers Portugueses que Luta contra a Guerra da Rússia*. CNN.

não sabem fazer melhor e não estão sob o controlo ou direção de alguém com conhecimentos mais abrangentes [28].

[28] Kurtzleben, D. (2022, March 27). *Volunteer Hackers from "IT Army" to Help Ukraine Fight Russia*. NPR. https://www.npr.org/2022/03/27/1089072560/volunteer-hackers-form-it-army-to-help-ukraine-fight-russia

3. A Dimensão Ciber dos Conflitos

A dimensão ciber dos conflitos é uma dimensão recente, mas é apenas uma evolução natural das técnicas e dos meios que evoluíram bastante nas últimas décadas. Hugo Fernandes mostrou como o fenómeno da guerra pode ser classificado de várias formas. Segundo este autor, as formas mais habituais classificam a guerra como regular ou convencional e irregular ou não convencional. Para Fernandes, as guerras regulares seguem o modelo clausewitziano onde os principais atores são os Estados e as suas forças militares regulares, e o confronto é político. Mas nas guerras irregulares os principais atores já não são os Estados e as suas forças armadas. Os atores nestas guerras são não-estatais, alguns desses autores podem ser armados, e esses grupos podem ser intranacionais (como etnias, clãs, entre outros) transnacionais (como empresas multinacionais, por exemplo), ou, supranacionais (organizações internacionais, por exemplo) [29].

O estudo de Hugo Fernandes mostrou que as guerras ou os conflitos armados orientam-se cada vez mais para uma maior destruição com contenção da força usada, o que leva à utilização de atores não-convencionais que se podem caraterizar como regulares, irregulares e criminais. Estes diferentes elementos trabalham em conjunto para a obtenção de objetivos comuns num novo Estado. Para Fernandes, a verdadeira questão é conseguir identificar, entender e combater estas novas estratégias dos Estados [30]. Pode-se acrescentar que o IT Army é uma destas novas estratégias que é necessário entender e identificar.

A comunidade internacional e em particular a comunidade que lida com a legislação, começou a olhar para as ciberoperações nos anos da década de 1990 [31]. Algumas ciberoperações mostraram a importância do elemento ciber nas relações internacionais na primeira década de 2000, que levou ao desenvolvimento do conceito de

[29] Fernandes, H. (2016). As Novas Guerras: O Desafio da Guerra Híbrida. *Revista de Ciências Militares*, *IV*(2), p. 18.
[30] Fernandes, H. (2016). As Novas Guerras: O Desafio da Guerra Híbrida, *Revista de Ciências Militares*, *IV*(2),pp. 18-20.
[31] Schmitt, M. N. (2013). Introduction. In *Tallinn Manual on the International Law Applicable to Cyber Warfare*, p. 1. Cambridge University Press. Consultar, para mais informações, por exemplo: Arquilla, J., & Ronfeldt, D. (1997). Cyber War is Coming!. In J. Arquilla & D. Ronfeldt (Edts.), *In Athena's Camp: Preparing for Conflict in the Information Age*, pp. 23-60. National Defense Research Institute RAND. https://doi.org/10.7249/MR880

ciberguerra [32]. Mas a preocupação do Direito Internacional é atualmente como responder a este desafio no ambiente ciber porque o Direito Internacional foi crescendo e aumentando o seu âmbito ao longo dos séculos, mas tem por base um mundo com outras tecnologias. Para Schmitt, em 2013, o universo ciber ainda escapava ao entendimento do Direito Internacional [33].

Até ao século XX existiram apenas dois domínios em qualquer guerra, o domínio terrestre e o marítimo. O domínio aéreo, o 3º domínio, começou a desenvolver-se com a I Guerra Mundial (1914-1919) quando a aviação começou a ser utilizada em manobras de suporte nos domínios terrestre e marítimo, mas foi desenvolvendo a sua própria autonomia nos anos seguintes. O 4º domínio é o espaço e a consequente exploração espacial. Este domínio surgiu com o *terminus* da II Guerra Mundial (1939-1944) e do envolvimento na Guerra Fria. O ciberespaço veio acrescentar um novo domínio à estratégia das nações, o 5º domínio. Este domínio desenvolveu-se no último quarto do século XX e está em pleno desenvolvimento neste momento [34]. Várias fontes aceitam que o ciberespaço é neste momento considerado como o 5º domínio da guerra [35].

Na esteira da desintegração da URSS e do advento das novas tecnologias que iriam formatar as guerras do futuro começou a desenhar-se o conceito de ciberguerra. John Arquilla e David Ronfeldt separaram a guerra da informação pensada como *netwar* da ciberguerra. A *netwar* referiu-se na última década do século XX a conflitos relacionados com informação a um nível maior, entre sociedades ou entre nações. Para os autores a *netwar* era uma forma de causar disrupção ou mudar a opinião que a população alvo tem de si própria e do mundo que a rodeia. A *netwar* pode ser social, económica, política, militar, entre outras formas de uma guerra que gira à volta da informação. Já o conceito de ciberguerra refere-se à prepação e execução de operações militares cujo objetivo é prejudicar ou mesmo destruir os sistemas de informação e comunicação do adversário. O objetivo deste tipo de operações militares é tentar conhecer tudo o que há para conhecer

[32] Fernandes, J. P. (2012). A Ciberguerra como Nova Dimensão dos Conflitos do Século XXI. *Relações Internacionais*, *33*, p.60.
[33] Schmitt, M.N. (2013), Introduction. In *Tallinn Manual on the International Law Applicable to Cyber Warfare*, pp. 3-4. Cambridge University Press.
[34] Honorato, M. da C., Santos, L. F., & Mateus, R. M. (2017). *O Ciberespaço como 5º Domínio Operacional. Impacto Estratégico na Política de Defesa Nacional* [Repositório Comum], p. 6.
[35] Council of the European Union. (2014). *EU Cyber Defense Policy Framework*. p. 2; Honorato et al., (2017), p. 6 e seguintes.

sobre o adversário e tentar que o adversário não conheça muito sobre o outro que está a provocar as disrupções [36].

O ciberespaço passou a ser utilizado mais correntemente como campo de desenvolvimento de ações hostis no início do século XXI. Começou com ações hostis individuais (hackers ou em português piratas informáticos), mas as organizações criminosas rapidamente se adaptaram a esta nova realidade (cibercrime), descontentes políticos utilizam também o ciberespaço (hactivismo). Os Estados e outros atores como organizações terroristas estão a utilizar o ciberespaço para desenvolver as suas atividades contra outros Estados e organizações ou na defesa dos seus interesses [37].

Weedon afirma que em 2015 ainda se pensava em ciberataques e em ciberguerra como fenómenos independentes e limitados apenas ao domínio cibernético, ou seja, não conectado aos domínios habituais de um conflito. Para a autora, a realidade demonstrou que os assaltos através da *internet* a alvos específicos estão subjacentes a um contexto geopolítico, e para ela, é pouco provável que uma ciberguerra seja travada apenas no domínio ciber. Os governos têm usado ferramentas e estratégias do espaço cibernético para fazer avançar as suas políticas, para coagir as pessoas e também como complemento para fazer avançar as forças armadas no terreno [38].

O ciberespaço, ou espaço digital não possui uma definição universal [39]. A definição apresentada pela Forças Armadas Norte Americanas é muito elucidativa: o ciberespaço é um domínio global dentro do ambiente da informação. É uma infraestrutura interdependente que inclui a *internet*, mas também redes de comunicações, sistemas de computadores e os periféricos associados [40].

Honorato e al., mostraram que na altura do seu trabalho, o ciberespaço era considerado como possuindo elementos tangíveis e intangíveis e a informação era uma

[36] Arquilla, & Ronfeldt, (1993). Cyber War is Coming!, pp. 28, 30.
[37] Honorato et al., (2017). *O Ciberespaço como 5º Domínio Operacional. Impacto Estratégico na Política de Defesa Nacional*, p. 6.
[38] Weedon, J. (2015). Beyond "Cyber War": Rússia's Use of Strategic Cyber Espionage and Information Operations in Ukraine. In *Cyber War in Perspective: Rússian Agression Against Ukraine*, pp. 67–77. NATO Cooperative Cyber Defense Centre of Excellence.
[39] Honorato et al., (2017). *O Ciberespaço como 5º Domínio Operacional. Impacto Estratégico na Política de Defesa Nacional*; Carvalho, A. R. (2019). Ciberespaço e os Novos Desafios à Soberania e à Segurança dos Estados. *IDN Cadernos*, *36*, 219–235; Moreira, J. M. (2012). O Impacto do Ciberespaço como Nova Dimensão nos Conflitos [Trabalho de Investigação, Repositório Comum], p.4. https://comum.rcaap.pt/handle/10400.26/12369
[40] Office of the Chairman of the Joint Chiefs of Staff. (2021). *DOD Dictionary of Military and Associated Terms*. The Joint Staff, p. 55. https://irp.fas.org/doddir/dod/dictionary.pdf

das componentes do ciberespaço. Para estes autores, o ciberespaço existe numa dimensão que interseta os outros domínios estratégicos (domínios terrestre, marítimo, aéreo e espaço) [41].

O ciberespaço pode ser pensado apenas como informação contida e armazenada num ambiente não físico, mas existe também o espaço físico e material (*Internet* das Coisas, por exemplo) em que os objetos se ligam em rede através da internet para transmitir, partilhar informação e funcionar melhor. Tudo isto permitiu elevar o nível de vida das sociedades no século XXI. Muitos dos sistemas da vida diária dependem do espaço virtual, como sistemas de produção e distribuição de energia ou de água potável, sistemas de transportes, sistemas financeiros, telecomunicações, entre outros. Mas este ambiente virtual também tem sido alvo de utilizações ilícitas ou desconformes à norma [42].

Moreira define ciberataque como: «um ataque lançado geralmente a partir de um computador recorrendo ao método de intrusão e que tem como finalidade adquirir, explorar, perturbar, romper, negar, degradar ou destruir informação constante em computadores ou em redes de computadores, em sistemas e equipamentos eletrónicos ligados a outros equipamentos ou sistemas ou que partilham a mesma estrutura de energia ou o mesmo espaço de emissão eletromagnética, bem como os próprios computadores, redes de computadores, sistemas e equipamentos » [43]. No que parece ser, segundo as fontes disponíveis, como a melhor e mais detalhada definição do termo encontrada pela autora deste documento. É também uma das definições que melhor define o conceito, embora os avanços tecnológicos possam tornar esta definição como ultrapassada num muito breve espaço de tempo.

No início do século XXI, os cenários estratégicos mudaram. Novas ameaças para a paz, segurança e estabilidade internacionais como o terrorismo transnacional ou uma multitude de diferentes ataques através do ciberespaço moldam o pensamento estratégico do século XXI. A superioridade militar já não é garantia de segurança para uma nação. Os ambientes de mar, terra, ar e espaço já não são o suficiente para garantir que uma nação mantém um elevado nível de segurança. Os ciberataques são levados a cabo por

[41] Honorato et al., (2017), *O Ciberespaço como 5º Domínio Operacional. Impacto Estratégico na Política de Defesa Nacional*, pp. 13-15.
[42] Moreira, J.M (2012), O Impacto do Ciberespaço como Nova Dimensão nos Conflitos, p. 5.
[43] Moreira, J. M (2012), O Impacto do Ciberespaço como Nova Dimensão nos Conflitos, p. 6.

motivações intelectuais (os hackers procuram ficar famosos) e económicas (obter benefícios económicos de forma ilegal), mas também políticas (ciberterrorismo, ciberespionagem e ciberguerra) [44].

Para leigos na matéria, o ciberespaço é um espaço que escapa às fronteiras geográficas e políticas e interliga todas as civilizações do planeta. O ciberespaço é não apenas informação que paira em computadores, mas a própria forma como esses computadores funcionam e interagem uns com os outros. O ciberespaço engloba tudo o que aparentemente é intangível mas que serve para fazer funcionar a rede de computadores num sentido mais amplo. Engloba também tudo o que é tangível, todos os periféricos que são necessários para criar e fazer existir um ciberespaço.

Porque o ciberespaço não tem fronteiras, é necessário perceber o que é um ciberataque. A definição de ciberataque fornecida no *Manual de Tallinn* na sua Regra 92, é abrangente porque não define caraterísticas individualizadas, mas atitudes. Um ciberataque é uma operação no domínio ciber, que pode ser ofensiva ou defensiva, e que, no espectro do juízo comum, se pensa que pode provocar lesões ou morte em seres humanos, e danos ou destruição de objetos [45]. Esta é, na opinião da autora deste documento, a melhor definição de ciberataque que se pode conseguir. E carateriza um ciberataque pelas suas consequências, não por ser ou não ser dirigida contra adversários [46]. A definição de ciberataque é fulcral para este trabalho porque explica, em princípio, o que são as ações executadas pelas pessoas ou grupos de pessoas ou entidades que constroem o IT Army.

Em 2016, a NATO (OTAN - Organização do Tratado do Atlântico Norte) reconheceu o ciberespaço como domínio de operações. Admitiu que os ciberataques são tão prejudiciais para a sociedade que os sofre quanto ataques convencionais ou cinéticos (ataques armados) e como tal, a NATO precisa defender-se tão eficazmente no domínio do ciberespaço quanto o faz já nos domínios terrestre, aéreo e marítimo. O domínio do

[44] Rio Durán, J. J. (2011). La Ciberseguridad en el Ámbito Militar. In *Ciberseguridad, Retos, y Amenazas a la Seguridad Nacional en el Ciberespacio* (Vol. 149, pp. 218, 221-222). Instituto Español de Estudios Estratégicos, & Instituto Universitario «General Gutierrez Mellado».
[45] Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Regra 92, p. 415.
[46] Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Regra 92, p. 417, parágrafo 7.

ciberespaço é fulcral para que a NATO mantenha e amplie o seu âmbito de dissuasão e defesa [47].

Honorato et al. (2017), José Pedro Fernandes (2012) ou João Manuel Moreira (2012) mostraram que o ciberespaço é considerado como um domínio da guerra. Mas consideram que é muito difícil definir um ciberataque como um ataque armado, porque o conceito de ataque armado tem evoluído nas últimas décadas e para começar, nunca esteve muito bem definido.

O Artigo 51 da Carta das Nações Unidas define que um ataque armado pode despoletar o direito de um Estado se defender de forma individual ou coletiva. No entanto é muito difícil definir o que é um ataque armado porque continua, nos dias de hoje, a ser uma questão de interpretação e qualificação. Oorsprong et al. afirmam que é ainda mais difícil estabelecer um nível base a partir do qual um ciberataque, conduzido sem estar a apoiar as forças cinéticas (forças armadas) no terreno, pode ser considerado um ataque armado. Mas para estes autores tal é de vital importância, pois que, saber se o ciberataque ultrapassa ou não o limiar para o ataque armado ofereceria ao Estado vitimizado uma base jurídica para recorrer à legitima defesa dentro das relações do Direito Internacional [48].

Para Lopes (2020), o *Manual de Tallinn* mostra que uma operação ciber pode ser caraterizada como uso da força da mesma forma que um ataque cinético convencional poderia ter esse efeito. Lopes confirmou também, na sua interpretação, que um ataque ciber poderá despoletar o direito à legítima defesa desde que o ataque ciber possa ser comparado a um ataque armado, o que está dependente da escala e efeitos da ciberoperação [49].

Os peritos do *Manual de Tallinn* e Oorsprong et al. definem que uma operação cibernética pode ser considerada um ataque armado quando as consequências da operação no ciberespaço são suficientemente graves, e essas consequências são suficientemente graves quando provocam perda de vidas humanas, danos a essas vidas humanas ou

[47] North Atlantic Treaty Organization. (2016, July 9). *Warsaw Summit Communiqué Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8-9 July 2016*. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

[48] Oorsprong, F. M., Ducheine, P. A., & Pijpers, B. M. (2021). *Armed Attack in Cyberspace Clarifying and Assessing When Cyber-Attacks Trigger the Netherlands'Right to Self.Defense* (Nº 2021-09; Amsterdam Law School Legal Studies Research Paper), pp. 2-3.

[49] Lopes, J.A. (2020). Uso da Força e Direito Internacional Direito em Tempos de Cólera, . In *Regimes Jurídicos Internacionais,*(Vol. 1, p. 89). Universidade Católica Editora Porto.

extensiva destruição de propriedade [50]. Mas mesmo assim os parâmetros não são claros e simples de determinar. Talvez por isso nenhum país tivesse até 2021, altura do artigo de Oorsprong et al., explicitamente definido um ataque cibernético de que tivesse sido vítima, como ataque armado [51].

O conceito de ciberguerra está ligado a ciberoperações executadas em quadros e em tempos de guerra. Neste caso, os ciberataques são mais complexos e realizados contra os interesses de Estados adversários. Estas ciberoperações trazem consigo consequências graves e extensas para o país atacado. E neste caso, a ciberoperação é denominada como um ciberataque e é equiparada a um ataque armado. Para Martins, este tipo de operações estão sob o comando e domínio do Departamento de Defesa Nacional, e este departamento cumpre as orientações e os planos de guerra definidos no país. Os ciberataques despoletam a ciberdefesa de um país, e neste campo incluem-se todas as atividades de prevenção, reação e monitorização de ameaças que coloquem em perigo a soberania do país e uma adequada resposta é, segundo o autor, feita através do departamento de defesa nacional [52].

Com Schmitt o debate continua. Os limites ou fronteiras do que pode ser classificado como ciberataque estão ainda envoltos em neblinas. Ele questiona, para futuras reflexões, se será possível agregar os efeitos de múltiplas ciber operações para atingir as fronteiras do ataque armado. Schmitt questiona também com quanta antecedência pode ser montada a operação de legítima defesa ou quando é que uma resposta a uma ciberataque se transforma apenas em retaliação. Outra pergunta que Schmitt avança é se e quando, se no direito existe o direito de legítima defesa mesmo que não se consiga imputar o autor não-Estadual a um Estado. São várias as perguntas lançadas por Schmitt para levar a desenvolvimentos futuros [53].

Nenhum Estado é dono do ciberespaço, mas o Estado pode exercer prerrogativas de soberania sobre qualquer ciberinfraestrutura localizada no seu território, bem como sobre as atividades que estão associadas a essa ciberinfraestrutura. Assim, por um lado, a

[50] Oorsprong et al., (2021), p. 7; Schmittt, (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Regra 71, pp. 339-348.
[51] Oorsprong et al.,(2021), *Armed Attack in Cyberspace Clarifying and Assessing When Cyber-Attacks Trigger the Netherlands'Right of Self-Defence*, p. 9.
[52] Martins, I. M. (2022). *A Imputação de Ciberataques aos Estados* [Dissertação de Mestrado, Repositório Universidade Católica Portuguesa], p.20. https://repositorio.ucp.pt/bitstream/10400.14/39892/1/203156218.pdf
[53] Schmitt, M. N. (2022, July 28). *The Evolution of Cyber Jus Ad Bellum Thresholds*. Ukraine Symposium. https://lieber.westpoint.edu/evolution-cyber-jus-ad-bellum-thresholds/

ciberinfraestrutura tem de obedecer às leis e regulamentos do país, por outro lado, o país tem de estar pronto para defender essa ciberinfraestrutura (estadual ou particular), em consequência desse princípio da soberania [54].

Os peritos do *Manual de Tallinn* identificaram que uma ciberoperação dirigida contra a ciberinfraestrutura de outro país pode violar a soberania do outro Estado e os peritos concordaram que viola a soberania do outro Estado se causa dano [55].

Em conclusão, as variadas notícias dão conta de operações no ciberespaço que o IT Army conduziu como negação de serviço, entre outros. Este tipo de operações, desde que não despoletadas para ajudar o ataque cinético, não ultrapassa os limites para o ataque armado como se viu na documentação produzida por OOrsprong et al., por exemplo. De igual forma, se este tipo de operações não provoca danos extensos em infraestruturas ou em vidas humanas, ou se não existe perda de vidas humanas, não é considerado ataque armado, respeitando os atuais limites de ataque armado apresentados no *Manual de Tallinn*.

Para que uma operação no domínio do ciberespaço ultrapasse os limites e se transforme num ciberataque precisa de ter consequências comparáveis às de um ataque cinético, provocar perdas de vida ou danos na saúde das pessoas desse território, ou danos extensos nas infraestruturas desse território. Como se mostrou atrás, os limites do que é considerado um ciberataque não são muito explícitos e fáceis de medir, mas os danos, em pessoas, bens ou infraestruturas, precisam de ser extensivos.

[54] Schmitt, M. N. (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, pp. 11-29.
[55] Schmitt, M. N. (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, pp. 20-21, parágrafos 11 a 13.

4. A Imputação dos Ciberataques

4.1. Definição de Imputação Funcional

Quando ocorre uma operação ilícita no ciberespaço que pode ser atribuível a um Estado, esse Estado é imputado com essa responsabilidade. Espera-se que o Estado ofensor acate determinadas consequências. Essas consequências incluem, entre outras medidas, que o Estado cesse o seu comportamento danoso, e que faça reparações por qualquer dano que a sua conduta tenha causado [56].

Para Martins, a imputação jurídica tem dois momentos distintos. Num primeiro momento é necessário ligar o ciberataque a um infrator, através da imputação técnica, e num segundo momento é necessário avaliar e validar o *standard of proof*. Ou seja, nesse segundo momento analisa-se a quantidade de provas necessárias e o nível de certeza que essas provas geram para poder passar para a imputação funcional [57].

Para Eichensehr, a imputação de um ciberataque tem aspetos técnicos, legais e políticos e por isso, torna-se um grande imbróglio. Eichensehr reclama que o sistema de imputação atual é descentralizado, descoordenado e basicamente confuso, pois ele alega a existência de várias entidades que são capazes de fazer essa imputação mas que agem sem coordenação entre si. Essas entidades são entidades governamentais e não-governamentais. A contribuir para todo o imbróglio está também o facto de existir uma infinidade de mecanismos de imputação [58].

Eichensehr alega que os objetivos da atribuição – dissuadir atos futuros de ilicitude semelhante, promover a defesa, estabelecer as bases para ações de resposta,

[56] Maddocks, J. (2022). State Responsability for Non-State Actor's Conduct. *Ukraine Symposium*. https://lieber.westpoint.edu/state-responsibility-non-state-actors-conduct/
[57] Martins, I.M. (2022). *A Imputação de Ciberataques ao Estado*, p. 28.
[58] Eichensehr, K. E. (2020). The Law and Politics of Cyberattack Attribution. *U.C.L.A. Law Review*, *520*, pp. 523 e 526. Entre as diversas entidades capazes de fazer uma atribuição ou imputação de crimes no ciberespaço que violam o Direito Internacional encontram-se os orgãos de Estado diretamente ligados a essas atividades e no campo das entidades não-governamentais podemos encontrar empresas como a Mycrosoft, ou outras organizações como o CyberPeace Institute, por exemplo (ver CyberPeace Institute. (2023). *CyberPeace Institute*. CyberPeace Institute. https://cyberpeaceinstitute.org/).

promover a estabilidade e evitar o conflito entre nações – não estão a ser conseguidas com as atuais políticas de imputação [59].

Mesmo que seja possível fazer a atribuição em termos técnicos e identificar as máquinas responsáveis pelo ciberataque, é difícil estabelecer a identificação da entidade responsável. Mas conhecer a máquina que lançou o ataque pode ajudar a identificar o indivíduo, e, conhecer o indivíduo por trás da máquina pode mostrar pistas para identificar a entidade específica responsável pela intrusão. Até 2017 só os Estados Unidos da América conseguiram fazer atribuições entre Estados, altura em que outros países começaram também a fazer atribuições de ciberataques entre Estados [60].

Eichensehr mostra que as acusações de atribuição de ciberataques deviam ser consubstanciadas com evidências legais que permitam comprovar as acusações por outras entidades e Estados. Mas mostrar as evidências dessas ações é muito importante para a entidade infratora pois assim fica a saber como foi identificada. Em ações futuras a entidade infratora aprende, com esses dados de identificação, a evitar essas armadilhas no futuro. Mas pela lei do Direito Internacional, não é necessário revelar as provas dessas acusações. A autora salienta que quando um Estado identifica e atribui responsabilidade por um ciberataque a outro Estado, o Estado que identificou a responsabilidade pelo ciberataque encontra pressões externas e políticas para não tomar medidas extra. Como é difícil tomar medidas extra, isso faz com que seja menos provável para um Estado fazer a atribuição de ciberataques de uma forma pública [61].

Finlay e Payne mostraram que a imputação é um problema que tem duas faces. Por um lado, existe o problema técnico de identificar a verdadeira origem de um ataque cibernético e identificar os que estiveram por trás desse ataque. Por outro lado, existe a questão jurídica, que é uma discussão sobre se, quando, e como, é que é possível haver atribuição baseada em evidências ou provas que mostrem que um Estado pode ser responsabilizado sob as regras do Direito Internacional no domínio cibernético [62].

---

[59] Eichensehr, K. E. (2020). The Law and Politics of Cyberattack Attribution, *U.C.L.A. Law Review*, *520*, p.562.
[60] Eichensehr, K. E. (2020), The Law and Politics of Cyberattack Attribution, *U.C.L.A. Law Review*, *520*, p. 530.
[61] Eichensehr, K. E. (2020), The Law and Politics of Cyberattack Attribution, *U.C.L.A. Law Review*, *520*, pp. 532, 545.
[62] Finlay, L., & Payne, C. (2019). The Attribution Problem and Cyber Armed Attacks. *American Journal of International Law Unbound, 113*, p.203.

A imputação funcional é um conceito que permite, em Direito, obter atribuição ou imputação da responsabilidade por um acto ilícito cometido por um agente A à autoria de um agente B considerando que o agente A agiu sob a égide do Agente B. Em Direito Internacional é um conceito que permite atribuir responsabilidade por um facto ilícito a um Estado, que é uma pessoa de direito jurídico, por ações cometidas por um dos seus agentes físicos. Assim sendo, para Tavares, este é o princípio geral de «atribuição das condutas ao Estado» [63].

No pensamento de Condorelli e Kress, a palavra atribuição ou imputação faz referência a um conjunto de critérios com conexões específicas e as condições que têm de ser cumpridas, segundo o Direito Internacional, para uma ação poder ser imputada a um Estado [64]. É importante poder fazer esta imputação porque só assim o Estado que sofreu a ação ilicita pode exigir o cessar do acto, a sua não repetição e o dever de reparação pela ação ilicita sofrida, sob a égide do Direito Internacional [65].

Os aspetos legais e políticos misturam-se nas relações entre os Estados. Martins em 2022 mostrou que fazer uma imputação era mais uma questão política do que jurídica. Martins colocou a imputação política numa segunda fase do sistema de imputação, logo a seguir à imputação técnica. Para se fazer a imputação política é necessário que o Estado ofendido reconheça publicamente que foi vítima de um ciberataque. Mas as múltiplas pressões que o Estado pode sofrer para ter mais cuidado com este tipo de imputação leva a que muitas vezes este não seja um caminho trilhado. Além do mais, é um momento que, segundo a autora, exige um *standard of proof* bastante elevado, ou seja, exige evidências bastante convincentes de que o Estado infrator acusado é de facto o Estado infrator [66].

---

[63] Tavares, M.I. (2020), Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilícitos Fechar o Círculo . In *Regimes Jurídicos Internacionais.* (Vol. 1 p. 642). Universidade Católica Editora Porto.

[64] Condorelli, L., & Kress, C. (2010). The Rules of Attribution: General Considerations. In J. Crawford, A. Pallet, & S. Olleson (Eds.), *The Law of International Responsability* (Vol. 3, pp. 221–224). Oxford University Press.

[65] Koenders, B. (2017). Foreword. In M. N. Schmitt (Ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.), pp. xxv-xxviii. Cambridge University Press; Momtaz, D. (2010). Attibution of Conduct to the State: State Organs and Entities Empowered to Exercize Elements of Governmental Authority. In *The Law of International Responsability* pp. 237–246; Zaytseva, (2014). Responsabilidade Internacional dos Estados: Projeto da Comissão de Direito Internacional sobre a Responsabilidade dos Estados por Atos Internacionalmente Ilícitos, pp. 369-389; Schmitt, (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, pp. 142-152.

[66] Martins, I.M.(2022), *A Imputação de Ciberataques aos Estados*, [Dissertação de Mestrado, Repositório Universidade Católica Portuguesa] p. 27.

Para Martins, a imputação política não deve ser a base, por si só, de uma resposta a um ciberataque. Só com imputação política não se pode tomar ações de resposta sob preço de essas ações de resposta virem a ser consideradas ilícitas. É necessário que o processo de imputação inclua também a imputação jurídica [67].

Martins mostra que a imputação política se refere à atribuição de responsabilidade com base em considerações políticas, diplomáticas ou de relações públicas. Os líderes políticos tomam decisões com base em julgamentos políticos e não é um julgamento feito com base em princípios científicos ou legais. Por isso, a atribuição pode ser feita de forma mais lata e flexível, e pode ser uma atribuição incorreta, ou que venha a danificar um país terceiro que não teve nada a ver com o ciberataque, mas que aparentemente, segundo a análise técnica inicial, teve um papel nesse ciberataque [68].

Para Tavares, o facto de se cometer um facto internacionalmente ilícito, qualquer que seja a natureza da norma violada, abre as portas para se procurar a imputação por responsabilidade internacional. Já não é necessário «debater o papel do dano ou da culpa para efeitos de responsabilidade» [69]. Mas só se pode caraterizar o facto como internacionalmente ilícito se, quer numa ação quer numa omissão, o comportamento ilícito for necessariamente um comportamento estadual [70].

Segundo o Artigo 2º do PARI, existe um facto internacionalmente ilícito do Estado quando esse facto é um comportamento consistente com uma ação ou omissão atribuível ao Estado à luz do Direito Internacional e quando esse comportamento constitui uma violação da obrigação internacional do Estado [71].

---

[67] Martins, I.M. (2022), *A Imputação de Ciberataques aos Estados*, [Dissertação de Mestrado, Repositório Universidade Católica Portuguesa], p. 27.
[68] Martins, I. M. (2022). *A Imputação de Ciberataques aos Estados* [Dissertação de Mestrado, Repositório Universidade Católica Portuguesa], p. 27.
[69] Tavares, M. I. (2020). Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilicitos Fechar o Círculo. In *Regimes Jurídicos Internacionais,* (Vol. 1, p. 639). Universidade Católica Editora Porto. Veja-se o caso de Fosfatos em Marrocos, Tribunal Permanente de Justiça Internacional, Itália c. França, objeções preliminares, 14 Junho 1938 In *Regimes Jurídicos Internacionais Questões, Casos e Materiais*, (Vol. 2, p. 623). Universidade Católica Editora Porto.
Pode-se também verificar, o caso Rainbow Warrior, Nova Zelândia c. França, Tribunal Arbitral, 30 Abril 1990. In *Regimes Jurídicos Internacionais Questões, Casos e Materiais*, (Vol. 2, pp. 623-624).
[70] Tavares, M. I. (2020). Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilícitos Fechar o Círculo, In *Regimes Jurídicos Internacionais* ,(Vol. 1, p. 634). Universidade Católica Editora Porto.
[71] *Projet d'Articles Sur La Responsabilité de l'État Pour Fait Internationalement Illicite* (2005), p. 388.

Tavares defende que, com o Artigo 2º do PARI, para que exista responsabilidade de um Estado por um facto ilícito, quer de ação quer de omissão, é necessário identificar dois elementos:

- o elemento subjetivo o qual mostra que é necessário identificar a conduta de ação ou omissão e imputar essa ação ao Estado;
- o elemento objetivo que mostra que aquela conduta de ação ou de omissão viola uma norma primária do Direito Internacional e com isso se prova a ilícitude da ação ou omissão do Estado [72].

O Artigo 4º do PARI estabelece o princípio geral que mostra o mecanismo principal de imputação jurídica. Qualquer entidade do Estado que executa um facto internacionalmente ilícito, por ação ou omissão, é considerado à luz do Direito Internacional, como parte desse Estado e a sua conduta como uma conduta de Estado. E para ser considerado um orgão do Estado é necessário que seja assim considerado à luz do Direito Interno desse Estado [73]. Só interessa, para o Direito Internacional, pessoas que estejam a agir em orgãos do Estado e sobre a qualidade de agentes desse Estado. Para atribuir um facto ao Estado é necessário identificar os agentes que executam esse facto bem como assegurar a relação desses agentes ao Estado.

De acordo com Tavares, o Artigo 4º do PARI é a regra geral, o principio geral sobre o qual são atribuíveis as condutas ao Estado. As funções que estão a ser executadas pelos diversos orgãos ou agências do Estado, seja legislativa, executiva, judicial, policial entre outras, são todas elas, de igual importância. De igual forma, qualquer que seja a forma administrativa que esse Estado apresente, todas esses ramos do Estado são, à luz do Direito Internacional, igualmente Estado [74]. O Estado é uno e como tal responde por todas as suas partes de igual forma.

Por outro lado, se a entidade está reconhecida no Direito Interno do Estado e executa funções que são do Estado, então as ações ou omissões dessa entidade ou agência

---

[72] Tavares, M. I. (2020). Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilícitos. Fechar o Círculo. In *Regimes Jurídicos Internacionais* ,(Vol. 1, pp. 639). Universidade Católica Editora Porto. Ver Caso nº21, 2 Abril 2015, Tribunal Internacional do Direito do Mar, parecer consultivo, pedido submetido pela Comissão Sub-Regional de Pescas. In *Regimes Jurídicos Internacionais Questões, Casos e Materiais*, (Vol. 2, pp. 624-625). Universidade Católica Editora Porto.

[73] *Projet d'Articles Sur La Responsabilité de l'État Pour Fait Internationalement Illicite*, 2005, p. 389.

[74] Tavares, M. I. (2020), Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilícitos Fechar o Círculo. In *Regimes Jurídicos Internacionais* (Vol. 1, pp. 642-643). Universidade Católica Editora Porto.

do Estado, são igualmente responsabilidade do Estado porque é como se do Estado se tratasse. Para Tavares, nestes casos, a imputação funcional é fácil de conseguir [75].

Segundo Tavares, quando o Estado reconhece no seu Direito Interno a existência de um órgão ou entidade como órgão ou entidade do Estado, então, qualquer que seja a conduta desse orgão, ela é imputável ao Estado. Para a autora, nestes casos é mais fácil produzir uma operação de imputação jurídica [76].

A Regra 15 do *Manual de Tallinn* transfere muito do Artigo 4º do PARI para o universo ciber. Quaisquer ciberoperações levadas a cabo por agentes do Estado, ou por pessoas ou entidades reconhecidas pelo Direito Interno desse Estado, a quem foi dada autoridade para exercer prerrogativas do Estado, são atribuíveis a esse Estado [77].

Mas no *Manual de Tallin* adiantaram-se ao PARI continuando, na mesma regra 15, ao afirmar que as pessoas, ou orgãos, mesmo que não reconhecidos no Direito Interno do Estado podem ver as suas ações como responsabilidade do Estado no que ao Direito Internacional diz respeito.

Segundo a Regra 15 do *Manual de Tallinn*, pessoas, grupos de pessoas ou entidades podem ser equiparados a orgãos do Estado mesmo que tal não esteja salvaguardado no Direito Interno do Estado, apenas no caso em que essas pessoas, grupos de pessoas ou entidades estivessem numa situação de total controlo ou dependência por parte do Estado. Basicamente, apenas nos casos em que essas pessoas, grupos de pessoas ou entidades fossem simplesmente um instrumento para o Estado conseguir os seus fins é que as ações ou omissões dessas pessoas, grupos de pessoas ou entidades seriam equiparadas a ações ou omissões do próprio Estado [78].

O problema torna-se mais complicado quando o orgão ou entidade não é reconhecido diretamente através do Direito Interno do Estado. Mas para esses casos existe

[75] Tavares, M. I. (2020), Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilícitos. Fechar o Círculo. In *Regimes Jurídicos Internacionais* (Vol. 1, pp. 643-644). Universidade Católica Editora Porto.
[76] Tavares, M.I. (2020), Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilicitos Fechar o Círculo. In *Regimes Jurídicos Internacionais* (Vol. 1, p. 643). Universidade Católica Editora Porto.
[77] Schmitt, M.N.(2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 87.
[78] Schmitt, M.N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 88.

o Artigo 5º do PARI, que é distinto do Artigo 4 do PARI, embora se complementem. Só se pode ativar o Artigo 5º caso não seja possível ativar o Artigo 4º do PARI.

O Artigo 5º do PARI discute o comportamento de uma pessoa ou de uma entidade que exerça prerrogativas de autoridade pública mas não é oficialmente um orgão do Estado. Basicamente, mostra o mesmo que parte da Regra 15 do *Manual de Tallinn*, no parágrafo supra. Este artigo é ativado nos casos em que é necessário fazer uma imputação sobre pessoas, grupos de pessoas ou entidades que não são reconhecidos como orgão ou agentes do Estado. Neste caso é necessário analisar se as funções exercidas e sobre mira da imputação são de facto prerrogativas de autoridade pública [79].

Em conclusão, de acordo com as recomendações do PARI, para fazer a imputação de qualquer ato ilícito ao IT Army é necessário comprovar, na mais fácil das opções (Artigo 4º do PARI e Regra 15 do *Manual de Tallinn*), que o IT Army é um orgão do Estado ucrâniano. Neste momento, e para este documento, foi encontrada uma notícia em inglês em que o Estado da Ucrânia, através do seu ministro, reconheceu o IT Army como um orgão de Estado, e como parte do esforço de modernização do país [80]. Existe um outro documento que refere que os voluntários do IT Army serão reconhecidos como membros das reservas das Forças Armadas ucranianas [81].

Partindo do princípio de que estes documentos mostram os voluntários do IT Army como elementos do Estado da Ucrânia estão corretos e o IT Army está a caminho de ser oficialmente reconhecido como um orgão do Estado da Ucrânia, quaisquer ações e omissões executadas pelo grupo poderão ser imputadas ao Estado sob o artigo 4º do PARI ou a Regra 15 do *Manual de Tallinn*. Mas isso ainda não aconteceu neste momento.

Numa fase posterior dos acontecimentos, quando o IT Army deixar de ser um recurso operacional poderá ser possível descobrir mais sobre as suas ações ou omissões e também sobre os seus membros. Talvez o estatuto de orgão do Estado da Ucrânia já esteja reconhecido nessa altura.

---

[79] Tavares, M. I. (2020), Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilicitos Fechar o Círculo, . In *Regimes Jurídicos Internacionais* (Vol. 1, pp. 645-646). Universidade Católica Editora Porto.

[80] *Ukraine Creates IT Army of 300,000 Specialists - Fedorov*. (2022, May 24). Interfax - Ukraine. https://en.interfax.com.ua/news/general/834508.html

[81] Buchan, R. & Tsagourias, N. (2022). *Ukranian "IT Army": A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?* Blog of the European Journal of International Law. https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/

Mas se não se comprovar que o IT Army é um orgão do Estado, poderá ser uma agência do Estado? Poderá ser comprovado que o IT Army exerceu funções que estão adstritas ao próprio Estado sobre o Artigo 5º do PARI? Funções como defesa e ataque no ciberespaço, por exemplo? Mas mesmo neste caso é necessário que haja reconhecimento, por parte do Estado, e que a agência se relacionou com o próprio Estado.

As funções de ciberdefesa de um Estado, em princípio são uma prerrogativa do próprio Estado. Sabe-se que o Estado da Ucrânia não tinha defesas no 5º domínio da guerra, mas que adquiriu essas competências posteriormente, com o auxílio de agências e empresas internacionais. Se se conseguir demonstrar que o IT Army esteve a exercer prorrogativas de Estado, nesse caso é possível ativar o Artigo 5º do PARI ou a Regra 15 do *Manual de Tallinn*. Em princípio, não será difícil ativar este artigo do PARI porque a ciberdefesa e o ciberataque são prerrogativas de Estado. O Estado tem o dever de soberania e como tal tem o dever de defender as ciberinfraestruturas que se dizem ucranianas.

Assim, no caso de o IT Army não ser reconhecido como orgão do Estado, poderá ser comprovadamente um agente privado a exercer prerrogativas do Estado. Neste caso, também pelo Artigo 5º do PARI é possível conseguir uma imputação. Em princípio, pensa-se que o IT Army tem funções de defesa e de ataque contra ciberatacantes e ciberataques.

Sabe-se que o IT Army se compõe por pessoas ucranianas e não-ucranianas, supostamente por peritos em IT. Mas é tudo o que se sabe de concreto sobre este grupo de pessoas que se pensa nem se conhecem uns aos outros. E também, alegadamente, nem os próprios voluntários sabem quantos são os voluntários que compõem o dito IT Army [82].

Para ativar o Artigo 4 do PARI será necessário demonstrar que o IT Army agiu como agente do Estado da Ucrânia. Para ativar o Artigo 5 do PARI será necessário demonstrar que o IT Army executou prerrogativas adstritas ao Estado propriamente dito, neste caso a Ucrânia. Mas e se não se conseguir no futuro determinar o estatuto do IT Army dentro da Ucrânia? É possível fazer uma operação de imputação que ultrapasse os Artigos 4 e 5 do PARI?

[82] Rodrigues, J. G. (2023, February 23). *"Atacamos Tudo Menos Hospitais e Serviços Essenciais". Por Dentro do Grupo de Hackers Portugueses que Luta contra a Guerra da Rússia*. CNN.

4.2. Comportamentos sobre Direção e Controlo

Existe uma maior discussão quando é necessário imputar um facto ilícito à ação de pessoas ou organizações que não são agentes diretos do Estado ou entidades autorizadas a exercer prerrogativas de autoridade pública. O Artigo 8 do PARI e a Regra 17 do *Manual de Tallinn* lidam com esta situação.

O Artigo 8º do PARI claramente enuncia que, quando a pessoa, grupo de pessoas ou entidade tiver de facto atuado sobre as instruções, sobre a direção ou sobre controlo de um Estado, então a atuação dessa pessoa, grupo de pessoas ou entidade será imputada ao Estado [83].

Tavares mostra que saber quando é que as pessoas ou grupo de pessoas agiram sobre a direção ou controlo do Estado é muito controversa com alguns casos de jurisprudência. De acordo com essa jurisprudência, tem sido complicado estabelecer o que é «sobre as direções», «sobre controlo» ou «sobre as instruções» [84].

A jurisprudência existente para ajudar a discernir estes termos ou frases mostra que os entendimentos exercidos são bastante diferentes entre si. Como mostrou Tavares: «As posições da doutrina não são unânimes» [85].

Os casos apresentados por Tavares (2020) exemplificam esta disparidade de posições. A autora identificou dois casos emblemáticos do Tribunal Internacional de Justiça, e um caso do Tribunal Penal Especial para a Ex-Jugoslávia, que serão apresentados de seguida.

No caso das Atividades Militares e Paramilitares na Nicarágua e contra esta foi decidido que para seguir o direito de responsabilidade internacional e para um país ser considerado responsável pelas ações de um grupo de pessoas teria que ser demonstrado que o grupo de pessoas estaria dependente do Estado estrangeiro e teria que ser provado que o Estado teria controlo sobre o grupo de pessoas. Este Tribunal considerou, que, neste

---

[83] *Projet d'Articles Sur La Responsabilité de l'État Pour Fait Internationalement Illicite et Commentaires Relatifs*, (2005), p. 390.

[84] Tavares, M. I. (2020), Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilicitos Fechar o Círculo. In *Regimes Jurídicos Internacionais* (Vol. 1, p. 648). Universidade Católica Editora Porto. Ver caso Atividades militares e paramilitares na Nicarágua e contra esta (Nicarágua contra Estados-Unidos), Acórdão do TIJ, 27 Junho 1986. In *Regimes Jurídicos Internacionais Questões, Casos e Materiais*, (Vol. 2, pp. 640-645). Universidade Católica Editora Porto.

[85] Tavares, M. I. (2020), Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilicitos Fechar o Círculo. In *Regimes Jurídicos Internacionais* (Vol. 1, p. 654). Universidade Católica Editora Porto.

caso, o controlo não estava demonstrado, pois que mesmo sem o apoio do Estado estrangeiro o grupo de pessoas continuou a existir e a provocar danos. O Tribunal considerou não haver um controlo efetivo. No entanto, o Tribunal considerou que o Estado estrangeiro tinha violado o princípio da não-ingerência ao ter financiado o grupo de pessoas durante algum tempo, numa clara violação do direito internacional [86].

O Tribunal Penal Especial para a Ex-Jugoslávia (Câmara de Recurso) no caso Dusko Tadic, também se referiu à imputação da conduta de um grupo de pessoas a um Estado, mas nesta circunstância tratou-se de um grupo de pessoas com estrutura e organização militar. Neste caso, este Tribunal em específico considerou não ser necessário demonstrar a existência de instruções específicas ou um controlo total para imputar a conduta das pessoas ao Estado. Porque para este Tribunal, o facto de ter havido financiamento e supervisão global das atividades do grupo de pessoas que mantiveram uma estrutura militar é o suficiente para demonstrar um controlo global [87].

No caso de Genocídio, tratado pelo Tribunal Internacional de Justiça, este Tribunal decidiu separar os dois elementos de pessoas que atuam como orgão do Estado ou pessoas que actuam sob instruções do Estado. O que nos dias de hoje e no ambiente cibernético é tratado no Artigo 4º e 8º do PARI. Este Tribunal considerou que o Estado que foi imputado não tinha incorrido nas violações de que era acusado nem através dos seus orgãos de Estado (Artigo 4º), nem através das instruções que deu às pessoas (Artigo 8º). No entanto o Estado acusado foi considerado responsável pela obrigação de prevenir o genocídio que aconteceu [88].

Nestes três casos de jurisprudência constrói-se a diferença entre controlo efetivo e controlo global. Para a ação do grupo de pessoas ser diretamente imputada ao Estado sobre o Direito Internacional, tem de se mostrar que o grupo de pessoas era totalmente controlado pelo Estado, de tal forma que o grupo se dissiparia se deixasse de ter a direção

[86] Tavares, M. I. (2020), Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilicitos Fechar o Círculo. In *Regimes Jurídicos Internacionais* (Vol. 1, p. 649). Universidade Católica Editora Porto.
[87] Tavares, M. I. (2020), Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilicitos Fechar o Círculo. In *Regimes Jurídicos Internacionais* (Vol. 1, pp. 649-650). Universidade Católica Editora Porto. Ver caso do Tribunal Penal Especial para a Ex-Jugoslávia (TPEJ), Prosecutor v. Dusko Tadic, IT-94-1-A, Câmara de Recurso, Julgamento, 15 Julho 1999. In *Regimes Jurídicos Internacionais Questões, Casos e Materiais*, (Vol. 2, pp. 646-650). Universidade Católica Editora Porto.
[88] Tavares, M. I. (2020), Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilicitos Fechar o Círculo. In *Regimes Jurídicos Internacionais* (Vol. 1, pp. 650-651). Universidade Católica Editora Porto. Ver caso do TIJ, Aplicação da Convenção para a prevenção e repressão do Crime de Genocídio, Bósnia-Herzegovina c. Sérvia e Montenegro, Acórdão, 26 de Fevereiro 2007. In *Regimes Jurídicos Internacionais. Questões, Casos e Materiais*, (Vol. 2, pp. 650-655). Universidade Católica Editora Porto.

e o controlo do Estado. Isto é considerado controlo efetivo. O controlo global refere-se à existência de apoio logístico, apoio financeiro, coordenação e planeamento das atividades e se o grupo for organizado, pode-se dispensar o critério de haver instruções específicas [89].

Para que o Artigo 8º do PARI seja passível de aplicação é necessário, primeiro que o Artigo 4º e o Artigo 5º do PARI não tenham sido aplicados e ter em atenção a possibilidade dos dois tipos de controlo, o controlo efetivo e o controlo global. No caso do grupo de pessoas manter uma organização, então o controlo necessário será apenas o controlo global. Cada caso tem de ser analisado consoante as suas caraterísticas próprias porque utilizar o controlo global pode ser um critério demasiado abrangente e utilizar o controlo específico pode ser um critério demasiado exigente [90].

A Regra 17 do *Manual de Tallinn* discute a atribuição de ciberoperações a atores não-estaduais. E nestes casos, as ações ou omissões das pessoas, grupo de pessoas ou entidades são imputáveis ao Estado quando as suas ações ou omissões tenham ocorrido sobre ordens, instruções ou controlo do próprio Estado, ou no caso em que o Estado adota as ações ou omissões cometidas por essas pessoas, grupos de pessoas ou entidades como ações ou omissões do próprio Estado [91].

Por regra geral, o *Manual de Tallinn* salienta, as ações no domínio ciber de pessoas ou grupos de pessoas privadas não são atribuíveis aos Estados. Mas essa regra geral tem exceções. As exceções referem-se a pessoas ou grupos de pessoas serem considerados como atores não-estaduais [92].

Os grupos podem ser considerados atores não estaduais se tiverem hierarquia ou não possuírem qualquer hierarquia, com organização de algum tipo, ou sem qualquer organização, quer possuam personalidade jurídica num Estado ou não. Como exemplos, o *Manual de Tallinn* mostra alguns atores não-estaduais como o grupo Anonymous (grupo informal de hackers), organizações criminosas que promovem o cibercrime, entidades

[89] Tavares, M. I. (2020), Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilicitos Fechar o Círculo. In *Regimes Jurídicos Internacionais* (Vol. 1, p. 654). Universidade Católica Editora Porto.
[90] Tavares, M. I. (2020), Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilicitos Fechar o Círculo. In *Regimes Jurídicos Internacionais* (Vol. 1, p. 654). Universidade Católica Editora Porto.
[91] Schmitt, M.N. (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, pp. 94-100.
[92] Schmitt, M.N. (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 95.

legais e comerciais como empresas de IT, empresas de hardware e de software, ciberterroristas ou insurgentes [93].

Quando as situações não são inseridas na Regra 15, nas quais a conduta das pessoas, grupo de pessoas ou agências é autorizada pelo Estado, então poderão ser inseridas neste Artigo 17. Neste artigo a conduta de pessoas, grupos de pessoas ou entidades poderão ser atribuíveis ao Estado no caso de haver uma ligação factual entre as pessoas, grupos de pessoas ou Estado. Ao dar instruções, direções específicas ou ao exercer o controlo sobre as pessoas, grupos de pessoas ou entidades, o Estado assume a responsabilidade pela sua ação ou omissão. Ao agir sobre as instruções de um Estado, geralmente aceita-se que a conduta destas pessoas foi aceite pelo Estado [94].

O *Manual de Tallinn* especifica uma situação que carateriza muito bem o que se pensa que se sabe sobre o IT Army. Segundo o *Manual de Tallinn*: «Consider, for instance, the case of unantecipated massive cyber operations directed against a State. The State has no standing cyber defense organizations. Therefore, the State instigates private individuals and groups to act as volunteers to help respond to the crisis; the individuals and group are an instrument of the State and acting on its behalf.»[95]

O grupo internacional de peritos que construiu o *Manual de Tallinn* concorda que a frase «controlo efetivo» como foi usado nos casos do TIJ *Nicarágua* e do *Genocídio* indica o sentido correto em que se pode usar a frase no universo ciber [96].

Neste momento pensa-se que há sincronização de ações e partilha de software para essa sincronização. A entrevista ao hacker português publicada no jornal Expresso não parece confirmar essa opção [97]. Mesmo assim, será que a sincronização de ações e partilha de recursos é feita por controlo, ou sobre diretrizes do Estado da Ucrânia (Artigo 8º do

[93] Schmitt, M.N.(2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 95.
[94] Schmitt, M.N. (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 95.
[95] Schmitt, M.N. (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 95. Tradução: «Considere-se, por exemplo, o caso de ciberoperações em número massivo a serem dirigidas contra um Estado. O Estado não tem quaisquer ciber organizações de defesa. Logo, o Estado insta pessoas privadas e grupos a agir como voluntários para ajudar a responder à crise. Fica claro, que durante o incidente eles estão a agir como auxiliares do Estado na resposta à crise; os individuos e o grupo são um instrumento do Estado e agem em seu nome.»
[96] Schmitt, M.N. (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 96.
[97] Soares, T. (2023, April 23). Hackers Pró-Rússia Criam "Caos" no Ocidente: A Guerra Cibernética Está Cada Vez Mais Perigosa. *Expresso*. https://expresso.pt/internacional/guerra-na-ucrania/2023-04-23-Hackers-pro-Russia-criam-caos-no-ocidente-a-guerra-cibernetica-esta-cada-vez-mais-perigosa-53e3774a

PARI e Regra 17 do *Manual de Tallinn*)? O Estado tem controlo efetivo ou geral das operações?

Segundo o *Manual de Tallinn* existe diferença entre controlo efetivo e controlo geral (limite mais baixo). Para os peritos do *Manual de Tallinn*, o controlo efetivo está a ser exercido sobre um ator não-estadual sempre que o Estado determina a execução e a forma como a operação é executada. O controlo efetivo inclui duas capacidades. A capacidade de fazer com que as diversas atividades que constituem a operação sejam levadas a cabo e também a capacidade para parar e cessar com essas atividades [98].

Com atenção a todas estas informações, não se pode considerar que exista controlo efetivo sobre as atividades do IT Army pelo Estado da Ucrânia. O hacker português falou em descoordenação, em falta de direção e controlo. Tanto mais que o grupo de portugueses selecionava os alvos e selecionava o melhor momento para provocar o ciberataque de forma a não provocar vítimas humanas desnecessárias, pelo menos na leitura da entrevista. O hacker português também discutiu o facto de alguns dos seus colegas só atrapalharem a atuação dos outros. Não estão aqui reunidos os pressupostos que o *Manual de Tallinn* alavancou para responsabilizar um Estado pela ação de um grupo de indivíduos que estaria a agir como entidade auxiliar do Estado. Não existe um controlo efetivo. Não existe a capacidade para modelar a operação, para controlar a forma como se desenrola ou para cancelar a ciberoperação caso seja necessário.

No entanto, é possível fazer uma imputação através do Artigo 8º do PARI porque o limite de imputação é o limite mais abrangente, o controlo global, pois que se pensa que o grupo de voluntários está sobre as ordens de militares e mantém-se de alguma forma organizado. Como, em princípio existe controlo pelo Estado da Ucrânia, esse Estado criou um vínculo entre o próprio Estado e as pessoas ou grupo de pessoas que se voluntariaram para o IT Army.

[98] Schmitt, M.N.(2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 96.

5. Perspetivas para o Futuro

Ao longo desta investigação cheguei às seguintes conclusões. O IT Army é um recurso operacional da Ucrânia na sua guerra contra ciberataques. Mas não se sabe muito sobre o IT Army. Aliás, o que se sabe sobre o IT Army, mesmo quando transmitido por pessoas que se dizem como elementos do IT Army, é muito contraditório.

Como demonstrei no decurso deste trabalho, é possível fazer a imputação ao Estado da Ucrânia das ações executadas pelo IT Army sobre o Artigo 4º do PARI. Existe um documento que afiança que o estatuto de combatente poderá ser em breve atribuível às pessoas que pertencem ao grupo de pessoas conhecido como IT Army. Se as pessoas que integram este grupo foram integradas como reservistas das Forças Armadas, o Estado da Ucrânia está a reconhecer as ações deste grupo como ações do Estado da Ucrânia. Isso facilitará bastante qualquer processo de imputação que a nação que se considerar prejudicada poderá requerer.

De igual forma, no caso de o IT Army não ser oficialmente reconhecido como um orgão do Estado da Ucrânia, é mesmo assim possível executar um processo de imputação. O IT Army nasceu da necessidade da Ucrânia se defender de ciberataques massivos e para os quais não tinha meios humanos ou materiais. Uma chamada para obter a ajuda de voluntários levou à criação de um grupo de pessoas que em princípio estão a exercer prerrogativas apenas atribuíveis ao Estado. A defesa e ataque no ciberespaço são prerrogativas de Estado. Quando o IT Army se identifica com esse trabalho está a cumprir com as prerrogativas do Estado que o Estado da Ucrânia não conseguiu cumprir sem a ajuda de voluntários.

É possível imputar a conduta do IT Army à Ucrânia se se quiser utilizar a Regra 15 do *Manual de Tallinn*. Precisamente pelos mesmos motivos elencados para o Artigo 4º e 5º do PARI.

Também é possível utilizar o Artigo 8º do PARI ou a Regra 17 do *Manual de Tallinn* para imputar a conduta dos voluntários do IT Army ao Estado da Ucrânia. Pensa-se que o IT Army possui algum tipo de organização e pertencerá às Forças Armadas (coisa que neste momento não é possível comprovar com as fontes que construíram este trabalho). Então não será necessário considerar que é preciso encontrar evidências de que as ações do IT Army foram totalmente controladas pelo Estado da Ucrânia (controlo

efetivo). Basta a existência de um controlo global. Parece existir financiamento, apoio logístico e também instruções específicas quanto aos alvos a que o IT Army se dedica. Talvez não exista a capacidade para cancelar operações (Regra 17 do *Manual de Tallinn*), mas isso não é necessário num quadro de controlo global (Artigo 8º do PARI).

«This is an area of the law that will remain in flux for some time» [99]. O Direito Internacional, desenvolvido ao longo de séculos, tem de se adaptar aos novos desafios. O universo digital não tem fronteiras e é incomensurável.

Conceitos como ciberataque, ou simplesmente ataque vão ter de ser reescritos e mais bem definidos no futuro. O foco terá de ser mais restringido e determinado em evidências, e até se terá de determinar que tipo de evidências poderão ser admissíveis como prova.

No ciberespaço será necessário, estabelecer critérios mínimos para validar as alegações (*standard of proof*) de violações de conduta entre Estados. Ainda não existe um *standard of proof* universal e pertinente a cada tipo de ilicitude. Talvez ajudasse a existência de uma ou várias agências internacionais, independentes e reconhecidas por todos os países. Estas agências seriam capazes de identificar as violações de conduta entre estados ao nível do ciberespaço e estabelecer *standards of proof* de cumprimento obrigatório e transparente. Isso iria nivelar esse campo do *standard of proof*.

Em simultâneo, será necessário criar um orgão internacional, sob o manto do Direito Internacional, e muito provavelmente das Nações Unidas, capaz de validar o trabalho das agências internacionais, quer os critérios quer os passos efetuados para a recolha de evidências, quer as próprias evidências (validar as provas e os procedimentos efetuados como se se tratasse de um caso policial no espaço físico).

O futuro que nos espera neste campo vai trazer mudanças, mas a vida e a coexistência são isso mesmo. Uma miríade de mudanças que vão provocar avanços e recuos civilizacionais. Dirimir estas questões jurídicas será um avanço civilizacional.

O ciberespaço é uma nova dimensão e como tal tem de ser encarado. É um campo, que embora utilize as regras do espaço físico, ultrapassa esse espaço físico e precisa de

[99] Schmitt, M.N. (2014), Rewired Warfare: Rethinking the Law of Cyber Attack, p. 204. Tradução da autora: «Esta é uma área do direito que permanecerá em fluxo por algum tempo».

mais regras e essas regras precisam ser trabalhadas especificamente para este campo ser validado, utilizado e percebido.

Bibliografia

Arquilla, J., & Ronfeldt, D. (1997). Cyberwar is Coming! In J. Arquilla & D. Ronfeldt (Eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (pp. 23–60). National Defense Research Institute RAND. https://doi.org/10.7249/MR880

Biggerstaff, W. C. (2023). *The Status of Ukraine's "IT Army" under the Law of Armed Conflict*. Lieber Institute West Point. https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/

Buchan, R., & Tsagourias, N. (2022). *Ukrainian "IT Army": A Cyber Levée en Masse or Civilians Directly Participanting in Hostilities*. Blog of the European Journal of International Law. https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/

Carvalho, A. R. (2019). Ciberespaço e os Novos Desafios à Soberania e à Segurança dos Estados. *IDN Cadernos*, *36*, 219–235.

Condorelli, L., & Kress, C. (2010). The Rules of Attribution: General Considerations. In J. Crawford, A. Pallet, & S. Olleson (Eds.), *The Law of International Responsability* (Vol. 3, pp. 221–236). Oxford University Press. https://styluscuriarum.files.wordpress.com/2018/08/condorelli-kress-the-rules-of-attribution_-general-considerations-2010.pdf

Council of the European Union. (2014). *EU Cyber Defense Policy Framework*. 1–14. https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf

CyberPeace Institute. (2023). *CyberPeace Institute*. CyberPeace Institute. https://cyberpeaceinstitute.org/

Eichensehr, K. E. (2020). The Law and Politics of Cyberattack Attribution. *U.C.L.A. Law Review*, *520*, 520–598.

Fernandes, H. (2016). As Novas Guerras: O Desafio da Guerra Híbrida. *Revista de Ciências Militares*, *IV*(2), 13–40.

Fernandes, J. P. (2012). A Ciberguerra como Nova Dimensão dos Conflitos do Século XXI. *Relações Internacionais*, *33*, 53–69.

Finlay, L., & Payne, C. (2019). The Attribution Problem and Cyber Armed Attacks. *American Journal of International Law Unbound*, *113*, 202–206. https://doi.org/10.1017/aju.2019.35

Honorato, M. da C., Santos, L. F., & Mateus, R. M. (2017). *O Ciberespaço como 5º Domínio Operacional. Impacto Estratégico na Política de Defesa Nacional* [Repositório Comum]. http://hdl.handle.net/10400.26/21956

IT Army. (2023, July 18). Wikipedia. https://en.wikipedia.org/wiki/IT_Army_of_Ukraine

IT Army of Ukraine. (2023). *IT Army of Ukraine*. IT Army of Ukraine. https://itarmy.com.ua/?lang=en

Koenders, B. (2017). Foreword. In M. N. Schmitt (Ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed., pp. XXV–XXVIII). Cambridge University Press.

Kurtzleben, D. (2022, March 27). *Volunteer Hackers from "IT Army" to Help Ukraine Fight Russia*. NPR. https://www.npr.org/2022/03/27/1089072560/volunteer-hackers-form-it-army-to-help-ukraine-fight-russia

Lewis, J. A. (2022). *Cyber War and Ukraine*. https://www.csis.org/analysis/cyber-war-and-ukraine

Lopes, J. A. (Ed.). (2020a). *Regimes Jurídicos Internacionais, Questões, Casos e Materiais* (Vol. 2). Universidade Católica Editora Porto.

Lopes, J. A. (2020b). Uso da Força e Direito Internacional Direito em Tempos de Cólera. In *Regimes Jurídicos Internacionais* (Vol. 1, pp. 80–109). Universidade Católica Editora Porto.

Maddocks, J. (2022, November 4). *State Responsability for Non-State Actor's Conduct*. Ukraine Symposium; Lieber Institute West Point. https://lieber.westpoint.edu/state-responsibility-non-state-actors-conduct/

Martins, I. M. (2022). *A Imputação de Ciberataques aos Estados* [Dissertação de Mestrado, Repositório Universidade Católica Portuguesa]. https://repositorio.ucp.pt/bitstream/10400.14/39892/1/203156218.pdf

Momtaz, D. (2010). Attibution of Conduct to the State: State Organs and Entities Empowered to Exercize Elements of Governmental Authority. In *The Law of International Responsability* (pp. 237–246).

Moreira, J. M. (2012). *O Impacto do Ciberespaço como Nova Dimensão nos Conflitos* [Trabalho de Investigação, Repositório Comum]. https://comum.rcaap.pt/handle/10400.26/12369

Nations Unies. (2005). *Projet d'Articles sur la Responsabilité de l'État pour Fait Internationalement Illicite*. Nations Unies. https://legal.un.org/ilc/texts/instruments/french/draft_articles/9_6_2001.pdf

North Atlantic Treaty Organization. (2016, July 9). *Warsaw Summit Communiqué Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8-9 July 2016*. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Office of the Chairman of the Joint Chiefs of Staff. (2021). *DOD Dictionary of Military and Associated Terms*. The Joint Staff. https://irp.fas.org/doddir/dod/dictionary.pdf

Oorsprong, F. M., Ducheine, P. A., & Pijpers, B. M. (2021). *Armed Attack in Cyberspace Clarifying and Assessing When Cyber-Attacks Trigger the Netherlands' Right of Self-Defence* (No. 2021–09; Amsterdam Law School Legal Studies Research Paper).

Pearson, J. (2022). *Ukraine launches "IT Army" Takes Aim at Russian Cyberspace*. Reuters. https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/

Pinho, A. L. (2022). Ciberdefesa, Ciberdissuasão e Poder Nacional no Ciberespaço. *IDN Brief*, *Julho*, 1–3.

Rio Durán, J. J. (2011). La Ciberseguridad en el Ámbito Militar. In *Ciberseguridad, Retos y Amenazas a la Seguridad Nacional en el Ciberespacio* (Vol. 149, pp. 217–256). Instituto Español de Estudios Estratégicos, & Instituto Universitario «General Gutierrez Mellado».

Rodrigues, J. G. (2023, February 23). *"Atacamos Tudo Menos Hospitais e Serviços Essenciais". Por Dentro do Grupo de Hackers Portugueses que Luta contra a Guerra da Rússia*. CNN. https://cnnportugal.iol.pt/ciberataque/ciberseguranca/atacamos-tudo-menos-hospitais-e-servicos-essenciais-por-dentro-do-grupo-de-hackers-portugueses-que-luta-contra-a-guerra-da-russia/20230223/63f67feb0cf2c84d7fc94ad2

Schmitt, M. N. (2013). Introduction. In *Tallinn Manual on the International Law Applicable Cyber Warfare* (pp. 1–11). Cambridge University Press.

Schmitt, M. N. (2014). Rewired Warfare: Rethinking the Law of Cyber Attack. *International Review of the Red Cross*, *96*(893), 189–206. https://doi.org/10.1017/S1816383114000381

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge University Press.

Schmitt, M. N. (2022, July 28). *The Evolution of Cyber Jus Ad Bellum Thresholds*. Ukraine Symposium. https://lieber.westpoint.edu/evolution-cyber-jus-ad-bellum-thresholds/

Soares, T. (2023, April 23). Hackers Pró-Rússia Criam "Caos" no Ocidente: A Guerra Cibernética Está Cada Vez Mais Perigosa. *Expresso*. https://expresso.pt/internacional/guerra-na-ucrania/2023-04-23-Hackers-pro-Russia-criam-caos-no-Ocidente-a-guerra-cibernetica-esta-cada-vez-mais-perigosa-53e3774a

Soesanto, S. (2022). *The IT Army of Ukraine Structure, Tasking, and Ecosystem*. https://doi.org/10.3929/ethz-b-000552293

Tavares, M. I. (2020). Responsabilidade Internacional dos Estados por Factos Internacionalmente Ilícitos Fechar o Círculo. In *Regimes Jurídicos Internacionais* (Vol. 1, pp. 631–732). Universidade Católica Editora Porto.

The NATO Cooperative Cyber Defense Centre of Excellence. (n.d.). *The Tallin Manual*. CCDCOE. Retrieved July 19, 2023, from https://ccdcoe.org/research/tallinn-manual/

Ukraine Creates IT Army of 300,000 Specialists - Fedorov. (2022, May 24). Interfax - Ukraine. https://en.interfax.com.ua/news/general/834508.html

Weedon, J. (2015). Beyond "Cyber War": Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine. In *Cyber War in Perspective: Russian Agression Against Ukraine* (pp. 67–77). NATO Cooperative Cyber Defense Centre of Excellence.

Zaytseva, O. (2014). Responsabilidade Internacional dos Estados: Projeto da Comissão de Direito Internacional sobre a Responsabilidade dos Estados por Atos Internacionalmente Ilícitos. *Jurismat*, *4*, 369–389. https://recil.ensinolusofona.pt/bitstream/10437/6396/1/jurismat4_369-390.pdf