**UNIVERSIDADE CATÓLICA PORTUGUESA**

# A imputação de ciberataques aos Estados

Inês Maria Araújo Martins

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2022

**UNIVERSIDADE CATÓLICA PORTUGUESA**

# A imputação de ciberataques aos Estados

Inês Maria Araújo Martins

Orientador: José Alberto Azeredo Lopes

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2022

## Resumo

O ciberespaço tem-se assumido como um desafio para alguns regimes jurídicos do Direito Internacional. A presente dissertação, apesar de abordar os desafios presentes noutros regimes, terá como foco aquele que se levanta no regime da responsabilidade internacional, mais especificamente, o da imputação de ciberataques a Estados.

Assim, num primeiro momento, irá abordar os diferentes domínios que o ciberespaço dispõe para a perpetração de ciberataques, o que representa para conflitos híbridos e as implicâncias nas políticas de defesa dos Estados e das organizações, no âmbito da ciberdefesa e cibersegurança.

Feito o enquadramento do domínio onde as operações em análise têm lugar, passaremos ao tema central da dissertação, a imputação de ciberataques aos Estados. Neste contexto, serão abordados os diferentes processos de imputação: técnica, política e jurídica, assim como as dificuldades associadas a cada uma delas. Mais, exemplificaremos, com casos de ciberataques reais, a importância da interligação dos vários processos da imputação, para que se obtenha uma imputação do ciberataque ao Estado mais esclarecida.

De seguida, abordaremos a importância que a imputação de ciberataques desempenha no regime da responsabilidade internacional, assim como na restauração da segurança e paz internacional.

Por fim, serão referidas, e criticadas, soluções apresentadas por algumas entidades privadas, para que se verifique uma evolução nos processos da imputação.



**Palavras-chave:** Ciberespaço, ciberataques, imputação, responsabilidade, ciberdefesa, cibersegurança.

## Abstract

Cyberspace has been assumed as a challenge for some International Law's legal regimes. This dissertation, despite addressing other legal regimes' challenges, will focus on the one that arises from the international responsibility regime, more specifically, the attribution of cyberattacks to States.

Thus, at first, we will address the different domains that cyberspace has for the perpetration of cyberattacks, what it represents for hybrid conflict and the implications for States and organizations defense policies, regarding cyberdefence and cybersecurity.

After framing the domain where the operations under analysis take place, we will move to the dissertation starring theme, the attribution of cyberattacks to States. In this context, the different processes of attribution (political, legal, technical) will be address, as well as the associated difficulties of each one of them. Furthermore, we will exemplify, with real cyberattacks cases, the importance of connecting the various attribution processes to obtain a more enlightened attribution.

Next, we will address the importance that attribution of cyberattacks plays in the international responsibility regime, as well as in the restoration of international security and peace.

Finally, we will mention, and criticize, solutions presented by some private entities to improve attribution processes.



**Keywords:** Cyberspace, cyberattacks, attribution, responsibility, ciberdefence, cybersecurity.

# Introdução

A rapidez e eficácia com que hoje em dia obtemos e difundimos informação deve-se à evolução tecnológica que tem ocorrido a um ritmo bastante acelerado. No entanto, é igualmente devido a esse fenómeno que existe uma crescente dependência das sociedades modernas em relação à internet, que as leva a viver num mundo permanentemente *online*. Devido ao papel essencial que a tecnologia desempenha no nosso quotidiano, o ciberespaço constitui um domínio que merece a nossa crescente atenção[1].

O ciberespaço, atualmente, comporta as informações essenciais de todos os cidadãos, assim como dos Estados. As infraestruturas essenciais são totalmente dependentes da internet o que, apesar das vantagens, apresenta uma porta para vulnerabilidades, nunca exploradas. Vários atores, estaduais ou maliciosos, passam a deter uma ferramenta para se manifestar, sendo através da difusão de informação relevante, ou propaganda, como canal de comunicação para ordenar, ou prevenir, ataques ou mesmo para perpetrar ciberataques.

Esta evolução consubstancia um desafio para o Direito Internacional, na medida em que levanta questões relacionadas com os vários regimes jurídicos que abarca. Põe à prova conceitos relacionados com o regime jurídico do uso da força, assim como do Direito Internacional Humanitário e da Responsabilidade Internacional.

Atendendo aos desafios relacionados com a ascensão do ciberespaço, num primeiro momento do nosso estudo abordaremos a dimensão ciber dos conflitos híbridos modernos, explorando o conceito de ciberespaço e os domínios que este apresenta como mais relevantes no contexto de conflitos, sendo eles o domínio mediático de comunicação e o domínio de operações. Neste último, prestamos especial atenção à diferenciação dos conceitos de cibercrime, ciberataque e ciberguerra para clarificar quando estamos no âmbito do direito internacional ou do direito nacional.

Num segundo momento, prender-nos-emos com o que representa este novo domínio para as políticas de defesa e segurança, dos Estados e de organizações, assim como a necessidade de apostar na conetividade e partilha entre ambos. Assim, analisaremos como a ciberdefesa e cibersegurança apesar de visarem objetivos diferentes, podem melhorar com a interação entre os atores encarregues de cada uma.

[1] Cf. (Moniz, Impacto do Ciberespaço na Sociedade em Rede, 2018).

O terceiro momento do estudo, e tema central da dissertação, prende-se com a análise de um desafio específico ao direito internacional, levantado pelo ciberespaço, no âmbito do regime da responsabilidade internacional. A questão da imputação de ciberataques aos Estados enfrenta dificuldades relacionadas com os processos de identificação do autor de um ciberataque, nas suas vertentes técnica, política e legal. Este capítulo explorará cada uma das vertentes, interligando-as e representando-as com exemplos de ciberataques reais.

No seguimento do ponto anterior, temos o tema da importância da imputação de ciberataques aos Estados, explorando as respostas possíveis a um determinado ciberataque, atendendo às suas caraterísticas e severidade, apresentadas pelo regime da responsabilidade internacional.

Por fim, serão apresentadas algumas propostas de soluções para que se possa verificar um progresso dos processos de imputação. As soluções apresentadas pela *Microsoft*, *Atlantic Council* e Corporação *RAND*, passam pela criação de uma entidade internacional de imputação que, dependendo da proposta, varia na natureza, mas mantem o objetivo de obter uma imputação eficaz, eficiente e imparcial.

# I. A dimensão ciber dos conflitos híbridos modernos

Cada vez mais se tem ouvido falar do conceito de conflitos híbridos e da sua ascensão no Século XXI. Contudo, não se trata de um fenómeno novo. A natureza e os meios de condução de um conflito têm vindo a sofrer alterações devido às transformações da tecnologia, das realidades políticas e das ideologias[2]. Reflexo dessa transformação são as duas grandes guerras[3], a guerra fria[4], e os conflitos que envolveram atores não estaduais (por exemplo: ISIS, Al-Qeda)[5].

Apesar da sua larga existência, permanece um conceito contestado e merecedor de várias definições[6], sendo a apresentada por *Frank Hoffman* a mais vezes citada *"as ameaças híbridas incorporam uma série completa de diferentes modos de guerra, incluindo capacidades convencionais, táticas e organizações irregulares, atos terroristas, incluindo violência e coação indiscriminada, e desordem criminal. As guerras híbridas podem ser conduzidas tanto pelos Estados como por uma variedade de atores não estatais. Essas atividades multimodais podem ser conduzidas por unidades separadas, ou até pela mesma unidade, mas geralmente são dirigidas e coordenadas, operacional e taticamente, dentro do campo de batalha principal visando obter efeitos sinérgicos nas dimensões físicas e psicológicas do conflito. Os efeitos podem ser obtidos em todos os níveis da guerra."*[7]

Ora, apesar de o conceito de conflitos híbridos não constituir novidade, tem manifestado dimensões diferentes, que demonstram um aproveitamento dos avanços da tecnologia e caraterizam os conflitos híbridos modernos, como é o caso da utilização do ciberespaço.

---

[2] Cf. (Bhuiyan, 2018), págs. 341 e seguintes.
[3] Id. (Bhuiyan, 2018), págs. 344-347.
[4] Id. (Bhuiyan, 2018), págs. 347-348.
[5] Id. (Bhuiyan, 2018), págs. 349-351; (Hoffman, 2007), págs. 18 e seguintes.
[6] Cit. (Qureshi, 2020), pág. 176: *"spectrum wars with both physical and conceptual dimensions: the former, a struggle against an armed enemy and the latter, a wider struggle to control and support of the combat zone's indigenous population, the support of the home fronts of the intervening nations, and the support of the international community"*; Cit. (Bilal, 2021):*"[...] hybrid warfare remains entails an interplay or fusion of conventional as well as unconventional instruments of power and tools of subversion"*; Cit. (Ducaru, 2016), pág. 10: *"[...] is described as a shift away from a traditional force-on-force model to an approach which combines military and non-military tools in a deliberate and synchronized campaign to destabilize and gain political leverage over an opponent."*
[7] Tradução nossa. Ver original: (Hoffman, 2007), pág. 8.

## A. Ciberespaço

O ciberespaço pode ser entendido como *"[...] um novo domínio de acesso aberto e global, caraterizando-se pela ausência das tradicionais fronteiras físicas.*[8]*"* Trata-se de um domínio construído inteiramente pela mão humana, onde assenta a internet. Contudo, a sua constituição não passa meramente pelo plano virtual. De acordo com Paulo Moniz[9], o ciberespaço é composto por uma vertente física, que corresponde às infraestruturas de servidores, equipamentos de rede e links de comunicação que consubstanciam a internet, assim como por uma vertente lógica, que corresponde a aplicações e conteúdos onde ocorrem as trocas de informação.

Enquanto domínio aberto, o ciberespaço levou a que se verificasse uma alteração no paradigma das relações de poder[10]. Antes do ciberespaço, era do entendimento geral que o poder se encontrava concentrado maioritariamente nas mãos dos Estados. No entanto, com o desenvolvimento da tecnologia e com a crescente importância do ciberespaço, tornou-se possível que vários indivíduos, mesmo que com poucos recursos, e localizados em qualquer parte do mundo, adotassem uma voz mais ativa e influenciassem os acontecimentos do mundo. Assim, este domínio combina a existência de ameaças provenientes de atores estatais e não estatais e expõe vulnerabilidades civis e militares.

Tal permite-nos caraterizar o ciberespaço através de quatro elementos: baixas barreiras de entrada[11], possibilidade de ocultação[12], mutabilidade[13] e ausência de fronteiras geográficas, no seu sentido convencional.

---

[8] Cit. (Nunes, 2018), pág. 13.

[9] Cf. (Moniz, Impacto do Ciberespaço na Sociedade em Rede, 2018), pág. 19.

[10] De acordo com o autor, poder *"implica a capacidade de exercer "força" ou "influência" de modo a provocar um efeito desejado em determinado domínio"*, ao passo que ciberpoder se trata dessa capacidade no ciberespaço, ou seja, *"capacidade de usar o ciberespaço para criar vantagem ou eventos de influência em outros ambientes operacionais através de instrumentos de poder".* (Moniz, Terrorismo e Violência Política: Como Combater o Ciberterrorismo e a Radicalização, 2019), pág.61.

[11] Atualmente, qualquer pessoa pode, facilmente, aceder a um sistema por via de uma rede global com recurso a um computador, independentemente do sítio onde se encontre. Tal se pode verificar com o aumento da disponibilidade de ferramentas para que se proceda a um ciberataque, sendo cada vez menos necessário ter grandes capacidades tecnológicas para se proceder a uma ação criminosa. – Ver (Moniz, Terrorismo e Violência Política: Como Combater o Ciberterrorismo e a Radicalização, 2019), págs. 63-64 e (Jr., 2010), págs. 3-7.

[12] Ibid. 11: Facilidade com que os atores do ciberespaço têm em agir de forma mal-intencionada, uma vez que lhes é permitido esconder-se por detrás de identidades fictícias ou geografias remotas. Um bom exemplo do exercício do ciberpoder é, exatamente, a facilidade de ocultação.

[13] Ibid. 11: Encontra-se ligada à sua natureza, isto é, ao facto de se tratar de um espaço construído inteiramente pelo homem. Este domínio encontra-se suscetível a uma evolução constante, uma vez que a

Ora, devido a estas caraterísticas atrativas, o ciberespaço tem sido utilizado como ferramenta dos conflitos híbridos. Por um lado, o facto de se tratar de um domínio partilhado, rápido e eficaz faz com que seja utilizado como instrumento facilitador da disseminação de comunicações, propaganda, e, manipulação e distorção da informação. Por outro lado, serve de domínio de operações, complementando ou amplificando os efeitos das operações militares convencionais.

## B. O Ciberespaço como domínio mediático de comunicação

Este domínio pode ser utilizado por vários atores como uma ferramenta de comunicação. De todos eles, destacaremos a sua utilização por ciberterroristas.

Um dos principais objetivos dos terroristas na utilização do ciberespaço passa pela disseminação de propaganda, geralmente, através de mensagens, apresentações, revistas[14], áudios, vídeos e videojogos realizados pelas organizações terroristas. As maiores ameaças apresentadas na propaganda terrorista prendem-se com a forma como é utilizada, a intenção com que é disseminada[15] e o público que atinge. Assim, tanto se pode destinar a apoiantes potenciais ou reais, como pode ser focada no recrutamento, na radicalização ou, até mesmo, no incitamento ao terrorismo, por meio de mensagens que transmitem o orgulho, dedicação e realização desse objetivo extremista. A propaganda também pode ser utilizada para demonstrar a execução eficaz de ataques terroristas àqueles que fornecem apoio financeiro, ou, para manipular psicologicamente a crença de um individuo em certos valores sociais ou propagar um sentimento de ansiedade e medo na população ou num grupo da população. Tal demonstração, ou manipulação, pode dar-se através da divulgação de desinformação, boatos, ameaças de violência ou imagens provocatórias e demonstrativas de atos violentos.

---

tecnologia se encontra em constante progressão, o que se revela essencial para se compreender o exercício do poder no ciberespaço.

[14] Algumas das revistas online conhecidas são: a *Rumiyah* (7 edições publicadas em oito línguas – inglês, francês, alemão, russo, turco, uigur, indonésio e pashtum), a *Dabiq* (6 edições publicadas em inglês, até 2016, acabando por ser substituída pela revista *Rumiyah*), a *Inspire* (24 edições publicadas em inglês, pela Al-Qaeda da Península Arábica), a *Al-Naba* (69 edições publicadas em árabe, desde 2014), a *Dar Al-Aslam* (6 edições publicadas em francês, entre 2015 e 2016), a *Konstaninniyye* (6 edições publicadas em turco, entre 2015 e 2016), e a *Istok* (publicada em russo, entre 2015 e 2016). Sobre esta matéria, ver: (Elias, 2019).

[15] Note-se, no entanto, que nem toda a propaganda disseminada é considerada proibida, uma vez que tal poderia ser considerado violador do direito à liberdade de expressão. Assim, o indivíduo encontra garantido o direito a expressar a sua opinião, mesmo que esta seja contestada por outrem, dentro dos limites impostos pelo interesse público. Cf. (Casimiro, 2018).

De todos os objetivos referidos com que os terroristas disseminam propaganda, podemos destacar o recrutamento, o incitamento e a radicalização, para procedermos a uma análise mais detalhada de cada um deles. A propaganda terrorista é normalmente talhada para apelar a grupos mais vulneráveis e marginalizados da sociedade, pelo que capitaliza os sentimentos de injustiça, exclusão ou humilhação do seu alvo. Pode ainda ser adaptada, conforme a idade[16] ou o género, assim como a situação económica ou social que pretende atrair. O recrutamento também pode ser realizado clandestinamente em *websites*[17] protegidos com palavra-passe, ou chats de grupo restritos acessíveis pela internet.

Relativamente ao incitamento, temos que a internet providencia material abundante, assim como oportunidades de fazer *download*, de editar e distribuir conteúdo que possa ser considerado de glorificação ilegal, ou de provocação, que podem levar ao cometimento de atos terroristas. Todavia, é importante enfatizar a importância da distinção entre mera propaganda e disseminação de material com intenção de incitar ao cometimento de atos terroristas.

Por fim, temos a radicalização, podendo esta entender-se como recrutamento e o incitamento como atos interligados que levarão, num último momento ao cometimento do ato terrorista, sendo que a radicalização se refere ao processo de doutrinação. Esta, muitas vezes, acompanha a transformação de meros recrutas em indivíduos determinados a agir violentamente com base em ideologias extremistas. Neste processo, a propaganda pode ser disseminada quer pessoalmente, quer através da internet, e, não apresenta um período de eficácia definido, isto é, a doutrinação pode levar mais tempo para uns e menos tempo para outros.

Para além da propaganda, o ciberespaço pode facilitar o financiamento terrorista. O modo como os terroristas utilizam a internet para recolher fundos pode ser classificada

[16] Por exemplo, quando é pretendido recrutar menores, normalmente, utiliza-se propaganda sob a forma de cartoons, videoclipes populares ou jogos de computador. Veja-se: (UNODC, 2012)

[17] Um *website* terrorista normalmente inclui informação acerca da história do grupo ou organização; biografias dos seus líderes, fundadores e heróis; informações sobre as suas ideologias políticas ou religiosas; e notícias. Desta forma, temos que nos websites não é comummente mencionada a violência que estes grupos empregam nas suas ações, ao invés, investem na informação relativa às suas ideologias e à sua história. Cf. (Santos L. , 2018), (Santos, Nunes, Ralo, & Mendes, 2018) e (Elias, 2019).

em quatro categorias: solicitação direta[18], comércio eletrónico[19], pagamentos e transferências online[20], e através de organizações sem fins lucrativos[21].

Nos últimos anos, as organizações terroristas têm utilizado esta ferramenta para proceder a treinos dos seus membros. Na internet é possível encontrar informação e instruções pormenorizadas, sob a forma de manuais, áudios e vídeos[22], acerca da forma como se constroem explosivos e se planeiam atentados. Estas informações e instruções são transmitidas em várias línguas para poderem chegar ao máximo número de pessoas possível. Algum material instrutório disponível online incluía ferramentas de apoio ao desenvolvimento de atividades de contra informação e *hacking*.

O ciberespaço pode ser igualmente utilizado para que estas organizações procedam ao planeamento[23] dos seus ataques. Assim, quer a facilidade de se estabelecer comunicações seguras e praticamente anónimas, entre vários agentes, quer a partilha de informação em tempo real, permitem um planeamento de ataques terroristas com mais facilidade. Para além desta informação, cumpre ainda referir o facto de ser utilizada uma outra que se encontra disponível para o público em geral, como por exemplo, a informação disponibilizada no *Google Earth*, ou, até mesmo, informação partilhada pelas próprias possíveis vítimas no *Facebook*, *Instagram*, *YouTube*, entre outros.

Por fim, temos que a internet pode ser utilizada para que estas organizações possam proceder à execução destes ataques. Assim, o ciberespaço pode ser utilizado quer

[18] A solicitação direta refere-se à utilização de websites, chats de grupo e emails correntes de modo a recolherem doações dos seus apoiantes. Cf. (UNODC, 2012).
[19] O comércio eletrónico encontra-se relacionado com a venda de livros, áudios e vídeos a apoiantes através de websites. Cf. (UNODC, 2012)
[20] Algumas instituições que permitem o pagamento online podem ser exploradas através de meios fraudulentos, como roubo de identidade, roubo de cartão de crédito, fraude eletrónica e crimes de propriedade intelectual. Cf. (UNODC, 2012).
[21] Trata-se de organizações que parecem legitimas, mas que na verdade são utilizadas para fins ilegítimos, como a recolha de fundos para apoiar organizações terroristas. Algumas organizações foram descobertas como tendo por objetivo financiar organizações terroristas no Médio Oriente. Foi o caso da *Benevolence International Foundation*, *Global Relief Foundation* e *Holy Land Foundation for Relief and Development.* Cf. (UNODC, 2012).
[22] Por exemplo, a revista *Inspire* foi criada e publicada com o intuito de facilitar o treino para o jihad em casa. A revista continha um vasto material ideológico que visava encorajar o terrorismo, incluindo discursos atribuídos a Osama Bin Laden, Sheikh Ayman al-Zawahiri e outras figuras conhecidas da Al-Qaeda.
[23] No caso *Public Prosecutor v. Hicheur*, de 4 de maio de 2012, n.º 0926639036, do Tribunal de Grande Instance de Paris, foi ilustrado as várias formas como a internet pode ser utilizada para facilitar a preparação de atos terroristas.

para coordenar e perpetrar ataques físicos[24], quer para levar a cabo outras ações que visam gerar o medo e o pânico na comunidade[25].

## C. Ciberespaço enquanto domínio de operações

Demonstrando a preocupação com o aumento do impacto do ciberespaço na segurança internacional, a NATO reconheceu o ciberespaço como o quarto domínio operacional, na Cimeira de Varsóvia em 2016. O reconhecimento formal neste sentido, não só pela NATO, mas também pelos Estados, implicou uma alteração nas preocupações nacionais ao nível da proteção e salvaguarda nacionais.

As operações que ocorrem neste domínio admitem várias formas, como por exemplo, a extração de dados ou espionagem; manipulação de dados e informação; e a perpetração de ciberataques que, por sua vez, podem servir como meio, tanto para facilitar como complementar as operações convencionais, ou como fim em si mesmo. Algumas ciberoperações são mais sofisticadas que outras, uma vez que têm por base inovações tecnológicas revolucionárias. Essas operações desafiam os conceitos tradicionais relacionados com esta matéria, por influência da perspetiva ciber, o que levou a que grande parte da doutrina, especialistas e mesmo organizações, se tenham dedicado a explorar e esclarecer as diferenças entre conceitos, como: cibercrimes, ciberataques e ciberguerra.

A clarificação teórica destes conceitos ajuda a esclarecer questões jurídicas, como por exemplo, a de saber quais os regimes jurídicos a aplicar; a quem se deve atribuir a responsabilidade; e quais os mecanismos legais possíveis de acionar, quando perante situações de cibercrime, ciberataque ou ciberguerra.

Quando falamos de cibercrimes, temos, necessariamente, de referir a Convenção de Budapeste de 2001[26], um tratado multilateral que visa aumentar a cooperação e harmonização do direito doméstico entre os Estados signatários para combater crimes perpetrados no ciberespaço, tais como os dirigidos, tendencialmente, contra pessoas ou contra interesses patrimoniais ou, contra dados e informação. Entende-se, assim, por

[24] Tome-se por exemplo o ataque de 11 de setembro de 2001, onde a internet foi intensamente utilizada para a coordenação dos participantes no atentado.
[25] Tome-se por exemplo, a difusão de vídeos de decapitações, apedrejamentos e homicídios pelo autodesignado "Estado Islâmico".
[26] A igualmente designada Convenção do Conselho da Europa sobre o Cibercrime de 2011, divide a atenção em 3 domínios: direito penal substantivo (artigos 2.º a 13.º); direito processual penal (artigos 14.º a 22.º); e cooperação internacional (artigos 23.º a 35.º).

cibercrime *"todo o ato em que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é o alvo desse ato"*[27].

Portugal ratificou a referida Convenção levando a que a Assembleia da República aprovasse a atual Lei do Cibercrime, n.º 109/2009. Tal contribuiu para a atualização e harmonização legislativa com vista a uma mais eficaz criminalização das condutas referidas. Para além disso, capacitou os órgãos de investigação criminal e os órgãos de polícia criminal na prossecução dos seus objetivos no ciberespaço. Assim, o plano de atuação para lidar com a segurança no ciberespaço, isto é, a cibersegurança, passa pela prossecução criminal destes atos e pela condenação concreta do autor do crime[28].

O conceito de ciberataque foi definido pelo grupo de especialistas encarregue da produção do manual de Tallinn (doravante manual), na regra 92, como *"uma operação ciber, ofensiva ou defensiva, que razoavelmente se espera que provoque lesões ou morte de pessoas ou danifique ou destrua objetos"*[29]. Para além deste, a doutrina[30] e algumas organizações internacionais[31], apresentaram outras definições. A par da definição de ciberataque, o manual esclarece o conceito de ataque, adotando a definição presente no artigo 49.º/1 do PA I: *"[a] expressão "ataque" designa os actos de violência contra o adversário, quer sejam actos ofensivos, quer defensivos."*[32] Ora, sendo o conceito de ataque inerente ao conceito de ciberataque, temos que este último se distingue de

[27] Cit. (Santos L. , 2018), pág. 28.
[28] O mesmo objetivo de levar à justiça criminosos, também se aplica a terrorismo ou espionagem, envolvendo neste caso os serviços de informações nacionais.
[29] Tradução nossa
[30] Cit. (Hughes & Shaffer, 2020), *"[...] tentativas de danificar o adversário através de ataques sobre os computadores, redes de informação ou qualquer outra faceta da sociedade moderna de tecnologias da informação"*, pág. 300 (tradução nossa); Cit. (Hathaway, et al., 2012), *"Um ciberataque consiste em qualquer ação tomada com vista a prejudicar o funcionamento de uma rede de computadores devido a objetivos políticos ou de segurança nacional"*, pág. 826 (tradução nossa).
[31] De acordo com (Comite Internacional da Cruz Vermelha, 2011): *"[…] It is sometimes claimed that cyber operations do not fall within the definition of "attack" as long as they do not result in physical destruction or when its effects are reversible. […]."*
[32] Ora, estando nós num contexto em que um Estado ataca um outro Estado no domínio ciber, quer no âmbito de um conflito armado já a decorrer, ou despoletando, com essa ação, um conflito armado novo, as regras de Direito Internacional Humanitário serão aplicadas (veja-se nesse sentido: (Tavares, 2020), pág. 246, tal como nos indica a regra 80 do Manual. Ou seja, aplicam-se as Convenções de Genebra, assim como os Protocolos Adicionais, ao conflito armado (note-se que, a aplicação das regras de DIH não depende da qualificação do evento sob o *jus ad bellum*, uma vez que de acordo com o princípio da igualdade de aplicação, mesmo o recurso à força armada ilícito, do ponto de vista do jus ad bellum, está sujeito ao direito do conflito armado. Tal é refletido no §5 do Preâmbulo do Protocolo Adicional I). Mais se acrescenta que, a perpetração de ataques no domínio ciber, enquanto força militar, em nada altera a qualificação do conflito e as regras que se lhe aplicam. Assim, se se tratar de um conflito interestadual, aplicar-se-ão as regras de conflitos internacionais (ver regra 82 do Manual), e, caso se trate de um conflito não-internacional (ver Regra 83 do Manual) aplicam-se as regras relativas a estes.

ciberoperação em geral, ao exigir a ocorrência de "atos de violência"[33]. A clarificação deste conceito é essencial, uma vez que representa o primeiro passo para a imputação, isto é, representa a delineação do objeto da imputação. Assim, se perante um evento este for classificado como ciberataque, identifica-se o objeto da imputação, o que permite que se prossiga para a identificação do agente perpetrador e o regime jurídico que permita responsabilizá-lo. O regime jurídico variará consoante o agente que for identificado como responsável, sendo que o objeto de estudo da dissertação se prende com o regime jurídico da responsabilidade dos Estados, mais especificamente, no elemento da imputação.

Atualmente, a perpetração de ciberataques[34] pode ser originada por diferentes métodos[35], sendo que os mais utilizados são a negação de serviço, *defacement*, *logic bomb*, *sniffer*, cavalo de Tróia, vírus, *worm* e *botnet*. Na negação de serviço, os utilizadores autorizados perdem o acesso ao sistema e vice-versa. A partir de um sistema, o invasor começa a imergir nos computadores alvo acedendo a mensagens e bloqueando o fluxo de dados, levando a que o sistema não consiga aceder à internet nem comunicar com outros sistemas. Já na negação de serviços distribuído, o agente ao invés de lançar um ataque a partir de uma única fonte, utiliza uma rede de sistemas informáticos infetados. O *defacement* não tem como objetivo aceder ou extrair informações, mas sim deixar uma mensagem, modificando a aparência do conteúdo[36]. A *logic bomb* consiste num código dentro de um programa que realiza atos destrutivos com base na ocorrência de um evento específico[37]. O cavalo de Troia é um programa, por norma malicioso, disfarçado de um programa relevante para o utilizador[38]. O *sniffer* é um programa utilizado para escutar conversas eletrónicas e ganhar acesso a informação que de outra forma não estaria disponível[39]. O vírus é um *malware* capaz de se multiplicar. Este pode diferir na sua natureza e objetivos, pelo que existem vários tipos de vírus[40]. Por seu turno, a *worm* é essencialmente um programa capaz de se replicar e propagar de uma forma autónoma, podendo implodir um sistema devido ao consumo excessivo de espaço dos

[33] Esclareça-se apenas que, segundo o grupo de especialistas, o termo "atos de violência" deve ser entendido no sentido dos efeitos provocados pelo ataque, e não da natureza deste. Assim, desde que as consequências do evento sejam destrutivas, este poderá considerar-se um ataque que, se ocorrer no espaço ciber, designar-se-á de ciberataque.
[34] Neste sentido, veja-se: https://www.aura.com/learn/types-of-cyber-attacks
[35] Passando pelo *hacking* e pela utilização de *softwares maliciosos*.
[36] Cf. (Fujita, Nguyen, Vu, Banh, & Puta, 2018), págs. 116 e ss.
[37] Cf. (Stephenson & Gilbert, 1999), pág.38.
[38] Cf. (Stephenson & Gilbert, 1999), pág.36.
[39] Cf. (Tipton & Krause, 2003), pág. 223.
[40] Cf. (Stephenson & Gilbert, 1999), págs. 31-35.

recursos de processamento[41]. Por último, temos a *botnet* que se trata de uma rede de sistemas infetados, explorada sem que os seus proprietários se apercebam. A *botnet* visa recolher informação sensível de sistemas governamentais e comerciais, roubar dados pessoais, distribuir *spam* e lançar ataques de negação de serviço que enchem os servidores, podendo danificar os serviços *online*[42].

Por fim, temos o conceito de ciberguerra que *"corresponde a uma ação planeada e executada numa perspetiva militar"*[43]. Atende aos ciberataques de nível mais alto e complexo realizados contra os interesses ciber de outros países e desencadeia consequências severas. Desta forma, podemos estar perante uma situação em que os efeitos de um ciberataque correspondem aos efeitos de um ataque armado ou uma situação em que uma ciberoperação ocorra no contexto de um ataque armado. O comando e a gestão dessas situações competem à Defesa Nacional, que agirá dentro dos planos de atuação definidos no âmbito da ciberdefesa.

Posto isto, podemos concluir que, apesar de todos os conceitos se referirem a operações que ocorrerem no domínio ciber, distinguem-se no que diz respeito ao seu tratamento jurídico. Para além disso, vimos que, em algumas situações são desencadeados planos de cibersegurança, ao passo que noutras são desencadeados planos de ciberdefesa, pelo que se revela essencial distinguirmos estes conceitos.

[41] Cf. (Stephenson & Gilbert, 1999), págs. 37-38.
[42] Cf. (Tiirmaa-Klaar, Gassen, Gerhards-Padilla, & Martini, 2013), págs. 3-4.
[43] Cit. (Moniz, Impacto do Ciberespaço na Sociedade em Rede, 2018), pág. 24.

# II. Ciberdefesa e Cibersegurança

Desde o 11 de setembro de 2001 tem-se verificado um aumento da sofisticação e frequência com que os ciberataques têm vindo a ocorrer. Esse crescimento deve-se à evolução tecnológica, ao crescimento de campanhas ciber, patrocinadas por Estados, tendo em vista o ataque de outros Estados, e uma maior conetividade entre os *hackers*. A consequência do aumento de ciberataques tem, igualmente, contribuído para uma maior atenção por parte dos Estados. Estes passaram a discutir esta matéria e a focarem-se na pesquisa relativa ao melhoramento do processo de construção de políticas de ciberdefesa e cibersegurança. Já é visível o esforço nacional de alguns governos, que têm atendido à necessidade de desenvolver e reforçar as capacidades ciber nacionais, para propósitos ofensivos e defensivos, tendo iniciado centros de ciberdefesa nacionais[44], assim como iniciativas bilaterais[45] e organizações internacionais[46].

Ao mesmo tempo, este crescimento tem vindo a levantar algumas questões jurídicas ligadas à segurança e defesa no ciberespaço, que se podem identificar enquanto questões de cibersegurança e de ciberdefesa. Estes conceitos podem distinguir-se pelos diversos graus de segurança envolvida, intervenientes e formas de resposta.

De uma forma geral, entende-se por cibersegurança *"o conjunto das atividades, que ocorrem no ciberespaço, de prevenção monitorização e resposta às ameaças que, pela sua natureza disruptiva, coloquem em risco o bem-estar e salvaguarda dos direitos dos cidadãos ou organizações."*[47] A competência para assegurar a cibersegurança cabe a um conjunto de organizações e, a nível nacional, cabe às Forças de Serviço de Segurança, CNCS e ANPC. Por seu turno, entende-se que a ciberdefesa inclui as *"atividades de prevenção, monitorização e reação a ameaças que coloquem em risco a soberania nacional, sendo que compete às Forças Armadas a missão da ciberdefesa"*[48]. Dito de outra forma, ciberdefesa refere *"questões de segurança no contexto da atualização de meios eletrónicos que envolvam a segurança do próprio Estado – abrangendo a*

[44] No caso dos Estados Unidos, *U.S Cyber Command*, 2008; na Alemanha, *Germany's Nationales Cyber-Abwehrzentrum*, 2011; e no Reino Unido, *UK's National Cyber Security Centre*, 2016.
[45] Tome-se como exemplo o *Cyber Defense Policy Working Group*, estabelecido em 2013, entre os Estados Unidos da América e o Japão.
[46] Tome-se como exemplo o *NATO's Cooperative Cyber Defence Centre of Excellence*, 2008 e *European Cyber Security Organization*, 2016.
[47] Cit. (Moniz, Impacto do Ciberespaço na Sociedade em Rede, 2018), pág. 23.
[48] Ibid. 48.

*segurança das várias dimensões que o compõem: povo, território e poder político"*[49], ao passo que cibersegurança refere-se a *"todas as demais questões de segurança no contexto da utilização de meios eletrónicos"*[50].

Desta forma, é percetível a importância da distinção dos referidos conceitos, uma vez que, com os recursos disponíveis, os fenómenos que têm lugar no ciberespaço tornam difícil a perceção dos cenários onde atuam as forças de segurança e as forças armadas. Imagine-se que uma infraestrutura crítica de energia nacional é atacada. Atendendo aos recursos disponíveis e associados à natureza do ciberespaço, podemos ficar incertos quanto ao objetivo pretendido, isto é, se o ataque visava atingir a organização, através dos seus serviços e utilizadores, ou se intencionava colocar em causa a soberania do país. Para além disso, acresce, quer num quer noutro, a dificuldade em imputar o ataque. A dificuldade de atribuir o ciberataque a um responsável associa-se a diversas variantes que analisaremos no capítulo seguinte.

[49] Cit. (Casimiro, 2018), pág.48
[50] Ibid. 50.

# III. As dimensões da atribuição de ciberataques aos Estados

*"A responsabilidade é o corolário necessário ao direito"*[51] e, como tal, foi desde cedo objeto de atenção da Comissão de Direito Internacional no sentido da sua codificação. Como resultado, foi elaborado o PARI, que consagra uma responsabilidade estadual, por fatos ilícitos e de natureza essencialmente objetiva (enquanto princípio-regra). Note-se, contudo, que, apesar da matéria da responsabilidade não se esgotar com a responsabilidade internacional dos Estados por factos internacionalmente ilícitos[52], apenas ela será objeto da nossa atenção durante o nosso estudo.

A estrutura deste regime pressupõe, primeiramente, a comissão de um facto internacionalmente ilícito[53] composto por dois elementos: o elemento subjetivo[54] (*"[....] o comportamento tem que violar uma norma primária de direito internacional, isto é, a ilicitude"*) e o elemento objetivo[55] (*"[...] a conduta, que pode consistir numa ação ou omissão, tem de ser estadual"*, ou seja, imputável ao Estado). Ora, de acordo com o segundo elemento, sobre o qual recairá a nossa atenção, a conduta, independentemente de se tratar de uma ação ou omissão, terá de ser uma conduta estadual, isto é, terá de nos permitir atribuir os atos de um indivíduo ou órgão a um Estado. Por outras palavras, *"*[a] *operação de imputação ou atribuição é* [...] *uma ficção legal que consiste em atribuir os atos de uma pessoa física a um Estado – uma pessoa jurídica"*[56].

Posto isto, tornam-se essenciais os critérios que imputam condutas ao Estado, uma vez que nos permitem determinar quando um Estado atua. Atualmente, tal assume um papel ainda mais relevante, visto que foram surgindo fenómenos não antes considerados, tais como: a utilização de entidades privadas para exercerem poderes públicos; o crescendo das ações de atores não estaduais (desde atores maliciosos a atores não maliciosos); e o desenvolvimento da tecnologia, que dificulta a imputação de determinada conduta a um Estado.

Uma das razões da dificuldade de imputação associada ao desenvolvimento de novas tecnologias, prende-se com a perpetração de ciberataques. A imputação de ciberataques, que pode ser definida como a *"identificação do ator responsável por um*

[51] Cit. Caso Barcelona Traction, Light and Power Company Limited (Bélgica c. Espanha), pág. 33, §36.
[52] Neste sentido ver: (Tavares, 2020), págs. 634-638, vol. I.
[53] Artigo 1.º do PARI.
[54] Cit. (Tavares, 2020), pág. 639.
[55] Cit. Ibid. 55.
[56] Cit. Ibid. 55, pág. 641.

*ciberataque"*[57] é bastante complexa, uma vez que o seu processo pode resultar em respostas bastante diferentes[58], dependendo do tipo de imputação em causa[59], isto é, imputação técnica, imputação política e imputação jurídica. Apesar de distintos quanto à natureza, método e objetivo, os diferentes processos de imputação não são mutuamente excluíveis. Antes pelo contrário. Para concluirmos se determinada conduta, neste caso, ciberataque, deve, ou não, ser imputada a um Estado é necessário considerar os resultados a que cada processo de imputação chega. Assim, se conseguirmos associar o computador de onde o ataque provém com as declarações que um Estado fez relativamente a determinado ataque e as regras de direito internacional que permitem considerar uma conduta como estadual, conseguiremos, mais facilmente, imputar a responsabilidade. Estas são, no entanto, situações improváveis, uma vez que nenhum Estado assumirá, facilmente, uma relação com um qualquer ciberataque.

## A. Imputação técnica

A imputação técnica é a *"identificação da máquina a partir da qual um ataque foi lançado"*[60], o que envolve a utilização de técnicas forenses que permitem o rastreio de pistas deixadas pelo intruso. A utilização destas técnicas tem sido dificultada devido ao desenvolvimento da tecnologia, que vem permitindo ferramentas de anonimato, como o TOR[61], que facilitam a invisibilidade do perpetrador ou a deturpação da sua localização. Contudo, tem-se registado esforços para melhorar a utilização destas técnicas e desenvolvido um leque de ferramentas que permitem rastrear o computador utilizado para o ciberataque. Tome-se como exemplo, os *honeypots*. Os *honeypots* são uma ferramenta desenhada para funcionar como uma armadilha para os intrusos, uma vez que permite a monitorização clandestina do seu comportamento, levando a que futuras intrusões sejam mais facilmente identificadas e associadas ao perpetrador. Uma outra fonte de informação

[57] Cf. (Finnemore & Hollis, 2020), pág. 985; (Eichensehr, The Law and Politics of Cyberattack Attribution, 2020),pág. 522; (Buchan, 2012), pág. 4.
[58] Independentemente da resposta a que o processo de investigação nos guie, é importante que este seja diligente e preciso, uma vez que *"a imputação correta de ciberataques é um predicado crucial para um amplo conjunto de ações relacionadas ou reativas"* - Cit. (Eichensehr, The Law and Politics of Cyberattack Attribution, 2020), pág. 520: *"accurate attribution of cyberattacks is a crucial predicate to a wide range of related or responsive actions"*. No mesmo sentido, ver (Tran, 2018), pág. 384.
[59] Cf. (Buchan, 2012); (Eichensehr, Decentralized Cyberattack Attribution, 2019); (Lin, 2016); (Rid & Buchanan, 2015) e (Finlay & Payne, 2019).
[60] Cf. (Eichensehr, The Law and Politics of Cyberattack Attribution, 2020), pág. 523; entre outros.
[61] *Onion- routing* que permite encobrir o endereço de IP quando estão online.

consiste na *instrumentação pré-posicionada*, que ocorre em sistemas e *networks* que o intruso possa utilizar no seu ataque, permitindo que o fluxo de dados seja registado para que, quando devidamente interpretado, seja possível a identificação da natureza e fonte da atividade ciber maliciosa. Ferramentas mais específicas como as *text string*[62] e os *timestamps*[63] podem, igualmente, implicar a descoberta do atacante como pudemos ver em casos como o da *Sony Pictures Entertainment* e *DNC*, respetivamente.

*Sony Pictures Entertainment, 2014*

Em 2014, a *Sony Pictures Entertainment* foi vítima de um ataque aos seus sistemas de rede. Os hackers responsáveis pelo ataque, "*Guardians of Peace*"[64], fizeram *download* e publicaram *online* os registos da *Sony*, incluindo informação pessoal dos trabalhadores, como números de segurança social e registos médicos; lista dos salários dos funcionários; comunicações internas, como emails com conteúdo sensível; guiões e filmes não lançados. De seguida apagaram estes registos dos computadores da *Sony*. No total, este ataque afetou mais de três mil computadores e oitocentos servidores, ficando famoso por ter levado ao cancelamento da comédia *"The Interview"*, onde os atores Seth Rogen e James Franco assassinavam o líder da Coreia do Norte, Kim Jong Un.

Vinte e cinco dias após o ataque, o FBI imputou-o publicamente à Coreia do Norte, declarando com "alta confiança" que o ataque teve origem na Coreia do Norte. Tal conclusão foi obtida por se atender ao contexto, uma vez que a Coreia do Norte tinha meios e motivos, mas também pelas provas forenses. Oficiais do FBI encontraram semelhanças com o ataque *DarkSeoul*, perpetrado previamente pela Coreia do Norte contra os bancos da Coreia do Sul. Para além disso, encontraram provas de que o código malicioso foi produzido em computadores com as definições programadas em coreano.

[62] As *text string* descobertas num ciberataque podem incluir a língua em que os nomes das funções do software malicioso foram programados, implicando um dado atacante. (Eichensehr, The Law and Politics of Cyberattack Attribution, 2020).
[63] Os t*imestamps* podem indicar a altura em que o *malware* foi compilado, a hora da infeção, e os horários de trabalho dos atacantes. (Eichensehr, The Law and Politics of Cyberattack Attribution, 2020).
[64] Grupo de *hackers* apoiado pelo governo da Coreia do Norte.

*DNC Hack, 2016*

Neste caso, os hackers, de pseudónimo "Guccifer 2.0", infetaram e-mails visando roubar credenciais que lhes permitisse ter acesso à rede do Comité Nacional de Democratas, dos Estados Unidos. Os hackers, de acordo com o relatório da *Symantec*, publicaram cerca de vinte mil e-mails do Comité através do website *DNCLeaks* e *WikiLeaks*, sabotando a campanha presidencial do Senador Bernie Sanders, causando a demissão da Presidente do Comité, Debbie Wasserman Schultz, e, em última instância, evitando a vitória de Hilary Clinton.

Os serviços de inteligência dos Estados Unidos concluíram com "alta confiança" que o ataque foi perpetrado pela Rússia. Apesar de não terem fornecido publicamente provas que fossem nesse sentido, empresas de segurança privadas, que foram consultadas durante a investigação, revelaram provas de que a Rússia tinha sido responsável pelo ataque. Concluíram que os hackers utilizaram as mesmas ferramentas de extração de dados e um código idêntico aos utilizados por um grupo de hackers russo que trabalha para a FSB (serviços secretos russos). Notaram, igualmente, que a assinatura digital estava no alfabeto cirílico e que as operações tinham parado nos feriados russos e que as horas de trabalho se alinhavam com o fuso horário da Rússia. Ora, apesar das provas serem circunstâncias e, no caso da assinatura digital, poder ter sido plantada de forma incriminatória, a verdade é que as provas relacionadas com o fuso horário e os feriados, são mais improváveis de ter sofrido manipulação, uma vez que tal implicaria um nível de coordenação e custo bastante elevados.

Lamentavelmente, identificar o terminal físico ou o endereço de *IP* de onde se origina um ciberataque revela pouco, ou nada, sobre a identidade e os motivos do ator por detrás do teclado[65]. Há uma enorme diferença, tanto legal quanto política, entre um hacker independente que procura um desafio ao atacar um sistema de um governo, ou, um coletivo de hackers que pretende fazer uma declaração política, e, um Estado que viola o direito internacional. Assim, a imputação técnica pode ser entendida como um facilitador, uma vez que permite aos Estados seguir para a imputação política e legal.

[65] Cf. (Tsagourias & Farrell, 2020), pág. 234.

## B. Imputação política

A imputação política exige que um Estado admita publicamente que foi vítima de um ciberataque. A imputação pública[66] de ciberataques, quer sob a forma de declarações oficiais[67], exigências diplomáticas para que o Estado infrator cesse o ataque, ou até mesmo acusações criminais domésticas de atores estrangeiros a outros Estados[68], é um fenómeno recente e tem vindo a ser acompanhado pelo apoio, igualmente público, de outros Estados[69]. A imputação política trata um processo altamente complexo que requer a consideração de múltiplos fatores: o como, se, quando e de que forma responsabilizará publicamente o autor; as relações que mantem com o Estado; a mensagem que quer passar para o eleitorado doméstico; a mensagem que quer passar para os restantes Estados; as consequências que tal ação desencadeará, entre outras questões. Tendo em conta que tal decisão culmina no balanço abrangente entre a pressão doméstica e as relações interestaduais, justifica-se a prática dos Estados no sentido de uma exigência de um *standard of proof* alto aquando da imputação política[70], apesar de não existir nenhuma norma que o determine.

---

[66] Sobre a imputação pública, ver: (Derian-Toth, et al., 2021); (Egloff F. , 2020); (Finnemore & Hollis, 2020) e (Lin, 2016).

[67] *"Today the Biden administration is taking actions to impose costs on Russia for actions by its government and intelligence services against U.S. sovereignty and interests. […] This includes, in particular,[…]* ***violate well-established principles of international law, including respect for the territorial integrity of states****."* – Estados Unidos da América, Abril 2021; *"This attack, we believe* ***quite strongly****, came from a foreign state […] North Korea was the state that we believe was involved this worldwide attack […] I can't obviously go into the detailed intelligence, but it is* ***widely believed*** *in the community and across a number of countries that North Korea had taken this role […]."* – Reino Unido, Outubro 2017 (negrito nosso). Ver: https://www.nytimes.com/2017/10/27/world/europe/uk-ransomware-hack-north-korea.html.

[68] Veja-se, por exemplo, o *press release* que anuncia que a primeira vez que os Estados Unidos acusaram criminalmente contra cinco hacker militares chineses por *hacking* de computadores, espionagem económica e outras ofensas dirigidas a seis vítimas americanas nas indústrias de energia nuclear, metais e produtos solares dos EUA: *"Cyber theft is real theft and we will* ***hold state sponsored cyber thieves accountable*** *as we would any other transnational criminal organization that steals our goods and breaks our laws."* – Estados Unidos, Maio 2014 (negrito nosso). Ver: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[69] *"Foreign Minister Sven Mikser said that Estonia condemns Russia's cyber attacks against Ukraine and calls on Russia to* ***act responsibly and in accordance with international law*** *in cyber space"* – Estónia, Fevereiro, 2018; *"The Netherlands shares the concerns of other international partners regarding the damaging and undermining the GRU's actions. It supports the conclusion, presented today by the UK, that GRU cyber operations such as this one* ***undermines the international rule of law***" – Países Baixos, Outubro, 2018; *" […] Over the past 12 months, Australia has witnessed Russia use malicious activity to* ***undermine international stability, security, and public safety****. Australia* ***condemns such behaviour****."* – Austrália, Abril 2021 (negrito nosso).

[70] *"The U.S. Intelligence Community USIC) is* ***confident*** *that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations."* – Outubro 2016; *"The UK's National Cyber Security Centre assesses it is* ***highly likely*** *that North Korea actors known as the Lazarus Group were behind the WannaCry ransomware campaign – one of the most*

Desta forma, entendemos que a imputação política, só por si, não deve ser a base de uma possível ação de resposta ao ciberataque por parte de um Estado vítima. Deve ser sempre conjugada com a imputação técnica e jurídica, sob pena de ao Estado lhe vir ser imputada, *à posteriori*, a ação de resposta como ilícita.

## C. Imputação jurídica

A imputação jurídica, para beneficiar de um melhor entendimento, deve ser analisada em dois momentos diferentes. O primeiro momento prender-se-á com a conexão do ataque a um infrator de acordo com as regras, nacionais ou internacionais, aplicáveis. E, o segundo momento, analisará a quantidade de provas necessárias e o nível de certeza exigido (*standard of proof*) para que se dê a imputação da responsabilidade de um Estado.

### 1. Normas que atribuem o ataque ao infrator

Tal como referido anteriormente, apenas discutiremos a imputação que denota *"uma situação em que a conduta de um indivíduo ou grupo é considerada de um Estado"*[71], à qual se aplica o regime jurídico da responsabilidade internacional do Estado por factos internacionalmente ilícitos previsto no PARI, nos termos do artigo 1.º. No mesmo sentido, está a regra 14 do Manual, que determina que um Estado é internacionalmente responsável *"quando um ataque cibernético contrário ao Direito Internacional lhe seja imputável"*[72].

De acordo com o princípio geral da imputação, previsto no artigo 4.º do PARI e na Regra 15 do Manual, um ataque pode ser imputado ao Estado infrator, quando for perpetrado por qualquer órgão estadual[73]. Por seu turno, existem provisões que permitem

*significant to hit the UK in terms of scale and disruption."* – Dezembro, 2017; *"NCSC assesses with **high confidence** that the GRU was **almost certainly** responsible."* – Outubro 2018. (negrito nosso).

[71] *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, comentário ao artigo 2, §12.

[72] (Schmitt, Manual de Tallinn 2.0 sobre o Direito Internacional Aplicável às Operações Cibernéticas , 2017), §84-87. Ver ainda Relatório (UNGGE, A/68/98, 2013), §23; relatório (UNGGE, A/70/174, 2015), §28(f).

[73] Veja-se o artigo 4.º do PARI e o Diferendo relacionado com a imunidade de processo legal de um relator especial da Comissão de Direitos Humanos, Parecer Consultivo, TIJ, 29 de abril de 1999, §62: *"[...] A conduta de um órgão de um Estado deve ser considerada como um ato desse Estado ao abrigo do direito internacional, quer esse órgão pertença ao poder constituinte, ao legislativo, ao executivo, ao judicial ou a qualquer outro poder, quer as suas funções tenham um caráter internacional ou interno e quer assumam uma posição superior ou subordinada na organização do Estado [...]."*

considerar uma conduta como estadual, mesmo sem a atuação de um órgão ou agente. Tal acontece, por exemplo, nos termos do artigo 5.º do PARI e da Regra 15 do Manual, que determinam que serão imputadas ao Estado as condutas de entidades particulares legalmente autorizadas a exercer prerrogativas de autoridade pública por um Estado e nesse âmbito[74]; nos termos do artigo 6.º do PARI e na Regra 16 do Manual[75], que referem as situações dos órgãos postos à disposição de um Estado por outro Estado; nos termos do artigo 7.º do PARI e da Regra 16, §5 do Manual que se referem às situações em que o órgão ou entidade agem em excesso de poder ou contra instruções relativas ao seu exercício[76]; e nos termos do artigo 11.º do PARI, que regula a situação em que os comportamentos são reconhecidos e adotados como seus pelo Estado[77].

Para além destas, temos ainda as situações em que o Estado será responsabilizado pela conduta de uma pessoa que *"agia, de facto, sob as suas instruções ou sob a direção ou controlo"*, conforme o previsto no artigo 8.º do PARI e Regra 17 do Manual. No comentário ao Projeto de Artigos, a Comissão de Direito Internacional indicou que os termos "instrução", "direção" e "controlo" devem ser entendidos disjuntivamente[78]. Todavia, os tribunais tendem a tratar os conceitos "direção" e "controlo" em conjunto impondo-os como um requisito singular da imputação[79]. O grupo de especialistas concordou que, o teste do controlo efetivo defendido pelo TIJ nos casos *Nicarágua*[80] e do *Genocídio*[81] captura a intenção do conceito. No seu entender, o apoio ou incentivo de um Estado *vis-á-vis* uma entidade privada, ou as suas operações cibernéticas, é insuficiente

[74] Assim, os ciberataques que decorrem da contratação de empresas privadas ou de indivíduos, podem levar à imputação legal do Estado que habilitou os respetivos, pela sua lei, a exercer elementos da autoridade pública.
[75] Esta regra aplicar-se-ia, por exemplo, numa situação em que um especialista do CERT do governo de um Estado remetente fosse colocado à disposição do Estado recetor para lidar com operações cibernéticas direcionadas apenas ao Estado recetor, desde que este último exerça direção exclusiva e controle os especialistas. Tal mantém-se verdadeiro, mesmo que os peritos sejam disponibilizados apenas remotamente, veja-se Regra 16 do Manual, §4.
[76] Artigo 7.º do PARI.
[77] Por vezes, os Estados podem encontrar vantagens, por norma, políticas, em assumir um comportamento como seu. Pode assim, querer demonstrar ao seu eleitorado doméstico a força que tem no contexto cibernético ou, até mesmo, a posição que adota perante ações de outros países.; Veja-se ainda, a propósito do silêncio enquanto aceitação tácita da imputação no contexto dos ciberataques, a intervenção de Robert E. Barnsby, *"Why Certain States are Happy to have Cyber Attacks Attributed to Them"*, no contexto da *11th International Conference on Cyber Conflict (CyCon 2019)*.
[78] *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, comentário ao artigo 8, §7.
[79] Cf. (Crawford, State Responsibility: The General Part, 2013), pág. 146.
[80] Veja-se o Caso Atividades militares e paramilitares na Nicarágua e contra esta, TIJ, §115.
[81] Veja-se o Caso Aplicação da Convenção para a prevenção e repressão do crime de genocídio, Bósnia-Herzegovina c. Sérvia e Montenegro, TIJ, §400.

para imputar responsabilidade ao Estado, pois o controlo efetivo não abrange a ação de um Estado considerada suplementar à ação desse ator no seu ataque[82].

Em qualquer dos casos supramencionados, será sempre necessário, num primeiro momento, identificar o indivíduo, ou indivíduos, por detrás do computador para posteriormente, poder estabelecer a ligação entre este e o Estado. Apesar das técnicas forenses, utilizadas no âmbito da imputação técnica, não serem capazes de determinar definitivamente a identidade da pessoa, não deixam de ser essenciais. Através da tecnologia, os investigadores podem consultar historiais e concluir, por exemplo, que o endereço de *IP* detetado foi já associado a alguém no passado; que o processo de autenticação, através do qual um indivíduo específico fica ligado a determinados privilégios no sistema do computador, permita rastrear o usuário. Por outro lado, caso o usuário aceda não apenas ao sistema do computador local, mas também à internet, o *ISP* poderá ser útil, uma vez que esclarecerá as atividades na internet dos seus subscritores enquanto indivíduos. Meios técnicos, como por exemplo, a forma como alguém utiliza o teclado do computador, poderão, igualmente, apontar para um indivíduo específico. Apesar destas vidências fornecerem informação útil sobre um sujeito, revela-se essencial uma base de dados que permite proceder à comparação necessária e, consequente, revelação do indivíduo específico. Sem a base de dados será possível identificar que se trata de um indivíduo responsável por uma, ou mais intrusões, mas não qual o indivíduo em específico.

O contexto político revela-se, igualmente, essencial nesta matéria, uma vez que se um ator beneficiar com um ciberataque por razões políticas, económicas, ou outras, tal poderá ser entendido como um fator influenciador na imputação. No mesmo sentido, deve considerar-se como indicadores políticos relevantes, o tipo de alvo selecionado e o conhecimento especializado requerido para o explorar. Tome-se como exemplo, o caso *Stuxnet*.

[82] Tome-se como exemplo a situação em que um Estado fornece um *malware* a uma entidade particular. Tal não equivale, sem mais, a um controlo efetivo sobre as operações que serão levadas a cabo com a utilização desse *malware*. Mas, se o Estado planear e supervisionar uma operação que visa utilizar as atualizações de um software para implantar vulnerabilidades num software utilizado por outro Estado nos seus computadores governamentais, celebrando um contrato confidencial com a empresa que produz o software, para que incorpore os *exploits* no *software*, e, posteriormente, dirija o processo de implantação, então estaremos perante um controlo efetivo e o Estado poderá ser responsabilizado pelas ações da entidade privada.

*Stuxnet, 2010*

Em 2010, na sequência de falhas inexplicáveis nas centrifugadoras de urânio iranianas, uma empresa de segurança tecnológica bielorrussa foi contratada para averiguar o problema. A empresa descobriu um vírus, *Stuxnet*, que foi desenhado para se infiltrar lentamente nos sistemas de controlo responsáveis pela velocidade e acionamento das válvulas das centrifugadoras e, posteriormente, destruí-las. Os especialistas concluíram que se tratava de um ataque com um alvo específico, pois o vírus procurava ativamente uma configuração específica correspondente aos sistemas de controlo das válvulas. No decorrer da descodificação do *Stuxnet,* concluíram que este estava estruturado em duas bombas digitais, sendo que a bomba pequena seria responsável por manipular a velocidade do rotor das centrifugadoras, ao passo que, a bomba maior seria dirigida às cascatas das centrifugadoras, manipulando as suas válvulas[83]. Apesar das consideráveis tentativas de camuflagem, os peritos concluíram que o ataque tinha sido levado a cabo pelos Estados Unidos e Israel. O contexto político entre o Irão, os Estados Unidos e Israel, permitiu deduzir que os atacantes tinham meios e motivos para levar a cabo o ciberataque, não sendo de desvalorizar a especificidade do alvo. A escala do ataque pode, igualmente, ser reveladora da identidade do Estado perpetrador e, neste caso, poucos seriam os Estados com capacidade, recursos[84] e serviços de inteligência para desenvolver uma ameaça desta dimensão.

O caso *Stuxnet*, a par dos casos *Sony Entertainment* e *DNC*, são o reflexo da necessidade de interligação dos tipos de imputação para que seja possível identificar o autor dos ciberataques. Assim, para que possamos imputar legalmente e responsabilizar um Estado por um determinado ciberataque, será sempre essencial o papel dos analistas forenses e dos seus métodos, assim como do contexto político.

[83] TED Talk de Ralph Langner, responsável pela investigação e descodificação do *Stuxnet*, onde explica a constituição do vírus.
[84] O facto de o código ter quatro *zero-day exploits* foi um indicador de que, com alta probabilidade, seria um Estado que estaria por detrás do ataque.

## *2. Standard of proof*

Num segundo momento da imputação legal, cumpre-nos responder à questão de saber qual o *quantum* de prova necessário *(standard of proof)* [85] para substanciar os factos que levam à imputação da responsabilidade do Estado. Há uma ausência de um corpo de normas uniformizado relativo à produção de provas no direito internacional, o que torna as investigações e imputações de ciberataques entre Estados mais complicadas. Contudo, pode também argumentar-se que não existe uma clara vontade dos Estados em estabelecer esse corpo de normas que determine qual o *standard of proof* necessário para o caso concreto, e quais as provas que devem ser apresentadas no sentido de preencher esse mesmo *standard*. Acordar pela adoção de algo mais concreto, poderá levar a que Estados, que pretendam imputar determinados ciberataques, tenham que revelar as suas fragilidades tecnológicas, ou partilhar informações delicadas, dados e mecanismos tecnológicos que não pretendam que sejam públicos.

Quando os Estados recorrem a meios judiciais, os tribunais, por norma, determinam os seus próprios *standards* consoante os casos em análise, o que leva á existência de *standards of proof* variáveis consoante o tribunal e a natureza do litígio em análise[86]. O *standard of proof* escolhido pelo TIJ resulta da aplicação do método *"sliding scale",* que adapta o *quantum* dos factos necessários à severidade da norma envolvida[87].

---

[85] O conceito *de standard of proof* não deve ser confundido com o conceito de *burden of proof* (ónus da prova). Se por um lado *standard of proof* é a quantidade de prova necessária para substanciar os factos da imputação realizada pela parte, o conceito de *burden of proof* determina que parte deve proceder à prova, ou seja, é a obrigação de uma parte em demonstrar que tem prova suficiente sobre a questão levantada no caso concreto. Assim, no caso do *standard of proof*, a parte que deve proceder à produção de prova já foi determinada, apenas não sabe a quantidade de prova que necessitará para fazer valer os factos levados à colação. Ao passo que, o *burden of proof*, visa determinar qual a parte que deve proceder à sustentação dos factos, não se prendendo com a questão da quantidade das provas, mas apenas com a questão da parte que as tem que apresentar. – Cf. (Roscini, 2015) e (Green, 2009).

[86] Note-se, contudo, que apesar de identificar o *standard of proof* que entende como aplicável, o tribunal não refere os mecanismos e o *quantum* necessário para que os referidos standards sejam considerados atingidos.

[87] Podemos identificar do mais ao menos rigoroso, o *standard*, de acordo com (Green, 2009), págs. 165-168: **"para além da dúvida razoável"** (provas indiscutíveis): *"[...] is a strict standard of proof, requiring that the preposition being presented is supported with evidence of a nature that there can be no "reasonable doubt" as to the factual validity of the proposition. Under this standard, then, a proposition must be virtually indisputable, given the evidence."*; **"claro e convincente"** (mais do que provável, mas aquém do indiscutível): *"[…] the party with the burden of proof must convince the arbiter in question that it is substantially more likely than not that the factual claims that have been made are true."*; **"preponderância de provas ou equilíbrio de probabilidades"** (mais provável do que improvável ou razoavelmente provável): *"This refers to evidence that is more convincing than the evidence that is offered in opposition to it, or evidence that establishes that the factual proposition of the relevant party was more likely than not."*; e ***"prima facie"*** (provas meramente indicativas da veracidade do referido): *"This represents a test of very low degree with regard to the assessment of evidence: it simply requires that evidence produced is indicative of the proposition claimed."*

Assim, se estivermos perante ofensas internacionais mais graves, como por exemplo a violação mais gravosa da proibição do uso da força, verifica-se a aplicação de um *standard of proof* mais exigente, uma vez que admitem o uso da força como lícito, ao abrigo da legitima defesa, o que, por sua vez, implicará consequências mais gravosas na hipótese de uma má imputação. Veja-se que, o *standard of proof* adotado pelo TIJ nestas violações mais gravosas, tem sido o da necessidade de provas "claras e convincentes", tal como se pode ver em alguns parágrafos dos casos *Nicarágua*[88], *Plataformas Petrolíferas*[89], e *República Democrática do Congo c. Uganda*[90]. Para além do TIJ, a *Comissão de queixas da Eritreia-Etiópia*[91] entendeu que a exigência de provas claras e convincentes também se aplica a situações em que o uso da força não atinge a magnitude de um ataque armado[92].

Por sua vez, o grupo de especialistas do Manual, concorda que, no geral, os Estados deverão agir razoavelmente, ou seja, como um Estado razoável faria perante circunstâncias semelhantes, aquando da consideração das respostas que disponha. Contudo, admitem que o conceito de razoabilidade é dependente do contexto e deve ser interpretado dentro desse. Além disso, concorda que a gravidade das operações cibernéticas contra um Estado e a robustez de qualquer resposta possível devem ser

---

[88] Caso das Atividades militares e paramilitares na e contra a Nicarágua, Julgamento, 1986, TIJ: *"The use of the term "satisfy itself" in the English text of the Statute (and in the French text the term "s'assurer") implies that the Court must attain the same degree of certainty as in any other case that the claim of the party appearing is sound in law, and, so far as the nature of the case permits, that the facts on which it is based are supported by* ***convincing evidence****."*, §29; *"[…] Yet despite the heavy subsidies and other support provided to them by the United States, there is no* ***clear evidence*** *of the United States having actually exercised such a degree of control in al1 fields as to justify treating the contras as acting on its behalf."*, §109. (negrito nosso).

[89] Caso das Plataformas Petrolíferas (República Islâmica do Irão c. Estados Unidos da América), acórdão quanto à questão de fundo, 2003, TIJ: *"In short, the Court has examined with great care the evidence and arguments presented on each side, and finds that the evidence indicative of Iranian responsibility for the attack on the Sea Isle City* ***is not sufficient*** *to support the contentions of the United States."*, §61; "This evidence is highly suggestive, but **not conclusive**.", §71. (negrito nosso).

[90] Caso das Atividades armadas no território do Congo (República Democrática do Congo c. Uganda), acórdão quanto à questão de fundo, 19 de dezembro de 2005, TIJ: *"[…] The Court must first establish which relevant facts it regards as having been* ***convincingly established by the evidence****, and which thus fall for scrutiny by reference to the applicable rules of international law."*, §72; *"[…] It confines itself to stating that it has not received* ***convincing evidence*** *that Ugandan forces were present at Mobenzene, Bururu, Bomongo and Moboza in the period under consideration by the Court for purposes of responding to the final submissions of the DRC."*, §91. (negrito nosso).

[91] Eritrea-Ethiopia Claims Commission - Partial Award: Jus Ad Bellum - Ethiopia's Claims 1-8, (Etiópia c. Eritreia), 2005, §12: *"It need not resolve these differences, because it is* ***clear from the evidence*** *that these incidents involved geographically limited clashes between small Eritrean and Ethiopian patrols along a remote, unmarked, and disputed border. The Commission is satisfied that these* ***relatively minor incidents*** *were not of a magnitude to constitute an armed attack by either State against the other within the meaning of Article 51 of the UN Charter."* (negrito nosso).

[92] Cf. (Roscini, 2015), pg.250.

mediadas pela razoabilidade.[93] Entendem, portanto, que quanto mais grave a violação, maior terá de ser a confiança nos factos que sustentam a imputação que desencadeia a resposta, uma vez que a robustez das respostas cresce com a severidade da violação.

Nas situações em que os Estados procedem à imputação da responsabilidade de outros Estados sem recorrem a meios judiciais, o *standard of proof* terá de ser inferido pelas suas práticas.

Quando um Estado é vítima de um ciberataque, por vezes, pode atender ao pragmatismo político e optar pela não resposta, isto é, pode, por exemplo, não querer reconhecer que foi vítima de determinado ataque, ou, querer manter as relações económicas ou diplomáticas que partilha com o Estado infrator. Independentemente do motivo, a inação como resposta do Estado vítima não exige, logicamente, produção de prova, nem está sujeita a qualquer *standard of proof*. O mesmo acontecerá, caso o objetivo do Estado vítima passe por protestar contra o ataque que sofreu, por exemplo, através de declarações oficiais que condenem o comportamento do Estado perpetrador e exijam a cessação desse comportamento. Tal não estará sujeito a qualquer *standard of proof*, nem exigirá que o Estado vítima produza provas, uma vez que se coaduna com a premissa de que mentir não é ilegal e, portanto, se um Estado pretender imputar a responsabilidade publicamente a outro Estado infundadamente, poderá fazê-lo. Em contrapartida, submete-se à possibilidade de o Estado infrator o condenar por proceder a acusações infundadas e, por sua vez, exigir que substancie as suas ações. Caso não esteja disposto ou capaz de fazê-lo, poderá enfrentar ceticismo por parte dos restantes Estados e danos à sua reputação, podendo ser entendido como um Estado imprudente. No mesmo sentido temos ainda as situações em que o Estado vítima procede a atos de retorsão contra o Estado infrator. Nestes casos, não se requer um *standard of proof*, uma vez que os atos de retorsão não envolvem a violação de obrigações legais internacionais. Todavia, poderá, de igual forma, enfrentar ceticismo e danos à sua reputação.

Para além da inação, protestos ou atos de retorsão, o Estado vítima pode adotar contramedidas que, ao contrário das referidas respostas, são pensadas para a induzir o cumprimento das obrigações internacionais que o Estado infrator violou. A inerente ilicitude de uma contramedida é excluída apenas se for tomada contra o Estado realmente responsável pelo ataque. Caso contrário, o Estado que adota a contramedida cometerá um facto internacionalmente ilícito. O risco político e legal que acompanha a possível

[93] Cf. (Schmitt, Manual de Tallinn 2.0 sobre o Direito Internacional Aplicável às Operações Cibernéticas , 2017), págs. 81-82.

imputação incorreta, e consequente adoção de contramedidas, parece mais bem considerado com a aplicação do *standard* da "preponderância de provas" / "balanço de probabilidades"[94], segundo o qual a adoção de contramedidas é válida à luz do direito internacional, caso a imputação se fundamente em provas suficientes para estabelecer que a identificação do Estado perpetrador é provavelmente mais correta do que incorreta. Tendo em conta a gravidade da norma violada nesta situação, o objetivo da aplicação das contramedidas e as possíveis consequências que uma má imputação poderá causar no suposto Estado infrator, parece mais adequada a aplicação do *standard* da "preponderância de provas" do que a aplicação de outro *standard*. Caso se aplicasse o *standard* da *"prima facie"* o risco da má imputação seria muito elevado, pois os factos que se exigiriam não cobririam a gravidade das possíveis consequências decorrentes dessa má atribuição. Já se fosse exigido o *standard* da prova *"clara e convincente"* estaríamos a equiparar a gravidade das situações que levariam ao emprego das contramedidas, à gravidade das situações de uso da força e de ataque armado. Tal frustraria a aplicação das contramedidas por se tratar de uma exigência de prova demasiado elevada. Mais se poderá criticar quem entenda que se deve proceder à aplicação do *standard of proof "para além da dúvida razoável"*, uma vez que se estaria a sujeitar a aplicação de contramedidas a um ónus muito superior ao exigido para a aplicação, por exemplo, do uso da força no âmbito da legítima defesa[95].

Posto isto, cumpre ressalvar que não foi defendida a pretensão da adoção de um *standard of proof* uniforme e transversal a todas as disputas internacionais. As considerações feitas visam apenas alertar para a necessidade de adoção de *standards* consistentes e padronizados com os vários fatores a atender, de modo que haja segurança e certeza quanto a esta matéria no momento do Estado imputar determinado ciberataque a outro Estado.

[94] Cf. (Tsagourias & Farrell, 2020), págs. 965-966.
[95] Cf. (Davis, 2022), págs. 13-15.

# IV. Importância da imputação do ciberataque ao Estado

Uma vez feita a imputação do ciberataque ao Estado, surgem consequências jurídicas na sua esfera[96], isto é, o Estado vítima pode exigir cessação e garantias de não repetição[97] do facto, assim como, reparação[98] do prejuízo causado pelo mesmo. Ao contrário da cessação[99], as garantias de não repetição não são exigidas em todos os casos, mas apenas se as *circunstâncias o exigiram*[100]. A reparação é a consequência que surge na esfera do infrator sempre que é cometido um facto internacionalmente ilícito, que tendo em vista a "garantia da reparação integral do prejuízo causado", pode assumir a forma de *"restituição*[101]*, indemnização*[102] *e satisfação*[103]*, seja isolada ou conjuntamente"*[104].

O cumprimento destas obrigações decorrentes da responsabilidade internacional pode ser induzido pela adoção de contramedidas[105] por parte do Estado lesado[106]. As contramedidas foram já reconhecidas como lícitas pelo TIJ, nos casos *Gabcíkkovo-Nagymaros*[107] e *Atividades Militares e Paramilitares na e contra a Nicarágua*[108], e pelo tribunal arbitral, no caso *Acordo de Serviço Aéreo*[109]. Além da licitude das contramedidas, o TIJ, determinou que "o propósito das contramedidas deverá ser a indução do Estado responsável no cumprimento das obrigações internacionais, pelo que, a medida deverá ser reversível"[110]. Tal infere, por um lado, que, se a contramedida não for adotada tendo em vista o seu propósito de levar o Estado, a quem o ilícito foi imputado, a cumprir as suas obrigações internacionais, será ilícita. Por outro lado, a questão da reversibilidade

[96] Artigo 28.º do PARI e Regra 27 do Manual.
[97] Artigo 30.º do PARI e Regra 27 do Manual.
[98] Artigo 21.º do PARI e Regra 28 do Manual.
[99] Artigo 29.º do PARI e Regra 27, §6 do Manual.
[100] Ver: explicação do Caso *La Grand* presente em (Azeredo Lopes, et al., 2020), no doc. 458.
[101] Artigo 35.º do PARI e §2,3,4,5 do Manual.
[102] Artigo 36.º do PARI e §6,7,8 do Manual.
[103] Artigo 37.º do PARI e §9,10,11 do Manual.
[104] Artigo 34.º do PARI e Regra 29, §1 do Manual.
[105] Cit. *"as contramedidas são violações de obrigações internacionais por parte de um sujeito de direito internacional, adotadas em resposta a um facto internacionalmente ilícito prévio de outro sujeito, tendo em vista induzir o Estado recalcitrante a cumprir as suas obrigações internacionais. Por isso são um mecanismo de enforcement (...) do direito internacional."*, (Tavares, 2020), pág. 696, apud. Antonios Tzanakopoulos.
[106] Artigo 49 do PARI e Regra 21 do Manual.
[107] Caso Gabcikovo-Nagymaros (Hungria c. Eslováquia), acórdão, 25 de setembro de 1997, §82-83
[108] Caso Atividades Militares e paramilitares na e contra a Nicarágua, Nicarágua c. Estados Unidos, Julgamento, §249.
[109] Caso do Acordo de Serviço Aéreo (Estados Unidos da América c. França), decisão arbitral, 1978, RIAA (Reports of International Arbitral Awards), §80-96.
[110] Relatório do TIJ no Caso Gabcikovo- Nagymaros, §87.

está intimamente ligada à função instrumental da contramedida, na medida em que, implica uma reversão de ambas as partes, uma vez atingidos os objetivos da cessação e reparação. Este último, reforça o caráter temporário, essencialmente protetor e não punitivo[111] das contramedidas. Sendo que as contramedidas comtemplam ações que de outra forma seriam ilegais[112], o direito internacional impõe restrições à sua utilização. Assim, de acordo com a regra 23 do Manual, que vai ao encontro da matéria do artigo 51.º do PARI, as contramedidas, de natureza ciber, ou não, devem ser proporcionais ao dano a que respondem, isto é, *"os efeitos de uma contramedida têm de ser proporcionais com os danos sofridos, tendo em conta os direitos em questão"*[113]. Tal exige que, os Estados considerem a gravidade do facto ilícito e os efeitos que a contramedida produzirá, em comparação com os danos sofridos. Por outro lado, as Regras 22, 39, 41 e 108 do Manual, consonantes com o artigo 50.º do PARI, apresentam as matérias cujas contramedidas não podem afetar. Note-se que, com referência à opinião do juiz Simma no caso das Plataformas Petrolíferas[114], o grupo de especialistas concluiu no sentido de que as contramedidas ciber, não se devem elevar ao nível de ataque armado.

Neste sentido, um Estado que sofra um ciberataque pode, nos termos expostos, recorrer às contramedidas para levar o Estado a quem imputou o ataque a cumprir as suas obrigações internacionais. Apesar de poderem recorrer a contramedidas não cibernéticas, verifica-se que, por norma, os Estados recorrem a contramedidas cibernéticas, os designados *"hack backs"*. Contudo, alguns Estados apenas apresentam capacidade de resposta, quer dentro, quer fora, do plano ciber, quando em colaboração com outros Estados. Neste âmbito, é levantada a questão das contramedidas coletivas, que apesar de já ter surgido num contexto não ciber, apresentam uma relevância acrescida no contexto ciber. As contramedidas coletivas contrapõem-se às contramedidas bilaterais, uma vez que permitem que outros Estados, que não o Estado lesado, possam aplicar contramedidas ao Estado infrator. Este entendimento baseia-se na ideia de que a inexistência de resposta

---

[111] Cf. (Crawford, State Responsibility: The General Part, 2013), págs. 687-688.

[112] Cit. "*pacific unilateral reactions which are intrinsically unlawful, which are adopted by one or more States against another State, when the former consider that the latter has committed an internationally wrongful act which could justify such a reaction."* (Crawford, State Responsibility: The General Part, 2013), pág. 1135, apud. Alland.

[113] Caso Gabcikovo-Nagymaros (Hungria c. Eslováquia), acórdão, 25 de setembro de 1997, §85

[114] Caso das Plataformas Petrolíferas, §13 (opinião separada do juiz Simma): *"But we may encounter also a lower level of hostile military action, not reaching the threshold of an "armed attack" within the meaning of Article 51 of the United Nations Charter. Against such hostile acts, a State may of course defend itself, but only within the more limited range and quality of response (the main difference being that the possibility of collective self-defence does not arise, cf. Nicaragua) and bound to necessity, proportionality and immediacy in time in a particular strict way"*.

a um comportamento internacionalmente ilícito, representa uma ameaça aos Estados, à integridade do sistema jurídico internacional e à paz e segurança internacional. Assim, representam a importância de evitar que Estados vítima e sem recursos, não consigam levar o Estado responsável a desistir do facto ilícito. A favor da coletividade temos a Estónia[115] e alguma doutrina[116]. Por seu turno, defensores das contramedidas bilaterais entendem que, quantos mais Estados estiverem envolvidos na situação, maior será a probabilidade de destabilização da paz e segurança internacional, tendo em especial atenção, as consequências provocadas por uma possível má imputação. Assim, entendem que, nos termos do regime da legítima defesa, apenas se justifica a intervenção de Estados não vítimas quando o ilícito é severo ao ponto de se qualificar como ataque armado. Esta opinião é partilhada pela França[117], a maioria da doutrina[118] e pela jurisprudência do TIJ[119]. Em contrapartida, os Estados não vítima podem recorrer a medidas de retorsão[120]. Desde logo, diferem das contramedidas pela sua natureza licita e por na sua origem não ter de estar necessariamente um facto internacionalmente ilícito, podendo ser aplicadas quando um Estado se sinta prejudicado e vise punir o Estado infrator. Por outro lado, podem ser invocadas não só pelo Estado vítima, mas também por outros Estados. Consideram-se, portanto, amistosos *"atos sociopolíticos com relevância jurídica"*[121].

Por fim, os Estados poderão reagir com o uso da força, em sede de legítima defesa quando o ciberataque se possa qualificar como ataque armado. A regra de legítima defesa, apesar da sua natureza consuetudinária, encontra previsão no artigo 51.º da CNU. No mesmo sentido vai a regra 71 do manual que determina que *"[u]m Estado que seja alvo de uma operação cibernética que atinja o nível de um ataque armado pode exercer o seu*

---

[115] Durante a Conferência Internacional de Conflitos Ciber, em 29 de maio de 2019, Kersti Kaljulaid, presidente da Estónia, declarou que: *"Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation. The countermeasures applied should follow the principle of proportionality and other principles established within the international customary law … It is therefore important that states may respond collectively to unlawful cyber operations where diplomatic action is insufficient, but no law recourse to use of force exists. Allies matter also in cyberspace."* - https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/

[116] Veja-se, por exemplo (Kosseff, 2020) e (Schmitt & Watts, Collective Cyber Countermeasures?, 2021)

[117] Cf. https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/

[118] Tome-se, como exemplo, (Crawford, Brownlie's Principles of Public International Law, 2012), págs. 469-472.

[119] Casos do Sudoeste de África, Segunda Fase, Julgamento, 18 de julho de 1966, TIJ e Caso das Atividades militares e paramilitares na e contra a Nicarágua (Nicarágua c. Estados Unidos), Julgamento, 27 de junho de 1986, TIJ.

[120] Tome-se por exemplo, a suspensão de relações diplomáticas e expulsão de determinados diplomatas.

[121] Cit. (Crawford, State Responsibility: The General Part, 2013), pg. 677, apud. Noortman, em *Enforcing International Law: From Self-Help to Self-Contained Regimes* (2005).

*direito inerente de legítima defesa. Se uma operação cibernética constitui um ataque armado depende da sua escala e efeitos."*[122][123]

Determinar se a escala e os efeitos de um ciberataque atingem a severidade necessária para que consubstanciem um ataque armado nem sempre é linear. Existem situações claras, que levaram o grupo de especialistas a determinar unanimemente a constituição de ataque armado. Tal é o caso do ciberataque que fira, cause danos significantes, ou cause a morte de pessoas[124]. Contudo, ciberoperações que sejam altamente disruptivas, como as que interferem com infraestruturas essenciais ao Estado, levantam diferença de opiniões entre o grupo de especialistas. Alguns dos especialistas tomaram a posição de que a lesão do indivíduo ou o dano da propriedade são condição para se caraterizar um ciberataque enquanto ataque armado, ao passo que, outros entendiam que não é natureza destrutiva das consequências que importam, mas sim a extensão que efeitos disruptivos poderiam tomar, por exemplo na estabilidade do Estado.

Ao relacionar a matéria da legítima defesa com a matéria dos ciberataques, surgem igualmente questões relacionadas, por um lado, com o uso da força, e, por outro lado, com atores não estaduais.

Quanto à relação do artigo 51.º com o artigo 2.º/4, ambos da CNU, uma maioria do grupo de especialistas assumiu a posição de que um ataque armado cibernético consubstancia sempre "uso da força" cibernético, no âmbito do artigo 2.º/4, não sendo o inverso verdade. Assim, o conceito de "uso da força" não deve ser equiparado ao conceito de "ataque armado", pois tal como notou o TIJ[125], nem todo o uso da força atinge o nível de ataque armado, sendo necessário analisar a gravidade da escala e dos efeitos da operação em causa. Os Estados Unidos, por seu turno, adotaram uma visão minoritária sobre o assunto, sugerindo que não há um "intervalo" entre o uso da força e um ataque armado, pelo que todo o uso da força é um ataque armado, na ausência de uma justificação de legítima defesa ou de resoluções do Conselho de Segurança. Neste sentido, defende que quando perante um ciberataque, o Estado vítima poderá responder com uso da força no âmbito da legítima defesa.

---

[122] Tradução nossa.
[123] Para além das condições referidas na Carta, a legítima defesa apresenta outros requisitos que, apesar de não se encontrarem previstos no artigo 51.º da Carta, apresentam natureza consuetudinária. Tal vai no sentido da jurisprudência do TIJ e das regras 72 e 73 do Manual no que respeita às condições de necessidade, adequação, proporcionalidade e imediatez, e, por outro lado, no sentido da jurisprudência do TIJ e da regra 75 do Manual de Tallinn, no que respeita à comunicação ao Conselho de Segurança.
[124] Veja-se Regra 69, §8 e Regra 71, §8, ambas do Manual.
[125] Caso Nicarágua, julgamento, §191.

Quanto à aplicação do artigo 51.º CNU a atores não estaduais, existem duas visões a considerar. A primeira sugere que o uso da força só é uma resposta admissível por aplicação do artigo 51.º CNU, quando as operações dos atores não-estaduais forem imputadas a um Estado, tendo por base dois casos do TIJ[126], que argumentam neste sentido. Por seu turno, a segunda visão, presente em alguma doutrina e juízes do TIJ[127], apoiada pelos Estados Unidos e o grupo de especialistas, entende que o artigo 51.º CNU, ao não excluir a legitima defesa contra atores não estaduais, está, consequentemente, a admiti-la. Assim, o artigo ao referir apenas que o ataque armado é sofrido por um Estado, e nada dizer quanto aos autores deste, admite que os perpetradores possam ser autores não estaduais.

Questão diferente é a de saber quando é que um Estado vítima de ciberataques por parte de um grupo não estadual, pode imputar as condutas a outro Estado e utilizar a força, em sede de legítima defesa contra este. Neste sentido, o *locus classicus* normativo é o apresentado pelo TIJ no parágrafo 195 do caso da Nicarágua[128], que determina que, um ator não estadual que é "enviado" por um Estado para lançar ataques cibernéticos contra outro Estado, ou que esteja a agir "em seu nome" está, essencialmente, a operar sob as suas instruções ou sob o seu controlo efetivo, ou seja, há uma "participação substancial" por parte do Estado. Verificadas estas condições, é possível proceder-se à imputação. Contudo, o direito de responder em legítima defesa só surgirá quando as atividades cibernéticas possam ser consideradas um ataque armado. Assim, embora determinados atos sejam ilícitos, como por exemplo, fornecer armas cibernéticas ao grupo ou oferecer outro tipo de apoio para a condução das operações, tal não confere ao Estado lesado o direito a usar a força contra esse Estado.

[126] Veja-se neste sentido, *Consequências jurídicas da construção de um muro no território palestiniano ocupado*, Parecer Consultivo, TIJ 9 de julho de 2004, §138-139; e *Caso das atividades armadas no território do Congo* (República Democrática do Congo c. Uganda), acórdão quanto à questão de fundo, TIJ19 de dezembro de 2005, §141-147.

[127] Tome-se como exemplo a declaração de voto da Juíza Rosalyn Higgins no Parecer Consultivo sobre as Consequências jurídicas da construção de um muro no território palestiniano ocupado. (Azeredo Lopes, et al., 2020), pág. 129.

[128] Caso Atividades militares e paramilitares na Nicarágua e contra esta (Nicarágua c. Estados Unidos), acórdão quanto à questão de fundo, §195.

# V. Soluções para a evolução dos processos da imputação

Como pudemos ver, a imputação de ciberataques enfrenta diversas dificuldades que tornam o processo da responsabilização e sentimento de justiça na comunidade internacional uma miragem longínqua. As incertezas desencadeadas pelas falhas deste processo levam ao descrédito nas soluções atuais e ao aumento do sentimento de impunidade por parte dos perpetradores, o que pode sugerir que o ciberespaço não se encontra sob domínio normativo.

Contudo, temos assistido a um aumento de imputações públicas de ciberataques e a um apoio coletivo de outros Estados[129]. O progresso na imputação coletiva pode ser apontado noutra vertente, como por exemplo, a adoção da *Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities*[130], em 2017 e a adoção da *Brussels Summit Declaration*[131], pela NATO, em 2018.

Investigadores e especialistas têm vindo a tentar combater as incertezas associadas ao ciberespaço. O reflexo dos seus esforços passa pelos dois projetos do Manual de Tallinn proporcionados pela NATO CCDCE[132], que contribuiu, não tanto para a certeza das questões, mas para comandar a atenção dos Estados até elas[133]. Para além destes, outras entidades, como a *MICROSOFT*, *Atlantic Council* e a *Corporação RAND*, sugeriram mecanismos que, no seu entender, são capazes de tornar a metodologia da imputação de ciberataques mais eficiente e eficaz. Estes passam pela criação de uma Entidade Internacional de Imputação, que varia na sua natureza enquanto: puramente privada, com membros públicos e privados, e puramente intergovernamental. Independentemente da sua modalidade, tratar-se-ia sempre de uma plataforma globalmente neutra dedicada a imputar ciberataques de forma imparcial, legitima e válida.

[129] Id. 22.
[130] Versão atualizada: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf
[131] Cf. https://www.nato.int/cps/en/natohq/news_185000.htm
[132] (Schmitt, Manual de Tallinn 2.0 sobre o Direito Internacional Aplicável às Operações Cibernéticas , 2017) ; Manual de Tallinn sobre o Direito Internacional Aplicável às Operações Cibernéticas (Michael N. Schmitt ed., 2013).
[133] (Shany & Schmitt, 2020), pg. 197.

### *A. Atlantic Council*

Em 2014, o *Atlantic Council* sugeriu a criação de um Conselho Multilateral de Imputação e Adjudicação Cibernética (MCAAC) que serviria como um órgão puramente intergovernamental encarregado de investigar ciberataques visando imputar a responsabilidade ao Estado perpetrador[134]. Para tal poderia emitir recomendações ou encaminhar o assunto a órgãos políticos ou judiciários [135].

### *B. Microsoft*

Em 2016, a *Microsoft* propôs a criação de um órgão de imputação composto por especialistas técnicos de todos os governos, setor privado, académicos e civis[136]. Haveria assim uma partilha da investigação e reportagem de resultados que contribuiria para a imputação de ciberataques [137].

### *C.* Corporação *RAND*

Em 2017, os investigadores da *Corporação RAND* propuseram um "Consórcio Global de Imputação Cibernética" que excluía totalmente a intervenção dos Estados do processo da imputação. A sua composição passaria por especialistas técnicos de empresas de segurança cibernética e tecnologia da informação, assim como académicos e peritos de políticas cibernéticas, juristas e especialistas de política internacional[138].

As propostas contribuem para a centralização da imputação numa entidade internacional, que se opõe à descentralização que carateriza o sistema de imputação atual, que abrange imputações públicas e privadas, sob formas distintas. A centralização é apresentada como uma solução para o problema da imputação, uma vez que apresenta

[134] Cit. (Healey, Mallery, Jordan, & Youd, 2014), pág., 10 *"[…] would provide an international mechanism for arriving at a consensus attribution of illegal cyber campaigns by states and a formal process for adjudicating associated interstate disputes."*
[135] Cf. (Shany & Schmitt, 2020), pág. 215.
[136] Cit. (Charney, et al., 2016), pág. 1.
[137] Cf. (Shany & Schmitt, 2020), pág. 216.
[138] Cf. (Davis II, et al., 2017), pág. 29; ver (Shany & Schmitt, 2020), pág. 216.

algumas vantagens. A mais referida é a credibilidade[139], pois se se trata de uma entidade internacional e imparcial, não permitiria que os Estados infratores negassem o envolvimento em determinado ciberataque, o que facilitaria a imputação coletiva e as respostas dos Estados. Tal independência conduziria, igualmente, a uma maior predisposição em partilhar determinadas informações que, de outra forma, poderiam ser entendidas como confidenciais. O maior número de provas, por sua vez, levaria a imputações mais informadas e mais rápidas, diminuindo o risco das imputações incorretas. Por outro lado, ajudaria a padronizar a imputação, esclarecendo questões como o *standard of proof* e determinando os mecanismos indicados para imputações concretas.

Porém, podem ser destacadas várias desvantagens a esta solução. A primeira, e mais vezes apontada, prende-se com o desinteresse[140] demonstrado pelos Estados em desenvolver um mecanismo de imputação nos termos referidos, seja pela falta de detalhe apresentado (propostas da *Atlantic Council* e *Microsoft*); pelo desapreço em partilhar a imputação de um ciberataque com empresas, cujos motivos por detrás desta ação são incertos ou desconhecidos *(Microsoft)*; pela redundância que as propostas apresentam, uma vez que se um Estado pretender recorrer ao auxílio de uma entidade privada fá-lo-á *(Microsoft)*; ou, mais evidentemente, pela exclusão do seu papel na questão da imputação *(Corporação RAND)* [141]. Mesmo que os Estados se demonstrassem interessados em cooperar com a entidade internacional, não teriam a intenção, por exemplo, de partilhar determinados documentos ou informações de ordem confidencial, o que levaria à não obtenção dos resultados mencionados.

A realidade parece, portanto, não se coadunar com a possibilidade de se adotar uma das propostas, pelo que se deve considerar que a solução poderá não passar pela reestruturação da imputação nesse sentido, mas pelo melhoramento dos mecanismos que atualmente se utilizam para a levar a cabo.

[139] Ver: (Eichensehr, The Law and Politics of Cyberattack Attribution, 2020), págs. 215-217; (Tsagourias & Farrell, 2020), pág. 959; (Shany & Schmitt, 2020), pág. 216.
[140] Cf. (Tsagourias & Farrell, 2020), pág. 960.
[141] Cf. (Shany & Schmitt, 2020), pág. 217.

# Conclusão

Ao abordarmos a questão da evolução tecnológica podemos adotar uma visão mais otimista e considerar todas as comunidades que foram postas à nossa disposição e todos os benefícios que esta disponibilidade acarreta. A simplicidade quotidiana, a facilidade no acesso à informação, o contacto com a distância, são alguns exemplos. Porém, as desvantagens devem, igualmente, ser admitidas como reais, uma vez que são as maiores causadoras das preocupações associadas à modernidade, o que nos levou a várias conclusões.

Primeiramente, concluímos que os conflitos híbridos atingiram um nível de complexidade diferente com o aparecimento do domínio ciber. Como demonstração da preocupação com o crescente impacto do ciberespaço, os Estados adotaram novas políticas de ciberdefesa e cibersegurança. Devido às suas caraterísticas os Estados foram obrigados a considerar atos que, até então, não eram tidos como possíveis, e a dimensão que as consequências podem assumir. Assim, concluímos que o ciberespaço no seu domínio mediático de comunicação, quando utilizado por atores malicioso pode assumir um papel perverso, podendo refletir-se na disseminação de propaganda, recrutamento de novos atores, e, até mesmo no financiamento de atividades criminosas. Por outro lado, concluímos que o ciberespaço pode, igualmente, ser utilizado como um domínio de operações onde podem ser perpetrados ciberataques que complementem ataques convencionais ou que sejam um fim em si mesmos.

Segundamente, concluímos que estas possibilidades abriram caminho a questões de direito internacional, como a de saber como podemos imputar um ciberataque a um Estado num contexto ciber, onde a anonimidade e o *"outsourcing"* são uma constante. Neste âmbito, concluímos que apesar de os autores de ciberataques terem acesso a ferramentas que permitem a sua anonimidade, os Estados vítima têm conseguido combater estes métodos através da junção dos diversos processos de imputação. Assim, a imputação de ciberataques torna-se mais simples quando atendemos ao trabalho dos analistas forenses, que determinam qual o computador utilizado para lançar o ataque; ao contexto político entre o Estado vítima e o possível Estado perpetrador, analisando se existem motivos e capacidade para levar a cabo, ou patrocinar, o ciberataque; às normas de direito internacional, relativas à imputação que ditarão se é possível considerar determinado Estado como autor do ciberataque; e, por fim, ao *standard of proof* que nos

indica qual o *quantum* necessário para se proceder à imputação, atendendo às decisões do TIJ e à prática dos Estados, uma vez que não existe um padrão definido que determine o *standard of proof* exigido para os diferentes objetivos que a imputação possa tomar.

Terceiramente, concluímos que a imputação assume um papel preponderante para que o Estado vítima possa reagir ao ciberataque. Assim, dependendo do tipo de ciberataque que sofra, um Estado, para além da reparação, pode dispor de contramedidas, medidas de retorsão e do uso da força, em sede de legítima defesa. Para além deste objetivo, a imputação serve para impedir que o Estado autor se sinta impune aquando da perpetração destes ataques, o que contribui para a paz e justiça internacional.

Num quarto momento, tendo em vista melhorar os processos da imputação, foram apresentadas soluções por organizações, que, como pudemos concluir, estão longe de ser adotadas pelos Estados, pela falta de detalhe, desconfiança dos motivos, redundância do objetivo e falta de interesse em perder a capacidade de imputar os ciberataques.

Podemos, com tudo isto, concluir que, o ciberespaço apresenta desafios a vários níveis, incluindo ao nível do direito internacional. Contudo, a atenção dos Estados e das organizações, como por exemplo a NATO, tem recaído sobre este domínio, tentando torná-lo mais seguro, justo e equilibrado na sua utilização. Para tal, tem havido uma elevada coordenação e partilha de informação entre os diversos atores que tomam ações nesse espaço coletivo da humanidade.