UNIVERSIDADE CATÓLICA PORTUGUESA

UE e NATO no ciberespaço – o caso do conflito russo-ucraniano

Diogo Silva da Cunha

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2025

UNIVERSIDADE CATÓLICA PORTUGUESA

UE e NATO no ciberespaço – o caso do conflito russo-ucraniano

Diogo Silva da Cunha

Orientadora: Prof. Dra. Maria Isabel Tavares

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2025

À minha família e aos meus amigos.

Resumo

Reconhecido como um domínio operacional pela NATO em 2016, o ciberespaço assume uma relevância crescente no âmbito do direito do conflito armado. A sua militarização tornou as infraestruturas críticas de muitos países vulneráveis a ataques cibernéticos, exigindo, assim, uma resposta coordenada por parte dos principais atores internacionais.

De um ponto de vista jurídico, as operações no ciberespaço são reguladas pelo direito internacional humanitário e pelo disposto na Carta das Nações Unidas. Neste contexto, o *Manual de Tallinn* assume um papel fundamental ao estabelecer os critérios que determinam quando um ataque cibernético pode ser equiparado ao uso da força, fornecendo diretrizes para respostas proporcionais no domínio digital.

Nos últimos anos, a cooperação entre a NATO e a União Europeia tem-se aprofundado, sobretudo face à intensificação das ameaças híbridas e cibernéticas. A colaboração entre estas organizações revela-se, assim, imprescindível para enfrentar os desafios emergentes no ciberespaço, garantindo uma abordagem coordenada e eficaz na preservação da segurança internacional.

Palavras-chave: Ciberespaço, cibersegurança, ciberdefesa, guerra híbrida, cooperação.

Abstract

Recognised as an operational domain by NATO in 2016, cyberspace has been gaining increasing relevance in the context of the law of armed conflict. Its militarization has rendered the critical infrastructures of many countries vulnerable to cyberattacks, thus requiring a coordinated response from key international actors.

From a legal perspective, operations in cyberspace are regulated by international humanitarian law and the provisions of the United Nations Charter. In this context, the *Tallinn Manual* plays a fundamental role in establishing the criteria that determine when a cyberattack can be equated to the use of force, providing guidelines for proportional responses in the digital domain.

In recent years, cooperation between NATO and the European Union has deepened, particularly in response to the intensification of hybrid and cyber threats. The collaboration between these organisations is, therefore, essential to addressing emerging challenges in cyberspace, ensuring a coordinated and effective approach to safeguarding international security.

Keywords: cyberspace, cybersecurity, cyber defence, hybrid war, cooperation.

Índice

Lista de siglas e abreviaturas

NATO – North Atlantic Treaty Organization

UE – União Europeia

DoS – Denial of Service

DDoS – Distributed Denial of Service

NCIRC – NATO Computer Incident Response Capability

CDMA – Cyber Defence Management Authority

CDMB - Cyber Defence Management Board

NATO CCD COE – NATO Cooperative Cyber Defence Centre of Excellence

NCIA – NATO Communication and Information Agency

ENISA – European Union Agency for Cybersecurity

CERT – Computer Emergency Response Team

PCSD – Política Comum de Segurança e Defesa

EC3 – European Cybercrime Centre

RAP – Readiness Action Plan

ONU – Organização das Nações Unidas

TIJ – Tribunal Internacional de Justiça

TIC – Tecnologias de Informação e Comunicação

GRU – Direção-Geral de Inteligência

NSA – National Security Agency

FSB – Serviço Federal de Segurança

TUE – Tratado da União Europeia

OEWG – Open-Ended Working Group

EUISS – European Union Institute for Security Studies

GMF – German Marshall Fund

PEC – Pacto de Estabilidade e Crescimento

SAFE – Security Action for Europe

TFUE – Tratado sobre o Funcionamento da União Europeia

Introdução

Até à anexação ilegal da Crimeia pela Federação Russa, em 2014, a cooperação NATO-UE no ciberbespaço não tinha concretizado avanços significativos no que respeita ao desenvolvimento de políticas ou iniciativas conjuntas. No primeiro capítulo desta dissertação, procederemos a uma visão geral da génese da cooperação entre a União Europeia e a NATO no domínio do ciberespaço. Neste contexto, importa identificar as razões que, ao longo do tempo, dificultaram o aprofundamento desta relação estratégica no ciberespaço, cuja relevância é hoje incontornável, atendendo à crescente militarização dos recursos cibernéticos.

No contexto do conflito russo-ucraniano, a Rússia não se limita apenas a avançar sobre o território, integrando operações cibernéticas como instrumento de desestabilização internacional, propagação de desinformação e descredibilização institucional da Ucrânia. No segundo capítulo, procurar-se-á enquadrar as atividades cibernéticas desenvolvidas pela Rússia no âmbito da sua estratégia mais ampla de guerra híbrida. Neste contexto, o conceito de *hybrid warfare* revela-se essencial, bem como a análise da sua evolução desde a formulação inicial proposta por Frank G. Hoffman, em 2007.

Num terceiro momento, proceder-se-á à análise da questão jurídica associada à qualificação de um ciberataque como constitutivo de "uso da força" ao nível de um "ataque armado", suscetível de desencadear uma resposta legítima ao abrigo do artigo 5 do Tratado do Atlântico Norte e do artigo 51 da Carta das Nações Unidas. Esta análise passará pela ponderação do peso da ausência de definições jurídicas codificadas que permitam estabelecer critérios objetivos quanto à identificação do limiar entre o uso da força e o ataque armado. A avaliação da escala e dos efeitos de um ciberataque, os problemas na atribuição de responsabilidade por atos internacionalmente ilícitos, a prática de Estados e, claro, o papel da NATO e da UE, assumirão particular relevância neste contexto.

Por fim, no quarto capítulo, será analisada a evolução da cooperação entre a União Europeia e a NATO no domínio do ciberespaço ao longo dos últimos anos. Esta análise permitirá avaliar em que medida o agravamento das ameaças cibernéticas tem impulsionado uma maior coordenação institucional e operacional entre ambas as organizações no contexto da segurança coletiva.

1. O início da cooperação NATO-UE no ciberespaço

Nas últimas duas décadas, tanto a NATO como a União Europeia têm vindo a aceitar a realidade de que os conflitos irão, cada vez mais, possuir uma componente ciber, crescentemente sofisticada, que vai exigir uma resposta coordenada.

Alguns momentos na primeira década do milénio serviram de motor para o início desta cooperação, nomeadamente, ataques entre atores estatais. Um dos mais proeminentes foi o ciberataque da Rússia à Estónia, que acontece em 2007, após uma decisão governamental da Estónia de relocar um memorial da era soviética para um cemitério militar. Como é óbvio, este ataque insere-se num contexto geopolítico mais amplo de tensão entre os dois países, nomeadamente, devido à crescente aproximação da Estónia ao Ocidente, após a sua independência do regime soviético em 1991[1].

A Rússia dirige, então, à Estónia uma série de ciberataques, realizados ao longo de semanas, de DoS e DDoS, defacement de websites e grandes quantidades de spam de comentários e e-mails, que tiveram como alvos a infraestrutura da internet estoniana, o setor privado, bem como alvos governamentais, políticos, e outros pessoais e aleatórios[2].

É verdade que, já em 2002, na cimeira de Praga, a NATO tinha reconhecido a cibersegurança como um elemento crucial da sua estratégia de defesa. Como resultado, é criado o *Cyber Defence Program*, no qual se integrou o NATO Computer Incident Response Capability (NCIRC)[3], composto por especialistas e técnicos de cibersegurança, cujo objetivo é proteger os organismos e agências da NATO de ataques e evitar o acesso e roubo de informações confidenciais, destruição de dados, e interrupção ou dano às operações da NATO. Outro dos objetivos do NCIRC é ajudar os seus membros a lidar com as ameaças à cibersegurança.

Contudo, foi apenas em 2008, após o ataque russo à Estónia, que foi introduzida a primeira política da NATO a este respeito, a *Cyber Defense Policy*, aprovada oficialmente depois da Cimeira de Bucareste, juntamente com a criação de uma Cyber Defense Management Authority (CDMA) e um Cyber Defense Management Board (CDMB) para coordenar a defesa cibernética em todas as instituições civis e militares da NATO[4]. Também em 2008, é criado o Cooperative Defence Centre of Excellence (CCD

[1] Tikk, Kaska, & Vihul (2010).
[2] Tikk, Kaska, & Vihul (2010).
[3] Healey & Jordan (2014).
[4] Pfannenstiel & Cox (2024).

COE), em Talinn, na Estónia. Apesar de não fazer formalmente parte da NATO, o CCD COE coopera com a mesma na ciberdefesa e a sua liderança foi, inclusive, essencial para a criação do Manual de Tallinn, que analisa a aplicabilidade do Direito Internacional Humanitário ao ciberespaço[5], e cuja primeira versão foi publicada em 2013.

Durante o conflito entre a Rússia e a Geórgia de 2008, que aconteceu no contexto de uma disputa armada por Ossétia do Sul, grupos organizados de hackers russos direcionaram ataques DoS e DDoS, entre outros, para atingir sites e sistemas de comunicação governamentais da Geórgia[6].

Após este conflito, a NATO volta, em 2010, no seu *Strategic Concept,* adotado na Cimeira de Lisboa[7], a reafirmar a sua preocupação com as ciber-ameaças e com o papel preponderante que estas podem assumir na guerra convencional. No caso desta agressão à Geórgia, pôde observar-se que o objetivo era o de dificultar a coordenação das ações governamentais e contribuir para uma incapacidade do governo em comunicar com as suas forças armadas, bem como com a população. Infraestruturas militares e de média, bancos e instituições financeiras, e redes de telecomunicação, foram alguns dos vários alvos destes ataques[8].

Em 2011, é aprovada a segunda Cyber Defence Policy[9], pelos Ministros da Defesa da NATO. Os seus objetivos foram melhorar a coordenação entre os países-membros e estabelecer uma abordagem mais unificada para a ciberdefesa, trabalhar com parceiros, organizações internacionais, meios académicos e o setor privado, e evitar a duplicação de esforços.

A Operação Unified Protector**,** a intervenção de 2011 para proteger civis na Líbia, demonstrou a crescente dependência de tecnologias de informação a que as operações militares estão sujeitas. Neste contexto, a NATO aprovou o Plano de Ação de 2011 que, por sua vez, demonstrou a necessidade de proteção dos sistemas da NATO e estabeleceu a intenção de partilhar formação com parceiros da aliança, como outras organizações internacionais[10].

Em 2012, é criada a NATO Communication and Information Agency (NCIA), uma equipa responsável por fornecer serviços de comunicação à NATO. Está na linha da

[5] Ilves, Evans, Cilluffo, & Nadeau (2016).
[6] Tikk, Kaska & Vihul (2010).
[7] NATO (2010).
[8] Tikk, Kaska & Vihul (2010).
[9] Healey & Jordan (2014).
[10] Pfannenstiel & Cox (2024).

frente da defesa cibernética da NATO, sendo que uma das suas principais funções é o planeamento de capacidades de defesa, priorizando a inovação e aquisição de tecnologia avançada[11]. Abriga a equipa NCIRC e a NATO Information Security Operations Centre.

Quanto à União Europeia, já tinha, em 2004, estabelecido a European Network and Information Security Agency (ENISA), cujo objetivo inicial era partilhar conhecimento e práticas entre os Estados-Membros e, em 2010, é criado o European Union Computer Emergency Response Team (CERT-EU), uma equipa de segurança à semelhança da NCIRC da NATO, com o objetivo de reforçar a cibersegurança e responder às ameaças cibernéticas direcionadas às instituições e agências da União[12].

Contudo, foi apenas em 2013 que a UE criou a sua *Cybersecurity Strategy*. Algumas das metas desta estratégia eram aumentar a resiliência cibernética através do desenvolvimento de políticas e capacidades de ciberdefesa da União relacionadas com a Política Comum de Segurança e Defesa (PCSD), desenvolver os recursos industriais e tecnológicos para a cibersegurança, bem como estabelecer uma política coerente para o ciberespaço europeu[13].

Todavia, mesmo nos anos que se seguiram ao conflito Rússia-Geórgia, não houve uma grande ligação entre a NATO e a UE no domínio ciber. A este respeito, para reduzir duplicações, a União prometeu, na sua *Cybersecurity Strategy*, "explorar as possibilidades de a UE e a NATO complementarem os seus esforços para aumentar a resiliência das infraestruturas críticas das Administrações, da defesa e outras infraestruturas informáticas das quais dependem os membros de ambas as organizações"[14].

A NATO, enquanto aliança militar, tem um foco maior na ciberdefesa, em proteger as infraestruturas das suas agências e organismos, bem como as das forças armadas dos seus membros. A sua atuação carateriza-se, em grande parte, pelo desenvolvimento de capacidades para detetar, proteger, e, em alguns casos, reagir ofensivamente a ataques.

A UE, por sua vez, tem uma abordagem mais transversal na sua atuação, que é mais orientada para a cibersegurança. Aspetos como a proteção de dados, a regulação do setor da telecomunicação e a promoção de uma economia digital segura são algumas das

[11] Ilves, Evans, Cilluffo, & Nadeau (2016).
[12] Ilves, Evans, Cilluffo, & Nadeau (2016).
[13] União Europeia (2013).
[14] União Europeia (2013).

suas preocupações, para além de trabalhar no sentido de fortalecer a cibersegurança dos seus Estados-membros. Preocupa-se também com o combate ao cibercrime, nomeadamente através do European Cybercrime Centre (EC3) da Europol, que se concentra no cibercrime organizado, fraude nos pagamentos, crimes de alta tecnologia, exploração sexual de crianças e ataques a infratestruturas críticas[15].

Esta diferença de abordagens tem alguma influência naquilo que, ao longo dos anos, pode ter dificultado a cooperação das instituições no domínio ciber. Ao longo deste capítulo, podemos perceber que, embora alguns passos tenham sido dados no desenvolvimento das suas políticas próprias, existiu uma falta de políticas e estratégias comuns. Isto aliado ao facto de ambas a UE e a NATO, e os seus Estados-membros entre si, estarem em diferentes níveis de preparação, dificulta uma resposta conjunta aos incidentes cibernéticos, uma vez que a ciberdefesa e cibersegurança são operadas, principalmente, ao nível nacional.

Pode também ser apontada a ausência de uma perceção comum relativamente a essas ameaças e uma certa resistência à partilha de informações, sejam elas sobre ameaças ou sobre vulnerabilidades e níveis de preparação de cada Estado-Membro. Muitas vezes, estão em causa preocupações quanto à soberania nacional. Também os níveis de partilha de informação das instituições são diferentes. Se por um lado, a União Europeia, com o seu foco na cibersegurança, é mais transparente na partilha de informações, por outro, a NATO é mais propensa a manter as informações classificadas para si, nomeadamente aquelas sobre operações militares e de defesa.

Foi apenas com a anexação ilegal da Crimeia em 2014, por parte da Rússia, que a cooperação entre a UE e a NATO na ciberdefesa e cibersegurança foi expandida. Exemplo demonstrativo é o facto de, até 2014, terem realizado apenas um exercício militar conjunto em 2003, que não priorizou, de todo, os ativos cibernéticos[16].

[15] Ilves, Evans, Cilluffo, & Nadeau (2016).
[16] Lété & Pernik (2017).

2. Os ciberataques russos no contexto de hybrid warfare

Depois de o Parlamento russo ter aprovado uma lei que sancionava a utilização de força militar contra a Crimeia, e dias antes do referendo sobre o estatuto da Crimeia, unidades cibernéticas patrocinadas pelo Estado, organizações hacktivistas e cibercriminosos iniciaram os ciberataques ao leste da Ucrânia e à Crimeia[17].

Durante o processo de anexação, as infraestruturas de comunicação móvel e de internet da Ucrânia foram atacadas. A Rússia assumiu o controlo das infraestruturas de comunicação na Crimeia e os ucranianos ficaram impedidos de aceder a sites de notícias ucranianos, e as estações de televisão locais ficaram sujeitas à transmissão exclusiva de canais russos[18].

Complementarmente, equipamentos de interferência foram deslocados para o porto de Sevastopol para cortar as comunicações por rádio, e danos físicos foram infligidos à Ukrtelecom JSC, uma das maiores empresas de telecomunicações ucranianas[19], possivelmente como meio de desviar as atenções das operações militares na Crimeia, ou, simplesmente, para semear o caos[20]. Do mesmo modo, as redes de comunicação das forças militares ucranianas foram alvo de ataques, tendo a Rússia conseguido desativar até os telemóveis de militares ucranianos, bem como efetuar um corte de comunicações móveis do governo. Dados de GPS de telemóveis foram, inclusive, uma ferramenta de localização e monitorização de unidades do exército ucraniano[21].

Em maio de 2014, as eleições presidenciais democráticas na Ucrânia não se escaparam à interferência russa. O grupo hacktivista pró-russo CyberBerkut, alegadamente ligado ao grupo de hackers Fancy Bear, infiltrou-se na Comissão Central de Eleições da Ucrânia, tentando manipular os boletins de voto e erroneamente declarar o candidato de extrema-direita Dmytro Yarosh como o vencedor. Contudo, uma rápida atuação ucraniana na remoção do malware impediu que os hackers vingassem no seu objetivo de manipular as eleições presidenciais, tendo causado apenas um atraso na contagem dos votos[22].

Com estas atuações, a Rússia não se limitou simplesmente a avançar sobre o

[17] Harun & Süvari (2024).
[18] Roche & Blaine (2023).
[19] Harun & Süvari (2024).
[20] Barichella (2022).
[21] Roche & Blaine (2023).
[22] Barichella (2022).

território. Não só conseguiu desorganizar a resposta do governo ucraniano à invasão, como também enfraqueceu a capacidade de resistência das forças militares e populares. O controlo das comunicações foi, claramente, uma estratégia de impedimento da coordenação entre os diversos setores do governo e, ao mesmo tempo, uma tentativa de limitar o fluxo de informações entre o país e o mundo exterior. Por sua vez, as interferências nos processos eleitorais nada mais são do que tentativas de descredibilizar as instituições ucranianas.

As operações cibernéticas, em conjunto com outros componentes da guerra híbrida, foram, portanto, um aspeto essencial da ofensiva russa durante o conflito de 2014.

O termo "guerra híbrida" refere-se à fusão de diferentes componentes de guerra de modo a alcançar a superioridade no campo de batalha. O conceito foi introduzido, pela primeira vez, por Frank G. Hoffman, em 2007, que definiu as ameaças híbridas como aquelas que incorporam, coordenadamente, táticas convencionais e irregulares, terrorismo e desordem criminal. Estas ameaças podem ser realizadas tanto por Estados como por atores não estatais[23].

Surge, neste contexto, uma importante distinção entre duas escolas do conceito de guerra híbrida.

A primeira escola corresponde à definição circunscrita de Hoffman, que se foca na força cinética ou letal. Note-se que os aspetos de guerra, acima referidos, que foram utilizados pelo autor para definir "guerra híbrida" não incluem atos não cinéticos como ciberataques, atuações económicas e políticas, ainda que, no seu ponto de vista, sejam elementos que não devem ser totalmente desconsiderados. Hoffman associa, portanto, a guerra híbrida à coerção e a comportamentos criminais, mas a sua intenção inicial não era a de incluir ações nuclearmente não violentas, como atos económicos ou subversivos[24].

A título de exemplo, o conflito de 2008 com a Geórgia insere-se nesta primeira conceção de guerra híbrida, na medida em que a Rússia utilizou uma combinação de forças regulares, milícias locais e forças especiais, misturando métodos convencionais e irregulares de combate, o que distingue a guerra híbrida da dita tradicional. No passado, as operações convencionais e irregulares ocorriam de forma separada e as primeiras eram predominantes[25].

Contudo, a definição de guerra híbrida evoluiu para algo mais do que aquilo que

[23] Hoffman (2008).
[24] Hoffman (2008).
[25] Wither (2016).

Hoffman tinha inicialmente estabelecido quando a União Europeia e a NATO adotaram o conceito, após a anexação da Crimeia[26]. É aqui que surge a segunda escola do conceito.

A NATO, inicialmente alinhada com a visão militar de Hoffman, alargou a definição para incluir aspetos não militares, como meios de propaganda, ciberataques e sabotagem[27], como os verificados no processo de anexação da Crimeia. O conceito de guerra híbrida, nomeadamente na sua segunda conceção, ficou intrinsecamente ligado ao conflito russo-ucraniano.

Por exemplo, antes de 2014 e do surgimento desta nova interpretação de guerra híbrida, o conflito entre Israel e o Hezbollah em 2006 é um exemplo compatível com a definição contemporânea de guerra híbrida, na medida em que o Hezbollah combinou táticas convencionais e de guerrilha e, para além disso, fez um uso eficaz da Internet e meios de comunicação para influenciar a opinião global[28].

A Cimeira da NATO no País de Gales, em setembro de 2014, foi um momento crucial de reconhecimento formal da natureza híbrida do conflito, quando oficiais da NATO deram ênfase ao uso de táticas híbridas pela Rússia, que incluíam meios militares, paramilitares e civis. Resultou, ainda, na aprovação do Readiness Action Plan (RAP), que incluía um conjunto de medidas para melhorar a capacidade da NATO de responder a essas ameaças. Outro ponto destacado nesta Cimeira foi a importância da defesa cibernética e da proteção contra campanhas de desinformação[29].

A União Europeia, por sua vez, com o seu foco predominantemente político e económico, também favoreceu a perceção não-cinética de guerra híbrida, dada a sua escassa atividade e especialização em assuntos militares. Em 2016, na sua *Joint Framework on Countering Hybrid Threats*, reconheceu que:

"Embora as definições de ameaças híbridas variem e tenham de permanecer flexíveis para responder à sua natureza evolutiva, o conceito destina-se a abarcar a combinação de atividades coercivas com atividades subversivas, de métodos convencionais com métodos não convencionais (ou seja, diplomáticos, militares, económicos, tecnológicos) que podem ser utilizados de forma coordenada por intervenientes estatais ou não estatais para atingir objetivos específicos, mantendo-se, no entanto, abaixo do limiar de uma guerra formalmente declarada"[30].

[26] Muradov (2022).
[27] Bankov (2023).
[28] Wither (2016).
[29] NATO (2014).
[30] Comissão Europeia (2016).

Esta ampliação suscitou críticas que apontam uma ambiguidade potencialmente diluidora da utilidade do conceito de guerra híbrida, uma vez que o seu escopo é, agora, demasiado abrangente ao incluir todo e qualquer tipo de ato violento[31]. No Relatório Anual do Secretário-Geral de 2019, a NATO sugere que as potências hostis não precisam de ir para o campo de batalha para infligir danos aos seus adversários, desconsiderando, de alguma forma, a relevância exclusiva dos aspetos militares no conceito de guerra híbrida[32]. Algumas críticas apontam também o facto de esta ampliação potenciar situações em que um conflito que não envolve sequer meios militares seja apontado como um exemplo de guerra híbrida[33].

Qualquer uma das conceções de guerra híbrida podem ser aplicadas, de forma clara, ao conflito russo-ucraniano.

No que diz respeito à definição de Hoffman, desde a invasão russa de 2022, e embora a Rússia tenha iniciado o conflito com métodos convencionais, nomeadamente através de ataques aéreos e de mísseis, rapidamente recorreu a táticas de guerra não convencionais, como a espionagem. A utilização de forças irregulares, como as milícias Chechenas e os mercenários da Wagner, bem como a violência indiscriminada contra civis, em locais como Bucha, são, também, elementos-chave da guerra híbrida observada na Rússia, nomeadamente para desestabilizar a população e enfraquecer a resistência ucraniana[34].

No que toca à conceção contemporânea de guerra híbrida, na qual se inserem métodos como a instrumentalização do domínio ciber, a verdade é que o período que se seguiu à anexação da Crimeia em 2014 caraterizou-se por uma crescente de ciberataques constantes contra infraestruturas cruciais ucranianas.

Em dezembro de 2015, o vírus Black Energy afetou a rede de várias empresas de distribuição de energia. Como resultado, cerca de 30 estações elétricas foram afetadas e mais de 200 000 consumidores no oeste da Ucrânia sofreram cortes de energia que variaram de uma a seis horas[35].

Em dezembro do ano seguinte, membros ligados à Sandworm dirigiram um ataque, de menor escala, a uma subestação elétrica em Kiev, que resultou numa

[31] Bankov (2023).
[32] NATO (2020).
[33] Wither (2016).
[34] Bankov (2023).
[35] Barichella (2022).

interrupção significativa na distribuição de energia, causando um apagão que durou cerca de uma hora. Adicionalmente, dois vírus, o KillDisk e o BlackEnergy, interromperam as redes de comunicações internas do Ministério das Finanças, do Serviço do Tesouro do Estado e do Fundo de Pensões da Ucrânia, desativando vários computadores e destruindo bases de dados financeiras críticas, o que causou grandes atrasos nos pagamentos do orçamento[36].

A 27 de junho de 2017, a Sandworm realizou um outro ciberataque à Ucrânia, que ficou conhecido como NotPetya e que se caraterizou pela intrusão de um malware nos servidores de um famoso sofware ucraniano para pagamentos e declarações fiscais[37]. Entre os alvos iniciais estavam várias agências governamentais ucranianas, instituições financeiras, redes de transporte, grupos de media e empresas estatais, como a Ukrtelecom, o Aeroporto de Boryspil e o Ukrainian Railways, e até mesmo o setor da saúde. No total, mais de 1500 instituições foram vítimas do ataque, com muitos dos seus ficheiros informáticos sobrepostos ou permanentemente danificados[38].

Apesar de a Ucrânia ter sido o principal alvo de ataque, as repercussões do NotPetya foram sentidas noutros países, como nos Estados Unidos, Alemanha, Dinamarca e França e, ao todo, causou danos globais estimados em quase 10 mil milhões de dólares, sendo considerado um dos ciberataques mais destrutivos da história[39]. A própria Rússia, embora responsabilizada pelo ataque, sofreu os impactos transfronteiriços do vírus NotPetya, o que, de certa forma, demonstra a sua própria vulnerabilidade aos ativos cibernéticos que desenvolve[40].

Os ciberataques nunca encontraram, necessariamente, um término, tendo, na realidade, atingido um pico com o escalar da guerra em 2022. Nesse ano, em meados de janeiro, 70 sites governamentais, incluindo o dos Negócios Estrangeiros e dos Ministérios da Defesa, da Ciência e da Educação, foram alvo do ataque de malware WhisperGate e ficaram temporariamente sobre o controlo de hackers, que exibiram uma mensagem ameaçadora: "Wait for the worst"[41]. Em Fevereiro, um outro ataque DDoS voltou a afetar, durante algumas horas, sites governamentais, estações de rádio e dois dos maiores bancos nacionais– o Privatbank e o Oschadbank -, deixando os ucranianos sem acesso a serviços

[36] Kolodii (2024).
[37] Roche & Blaine (2023).
[38] Kolodii (2024).
[39] Barichella (2022).
[40] Kolodii (2024).
[41] Barichella (2022).

como apps e pagamentos online, enquanto as forças russas se concentravam ao longo da fronteira[42].

Como esperado, a invasão militar russa de 24 de fevereiro de 2022 foi acompanhada por inúmeros ciberataques ainda mais destrutivos. Na véspera da invasão, várias organizações ucranianas dos setores governamental, tecnológico, financeiro e energético foram atingidas com o malware HermeticWiper, capaz de destruir ou corromper dados, e que infetou centenas de computadores e redes[43]. Já no próprio dia 24 de fevereiro, ocorreu um ataque cerca de uma hora antes da invasão, que foi atribuído à Rússia e que interrompeu o acesso à internet via satélite KA-SAT da empresa Viasat para milhares de ucranianos, bem como para várias autoridades públicas e negócios durante mais de 2 semanas[44]. O Ministro da Transformação Digital da Ucrânia, à altura, Mykhailo Fedorov, confirmou uma segunda ronda de ataques DDoS que voltaram a afetar sites governamentais e de bancos ucranianos[45].

Ademais, foi detetada uma campanha de phishing conduzida por um grupo de hackers bielorrussos, com o objetivo de atacar membros do pessoal governamental europeu envolvidos na gestão da logística dos refugiados que fugiam da Ucrânia[46]. Também foi direcionado um ataque a uma estação de controlo fronteiriço da Ucrânia, atrasando o processo de passagem de refugiados para a Roménia[47].

O site de notícias ucraniano Kyiv Post reportou que esteve sob constante ataque desde o início do conflito armado no dia anterior. O ataque DDoS incapacitou os seus sistemas e tiveram de encontrar formas alternativas de publicação de notícias, nomeadamente, através de redes sociais. Embora a atribuição deste ataque seja inconclusiva, foi, claramente, uma tentativa de limitar o acesso do público à informação do conflito a escalar[48]. Adicionalmente, o Meta revelou que bloqueou inúmeras tentativas de campanhas de desinformação através de contas falsas de alto perfil, incluindo de oficiais militares e figuras públicas[49].

A 25 de fevereiro, foi lançado um outro vírus destrutivo, designado de Isaac Wiper, direcionado às redes de computadores governamentais ucranianas. Seguiu-se, em meados

[42] Antoniuk (2022).
[43] Barichella (2022).
[44] European Union (2022).
[45] Brumfield (2022).
[46] Przetacznik & Tarpova (2022).
[47] Berger (2022).
[48] CyberPeace Institute (s.d.).
[49] CyberPeace Institute (s.d.).

de março, o malware Caddy Wiper, que conseguiu infiltrar os sistemas de diversas entidades financeiras e governamentais. Além disso, a 28 de março, ciberataques afetaram a 'Ukrtelecom', que já havia sido alvo de ataques cibernéticos algumas vezes desde a anexação de 2014, causando uma redução de 13% na conetividade nacional.[50]

A tentativa de infiltração em Kiev por parte de unidades de reconhecimento e sabotagem russas, disfarçadas de civis ou com uniformes ucranianos, a circulação de vídeos falsos da rendição do Presidente Zelensky e relatos de tentativas de assassinato do mesmo são alguns exemplos de campanhas de desinformação instrumentalizadas naquilo que é uma guerra psicológica contra a população ucraniana, com a intenção de gerar caos, pânico e medo na população ucraniana, desmotivar a resistência e incentivar a rendição[51].

Também o próprio direito tem sido utilizado como uma estratégia de guerra híbrida, algo que é, hoje, caraterizado como *lawfare*. Em 2014, a anexação da Crimeia foi enquadrada pela Rússia num ato legal de autodeterminação, uma tentativa óbvia de justificação de algo que, claramente, violava o direito internacional e a integridade territorial da Ucrânia. Também a presença dos soldados russos, sem uniformes e insígnias, foi disfarçada como ação de voluntários locais e milícias, uma tática-chave de negação plausível. Já em 2022, a Rússia usou o reconhecimento das repúblicas separatistas de Luhansk e Donetsk como pretexto para uma suposta missão de paz, ocultando, desta forma, a verdadeira natureza da invasão[52].

Desde a anexação da Crimeia em 2014 até à invasão de 2022, os ciberataques encabeçados pela Rússia contra a Ucrânia não só foram uma demonstração das suas táticas híbridas, mas também um reflexo da crescente dependência do domínio ciber a que as operações convencionais de guerra estão sujeitas nos dias de hoje. Desde os ataques a infraestruturas críticas até à interferência direta nas eleições e campanhas de desinformação, a Rússia tem demonstrado uma crescente especialização na fusão das várias componentes de guerra, combinando elementos militares, tecnológicos e psicológicos para atingir os seus objetivos, enquanto simultaneamente desestabiliza a Ucrânia e a comunidade internacional.

[50] Barichella (2022).
[51] Bankov (2023).
[52] Marques (2023).

3. As problemáticas inerentes à classificação de um ciberataque como ataque armado no contexto do conflito russo-ucraniano

3.1. A ausência de uma definição codificada de "ataque armado" e "uso da força"

Os ciberataques russos à Ucrânia e ao Ocidente levantam questões sobre a sua qualificação como "uso da força" nos termos do artigo 2(4) da Carta da ONU.

A proibição do uso da força em direito internacional é uma norma consuetudinária de *jus cogens*, aplicável a todos os Estados, sejam ou não membros da ONU. Diz-nos o artigo 2(4) da Carta das Nações Unidas: "Todos os Membros devem abster-se, nas suas relações internacionais, da ameaça ou do uso da força contra a integridade territorial ou a independência política de qualquer Estado, ou de qualquer outra forma incompatível com os fins das Nações Unidas"[53].

Apesar desta proibição, a letra do artigo não faz referência explícita ao ciberespaço e a verdade é que os termos "uso da força" e "ataque armado", muitas vezes confundidos, não se encontram definidos em nenhum tratado ou convenção internacional, incluindo na própria Carta, que faz referência ao último para efeitos do exercício do direito à legítima defesa patente no seu artigo 51. Portanto, a qualificação de um ciberataque como ataque armado encontra de imediato um entrave na ausência de definições jurídicas codificadas. Contudo, a interpretação destes termos tem sido desenvolvida através de jurisprudência internacional.

No caso Nicarágua vs. Estados Unidos (1986), o Tribunal Internacional de Justiça explicitou que nem todo o uso da força corresponde a um ataque armado, para efeitos de legítima defesa individual e coletiva[54]. O TIJ afirmou que o fornecimento de armas, apoio logístico ou outro tipo de assistência, não é suficiente para caraterizar um ataque armado, embora possa ser qualificado como uso da força ou como intervenção ilícita nos assuntos internos de outro Estado[55].

Esta interpretação do TIJ está alinhada com o disposto na Resolução 3314 da Assembleia Geral da ONU que, apesar de não ser juridicamente vinculativa, é reconhecida pela sua influência no desenvolvimento do direito internacional consuetudinário a este respeito. No seu artigo 3, enumera alguns atos de uso da força que

[53] Nações Unidas (1945), artigo 2(4).
[54] Tribunal Internacional de Justiça (1986), Nicaragua vs United States of America, §191.
[55] Tribunal Internacional de Justiça (1986), Nicaragua vs United States of America, §195.

correspondem a uma agressão, entre eles, a invasão militar, o bombardeamento, os bloqueios navais e o envio de tropas, grupos armados e mercenários. Ou seja, menciona atos com um grau significativo de gravidade e intensidade[56].

Também na decisão Oil Platforms (Irão vs. EUA, 2003), o TIJ sublinhou que, para que um ato seja considerado "ataque armado" no âmbito do direito internacional, é necessário que este apresente uma certa gravidade, reafirmando que nem todo o uso de força entre Estados deve justificar o exercício do direito à legítima defesa, sendo necessário que o ato envolva uma violação considerável da soberania territorial de um Estado e cause efeitos materiais ou danos relevantes[57].

O entendimento do termo "uso da força", como está mencionado no artigo 2(4) da Carta da ONU, resume-se tradicionalmente a ações militares cinéticas, como ataques armados, que envolvem violência visível. Isto é algo que podemos observar, por exemplo, nos exemplos de atos de agressão enumerados no artigo 3 da Resolução 3314 da AG da ONU, acima mencionada. No entanto, os ciberataques são, muitas vezes, menos evidentes e envolvem danos que não são imediatamente físicos. A natureza virtual dos ciberataques pode resultar em danos económicos, interrupções de serviços essenciais ou roubo de dados, mas sem uma manifestação de violência física.

Neste sentido, a guerra cibernética desafia ainda mais o entendimento tradicional de "força", pois, para além de possuir, em muitas situações, um efeito extremamente indiscriminado, combina também elementos de força militar, coação económica e subversão. Durante a criação da própria Carta da ONU, houve debates sobre a definição de “força” no contexto do artigo 2(4), com alguns países a propor uma conceção mais ampla, que incluísse formas de coação, como qualquer pressão política ou económica que ameaçasse a autonomia dos Estados[58]. A delegação brasileira propôs, inclusive, uma referência a "força armada e económica", mas essa proposta foi posteriormente rejeitada[59].

Em 2009, o CCD COE da NATO lançou um projeto de investigação que resultou nos já mencionados Manuais de Tallinn 1.0 e 2.0. Estes dois documentos correspondem a uma análise de especialistas internacionais sobre como o direito internacional existente se aplica às operações cibernéticas. A regra 69 do Manual de Talinn define o "uso da

[56] Assembleia Geral das Nações Unidas (1974).
[57] Tribunal Internacional de Justiça (2003), Islamic Republic of Iran vs. United States of America, §51.
[58] Waxman (2011).
[59] Titiriga (2013).

força" no contexto cibernético, afirmando que uma operação cibernética constitui uso da força quando sua a escala e efeitos são comparáveis aos de operações não cibernéticas que configuram uso da força. Tal como o TIJ distinguiu entre níveis diferentes de gravidade de "uso da força" no caso Nicarágua vs. EUA, o Grupo Internacional de Especialistas do Manual de Talinn estabeleceu que a escala e os efeitos são fatores essenciais para determinar se uma ação constitui um ataque armado, justificativo de legítima defesa, nos termos da regra 71[60].

Existem algumas abordagens no meio académico para determinar se um ciberataque pode ser qualificado como um uso de força proibido pela Carta da ONU.

Em primeiro lugar, uma abordagem baseada no instrumento utilizado levará sempre a uma conclusão negativa uma vez que não há propriamente uma interação física, na medida em que uma operação cibernética pode ser realizada a qualquer distância. Contudo, esta é uma teoria que reúne alguns defensores no meio académico[61].

De seguida, uma abordagem baseada no objetivo sugere que qualquer operação cibernética que tenha como alvo um sistema informático suficientemente importante deve ser considerada um ataque armado[62]. De acordo com esta teoria, a força económica ou política que prejudique a integridade da independência territorial e política de um Estado deve ser sujeita às regras de uso da força com o objetivo de garantir a paz e segurança na comunidade internacional[63]. Há quem aponte que a aplicação consistente de uma abordagem baseada no objetivo aumentaria o risco de conflitos internacionais, pois até uma interferência mínima, justificaria o uso da força em legítima defesa[64].

Uma última abordagem baseada na escala e no efeito de um ataque sugere que quanto mais as consequências de uma operação cibernética se assemelham às de armas convencionais, mais provável é que seja considerada um uso da força ou um ataque armado, independentemente do tipo de instrumento utilizado ou alvo[65]. As armas cibernéticas são impossíveis de categorizar, ou seja, o que pode ser usado para diferenciar entre as várias armas ou ataques cibernéticos, continua a ser a gravidade do impacto, e isto, infelizmente, será sempre uma abordagem pós-facto.

---

[60] Schmitt (Ed.) (2017).
[61] Spáčil (2022).
[62] Spáčil (2022).
[63] Leng (2023).
[64] Spáčil (2022).
[65] Spáčil (2022).

Estas três abordagens caraterizam-se pela convergência na ideia de que um ciberataque, se constitutivo de um conjunto de requisitos, pode ser considerado um ataque armado. Contudo, a discussão acerca da qualificação de um ciberataque como ataque armado parece preferir, como já tivemos oportunidade de observar, a abordagem centrada nos seus efeitos.

De facto, vários países, como a Alemanha, a Estónia, a Itália, os Países Baixos, a Nova Zelândia, a Noruega, Singapura, a Suíça e o Reino Unido, afirmam que a escala e os efeitos da operação cibernética devem ser considerados para avaliar se a mesma equivale a um ataque armado, comparando-a com ataques tradicionais[66]. Conforme já foi constatado, o próprio artigo 71 do Manual de Talinn faz referência à escala e aos efeitos de um ciberataque para a sua qualificação como ataque armado.

A União Europeia, na sua *Declaration on a Common Understanding of International Law in Cyberspace*, marcou a posição de que, de acordo com o Artigo 2(4) da Carta das Nações Unidas e o direito internacional consuetudinário, a ameaça ou o uso da força contra a integridade territorial ou a independência política de um Estado é proibido, incluindo a agressão definida pela Resolução 3314 da Assembleia Geral da ONU. Afirmou, também, que as operações cibernéticas podem causar danos significativos, afetando as Tecnologias da Informação e Comunicação (TIC) e, dependendo da sua escala e efeitos, podem ser comparáveis a um uso cinético da força, configurando assim um uso da força proibido pela Carta da ONU[67].

Em setembro de 2012, o Departamento de Estado dos EUA afirmou que atividades cibernéticas que resultem em mortes, ferimentos ou destruição significativa poderiam ser consideradas um uso da força, nos termos do artigo 2 (4) da Carta. No entanto, os EUA também reconhecem que existem casos em que ciberataques sem efeitos cinéticos fazem parte de um conflito armado e que esse tipo de ataques a, por exemplo, redes de informação durante um conflito armado devem ser regulados pelos mesmos princípios de Direito Internacional Humanitário, podendo justificar retaliações com força cinética proporcional. Além disso, atividades cibernéticas que constituam um ataque armado ou ameaça iminente podem ativar o direito de defesa de um país, conforme o artigo 51 da Carta da ONU[68].

Também o TIJ, no seu parecer consultivo sobre a legalidade da ameaça ou uso de

[66] Spáčil (2022).
[67] Conselho da União Europeia (2024).
[68] Theohary (2024).

armas nucleares de 1996 sugere que a qualificação de um ato como *uso da força* não depende do meio específico utilizado para o ataque, mas sim da gravidade do ato em questão.[69]

Através do Manual de Tallinn 1.0, o grupo de especialistas desenvolveu uma lista não exclusiva de fatores que podem ajudar na caraterização de uma operação cibernética como uso da força: gravidade, imediatismo, direcionalidade, grau de intrusão, mensurabilidade, caráter militar, envolvimento do Estado e presunção de legalidade[70].

Quanto à gravidade, se os danos se traduzirem em lesões físicas ou destruição de infraestrutura crucial, a ação vai ser considerada um uso da força[71].

Quanto ao imediatismo, a rapidez com que os efeitos de uma ação se manifestam vai sempre influenciar a resposta dos Estados e uma solução pacífica é mais difícil de encontrar nos casos em que os efeitos negativos de uma ação são sentidos de imediato[72].

Em relação à direcionalidade, se as consequências não forem diretamente causadas pela ação inicial, os Estados podem não considerar o ato como um uso da força. Relativamente ao grau de intrusão, um ataque cibernético que danifique a infraestrutura de um país sem violar fisicamente as suas fronteiras é menos invasivo do que um ataque militar convencional, que é, consequentemente, mais propenso a desestabilizar a ordem internacional [73].

No que respeita à mensurabilidade, no caso de ataques cibernéticos, quantificar o dano pode ser difícil, o que dificulta a caraterização do ato como uso da força, em contraste com situações de conflito armado.

Para além da necessidade de ser observado um caráter militar que enquadre a operação cibernética, o grau de responsabilidade de um Estado, do qual depende o seu envolvimento direto, é também um importante requisito a ser observado. Quanto maior a conexão entre o ataque e o Estado, maior a probabilidade de que outros países considerem esse ato como uma violação do direito internacional. Determinar a responsabilidade, especialmente em operações cibernéticas, pode ser desafiador devido à dificuldade em rastrear o envolvimento direto de um Estado[74].

Quanto à presunção de legalidade, em direito internacional, na ausência de

[69] Tribunal Internacional de Justiça (1996).
[70] Burkadze (2018).
[71] Schmitt (1999).
[72] Schmitt (1999).
[73] Theohary (2024).
[74] Theohary (2024).

proibição explícita, um ato é considerado legítimo. Portanto, existem atividades de coação que são legalmente permitidas, mesmo que realizadas através de meios cibernéticos[75]. A linha entre ciberataques hostis e atividades legítimas no ciberespaço, como a ciber-espionagem, é, muitas vezes, ténue, o que dificulta a ponderação do exercício à legítima defesa.

Como já pudemos observar anteriormente, inúmeras operações cibernéticas foram encabeçadas contra a Ucrânia ao longo do seu conflito com a Rússia. Mas o ciberataque de 24 de fevereiro ao satélite da empresa Viasat foi um que se destacou precisamente pela escala e o efeito que teve no povo e no exército ucraniano.

Procedendo a uma análise dos elementos do Manual de Talinn acima mencionados, não existem dúvidas quanto à gravidade do ataque, que resultou num corte de comunicações e energia na Ucrânia, mas, para além disso, a rede Viasat também servia como fornecedora de comunicação para as forças militares e de segurança da Ucrânia, interrompendo, assim, comunicações militares e afetando civis na Europa. Foi, como tal, direcionado aos sistemas de comunicação, mas causou danos colaterais significativos a civis.

Quanto ao imediatismo, o ataque afetou imediatamente os sistemas críticos e as operações militares ucranianas. Teve também um alto grau de intrusão, desativando completamente a infraestrutura do satélite. O impacto foi mensurável, na medida em que afetou a comunicação e o setor energético em várias regiões, tanto na Ucrânia como noutros países da Europa. O ataque teve, como sabemos, caráter militar, sendo acompanhado da invasão terrestre do território da Ucrânia, quase que simultaneamente.

Quanto ao elemento do grau de envolvimento do Estado, a Rússia foi amplamente responsabilizada pelo ataque. O Centro Nacional de Cibersegurança do Reino Unido, o Departamento de Estado dos EUA e o Conselho da União Europeia atribuíram oficialmente o ataque à Rússia. Os grupos Sandworm e APT44, alegadamente ligados ao GRU (Direção-Geral de Inteligência) da Rússia, foram identificados pela NSA. No entanto, a Rússia tem repetidamente negado envolver-se em operações cibernéticas ofensivas[76].

Por último, relativamente ao caráter legal da operação, embora possam ser identificados objetivos militares, o ataque causou danos a civis, levantando questões

[75] Schmitt (1999).
[76] Khalil, Bitar & Raj (2024).

sobre a sua proporcionalidade e legalidade. De acordo com as disposições do Artigo 52 do Protocolo Adicional I às Convenções de Genebra, os objetivos militares são limitados aos que contribuem diretamente para operações militares, sendo que a sua destruição, captura ou neutralização proporciona uma vantagem militar significativa[77]. A avaliação da proporcionalidade do ataque dependeria da comparação entre a interrupção das operações militares ucranianas e os danos causados a civis e infraestrutura civil. O ataque aos sistemas de telecomunicações afetou não só objetivos militares, mas também civis, com impacto na Ucrânia e noutros países da Europa[78].

Claro que o ataque à Viasat não é o único ciberataque passível de uma análise sob a orientação do artigo 2(4) da Carta. Também os ataques às redes elétricas de 2015 e 2016, bem como o NotPetya de 2017, foram massivos nas suas escalas e efeitos, mas os efeitos transbordantes e a direcionalidade indiscriminada que caraterizou o ataque à Viasat torna-o um bom exemplo para esta investigação.

Ainda que não seja considerado um uso da força para efeitos do artigo 2(4) da Carta, este ataque levanta outras questões. Para além dos efeitos sentidos na Ucrânia, afetou, por exemplo, uma importante empresa energética alemã, que perdeu a capacidade de monitorização remota de quase 6000 turbinas eólicas[79]. Se este tipo de operações russas causarem efeitos concretos nos membros da Aliança ou da UE, poderão qualificar-se como uma violação da soberania territorial desses países?

As interferências eleitorais por parte da Rússia na Ucrânia e nos EUA são também elas passíveis de uma análise à luz da violação da soberania de um Estado. Segundo a regra 4 do Manual de Talinn, uma ciberoperação viola a soberania de um Estado se produzir efeitos no seu território ou se interferir com funções inerentemente governamentais, como eleições[80]. Ainda não existe consenso quanto aos efeitos das ciberoperações que configuram uma violação da soberania territorial. A França adotou a posição extrema de que qualquer efeito no seu território já constitui violação da soberania, mas, no geral, reconhece-se que ciberoperações contra sistemas públicos ou privados podem violar a soberania estatal[81].

As ações russas, nomeadamente as suas interferências eleitorais, também podem ser consideradas à luz da proibição da intervenção nos assuntos internos ou externos de

[77] Nações Unidas (1977). Artigo 52 - Protection of civilian objects.
[78] Khalil, Bitar & Raj (2024).
[79] CyberPeace Institute (s.d.).
[80] Schmitt (Ed.) (2017).
[81] Schmitt (2022).

outro Estado, regra 66 do Manual de Talinn 2.0[82].

A intervenção ocorre através de coerção no "domaine reservé" do Estado[83]. O conceito de "domaine réservé" refere-se a áreas da soberania de um Estado que são protegidas de intervenção externa, ou seja, questões que não estão reguladas pelo direito internacional e, portanto, são de competência exclusiva do Estado, como a escolha do sistema político, social, económico e cultural, além das suas políticas externas. Exemplos incluem decisões políticas internas e organização de eleições. A interferência nas eleições presidenciais democráticas na Ucrânia em 2014, pelo grupo não estatal CyberBerkut, ligado ao Estado russo, de modo a declarar o candidato de extrema-direita Dmytro Yarosh como o vencedor, é um bom exemplo para esta ponderação.

Por outro lado, relativamente à interferência da Rússia nas eleições presidenciais dos EUA em 2016, a questão de se constituiu intervenção já é mais debatível, pois, embora tenha visado a prerrogativa soberana da escolha do sistema político, não o foi através de coerção, na medida em que a Rússia não interferiu na infraestrutura eleitoral propriamente dita[84].

No entanto, a extensão do conceito de "domaine réservé" tem sido debatida, pois o direito internacional tem, desde o surgimento do conceito, vindo a expandir-se, restringindo o alcance dessa área de soberania[85]. A intervenção deve forçar o Estado a agir ou a abster-se de agir de certa forma. No entanto, influenciar decisões sem impor tal coerção não basta para configurar intervenção e as operações devem incidir sobre áreas como atividades políticas ou militares, sendo que operações que apenas influenciem a opinião pública não atingem esse limiar[86].

[82] Schmitt (Ed.) (2017).
[83] CCD COE (s.d.).
[84] Tsagourias (2019).
[85] Ossoff (2021).
[86] Schmitt (2022).

3.2. O problema da atribuição

A Rússia tem demonstrado a sua capacidade de integrar atores não estatais nas suas estratégias cibernéticas, muitas vezes para evitar atribuição e responsabilização direta à luz do direito internacional, como técnica de negação plausível.

As atividades russas no domínio cibernético são apoiadas por um ecossistema de atores. Entre os atores estatais, salientam-se o FSB (Serviço Federal de Segurança) e o GRU (Direção-Geral de Inteligência). Este último encontra-se ligado a atores não estatais como o APT28 (Fancy Bear), que esteve envolvido em interferências eleitorais na Ucrânia e nos EUA; ao grupo SandWorm, responsável por vários ataques destrutivos como o NotPetya; e ao CyberBerkut, muitas vezes envolvido em campanhas de desinformação[87].

Esta caraterística do conflito russo-ucraniano reflete a realidade de que, com a variedade de atores no ciberespaço, surgem motivações racionais até àquelas completamente imprevisíveis, que podem não ser políticas ou económicas. Para o ataque ser considerado um ato de guerra, um Estado deve ser responsável pelas ações do ator não estatal, como especificam os princípios de responsabilidade internacional. Isto levanta o problema da atribuição no ciberespaço[88].

Sem a atribuição de um ciberataque, não é possível recorrer ao direito de legítima defesa, individual ou coletiva, ou aplicar sanções como medidas diplomáticas ou contramedidas estatais. Isto dificulta a tarefa que incumbe ao Estado de satisfazer os requisitos de imediatismo e necessidade exigidos para exercer legalmente o seu direito de legítima defesa[89].

Existem várias caraterísticas inerentes ao ciberespaço que complicam a tarefa de atribuição. Em primeiro lugar, o domínio ciber não tem fronteiras físicas e geográficas, na medida em que um ataque pode ser realizado a partir de qualquer lugar e, mesmo assim, possuir um elevado nível de gravidade no seu impacto e indiscriminação. Para além disto, o anonimato é algo que o carateriza. Ainda que se consiga identificar a pessoa ou o grupo responsável por um ciberataque, acresce o desafio jurídico de atribuir uma responsabilidade estatal.

A atribuição de um ciberataque começa com uma análise dos dados do ataque.

[87] Hakala & Melnychuk (2021).
[88] Ducaru, Caradaică, & Costea (2024).
[89] Finlay & Payne (2019).

Trata-se de uma atribuição técnica, que se refere à identificação da origem factual de um ciberataque, isto é, de quem o executou ou qual foi a infraestrutura utilizada, através de uma recolha de dados de todas as fases do ciclo de um ciberataque, desde a fase preparatória até à fase final. É uma análise que envolve técnicas forenses digitais, como a análise de malware e infraestrutura. Contudo, esta dimensão contém algumas limitações decorrentes, nomeadamente, das ferramentas que podem ser utilizadas para mascarar a atividade online, que são também elas um obstáculo à atribuição de responsabilidade no ciberespaço[90].

Quando um Estado assume publicamente a posição de vítima de um ataque cibernético, perpetrado ou patrocinado por outro Estado, estamos perante uma atribuição política. Isto pode acontecer através de declarações oficiais ou exigências diplomáticas para que o Estado ofensor termine a sua conduta, entre outras formas[91]. Este tipo de atribuição é, portanto, frequentemente utilizado para fins de dissuasão, diplomacia coerciva ou justificação de contramedidas. Como sabemos, tanto a Ucrânia como membros da NATO e da UE já realizaram inúmeras declarações de atribuição pública em resposta a ataques contra infraestruturas críticas. Note-se, por exemplo, que o Reino Unido, os EUA e o Conselho da UE, entre outros, se mobilizaram na atribuição à Rússia do ataque à internet por satélite ucraniana, em 2022, apesar de a Rússia negar o seu envolvimento veementemente[92]. Esta coordenação entre os governos aliados levou a uma atribuição mais credível deste ataque, que se destacou pela sua escala e efeitos.

Por último, a imputação jurídica refere-se à atribuição de responsabilidade internacional a um Estado por atos ilícitos no ciberespaço. Um Estado não será responsabilizado por um ato internacionalmente ilícito a menos que esse ato lhe seja atribuível, sendo que se reconhece que a imputação é mais facilmente realizada quando o ataque é perpetrado por um órgão do Estado, nos termos do artigo 4 dos *Draft Articles on State Responsability*[93].

Por sua vez, nos termos do artigo 8, a conduta de um ator não estatal pode ser atribuída a um Estado quando o ator não estatal agir sob as suas instruções ou sob a sua direção ou controlo[94]. A regra 17 do *Manual de Tallinn 2.0* incorpora este artigo, estabelecendo que um Estado pode ser responsabilizado internacionalmente por uma

[90] Tsagourias & Farrell (2020).
[91] Davis (2022).
[92] Blinken (2022).
[93] Davis (2022).
[94] Comissão de Direito Internacional (2001).

ciberoperação quando os autores do ataque atuem sob instruções, direção ou controlo efetivo do Estado, ou quando o Estado reconheça a atuação como sua, refletindo o artigo 11 dos *Draft Articles on State Responsability*. Para que haja responsabilidade, é ainda necessário que a conduta em causa constitua uma violação de uma obrigação internacional, como, por exemplo, a proibição do uso da força ou a violação da soberania de outro Estado. Por fim, a atribuição requer a existência de provas suficientes que demonstrem a ligação entre o Estado e o ataque[95].

A aplicação do artigo 8 é difícil devido à complexidade em definir o controlo efetivo de um Estado sobre grupos cibernéticos, especialmente quando estes operam de forma descentralizada e anónima. A natureza dispersa dos atores cibernéticos e a dificuldade em provar o controlo direto do Estado, mesmo com apoio financeiro ou logístico, são também fatores dificultadores.

O limiar elevado de um controlo efetivo é alvo de algumas críticas, especialmente no sentido em que parece incentivar os Estados a entregar este tipo de tarefas a atores não estatais, desde que sob uma supervisão mínima[96]. Um simples incentivo ou apoio de um Estado por meio de financiamento e fornecimento de recursos para grupos será insuficiente para a atribuição[97]. Uma possível solução seria reduzir o limiar de atribuição, evitando que os Estados fiquem impedidos de responder legalmente e que ajam fora da estrutura legal existente. Contudo, a falsa atribuição é também um risco que pode resultar de um diminuir do limiar de atribuição[98].

Quanto ao nível de prova exigido, ou *standard of proof*, o Tribunal Internacional de Justiça não estabelece um padrão uniforme para todas as situações, variando a sua interpretação consoante a gravidade da situação em concreto. No caso Bósnia Herzegovina vs. Sérvia e Montenegro (2007), o TIJ concluiu que, para estabelecer a responsabilidade de um Estado por genocídio, o padrão de prova teria de ser mais elevado, exigindo uma prova "totalmente conclusiva"[99], mas não um nível de prova "além de uma dúvida razoável", que exige um nível de certeza quase absoluta[100].

Nos casos Nicarágua vs. EUA (1986) e Irão vs. EUA (Oil Platforms, 2003), o TIJ utilizou o padrão da "preponderância da prova", que estabelece que quando a maioria das

[95] Schmitt (Ed.) (2017).
[96] Tran (2018).
[97] Finlay & Payne (2019).
[98] Finlay & Payne (2019).
[99] Tribunal Internacional de Justiça (2007), Bosnia and Herzegovina vs. Serbia and Montenegro §209.
[100] Davis (2022).

provas apontam para uma conclusão provável, a atribuição nesse sentido é a correta[101].

Parece começar a ser entendimento geral no direito internacional que o padrão de prova apropriado para ciberataques que, na sua maioria, são menos gravosos, é o padrão da "preponderância da prova". A Agência de Segurança Nacional dos EUA, por exemplo, determinou que, no caso do ataque WannaCry, a "preponderância da prova" apontava para a responsabilidade da Coreia do Norte[102]. Aplicar um padrão excessivamente elevado, como o da "além de uma dúvida razoável" dificultaria a ação, enquanto a aplicação de um padrão mais baixo pode afetar a fiabilidade e levar a decisões erróneas. Também não faria sentido aplicar o padrão de prova "clara e convincente" a casos de ciberataques menos gravosos, uma vez que estaríamos a equiparar a sua gravidade aos casos de ataque armado.

Tanto a União Europeia como a NATO têm vindo a reforçar o papel da atribuição através de instrumentos como a EU Cyber Diplomacy Toolbox e a NATO Cyber Defence Pledge.

A Cyber Diplomacy Toolbox, adotada pela UE em 2017, destaca a importância de responder coletivamente a atividades cibernéticas maliciosas, incluindo através de medidas restritivas como sanções. Sublinhou, neste contexto, que a atribuição assume uma natureza predominantemente política, permitindo uma resposta conjunta mesmo quando não há atribuição comprovada. A Toolbox promove ainda a coordenação entre os Estados-Membros na partilha de informações técnicas e de inteligência, contribuindo para uma atribuição mais eficaz e coordenada[103].

Paralelamente, a NATO, em várias das suas iniciativas, como a Cyber Defence Pledge de 2016, incentiva a partilha de inteligência e a cooperação técnica entre os Estados-membros, o que facilita a identificação conjunta da origem dos ciberataques[104]. A partilha de informação é também um ponto central das 74 propostas comuns da UE e da NATO.

A UE, em específico, implementou em 2019 um regime de sanções cibernéticas para defender a União e os seus membros contra ciberataques[105]. Para além disso, um

[101] Davis (2022).
[102] Tsagourias & Farrell (2020).
[103] Conselho da União Europeia (2017).
[104] NATO (2016).
[105] Botek (2019).

outro regime de sanções foi adotado pela UE com foco na Rússia e, desde a invasão de 2022, 16 pacotes de sanções foram aplicados[106].

[106] Comissão Europeia (2025).

3.3.Os mecanismos de defesa coletiva da NATO e da UE

A defesa coletiva é uma medida excecional de direito internacional que justifica o uso da força por um Estado de forma defensiva, assim como por outros Estados que o apoiem. O Artigo 5 do Tratado do Atlântico Norte é o reflexo disso. O Tribunal Internacional de Justiça, no caso Nicarágua vs. EUA (1986), reconheceu o direito à defesa coletiva como um direito consuetudinário, baseado em normas estabelecidas, como o Artigo 51 e resoluções da Assembleia Geral[107].

Alguns meses depois da invasão e anexação da Crimeia pela Rússia, a NATO adotou a posição, na Cimeira de Gales de 2014, de que, caso as operações cibernéticas se qualifiquem como um ataque armado, o Estado vítima terá o direito de solicitar a invocação do direito à defesa coletiva, nos termos do artigo 5[108].

Como foi dito anteriormente, a classificação de um ato como uso da força, para efeitos dos artigos 2(4) e 51 da Carta das Nações Unidas, dependerá da sua escala e efeitos, mas poderá um ciberataque que não cause morte ou destruição significativa justificar a aplicação deste mecanismo?

Neste contexto, o Conselho do Atlântico Norte decide, por unanimidade, se um ciberataque justifica a invocação do Artigo 5. Contudo, a NATO escolhe deliberadamente não definir os termos da sua aplicabilidade[109]. Em vez disso, adota uma abordagem flexível, de análise caso-a-caso, com respostas que podem variar desde represálias diplomáticas a ataques militares, dependendo da gravidade do ataque.

Uma das razões apontadas para esta ambiguidade estratégica é que a incerteza vai tornar mais difícil para os potenciais adversários calcularem o risco de um ciberataque desencadear uma resposta de defesa coletiva. A ideia é criar um efeito dissuasório e, ao mesmo tempo, preservar a flexibilidade de avaliar cada situação caso a caso.

Adicionalmente, se um limiar claro fosse estabelecido, aumentaria a probabilidade de os adversários tentarem manter-se abaixo desse limite, continuando a realizar ciberataques prejudiciais, mas menos severos e, desta forma, poderia criar-se um precedente de ataques considerados aceitáveis.

Contudo, há quem defenda que a NATO deve atualizar as suas estratégias e esclarecer a sua posição sobre o artigo 5 uma vez que, sem uma posição clara, os

[107] Schmitt (2019).
[108] NATO (2014).
[109] Prucková (2022).

adversários podem explorar essa incerteza[110].

Nenhum incidente cibernético até hoje levou à invocação do Artigo 5. A 10 de novembro de 2022, o Secretário-Geral da NATO, Jens Stoltenberg, enfatizou que o ciberataque de fevereiro do mesmo ano ao provedor global de comunicações por satélite Viasat, que ocorreu horas antes da invasão terrestre da Ucrânia, causou danos colaterais sentidos muito para além da Ucrânia. Apesar destes efeitos transbordantes e direcionamento indiscriminado, no contexto de um conflito armado, a Aliança não deliberou publicamente sobre a aplicação do artigo 5[111].

No entanto, a NATO reconheceu, por exemplo, que ataques cibernéticos semelhantes aos que a Estónia sofreu em 2007 poderiam levar à sua invocação hoje[112].

De forma geral, o artigo 5 foi acionado apenas uma vez, em resposta ao ataque de 11 de setembro de 2001, o que reveste de particular interesse o facto de a única vez em que o mecanismo de defesa coletiva foi invocado ter sido em resposta a um ataque levado a cabo por um ator não estatal, a Al-Qaeda. Tal facto esclarece de forma definitiva quaisquer dúvidas sobre a aplicabilidade deste mecanismo a ataques perpetrados por atores não estatais[113].

A falta de danos materiais significativos e a dificuldade na atribuição dos ciberataques são fatores que dificultam uma resposta militar convencional à luz do artigo 5. Neste contexto, o artigo 4 do Tratado do Atlântico Norte surge como uma viável alternativa. Este artigo prevê que os Estados Membros consultem entre si se considerarem que a segurança, independência política ou integridade territorial de algum deles está sob ameaça, permitindo uma colaboração mais ampla entre os países, sem necessidade do recurso a meios militares, através, por exemplo, do empréstimo de servidores, apoio de especialistas e troca de experiências. Para além disso, este artigo não abrange outras ameaças à segurança cibernética, não só aquelas que cause danos físicos e materiais[114].

Existe também uma cláusula de assistência mútua no quadro legal da União Europeia. O artigo 42 (7) do Tratado da União Europeia diz-nos: “Se um Estado-Membro vier a ser alvo de agressão armada no seu território, os outros Estados-Membros devem prestar-lhe auxílio e assistência por todos os meios ao seu alcance, em conformidade com

[110] Bajarūnas (2025).
[111] Klipstein & Japaridze (2022).
[112] Prucková (2022).
[113] Schmitt (2019).
[114] Leshchuk (2019).

o artigo 51.º da Carta das Nações Unidas. Tal não afeta o caráter específico da política de segurança e defesa de determinados Estados-Membros. Os compromissos e a cooperação neste domínio respeitam os compromissos assumidos no quadro da Organização do Tratado do Atlântico Norte, ...[115]"

Tal como o mecanismo do artigo 5 da NATO, a cláusula de defesa mútua da União Europeia foi invocada uma única vez, aquando dos ataques terroristas de 2015 em Paris[116]. Contudo, apesar disto, existem algumas diferenças que podem ser apontadas relativamente ao mecanismo de defesa coletiva da NATO.

Segundo a letra da lei, os Estados-Membros da UE têm uma obrigação explícita de defender o Estado vítima, e devem fazê-lo "por todos os meios ao seu alcance", e não apenas através daqueles que considerem necessários. Em segundo lugar, o limiar para invocar uma "agressão armada" no contexto do artigo 42 (7) TUE parece ser mais baixo, comparativamente ao limiar para invocar um "ataque armado", no contexto do artigo 51 da CNU. Contudo, há também quem considere esta uma questão que suscita da tradução literal do francês[117].

A referência explícita à NATO na letra do artigo 42 (7) parece ser uma forma de reconhecimento de que, para os Estados-Membros da UE que também são membros da NATO, esta permanece a organização principal para a defesa coletiva. Para além disso, o artigo 42(7) do TUE reconhece a neutralidade de certos Estados-Membros da UE, ao especificar que "não afeta o caráter específico da política de segurança e defesa de determinados Estados-Membros"[118].

A Estratégia de Cibersegurança da UE de 2020 não oferece grandes respostas relativamente à aplicabilidade do artigo 42(7) TUE ao domínio ciber. Ciberataques que não afetam diretamente o território ou a infraestrutura física de um Estado normalmente não justificam a invocação do artigo 42(7). Além disso, como os ciberataques geralmente não atingem o limiar de um ataque armado, a invocação do artigo 42(7) será improvável na maioria dos casos. No entanto, se um Estado considerar que um ciberataque ultrapassa esse limiar, podem haver pedidos de assistência mútua.[119].

Para além das questões que advém da aplicabilidade destes mecanismos ao domínio ciber, existe ainda um outro problema digno de análise, o facto de a Ucrânia não

[115] União Europeia (2012).
[116] EEAS (2022). Artigo 42(7) TUE.
[117] Clapp & Verhelst (2022).
[118] Deen, Zandee & Stoetman (2022).
[119] Deen, Zandee & Stoetman (2022).

pertencer nem à União Europeia nem à NATO.

Como já foi mencionado acima, o artigo 42(7) TUE obriga os Estados-Membros da UE a fornecerem ajuda mútua se um dos seus membros for vítima de agressão armada no seu território, ou seja, a aplicação da defesa mútua da UE é limitada aos membros da União Europeia. Por sua vez, também o artigo 5 da NATO estabelece que um ataque armado contra um dos membros da aliança é considerado um ataque contra todos os membros, que devem tomar as medidas necessárias para defender o Estado atacado. No entanto, como a Ucrânia não é membro da NATO, este artigo também não se aplica.

Isto não implica que tanto a União Europeia como a NATO não tenham procurado prestar apoio voluntário à Ucrânia ao longo da última década, mas não no contexto formal das cláusulas dos artigos 42 (7) TUE e 5 do Tratado do Atlântico Norte. Por exemplo, a Ucrânia beneficiou de vários programas e exercícios do CCD COE, e foi, para além disso, a maior beneficiária dos programas "Science for Peace and Security" da NATO em 2014. Também a cooperação em questões de defesa cibernética no grupo de trabalho NATO-Ucrânia se destacam a este respeito[120].

Não obstante as problemáticas inerentes à aplicabilidade dos mecanismos de defesa coletiva da NATO e da UE, a Ucrânia tem o direito à legítima defesa. O artigo 51 da Carta estabelece que: "Nada na presente Carta prejudica o direito inerente à autodefesa individual ou coletiva, no caso de um ataque armado contra um Membro das Nações Unidas"[121]. A regra 71 do Manual de Talinn 2.0 reflete este artigo, ao reconhecer o direito à legítima defesa de um Estado que seja alvo de um ciberataque elevado ao nível de ataque armado.

Neste contexto, a Assembleia Geral da ONU adotou, em 2013, a Resolução A/RES/68/243 que afirma que a soberania dos Estados e as normas internacionais se aplicam às atividades relacionadas com as TIC e à jurisdição sobre a infraestrutura de TIC no território de cada Estado[122].

A União Europeia adota a posição de que um Estado que tenha sido alvo de um ciberataque que constitua ataque armado, ou seja, cuja escala e efeitos sejam comparáveis aos de um ataque cinético convencional, tem o direito de invocar a legítima defesa individual, nos termos do artigo 51º da Carta. Fatores relevantes para avaliar a escala e os

[120] Pfannenstiel & Cox (2024).
[121] Nações Unidas (1945), artigo 51.
[122] Assembleia Geral das Nações Unidas (2014).

efeitos de um ciberataque incluem danos ou destruição bens ou infraestrutura crítica, lesões ou morte de pessoas, etc. Ao mesmo tempo, a resposta deve cumprir os requisitos de necessidade e proporcionalidade. Vários Estados, como a França e os EUA admitem também a possibilidade de um ciberataque que não tenha efeitos físicos poder ser também ele categorizado como uso da força legitimador de uma resposta à luz do artigo 51, dependendo da sua escala e impacto[123].

O direito à defesa individual depende de um conjunto de fatores já analisados, nomeadamente, a classificação do ato como ataque armado que, por sua vez, dependerá da sua escala e efeitos, de uma correta atribuição desse ataque.

Para além disso, depende ainda do respeito por parte do Estado que invoca o seu direito de defesa de um conjunto de princípios, como a proporcionalidade e a necessidade. Estes requisitos não encontram definição na Carta das Nações Unidas.

O Grupo Internacional de Especialistas explica, na regra 72 do Manual de Talinn, que a análise do requisito de necessidade é feita através da existência de alternativas que não impliquem o uso da força, dando o exemplo de que defesas cibernéticas passivas, como firewalls, ou ativas que não impliquem o uso da força, devem ser preferidas a um ataque armado cibernético ou cinético.

Na regra 72 do Manual de Talinn, podemos encontrar também a proporcionalidade como um requisito necessário a atender no contexto da legítima defesa cibernética, espelhando os artigos 51 (5) (b) e 57 (2) do Additional Protocol I. O Grupo Internacional de Especialistas explica, na regra 72, que o tipo e a quantidade de força usada dependem do contexto, podendo ser superior ou inferior à do ataque original. Além disso, não é necessário que a resposta seja do mesmo tipo, importa é que seja adequada para cessar a agressão e proporcional ao objetivo defensivo, mesmo que o atacante seja imune a certos tipos de operações.

Na sequência da invasão russa em 2022, a Ucrânia formou o *IT Army* por meio de um canal no Telegram, convocando voluntários, profissionais tecnológicos e hackers, para realizar ataques cibernéticos contra alvos russos, como empresas de energia, bancos e sites governamentais, o Kremlin, entre outros[124].

Para além destes requisitos, existe um terceiro de iminência, para os casos de legítima defesa antecipatória.

Embora alguns autores defendam que a legítima defesa antecipatória deve ser

[123] NATO CCD COE (s.d.).
[124] Burgess, M. (2022).

encabeçada no momento exato em que o ataque está prestes a ser lançado, isto impossibilita um verdadeiro impedimento do ataque iminente e configura uma visão excessivamente restritiva no que concerne a natureza inerente de quase total imprevisibilidade de um ciberataque. Uma outra visão, apoiada pelos autores do Manual de Talinn, sugere que se deve atender à "última janela possível de oportunidade" para impedir o ataque. Ao mesmo tempo, é preciso uma análise da probabilidade de o ataque causar danos significativos suficientes para ser qualificado como um "ataque armado"[125]. Esta visão já permite uma ação antecipada.

No caso russo-ucraniano, Michael N. Schmitt, um dos principais autores e coordenadores do Manual de Talinn, defende que o direito à legítima defesa da Ucrânia começa aquando da anexação da Crimeia em 2014. As operações cibernéticas que atingem o nível de uso da força, e que podem ser atribuídas à Rússia ou a grupos não estatais sob a sua direção, são subsumidas na violação contínua da proibição do artigo 2(4) da Carta, a qual começou com a ocupação ilegal[126].

O mesmo raciocínio pode ser aplicado às operações cibernéticas que acompanharam e procederam a escalada do conflito em fevereiro de 2022, as quais também se inserem na violação cinética da proibição do uso da força que ocorreu quando a Rússia invadiu o território ucraniano. Esta é, de certa forma, uma perspetiva que reflete a conjuntura de problemáticas inerentes à classificação de um ciberataque, por si só, como uso da força e, consequentemente, como justificação para um Estado invocar o direito à legítima defesa.

Como já tivemos oportunidade de observar, os ciberataques, por natureza, levantam dificuldades evidentes de atribuição e de avaliação dos seus efeitos. A dúbia origem de um ataque dificulta, muitas vezes, uma convincente atribuição estatal, dado o recurso a autores não estatais, a manobras de mascaramento de atividades cibernéticas ilegais, entre outros fatores. Existem outras razões pelas quais os Estados não têm por hábito classificar uma operação cibernética como um uso da força elevado ao nível de ataque armado, ou até partilhar informações sobre a atribuição da responsabilidade por um ataque ciber a um Estado terceiro.

Existe ainda um problema de confiança internacional, na medida em que muitos Estados não apresentam publicamente todas as provas que sustentam a atribuição,

[125] Bethlehem (2019).
[126] Schmitt (2022).

nomeadamente por questões diplomáticas e geopolíticas ou de segurança nacional. Muitos Estados, incluindo a Austrália, Estónia, França, Alemanha, Itália e Suíça, afirmaram que não existe uma obrigação jurídica de atribuir ou de tornar públicas as decisões de atribuição, na medida em que o ato de atribuição é uma prerrogativa nacional, ficando à discrição de cada Estado[127].

Além disso, a escala e o impacto dos ciberataques são extremamente variáveis. Embora alguns tenham consequências muito graves, que podemos observar quando analisamos o historial de ciberataques russos à Ucrânia, como apagões elétricos e cortes de energia que duram semanas, interferência eleitoral ou sabotagem e destruição de infraestruturas críticas, muitos outros têm efeitos não tão sérios. Isto suscita dúvidas sobre se ultrapassam o limiar de gravidade necessário para se qualificarem ciberataques como ataque armado. Aliás, as operações cibernéticas, na sua maioria, têm efeitos muito limitados e a probabilidade de um Estado correr o risco diplomático e geopolítico de classificar um ato de um Estado terceiro como uso da força nestas circunstâncias é muito reduzido. Acresce que, tradicionalmente, a jurisprudência e a prática estatal associam o uso da força à destruição física, algo que a maioria dos ciberataques não produz diretamente.

A maioria dos Estados prefere manter a resposta a ataques cibernéticos no domínio diplomático, económico ou cibernético, evitando abrir precedentes que contribuam para a militarização do ciberespaço. A própria Rússia adota, na sua guerra cibernética, uma estratégia de se manter abaixo de um limiar de ataques considerados gravosos. A probabilidade de um dos seus ciberataques, por si só, causar morte ou danos físicos graves de modo a legitimar uma resposta individual ou coletiva é muito baixa. Este tipo de respostas vão sempre depender das atuações cinéticas no contexto da guerra híbrida russa.

A ausência de consenso internacional reforça esta relutância. As interpretações divergem quanto aos critérios jurídicos que definem o uso da força ou o ataque armado no ciberespaço. A prática estatal e a *opinio juris* sobre esta matéria ainda se encontram em construção, como demonstra, por exemplo, o Grupo de Trabalho Aberto (OEWG) das Nações Unidas. Existe também o receio de que a expansão do conceito de ataque armado ao domínio cibernético possa contribuir para a erosão do *jus ad bellum*, aumentando as possibilidades jurídicas de recurso à força e abrindo caminho a abusos de natureza política.

[127] NATO CCD COE (s.d.).

Por fim, os Estados demonstram preferência por respostas alternativas. Em vez de recorrerem à força armada, têm privilegiado sanções económicas, operações cibernéticas de retaliação, exposição de campanhas de desinformação ou apoio técnico a Estados vítimas de ataques. Ferramentas político-diplomáticas, como a *Cyber Diplomacy Toolbox* da União Europeia ou as declarações conjuntas da NATO, oferecem vias de resposta com menor risco de escalada.

Em 2019, a UE implementou um regime de sanções cibernéticas, com base na Toolbox. As sanções apenas podem ser aplicadas a atores não estatais e os ciberataques têm de ter efeitos significativos e constituir uma ameaça externa à União e aos seus membros, enquanto os atores internos permanecem sob jurisdição nacional. As sanções incluem a proibição de entrada na UE e o congelamento de fundos e recursos económicos. A inclusão e remoção de agressores da lista de sanções é da responsabilidade exclusiva do Conselho da UE, enquanto as decisões exigem unanimidade entre os Estados-Membros. Os visados têm direito a ser informados, apresentar observações e recorrer judicialmente[128].

Desde a invasão de 2022, 16 pacotes de sanções foram aplicados à Rússia pela UE. Estas já não estão diretamente ligadas ao regime de sanções de 2019, uma vez que essas foram concebidas para defender a UE e os seus membros de ameaças cibernéticas. O mais recente pacote de sanções foi adotado este ano, em janeiro, e inclui medidas financeiras, energéticas, comerciais, entre outras. Incluiu também a suspensão das atividades de 8 meios de comunicação que apoiam a guerra da Rússia na Ucrânia, como maneira de combater a desinformação, elemento estratégico da Rússia na sua guerra híbrida[129].

[128] Botek (2019).
[129] Comissão Europeia (2025).

4. A evolução da cooperação UE-NATO no domínio cibernético

Na declaração conjunta de 2016, assinada na Cimeira de Varsóvia, foi reconhecida a necessidade urgente de combater as ameaças híbridas, através de uma maior partilha de informação entre as duas instituições. Também foi destacada a necessidade de coordenação dos seus esforços na cibersegurança e defesa, no contexto das suas missões, operações, e exercícios[130].

A 10 de fevereiro de 2016, a União Europeia e a NATO assinaram um Acordo Técnico para estabelecer uma colaboração entre a NATO Computer Incident Response Capability (NCIRC) e a Computer Emergency Response (CERT) da União Europeia. Este acordo estabeleceu um quadro possibilitador de uma troca de informações e partilha de boas práticas entre as duas equipas[131].

Entre dezembro de 2016 e 2017, os Ministros dos Negócios Estrangeiros da NATO aprovaram 74 medidas específicas para reforçar a colaboração entre a NATO e a UE em sete áreas estratégicas de interesse comum, entre elas o combate às ameaças híbridas, cibersegurança e defesa[132]. A União Europeia e a NATO acordaram em proceder à troca de conceitos e promoção da interoperabilidade em normas de ciberdefesa; a uma abertura de cursos de formação a pessoal de ambas as organizações; ao incentivo à investigação e inovação tecnológica, reforçando os laços com o NATO CCD COE; e a uma participação recíproca nos seus exercícios. Esta cooperação oficial visou evitar a duplicação de esforços, promovendo, simultaneamente, uma abordagem comum num contexto em que a maioria dos países da UE também integra a NATO[133].

Desde a aprovação deste conjunto de medidas, nove relatórios foram publicados pela NATO, que nos ajudam a perceber o caminho que tem sido percorrido na sua concretização.

No âmbito das ameaças híbridas, a colaboração tem sido reforçada através da crescente interação entre a EU Hybrid Fusion Cell e a NATO Hybrid Analysis Branch, bem como através da participação ativa das equipas de ambas as instituições no Hybrid Centre of Excelence, em Helsínquia, através de workshops e treinos conjuntos[134]. Além

[130] NATO & União Europeia (2016).
[131] NATO (2016)
[132] NATO (2024).
[133]Trinberg, L. (s.d.).
[134] Conselho da União Europeia (2018).

disso, estratégias híbridas têm sido produzidas regularmente, abordando, por exemplo, ameaças a infraestrutura crítica e a crescente cooperação entre a Rússia e o Irão[135].

O Hybrid Centre of Excelence facilita a implementação das medidas propostas, promovendo a formulação de estratégias eficazes no âmbito da segurança híbrida, por meio de comunidades de interesse e redes informais de especialistas que trocam conhecimentos e formulam respostas estratégicas com impacto operacional[136].

A ciberdefesa e a cibersegurança continuam a ser áreas prioritárias de cooperação. O intercâmbio de informações e alertas sobre ameaças digitais tem sido constante, facilitado pelo Acordo Técnico entre a CERT-EU e o NCIRC. Exercícios conjuntos, como o Cyber Coalition da NATO e o Cyber Europe da UE, têm fortalecido a capacidade de resposta coordenada a incidentes de segurança digital. Além disso, workshops e conferências internacionais promovem o alinhamento de doutrinas e estratégias para fortalecer a resiliência cibernética das duas organizações[137].

A guerra na Ucrânia veio também destacar a importância do fortalecimento das parcerias de ambas a UE e a NATO para melhorar as suas capacidades de resposta a incidentes cibernéticos. Para além de prestarem apoio à Ucrânia, as medidas incluem iniciativas para mitigar os impactos da guerra em parceiros estratégicos como a Moldávia e a Geórgia[138].

Complementarmente, as organizações têm trabalhado em conjunto para monitorizar e expor campanhas de desinformação, especialmente no contexto da guerra na Ucrânia, utilizando plataformas como o Rapid Alert System da UE e o StratCom CoE da NATO[139]. Além disso, ações coordenadas de comunicação pública visam fortalecer uma narrativa baseada em factos.

A cooperação em políticas de defesa tem sido ampliada, garantindo um maior alinhamento estratégico entre a UE e a NATO. A segurança de infraestruturas críticas, como redes de telecomunicações e cadeias de abastecimento, também tem sido objeto de iniciativas conjuntas.

A declaração conjunta de 2018 veio reforçar, uma vez mais, a importância da cooperação contra ameaças híbridas e cibernéticas, apelando a uma maior partilha de

[135] NATO (2024).
[136] Lindstrom (dir.) (2019).
[137] NATO (2019).
[138] NATO (2021).
[139] NATO (2023).

informações e resiliência contra ciberataques e desinformação[140]. Uma nova declaração foi assinada entre a NATO e a UE, em 2023, na qual as organizações condenaram fortemente as ações russas, reafirmando o apoio à soberania e ao direito da Ucrânia à legítima defesa. Ambas as organizações se comprometeram, novamente, a reforçar a cooperação nas áreas da ciberdefesa e das ameaças híbridas, com o objetivo adicional de aprofundar essa cooperação em domínios emergentes, como a proteção de infraestruturas críticas, novas tecnologias e manipulação de informação[141].

Em dezembro de 2023, foi lançado o Mecanismo de Tallinn para reforçar o apoio à Ucrânia na sua resistência a ciberataques dirigidos a infraestruturas críticas, unificando os esforços de 12 nações, incluindo os Estados Unidos, Canadá, França, Alemanha, Itália, Reino Unido, entre outros, com a NATO e a União Europeia a participarem como observadores. As principais iniciativas incluem o fornecimento de tecnologia de ponta, tanto em forma de hardware como software, a oferta de formação avançada para oficiais de cibersegurança e a capacitação da Ucrânia para a deteção e neutralização de malware. O Mecanismo também apoia as comunicações por satélite, uma componente crítica da infraestrutura digital da Ucrânia que, como já tivemos oportunidade de observar, foi tantas vezes alvo de ataque por parte da Rússia[142].

Num relatório do European Union Institute for Security Studies (EUISS), Bruno Lété, Senior Fellow no German Marshall Fund of the United States (GMF), sugere a criação de um centro de informação comum entre a UE e a NATO no domínio cibernético e a criação de um corpo específico para coordenar respostas conjuntas a crises cibernéticas, com diretrizes claras baseadas no Manual de Tallinn. Uma partilha mais direta e eficaz de inteligência e boas práticas poderia mais rapidamente levar à sua uniformização e posterior aplicação prática. O especialista em defesa e segurança debate, ainda, sobre os benefícios que poderiam advir da criação de um fundo comum para países parceiros, coordenado pela UE e pela NATO, para desenvolver competências locais e promover a integração nos projetos de ciberdefesa[143].

Como já tivemos oportunidade de analisar no primeiro capítulo, existem algumas diferenças naquilo que é o foco de atividade de cada uma das instituições, o que, por sua vez, pode ter contribuído, ao longo dos anos, para uma escassa cooperação. Contudo, se

[140] NATO & União Europeia (2018).
[141] NATO & União Europeia (2023).
[142] Complex Discovery (2024).
[143] Lindstrom (dir.) (2019).

forem alvo de uma maior coordenação, as suas abordagens distintas podem funcionar a favor de uma maior cooperação no âmbito da ciberdefesa e segurança, bem como das ameaças híbridas. A NATO tem uma maior prontidão militar, enquanto a UE oferece integração política e económica. A cooperação entre ambas tem sido crucial, especialmente no contexto do conflito russo-ucraniano, e uma maior coordenação entre os seus focos de atividade, isto é, numa garantia da dissuasão militar por parte da NATO, enquanto a UE contribui com apoio financeiro, infraestrutural e humanitário, iria tornar-se ainda mais fundamental para a estabilidade internacional[144].

Uma maior autonomia estratégica por parte da UE e o fortalecimento do seu papel dentro da NATO, seria, também, benéfica para o futuro da ciberdefesa, especialmente face a um segundo mandado de Donald Trump na Casa Branca, cujas tendências isolacionistas podem enfraquecer os compromissos de segurança dos Estados Unidos com a Europa, ainda que sem uma retirada formal[145]. Além de impor sanções à Rússia, a UE financiou armamento para a Ucrânia e adotou a Declaração de Versalhes em março de 2022, que reforça o compromisso com uma maior autonomia em defesa, energia e economia. A declaração enfatiza a necessidade de cooperação entre os Estados-Membros para investimentos conjuntos em defesa e a redução da dependência de recursos russos[146].

Ambas a UE e a NATO devem identificar as áreas mais afetadas por uma redução do compromisso dos EUA, entre elas o domínio ciber e a guerra híbrida, priorizá-las estrategicamente, e abordar as ameaças globais de forma coordenada[147].

A respeito de uma maior autonomia na defesa da União Europeia, a 19 de março de 2025, foi publicado o *White Paper on European Defence – Readiness 2030*, como parte do Plano *Rearm Europe/Readiness 2030*. É um documento estratégico elaborado pela Comissão Europeia e pela Alta Representante da União Europeia para os Negócios Estrangeiros e Política de Segurança Kaja Kallas.

O documento reconhece que a segurança europeia enfrenta diversas ameaças híbridas que incluem ciberataques, sabotagem, interferência eletrónica nos sistemas globais de navegação e satélite e campanhas de desinformação. O seu principal objetivo é fechar as lacunas nas capacidades de defesa da UE, identificando áreas da defesa europeia que necessitam de reforço e propondo medidas para colmatar as suas

[144] Geri (2025).
[145] Spatafora (2024).
[146] Parlamento Europeu (2022).
[147] Spatafora (2024).

insuficiências, como o investimento em ferramentas de guerra cibernética e outras tecnologias militares avançadas, como inteligência artificial e computação quântica, e também na proteção de infraestruturas críticas. O plano inclui propostas para investimentos financeiros significativos, como um programa de empréstimos de 150 mil milhões de euros para projetos de defesa[148].

O *White Paper* sublinha a importância de apoiar o desenvolvimento das capacidades de defesa da Ucrânia, através do fornecimento de armamento, apoio à sua indústria de defesa, aprimoramento da mobilidade militar da UE e a garantia do acesso da Ucrânia a ativos espaciais europeus, bem como a sua integração nas iniciativas da UE para desenvolver capacidades de defesa.

Este documento serve como base para a iniciativa Readiness 2030, que pretende mobilizar até 800 mil milhões de euros para reforço da defesa da Europa.

Alguns aspetos jurídicos acompanham o cumprimento das propostas delineadas nesta iniciativa.

Em primeiro lugar, é proposto que os Estados-Membros utilizem a cláusula de escape nacional do Pacto de Estabilidade e Crescimento (PEC) para aumentar a despesa pública em defesa sem infringir as regras fiscais da União Europeia. O Security Action for Europe (SAFE)**,** um novo instrumento financeiro da UE, permitirá a concessão de empréstimos de até €150 bilhões aos Estados-Membros para investir na indústria de defesa da Europa, apoiados pelo orçamento da UE[149].

Uma vez que o artigo 41(2) do TUE proíbe que o orçamento da União Europeia seja usado para despesas militares e de defesa, o documento utiliza o Artigo 122º do TFUE como base legal para adotar medidas econômicas e financeiras urgentes. Este artigo, utilizado em contextos de emergência, tem sido a principal base para a criação de instrumentos financeiros excecionais. A Comissão Europeia enfatiza que as medidas são temporárias, o que levanta questões sobre a sua eficácia e a necessidade de medidas permanentes para a segurança e defesa da UE[150].

Por último, o documento menciona que a Comissão Europeia pretende lançar um Diálogo Estratégico com a indústria de defesa até junho de 2025, com o objetivo de harmonizar as regulamentações. A proposta inclui a modificação das estruturas de aquisição para acelerar as aquisições conjuntas e a implementação de isenções

[148] Gray & Bayer (2025).
[149] Vecchio (2025).
[150] Vecchio (2025).

temporárias de IVA para importações e fornecimentos de produtos de defesa. Como podemos observar, a União Europeia encontra-se agora num momento de plena consciência quanto à necessidade de autonomia e investimento na sua própria defesa.

Na Cimeira da NATO de 2024, em Washington, também a Aliança se comprometeu a fornecer à Ucrânia um financiamento de pelo menos 40 mil milhões de euros, reforçando o apoio à sua defesa contra as agressões russas. Os Aliados concordaram no estabelecimento do NATO Integrated Cyber Security Centre, para coordenar e melhorar a resposta cibernética da Aliança a ameaças e ataques no ciberespaço. Este centro, que opera sob o Comando de Ciberdefesa da NATO, tem como objetivo integrar e consolidar os esforços de defesa cibernética entre os países membros da NATO. A próxima cimeira irá realizar-se em Haia, em junho deste ano, e é esperado que também os países da Aliança se comprometam com um aumento do investimento em defesa[151].

[151] Agência Lusa (2025).

Conclusão

A cooperação entre a União Europeia e a NATO no ciberespaço tem registado um desenvolvimento notável ao longo dos últimos anos, refletindo a crescente complexidade, sofisticação e militarização dos recursos cibernéticos. O número de políticas e iniciativas conjuntas desde a anexação ilegal da Crimeia pela Federação Russa, em 2014, constitui um marco indicativo da mudança de paradigma provocada pelas ações russas neste contexto.

A análise jurídica das dinâmicas entre estes atores permite identificar diversos obstáculos persistentes à regulamentação do ciberespaço. A ambiguidade normativa e a pluralidade de interpretações dificultam não só a atribuição de responsabilidade estatal, como também a formulação de respostas legítimas, à luz da defesa individual e coletiva. Este panorama evidencia a necessidade de um esforço concertado por parte da UE e da NATO na modelação ou clarificação de normas globais aplicáveis à conduta dos Estados no ciberespaço.

Paralelamente, as atividades cibernéticas e as operações no âmbito da guerra híbrida suscitam relevantes questões jurídicas quanto à sua eventual qualificação como violações da soberania estatal ou interferência nos assuntos internos e externos de outros Estados.

Subsiste, ainda, uma relutância, por parte dos Estados, em qualificar estas operações como ataques armados. Neste sentido, as respostas continuam a privilegiar alternativas diplomáticas, económicas e cibernéticas.

A própria natureza dos ciberataques contribui para esta dificuldade: a ausência de contacto físico direto, a capacidade de execução remota, a disponibilidade de ativos a atores não estatais e o vasto leque de instrumentos disponíveis para mascarar atividades online tornam estas operações bastante elusivas. A sua imprevisibilidade, aliada ao seu potencial indiscriminatório, tornam os ativos cibernéticos dos mais perigosos da atualidade.

Referências bibliográficas

Jurisprudência

Tribunal Internacional de Justiça (1986), Nicaragua vs. United States of America. https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

Tribunal Internacional de Justiça (1986), Islamic Republic of Iran vs. United States of America. https://www.icj-cij.org/sites/default/files/case-related/90/090-20031106-JUD-01-00-EN.pdf

Tribunal Internacional de Justiça (1996). Advisory opinion on the legality of the threat or use of nuclear weapons. https://www.icj-cij.org/case/95

Legislação

Nações Unidas (1945). Carta das Nações Unidas. https://www.un.org/en/about-us/un-charter/chapter-1

Assembleia Geral das Nações Unidas. (1974). Resolução 3314 (XXIX): Definição de Agressão. *Nações Unidas.* https://crimeofaggression.info/documents/6/General_Assembly_%20Resolution_%203314.pdf

Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2ª ed.). *Cambridge University Press*. https://doi.org/10.1017/9781316822524

Nações Unidas (1977). Article 52 - Protection of civilian objects. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I). https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.34_AP-I-EN.pdf

Comissão de Direito Internacional (2001). Draft articles on responsibility of states for internationally wrongful acts. *Nações Unidas.* https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

União Europeia (2012). Consolidated version of the Treaty on European Union. *Official Journal of the European Union. https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF*

Documentos Oficiais

Assembleia Geral das Nações Unidas (2014). Resolution A/RES/68/243. https://docs.un.org/en/A/RES/68/243

NATO (2010). Strategic concept for the defence and security of the members of the North Atlantic Treaty Organization: Adopted by heads of state and government at the NATO summit in Lisbon, 19-20 November 2010. *North Atlantic Treaty Organization*. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

União Europeia. (2013). Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido. *Comissão Europeia*. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52013JC0001

NATO (2014). Wales Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. Press Release. https://www.nato.int/cps/cn/natohq/official_texts_112964.htm

Comissão Europeia (2016). Comunicação conjunta ao Parlamento Europeu e ao Conselho: Um quadro estratégico sobre a resiliência na ação externa da UE. *União Europeia.* https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52016JC0018

NATO (2020). Secretary General's annual report 2019. *NATO.* https://www.nato.int/nato_static_fl2014/assets/pdf/2020/3/pdf_publications/sgar19-en.pdf

União Europeia (2022). Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union. *Conselho da União Europeia.* https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

Conselho da União Europeia (2024). Declaration on a Common Understanding of International Law in Cyberspace. *União Europeia.* https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf

Conselho da União Europeia (2017). Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities ("Cyber Diplomacy Toolbox"). *União Europeia.* https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/pt/pdf

Comissão Europeia (2025). EU adopts the 16th package of sanctions against Russia. *European Commission. Finance.* https://finance.ec.europa.eu/news/eu-adopts-16th-package-sanctions-against-russia-2025-02-24_en

NATO (2016). Cyber Defence Pledge. https://www.nato.int/cps/em/natohq/official_texts_133177.htm

NATO (2019). Fourth Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf

NATO (2021). Sixth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf

NATO (2023). Eighth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/6/pdf/230616-progress-report-nr8-EU-NATO.pdf

NATO & União Europeia (2018). Joint declaration on EU-NATO cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. *Conselho da União Europeia* https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf

NATO & União Europeia (2023). Joint declaration on EU-NATO cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. *NATO*. https://www.nato.int/cps/en/natohq/official_texts_210549.htm

Conselho da União Europeia (2018). Third progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017. https://www.consilium.europa.eu/media/35578/third-report-ue-nato-layout-en.pdf

NATO (2024). Ninth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017. https://www.nato.int/nato_static_fl2014/assets/pdf/2024/6/pdf/240613-progress-report-nr9-EU-NATO.pdf

NATO & União Europeia (2016). Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. *Parlamento Europeu.* https://www.europarl.europa.eu/cmsdata/121580/20160708_160708-joint-NATO-EU-declaration.pdf

NATO (2016). NATO and the European Union enhance cyber defence cooperation. https://www.nato.int/cps/en/natohq/news_127836.htm

NATO (2024). Relations with the European Union. https://www.nato.int/cps/en/natohq/topics_49217.htm

Livros e artigos

Tikk, E., Kaska, K., & Vihul, L. (2010). Estonia 2007. Em *International cyber incidents: Legal considerations.* (pp.14-35). *Cooperative Cyber Defence Centre of Excellence (CCDCOE).* https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf

Healey, J., & Jordan, K. T. (2014). NATO's cyber capabilities: Yesterday, today, and tomorrow. *Atlantic Council*, pp. 1-9. https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf

Pfannenstiel, M., Cox, D. (2024). NATO's Cyber Era. *Army University Press*. *Military Review*. https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/NATOs-Cyber-Era-UA/

Ilves, L. K., Evans, T. J., Cilluffo, F. J. & Nadeau, A. (2016). European Union and NATO global cybersecurity challenges: A way forward. *Institute for National Strategic Security, National Defense University. PRISM, 6*(2), 126-141. https://www.jstor.org/stable/26470452

Lété, B., & Pernik, P. (2017). EU-NATO cybersecurity and defense cooperation. *The German Marshall Fund of the United States,* (38), 1-9. https://www.gmfus.org/sites/default/files/EU-NATO%20Cybersecurity%20and%20Defense%20Cooperation%20edit.pdf

Harun A. & Süvari, K. (2024). Unveiling Russia's secret weapon: cyber-electronic operations in hybrid warfare, *Defence Studies*, 1-16. https://doi.org/10.1080/14702436.2024.2421923

Roche, E., & Blaine, M. (2023). The Folly of Cyber War. *Journal of International Affairs*, 75(2), 131–144. https://www.jstor.org/stable/27231742

Barichella, A. (2022). Cyber Attacks in Russia's Hybrid War Against Ukraine and its ramifications for Europe, *Jacques Delors Institute*, 1-20. https://institutdelors.eu/wp-content/uploads/dlm_uploads/2022/09/PP281_The-cybersecurity-dimension-of-the-war-in-Ukraine_Barichella_EN.pdf

Hoffman, F. (2008). Hybrid warfare: The changing character of conflict. *Potomac Institute for Policy Studies*, 1-72. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Wither, J. K. (2016). Making Sense of Hybrid Warfare. *Connections*, *15*(2), 73–87. http://www.jstor.org/stable/26326441

Muradov, I. (2022). The Russian hybrid warfare: The cases of Ukraine and Georgia. *Defence Studies, 22*(2), 168–191. https://doi.org/10.1080/14702436.2022.2030714

Bankov, B. (2023). The decline of Russian hybrid warfare? Lessons from Ukraine. *Balkan Social Science Review, 22*(22), 319–342. https://doi.org/10.46763/BSSR232222319b

Kolodii, R. (2024). The pedagogy of cyber-war: Explaining Ukraine's resilience against Russian cyber-aggression. *Defense & Security Analysis, 40*(2), 270-291. https://doi.org/10.1080/14751798.2024.2326313

Antoniuk, D. (2022). DDoS attacks hit websites of Ukraine's state banks, defense ministry, and armed forces. *The Record.* https://therecord.media/ddos-attacks-hit-websites-of-ukraines-state-banks-defense-ministry-and-armed-forces

Brumfield, C. (2022). Russia-linked cyberattacks on Ukraine: A timeline. *CSO Online*. https://www.csoonline.com/article/571865/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html

Przetacznik, J., & Tarpova, S. (2022). Russia's war on Ukraine: Timeline of cyber-attacks (EPRS Briefing PE 733.549). *European Parliamentary Research Service.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

Berger, M. (2022). 400,000 Ukrainians flee to European countries, including some that previously spurned refugees. *The Washington Post*. https://www.washingtonpost.com/world/2022/02/26/europe-welcomes-refugees-ukraine-russia/

CyberPeace Institute. (n.d.). Attack details. *CyberConflicts.* https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details

Marques, J. R. M. (2023). NATO's Adaptation to Hybrid Warfare and the Legal Challenges. *Nova School of Law.* http://hdl.handle.net/10362/159057

Waxman, M. C. (2011). Cyber Attacks as "Force" Under UN Charter Article 2(4). *International Law Studies*, 87(4), 43–57. https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1882&context=faculty_scholarship

Titiriga, R. (2011). Cyber-Attacks and International Law of Armed Conflicts: A 'Jus Ad Bellum' Perspective. *SSRN*. https://doi.org/10.2139/ssrn.1946470

Spáčil, J. (2022). Cyber operations against critical financial infrastructure: A non-destructive armed attack? *International and Comparative Law Review, 22*(2), 27–42. https://doi.org/10.2478/iclr-2022-0013

Leng, Y. (2023). When can cyberattack constitute use of force: A case study of cyberattack in the Russia-Ukraine conflict. *Proceedings of the 4th International Conference on Educational Innovation and Philosophical Inquiries*, 2023, 1249. https://doi.org/10.54254/2753-7048/17/20231249

Theohary, C. A. (2024). Use of Force in Cyberspace. *Congressional Research Service*. https://www.congress.gov/crs-product/IF11995

Burkadze, K. (2018). A shift in NATO's Article 5 in the cyber era. *The Fletcher Forum of World Affairs, 42*(2), 215–226. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/forwa42&id=344&men_tab=srchresults

Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law, 37*, 885–937. https://ssrn.com/abstract=1603800

Khalil, A., Bitar, M., & Raj, S. A. K. (2024). A new era of armed conflict: The role of state and non-state actors in cyber warfare with special reference to Russia-Ukraine war. *TalTech Journal of European Studies, 14*(2), 49–72. https://doi.org/10.2478/bjes-2024-0016

Schmitt, M. (2022). Expert backgrounder: NATO response options to potential Russia cyber-attacks. *Just Security.* https://www.justsecurity.org/80347/expert-backgrounder-nato-response-options-to-potential-russia-cyber-attacks/

CCD COE (s.d.). Prohibition of intervention. *Cyber Law*. https://cyberlaw.ccdcoe.org/wiki/Prohibition_of_intervention#cite_note-8

Tsagourias, N. (2019). Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace. *EJIL: Talk! Blog do European Journal of International Law.* https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/

Ossoff, W. (2021). Hacking the domaine réservé: The rule of non-intervention and political interference in cyberspace. *Harvard International Law Journal*, 62(1). https://journals.law.harvard.edu/ilj/2021/04/hacking-the-domaine-reserve-the-rule-of-non-intervention-and-political-interference-in-cyberspace/

Hakala, J., Melnychuk, J., (2021). Russia's Strategy in Cyberspace (2021). Riga: NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/pdfjs/?file=/publications/download/Nato-Cyber-Report_15-06-2021.pdf?zoom=page-fit

Ducaru, S., Caradaică, M., & Costea, A. M. (2024). Can a cyberattack become an act of war? European and trans-Atlantic perspectives. *Romanian Journal of European Affairs, 24*(1), 1-XX. http://rjea.ier.gov.ro/wp-content/uploads/2024/06/Art.-1_Can-a-Cyberattack-Become-an-Act-of-War_Ducaru-et-al._2024_final.pdf

Finlay, L., & Payne, C. (2019). The attribution problem and cyber armed attacks. *American Journal of International Law, 113*, 202–206. https://doi.org/10.1017/aju.2019.35

Tsagourias, N., & Farrell, M. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. *The European Journal of International Law*, 31(3), 941-967. https://doi.org/10.1093/ejil/chaa057

Davis, J. K. (2022). Developing applicable standards of proof for peacetime cyber attribution. *Tallinn Papers*. https://ccdcoe.org/uploads/2022/03/Jeremy-K.-Davis-Standards_of_Attribution.pdf

Blinken, A. J. (2022). Attribution of Russia's malicious cyber activity against Ukraine. *U.S. Department of State*. https://2021-2025.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/

Tran, D. (2018). The law of attribution: Rules for attributing the source of a cyber-attack. *Yale Journal on Law & Technology, 20*(2), 376. https://yjolt.org/law-attribution-rules-attributing-source-cyber-attack

Botek, A. (2019). European Union establishes a sanction regime for cyber-attacks. *NATO Cooperative Cyber Defence Centre of Excellence*. https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/

Schmitt, M. N. (2019). The North Atlantic Alliance and Collective Defense at 70: Confession and Response Revisited. *Emory International Law Review, 34*(0), 85–120. https://scholarlycommons.law.emory.edu/eilr/vol34/iss0/7/

Bajarūnas, E. (2025, February 11). Using NATO's Article 5 against hybrid attacks. *Center for European Policy Analysis*. https://cepa.org/article/using-natos-article-5-against-hybrid-attacks/

Klipstein, M., & Japaridze, T. (2022, May 16). Collective cyber defense and attack: NATO's Article 5 after the Ukraine conflict. *European Leadership Network*. https://europeanleadershipnetwork.org/commentary/collective-cyber-defence-and-attack-natos-article-5-after-the-ukraine-conflict/

Prucková, M. (2022). Cyber attacks and Article 5: A note on a blurry but consistent position of NATO. *NATO Cooperative Cyber Defence Centre of Excellence*. https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/

Leshchuk, S. (2019). Cyber conflict in light of Article 5 of the North Atlantic Treaty: Cyberkonflikt w świetle artykułu 5 Traktatu Północnoatlantyckiego. *Historical and Political Problems of the Modern World, 39*, 12–20. https://doi.org/10.31861/mhpi2019.39.12-20

EEAS. (2022). Article 42(7) TEU - The EU's mutual assistance clause. *European Union*.https://www.eeas.europa.eu/sites/default/files/documents/Article%2042%287%29%20TEU%20-The%20EU%27s%20mutual%20assistance%20clause.pdf

Clapp, S., & Verhelst, A. (2022). A comparative analysis of Article 5 of the Washington Treaty (NATO) and Article 42(7) TEU (EU). *European Parliament*. https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/739250/EPRS_ATA(2022)739250_EN.pdf

Deen, B., Zandee, D., & Stoetman, A. (2022). Uncharted and uncomfortable in European defence: The EU's mutual assistance clause of Article 42(7). *Clingendael Institute*. https://www.clingendael.org/sites/default/files/2022-01/uncharted-and-uncomfortable.pdf

NATO Cooperative Cyber Defence Centre of Excellence. (s.d.). Self-defence. https://cyberlaw.ccdcoe.org/wiki/Self-defence

Burgess, M. (2022, February 27). Ukraine's volunteer 'IT army' is hacking in uncharted territory. *Wired*. https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/

Bethlehem, D. (2019). Evaluating the imminence of a cyber attack for purposes of anticipatory self-defense. *Columbia Law Review*. https://columbialawreview.org/content/evaluating-the-imminence-of-a-cyber-attack-for-purposes-of-anticipatory-self-defense/

Schmitt (2022). Russian cyber operations and Ukraine: The legal framework. *Lieber Institute West Point*. https://lieber.westpoint.edu/russian-cyber-operations-ukraine-legal-framework/

NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *Attribution*. https://cyberlaw.ccdcoe.org/wiki/Attribution

Trinberg, L. (s.d.). EU–NATO Relations: Hand in hand against cyberattacks. *NATO Cooperative Cyber Defence Centre of Excellence*. https://ccdcoe.org/incyder-articles/eu-nato-relations-hand-in-hand-against-cyberattacks/

Lindstrom, G. (dir.) (2019). The EU and NATO. The essential partners. *European Union Institute for Security Studies (EUISS)*. http://publications.europa.eu/resource/cellar/08e9e07b-cd30-11e9-992f-01aa75ed71a1.0001.01/DOC_1

Complex Discovery (2024). Tallinn Mechanism: A year of cybersecurity collaboration in defense of Ukraine. https://complexdiscovery.com/tallinn-mechanism-a-year-of-cybersecurity-collaboration-in-defense-of-ukraine/

Geri, M., (2025). A new strategic responsibility for the EU: EU-NATO cooperation against hybrid warfare from Russia. *Journal of Politics and Development* (2025*), 15*(1), 6-19.

Spatafora, G. (2024). Keeping EU-NATO cooperation alive under Trump 2.0. *European Union Institute for Security Studies.* https://www.iss.europa.eu/publications/commentary/keeping-eu-nato-cooperation-alive-under-trump-20

Parlamento Europeu (2022). The EU and the strategic implications of hybrid threats: A comprehensive approach. *European Parliamentary Research Service.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733589/EPRS_BRI(2022)733589_EN.pdf

Gray, A., & Bayer, L. (2025). EU proposes joint defence push amid Russia fears and US worries. *Reuters*. https://www.reuters.com/business/aerospace-defense/eu-proposes-joint-defence-push-amid-russia-fears-us-worries-2025-03-19/

Vecchio, A. (2025). The White Paper within the institutional constraints: The EU short-term defence policy "Readiness 2030". *Verfassungsblog*. https://verfassungsblog.de/the-white-paper-readines-2030/

Agência Lusa (2025). Países da NATO preparam-se para compromisso de 3,5% do PIB em defesa na cimeira de Haia. *Observador*. https://observador.pt/2025/04/02/paises-da-nato-preparam-se-para-compromisso-de-35-do-pib-em-defesa-na-cimeira-de-haia/