UNIVERSIDADE FERNANDO PESSOA

A GUERRA CIBERNÉTICA E A SEGURANÇA INTERNACIONAL

[Cybernetic War and International Security]

Projeto de Graduação

Licenciatura em Ciência Política e Relações Internacionais

Catarina Silva Carneiro

Orientador:

Dra. Ana Campina

Junho, 2025

Catarina Silva Carneiro

PROJETO DE GRADUAÇÃO

Licenciatura em Ciência Política e Relações Internacionais

Assinatura da/o discente: Catarina Silva Carneiro

Trabalho apresentado à Universidade Fernando Pessoa como parte dos requisitos para obtenção do grau de licenciado, sob a orientação da Professora Ana Campina.

Universidade Fernando Pessoa

Porto, Portugal, 2025

Agradecimentos:

A conclusão deste projeto de graduação representa não apenas o encerramento de uma etapa académica, mas também a concretização de um percurso pessoal repleto de desafios, aprendizagens e conquistas.

Agradeço, em primeiro lugar, aos meus professores, pelo conhecimento transmitido, pelo rigor científico e pela constante motivação para pensar criticamente os temas da atualidade, especialmente no domínio da segurança internacional. A todos os docentes do curso de Ciência Política e Relações Internacionais, o meu profundo reconhecimento.

À minha família, que sempre me apoiou incondicionalmente: aos meus pais e avós, que com carinho, sacrifício e incentivo me proporcionaram as bases para alcançar este momento, deixo o mais sincero agradecimento. A cada gesto de apoio e compreensão, mesmo nos momentos mais exigentes, o meu eterno obrigado.

Dirijo ainda uma palavra especial de gratidão à Professora Ana Campina, cuja dedicação, exigência e inspiração foram fundamentais para o meu crescimento académico e pessoal. A sua orientação e confiança deixaram uma marca profunda neste trabalho e ao longo de todo o meu percurso universitário.

A todos os que, de forma direta ou indireta, contribuíram para este projeto, fica o meu mais sincero obrigado.

Resumo

A análise do fenómeno da Guerra Cibernética no século XXI é um estudo imperioso, sobretudo considerando a sua crescente influência na segurança internacional, na soberania dos Estados e na Ordem Jurídica global. Partindo de um enquadramento teórico e histórico, esta investigação parte da distinção da Guerra Cibernética de outras ameaças digitais, como o cibercrime e o ciberterrorismo. Assim, é possível expor o seu carácter político-estratégico e o seu envolvimento de atores estatais e não estatais. Este estudo discute casos paradigmáticos, tais como, os ataques a *Stuxnet* (EUA/Israel vs Irão), à Estónia (2007), à infraestrutura da Ucrânia, durante o conflito com a Rússia, e a possível interferência russa nas eleições norte-americanas. Estas análises evidenciam como as ações cibernéticas se tornaram instrumentos de poder e dissuasão, capazes de produzir efeitos concretos sem recorrer à força física tradicional. Os desafios jurídicos associados à Guerra Cibernética, como a dificuldade de atribuir responsabilidades, a ausência de tratados vinculativos e as limitações do Direito Internacional Humanitário no Ciberespaço são temáticas fulcrais nesta investigação. Conclui-se a necessidade de fortalecer a cooperação internacional, desenvolver normas jurídicas capazes de dar resposta às necessidades da conjuntura atual, assim como, promover o investimento em diplomacia digital como resposta à intensificação dos conflitos digitais no sistema internacional contemporâneo.

Palavras-chave: Guerra Cibernética; Segurança Internacional; Cibercrime; Ciberterrorismo; Ciberespaço;

Abstract

This Graduation Project examines the phenomenon of cyber warfare in the 21st century, focusing on its growing influence on international security, state sovereignty, and the global legal order. Beginning with a theoretical and historical framework, the study distinguishes cyber warfare from other digital threats such as cybercrime and cyberterrorism, highlighting its political-strategic nature and the involvement of both state and non-state actors.

The work explores key case studies such as the Stuxnet attack (U.S./Israel vs. Iran), the 2007 cyberattack on Estonia, infrastructure attacks during the Russia-Ukraine conflict, and Russian interference in U.S. elections. These examples demonstrate how cyber operations have become instruments of power and deterrence, capable of producing concrete effects without the use of traditional physical force.

The research emphasizes the legal challenges posed by cyber warfare, including difficulties in attribution, the absence of binding treaties, and the limitations of International Humanitarian Law in cyberspace. The thesis concludes by highlighting the urgency of strengthening international cooperation, developing clear legal norms, and investing in digital diplomacy as a response to the intensifying digital conflicts in today's international system.

Keywords: Cyber Warfare; International Security; Cybercrime; Cyberterrorism; Cyberspace;

Índice

Lista de Figuras:

Lista de Gráficos

Gráfico 2: Distribuição percentual dos principais tipos de ataques cibernéticos no mundo em 2024. *Botnets* e *Infostealers* representam a maioria, seguidos por ameaças financeiras e *ransomware*

Lista de Siglas:

USCYBERCOM- *U.S. Cyber Command*

NSA- Agência de Segurança Nacional dos EUA

DDoS- Negação de Serviço Distribuída

EUA- Estados Unidos da América

NATO- Organização do Tratado do Atlântico Norte

PLCs- Controladores Lógicos Programáveis

CCDCOE- Centro de Excelência de Defesa Cibernética Cooperativa da NATO

GRU- Serviço de Inteligência Militar Russo

IRA- Agência de Pesquisa da Internet

DHS- Departamento de Segurança Interna dos EUA

CISA-Agência de Cibersegurança e Infraestruturas dos EUA

DIH- Direito Internacional Humanitário

CICV- Comitê Internacional da Cruz Vermelha

GGE- Grupo de Peritos Governamentais da ONU

OEWG- *Open-Ended Working Group*

NHS- Serviço Nacional de Saúde

UN GGE- Grupo de Peritos Governamentais das Nações Unidas

UIT- Programa Global de Cibercrime da União Internacional de Telecomunicações

GFCE- Global Forum on *Cyber Expertise*

Introdução

O aumento do uso e interação das tecnologias na vida cotidiana, atividades governamentais, económicas e sociais modificou o panorama geopolítico global, criando uma nova era marcada pelo fenómeno das guerras cibernéticas.

Neste projeto de graduação, analisa-se a interseção da cibernética, o digital e a segurança internacional, que tem sido um dos principais desafios das relações internacionais. O uso de ferramentais digitais para a elaboração de ataques, espionagem ou roubo de infraestruturas ou informações fundamentais, não só redefine as diferentes estratégias de defesa e ataque, mas também apresenta a necessidade de repensar em novos conceitos e formas de integridade territorial e soberania.

Num cenário onde as fronteiras físicas perdem relevância, com a disseminação da Internet e a globalização digital, o que permite aos agentes estatais e não estatais explorarem o ambiente digital e tirar partido dele seja na área da política, social, económica ou até militar.

Diante desta situação, é necessária a criação de normas, leis, diretrizes que permitam organizar e normatizar as relações sociais, económicas e políticas, além de serem essenciais também para a adaptação de estruturas e estratégias quando apresentados novos desafios, como é o caso na revolução tecnológica e crescente interconetividade digital.

Ao longo deste trabalho, pretende-se caraterizar e analisar o fenómeno deste tipo de guerra, recorrendo ao seu desenvolvimento histórico e evolução e diferenças das técnicas de ataque e defesa no espaço cibernético, alem disso, refletir sobre o panorama normativo internacional, apontando lacunas e avaliando os principais instrumentos jurídicos que regem a atuação de atores estatais e não estatais no espaço digital.

Serão também apresentados casos paradigmáticos de operações cibernéticas ofensivas e defensivas, com o objetivo de as compreender. Paralelamente, será também analisada a eficácia das estratégias de cooperação multilateral e das iniciativas da diplomacia digital, apontando desafios e oportunidades para a confiança entre Estados.

Capítulo 1- Enquadramento conceitual e histórico

O crescimento da digitalização nas sociedades atuais, desenvolveu um novo domínio estratégico denominado Ciberespaço. Este tornou-se um importante condutor para a Segurança Internacional atual, originando um novo conceito que é o caso da Guerra Cibernética. Esta recente forma de conflito, apesar de intocável e geralmente invisível, apresenta uma ameaça verdadeira e cada vez maior à soberania dos Estados e países, ao equilíbrio mundial e sobretudo, à segurança do povo.

1.1 O que é uma Guerra Cibernética?

A Guerra Cibernética pode ser determinada como a utilização e organização de capacidades digitais com objetivos prejudiciais, normalmente por estados ou atores, procurando danificar, ou comprometer infraestruturas essenciais como: redes de comunicação, rede elétrica, transporte ou comunicações, instituições públicas, setores estratégicos, agências governamentais, infraestruturas públicas, pessoas.

Para alguns, a Guerra Cibernética é diferente dos demais tipos de ciberataques por abranger, muitas vezes, objetivos políticos e por ser inserida em estratégias militares mais extensas. Richard Clarke, como ex conselheiro de cibersegurança da Casa Branca reforça que a guerra cibernética engloba consequências semelhantes as de típicas operações militar.

1.2 Evolução das Guerras no Contexto Tecnológico

O desenvolvimento da guerra provoca, historicamente, o progresso das tecnologias fundamentais. Desde o tempo das guerras entre tribos padronizadas baseadas no uso da força física e da proximidade com o próprio, passando pela guerra automatizada na Revolução Industrial e claro, pela Guerra Nuclear do século XX, do qual, cada etapa tecnológica modificou fortemente o formato como os conflitos são impedidos ou criados.

No final do seculo XX e início do seculo XXI, com o surgimento da Revolução da Informação, iniciou-se uma nova fase: o domínio da Guerra digital. Nesta circunstância, o ciberespaço passou a ser visto como o “quinto domínio” da guerra, junto com o ar, terra, mar e espaço.

1.3 Diferenças entre Guerra Cibernética, Cibercrime e Ciberterrorismo

No cenário dos riscos atuais à Segurança Internacional, é importante classificar entre 3 tipologias fundamentais de agressões no ciberespaço: Guerra Cibernética, cibercrime e Ciberterrorismo. Apesar de partilharem o uso de técnicas digitais como forma de ataque, variam consideravelmente em fatores como: objetivos, resultados esperados, motivações e sujeitos que estão inseridos. A guerra cibernética relaciona-se com ações lideradas por estados ou agentes estatais com o propósito de prejudicar algumas das principais estruturas do adversário. Alguns destes atos, normalmente fazem parte de uma estratégia militar mais extensa, podendo acontecer em tempos de relativa paz. Como analisa Thomas Rid (2013), a guerra cibernética determina-se pela sua dependência a objetivos políticos e pela sua competência de causar feitos estratégicos reais, idênticos aos provocados por operações militares convencionais.

Por outro lado, o Cibercrime engloba atividades ilegais cometidas com fins financeiros ou lucrativos, levadas maioritariamente por atores não estatais, como hackers individuais, grupos organizados ou redes transacionais de crime. Os crimes mais comuns englobam roubo de dados pessoais, fraudes bancárias, sequestro de sistemas via *ransomware, Phishing e smishing*, engenharia social, burlas online, falsificação de identidade e invasão de contas privadas. Este tipo de ataques, raramente tencionam prejudicar estruturas estatais ou provocar danos ao governo, no entanto, podem prejudicar a estabilidade económica ou a confiança dos cidadãos nas instituições.

De acordo, com Singer e Friedman (2014), o cibercrime, independentemente, da sua alta frequência, não deve ser confundido com uma ação de guerra, pois necessita do espaço político e militar que caracteriza os conflitos entre estados no espaço digital.

Por outro lado, o Ciberterrorismo, encontra-se em uma zona central. Refere-se à utilização da tecnologia da informação geralmente, por grupos terroristas não estatais para ameaçar ou realizar crimes ou ataques contra os cidadãos e instituições, com a finalidade de desenvolver objetivos de caracter ideológico, político ou religioso. Nesses casos, os ataques podem revelar se na forma de propaganda digital, ameaças virtuais, desfiguração de sites governamentais ou tentativas de sabotagem de infraestruturas.

Apesar de o impacto físico do Ciberterrorismo até á data seja limitado, este potencializa uma grande capacidade para desestabilizar sociedades ou provocar a sensação de medo e receio.

Da mesma forma, Kello (2027), afirma que a ameaça do Ciberterrorismo assenta principalmente no seu efeito psicológico e simbólico, e não tanto na sua eficácia agressiva direta.

Para lá das diferenças conceituais, existem repercussões práticas e jurídicas relevantes: A Guerra Cibernética está submetida ao debate sobre as normas impostas pelo Direito Internacional Humanitário, enquanto, o Cibercrime é tratado tanto pelas leis penais nacionais, como também pelas convenções internacionais especificas, como é o caso, da Convenção de Budapeste sobre o Cibercrime (2001). Já o Ciberterrorismo, por sua vez, apresenta desafios legais mais elaborados, devido à dificuldade de provar e definir as intenções dos terroristas no espaço digital.

Concluindo, é relevante notar que, na prática, essas 3 categorias podem nem sempre ser reciprocamente especificas. Por vezes, agentes estatais, podem recorrer a formas ilícitas para alcançar certos objetivos estratégicos (por exemplo espionagem ou extorsão), ou apoiar grupos não governamentais para ações que possibilitam uma negação verosímil. Essa interdependência, traduz se num Ciberespaço como um campo de batalha uniforme, incerto e extremamente político.

1.4 Principais atores estatais e não estatais

A guerra cibernética sendo um evento estratégico global, abrange uma variada série de atores estatais e não estatais que atuam no Ciberespaço com estímulos, habilidades e níveis de sofisticação diversos. O reconhecimento e estudo desses atores são essenciais para perceber a complexidade que as ameaças digitais atuais provocam e também como os desafios que elas apresentam à Segurança Internacional e à criação de políticas de defesa nacional.

Dentro dos atores estatais, distinguem-se potências com elevadas capacidades digitais tanto ofensivas como defensivas, que englobam os Estados Unidos, a Rússia, a China, o Irão e a Coreia do Norte. Estes Estados, são os que tem mantido um investimento grande no desenvolvimento de estruturas e instituições especializadas, como é o caso dos comandos cibernéticos, departamentos de inteligência digital e unidades de guerra eletrónica, com o objetivo de consolidar a sua influência estratégica e afastar adversários.

Os Estados Unidos, por exemplo, foram essenciais na institucionalização da guerra cibernética com a criação do USCYBERCOM em 2009, operando em articulação com a

NSA, tendo como principal missão realizar operações defensivas e ofensivas em tempos de paz, crise ou guerra (Libicki, 2012). Para além disso, os EUA têm sido denunciados por orientarem ataques elaborados, como o caso do *Stuxnet*, desenvolvido em parceria com Israel para sabotar o programa nuclear iraniano.

A Rússia, por outro lado, tem se distinguido pela utilização da guerra cibernética como um instrumento de guerra híbrida, ou seja, junta ataques digitais, desinformação e operações psicológicas. Alguns grupos ligados ao governo russo, como o APT28 (Fancy Bear) e o *Sandworm*, foram implicados em ataques contra a Ucrânia, Estónia e até mesmo nas eleições presidenciais dos EUA em 2016 (Nocetti, 2015). O modelo russo adota a terceirização para grupos semi-independentes, concedendo ao Estado, a possibilidade de negar o seu envolvimento.

A China, por outro lado, apresenta-se como outro ator central, sobretudo no campo da espionagem cibernética e do roubo de propriedade intelectual. As operações que são atribuídas ao grupo APT10, por sua vez, ligadas ao Ministério Da Segurança do Estado Chinês, mostram a dimensão das suas competências, habitualmente dirigidas a setores estratégicos como a defesa tecnológica e energética. Apesar de, a China afirmar que mantem uma postura defensiva no ciberespaço, a sua atividade tem levantado alguma inquietação no Ocidente (Segal, 2016).

O Irão e a Coreia do Norte também surgiram como potências cibernéticas regionais. O Irão tem trabalhado em desenvolver capacidades relevantes desde o ataque de *Stunext,* operando contra alvos sauditas, israelitas e norte-americanos. No caso da Coreia do Norte, é notória por ataques como o *WannaCry*, que impactou todo o mundo e por operações de cibercrime dirigidas a produzir recursos financeiros para sustentar o regime (Hultquist, 2019).

No que diz respeito a atores não estatais, distinguem-se os grupos hacktivistas, como o *Anonymous*, organizações de crime cibernético e empresas privadas de segurança digital que, eventualmente, operam como mercenários cibernéticos. Esses atores atuam com diferentes motivações- sendo estas muitas vezes, ideológicas, políticas ou até financeiras- geralmente são instrumentalizadas por Estados para desempenhar ataques sem deixar rastos diretos de envolvimento oficial.

O *Anonnymous*, por exemplo, opera segundo princípios de liberdade de informação e justiça social, concretizando ataques de DDoS, exposição de dados e campanhas de não cumprimento digital. Durante a guerra entre a Rússia e a Ucrânia, o grupo manifestou "guerra cibernética" à Federação Russa, ao invadir sites governamentais, redes de televisão estatais e bancos (Coleman, 2014).

Outro caso de ator não estatal considerável é a implicação de empresas privadas na venda de ferramentas de espionagem digital, como é o exemplo da empresa israelita NSO *Group*, que criou o software Pegasus, ao utilizar para monitorizar ativistas, líderes políticos e jornalistas em variados países. Esse evento demonstra a progressiva mercantilização da guerra cibernética, em que a alta tecnologia pode ser obtida por governos autoritários, milícias ou grupos com interesses próprios.

Também, grupos criminosos cibernéticos organizados, por vezes, atuam de forma transacional, o que apresenta uma ameaça relevante, não só em termos financeiros, como também pela hipótese de servirem como instrumentos de *proxy warfare* para regimes que procuram esconder a sua autoria em ataques de grande escala.

Em resumo, o cenário atual da Guerra Cibernética é caracterizada pela diferente autonomia e sofisticação por parte dos atores. Essa multiplicidade resulta numa extrema dificuldade em atribuir responsabilidades de forma inequívoca, dificulta a elaboração de respostas em concordância com o plano internacional e provoca os mecanismos típicos de segurança coletiva e dissuasão estratégica.

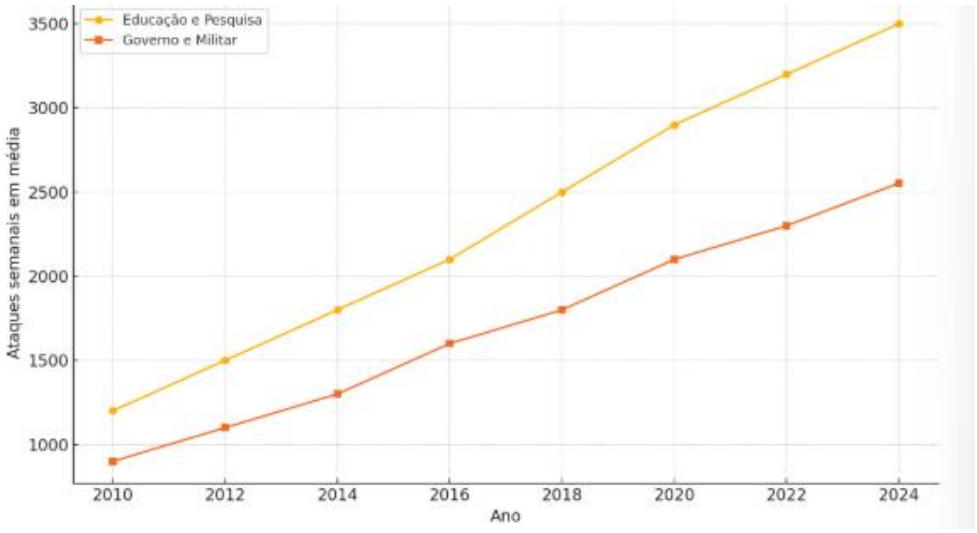
2. Guerra Cibernética no Século XXI

2.1 Impacto na Segurança Nacional e Global (Infraestruturas, Críticas, Governos e Militares)

No século XXI, a Guerra Cibernética tornou se uma área central da segurança internacional. Contrariamente, às formas comuns de conflito, a guerra digital caracteriza-se pela sua assimetria, ambiguidade jurídica, dificuldade de atribuição e pela capacidade de causar danos reais sem o uso da força física. As consequências dessa recene forma de conflito, influenciam diretamente a segurança global, internacional e nacional, particularmente as infraestruturas importantes, sistemas governamentais e estruturas militares.

Como se observa na Figura 1, os setores de Educação/Pesquisa e Governo/Militar têm sido os mais visados por ciberataques na última década. Estes dados ilustram a crescente vulnerabilidade de áreas estratégicas para o funcionamento dos Estados modernos, aumentando a preocupação com a segurança nacional e global.

Gráfico 1



Fonte: Adaptado *de Check Point Research*, 2024

No caso das infraestruturas críticas, como é o exemplo das redes elétricas, de água, saúde, transportes, telecomunicações, e serviços financeiros, fazem deste os alvos principais para ataques cibernéticos. Estes sistemas, que progressivamente, são mais informáticos, eletrificados, modernizados e interconectados, são extremamente vulneráveis a *malwares*, *ransomware* e ataques DDoS. O colapso desses serviços, pode provocar instabilidade social, quebra de serviços essenciais e pesadas perdas económicas. Como título exemplificativo disso, foi o ataque á rede elétrica da Ucrânia em 2015, atribuído e responsabilizado pelo grupo *Sandworn*, que lesou milhares de pessoas ao deixá-las sem energia em pleno inverno gelado (Lee, Assante & Conway, 2016).

Na esfera governamental, ataques tem sido concebido para fins de espionagem, manipulação de dados e sabotagem institucional. Agências públicas de vários países e estados, tem sido alvo de atentados na tentativa de obter dados significativos, como registos populacionais, dados fiscais, informações de inteligência e comunicações diplomáticas.

Um caso representativo, foi o ataque ao Escritório de Gestão Pessoal dos EUA (OPM) em 2015, que divulgou os dados de cerca de 21 milhões de agentes, sendo este ataque atribuído maioritariamente a agentes chineses (Nakashima, 2015).

No âmbito militar, os ataques digitais cada vez mais, são planeados e manobrados com estratégias de dissuasão. Os comandos cibernéticos, por sua vez, passaram a ser inseridos nas forças armadas, sendo efetuadas missões ofensivas e defensivas.

A noção de "ciberdominio", foi oficializado em países como EUA e a NATO, admitindo o Ciberespaço como um espaço operacional à semelhança do mar, terra, ar e espaço. Esse reconhecimento acarreta que um ataque cibernético significativo contra alguém da NATO, pode, em teoria, invocar o Artigo 5 do Tratado de Washington, o que prevê uma defesa coletiva.

Paralelamente, a Guerra Cibernética pressupões ameaças indiretas á segurança internacional, ao corroer a confiança entre Estados, aumentar o risco de escaladas acidentais e por sua vez, expor tratados sob controlo de armamento. Estes ataques sendo opacos e ambíguos, dificultam a definição correta de "ato de guerra", e consequentemente, provocam pressão sobre o direito humanitário e os mecanismos multilaterais de regulação.

Por fim, o impacto global da guerra cibernética também se observa na economia e na opinião pública. Ciberataques pesados podem danificar cadeiras globais de suprimento, bolsas de valores e grandes corporação, como nos mostrou o caso do ataque NotPetya (2017), que provocou prejuízos de bilhões de dólares em empresas de logística, petróleo, farmacêuticas e também no setor marítimo global (Greenberg, 2018). A guerra cibernética, como tal, ultrapassa o campo de batalha "comum", ao afetar diretamente a segurança cotidiana de sociedades inteiras.

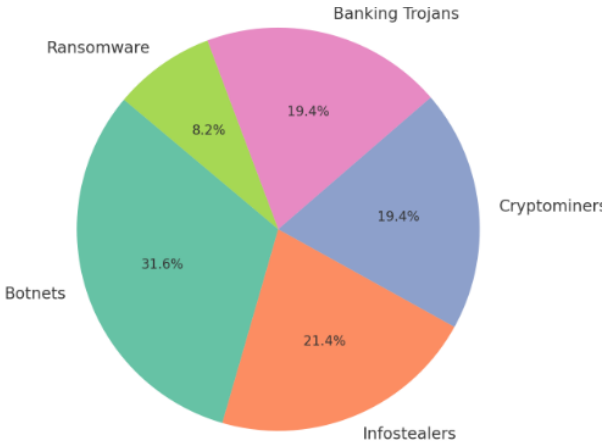
2.2 Desafios para a Soberania e a Defesa Nacional

A guerra cibernética estabelece uma reorganização intensa das noções tradicionais de soberania e defesa nacional. Se pensarmos na história, a soberania estava profundamente conectada á proteção das fronteiras físicas e ao monopólio do uso legitimo da força dentro de um território (Weber, 1919), no ambiente digital, essas fronteiras transformam-se difusas, porosas e desmaterializadas, originando novos locais de vulnerabilidade que provocam a autoridade do Estado. O primeiro grande desafio foca-se na dificuldade de

atribuição de ataques. Ao oposto de um ataque armado convencional, um ataque digital pode ser levado por atores estatais ou não estatais, escondendo por diversos níveis de *proxies* e camuflando através de técnicas de *spoofing* ou de servidores intermediários em jurisdições terceiras. Essa incerteza técnica e legal compromete a capacidade de reação dos Estados, dado que, uma resposta mal incumbida, pode transpor diplomaticamente o conflito e gerar repercussões internacionais graves (Rid & Buchanan, 2015).

A distribuição dos tipos de ataques, apresentada no Gráfico 2, evidencia a complexidade e diversidade das ameaças digitais enfrentadas pelos Estados. *Botnets*, infostealers e *ransomware* destacam-se como as ferramentas mais utilizadas, dificultando a proteção integral das infraestruturas críticas e exigindo estratégias sofisticadas de defesa.

Gráfico 2



Fonte: Adaptado de *Check Point Research*, 2024

Em segundo lugar, os Estados defrontam-se com limitações legais e institucionais para retribuir a ataques cibernéticos dentro de um espaço de legitima defesa. O direito internacional, nomeadamente a Carta das Nações Unidas, não é claro sobre o que engloba um "uso da força" no ciberespaço. Isso conduz à criação de uma "zona cinzenta" entre atos hostis, sabotagem e espionagem digital, na qual os Estados têm dificuldades em identificar, classificar e responder da mesma proporção às ameaças (Schmitt, 2013).

Ademais, o crescimento da dependência tecnológica e da interconexão global intensifica o risco de ataques cibernéticos e a hipótese de causarem danos secundários que ultrapassam as fronteiras do Estado-alvo. *Software* maliciosos podem divulgar-se de

forma não intencional para sistemas civis e infraestruturas essenciais de países terceiros, como ocorreu com vírus *NotPetya*, que teve como alvo a Ucrânia, mas influenciou empresas na Europa, Ásia e América (Greenberg, 2018). Da mesma forma, isso cria responsabilidades transacionais que incitam a soberania estatal clássica.

Da perspetiva da defesa nacional, os estados têm aderido a estratégias de ciberdefesa ativa, que contém a deteção antecipada de ameaças, operações de dissuasão e até ações ofensivas preventivas no ciberespaço. Todavia, esse tipo de comportamento, levanta preocupações éticas e jurídicas, particularmente, no que diz respeito ao princípio da proporcionalidade e da distinção no uso da força, conforme previsto no Direito Internacional Humanitário.

Além disso, a proteção contra ameaças cibernéticas exige uma cooperação cada vez maior entre setores públicos e privados, já que grande parte das infraestruturas críticas está sobre o controlo empresarial. Essa dependência coletiva porta um novo desafio à soberania: o Estado já não detém todo o controlo exclusivo sobre os meios de defesa da sua própria empresa digital.

Por fim, há questão da assimetria de capacidades cibernéticas. Estados pequenos ou em desenvolvimento enfrentam dificuldades acrescidas para criar estruturas adequadas de defesa e resposta, passando a ser alvos vulneráveis de potencias com orçamentos cibernéticos poderosos. Isso realça, o desequilíbrio no sistema internacional e pode simbolizar uma nova forma de imperialismo tecnológico, onde a soberania de países com menor capacidade é comprometida sem ser submetida à violência.

2.3 Ataque Stunext (EUA/Israel vs Irão)

O ataque *Stuxnet,* descoberto em 2010, apresenta um divisor de águas na história da Guerra Cibernética. Pela primeira vez na história em que um *malware* digital provocou danos físicos significativos a uma infraestrutura essencial, o que mostrou que operações cibernéticas podiam ter, por vezes, efeitos parecidos aos de um ataque militar típico, sem a necessidade de tropas ou armamento tradicional.

O *Stuxnet* foi um verme altamente desenvolvido, projetado para se infiltrar no sistema de controlo industrial da fábrica de enriquecimento do urânio em Natanz, no Irão.

O objetivo era sabotar o programa nuclear iraniano, provocando um atraso no enriquecimento de urânio sem que os trabalhadores da instalação percebessem. O código do *malware* procurava, especificamente, os PLCs da Siemens usados para regular a velocidade das centrifugas. O *Stuxnet* fazia com que a velocidade delas aumentasse drasticamente, resultando em destruição ou degradação, enquanto, simultaneamente o ocultava dos operários (Zetter, 2014).

O ataque foi maioritariamente atribuído aos EUA e Israel, numa operação realizada entre ambos supostamente denominada de "Operação Jogos Olímpicos", revelada em investigações jornalísticas e por ex-funcionarios do governo norte-americano (Sanger, 2012). Apesar de, nunca ter sido oficialmente demandado, as provas técnicas, como o nível de sofisticação do código, a segmentação geográfica e os recursos utilizados, indicam o envolvimento dos estares estatais de alto nível.

O *Stuxnet* foi espalhado via *pen drives*, contornando *firewalls* e desconexões físicas, e foi construído para atuar de forma quase indetetável, ligando-se apenas quando identificado especificamente o ambiente dos sistemas industriais iranianos. No entanto, o *malware* acabou por se disseminar inadequadamente para computadores fora do Irão, revelando a sua existência ao público e especialistas de segurança cibernética de todo o mundo.

Este episódio, denunciou o início do uso do Ciberespaço como campo de batalha ofensivo em termos de paz, alterando o que é considerado um "ato de guerra". O *Stuxnet* mostrou que ataques digitais podem ser extremamente precisos, não letais em termos de capital humano, mas avassaladores em termos estratégicos, levantando questões jurídicas e éticas sobre o uso legitimo da força no ciberespaço.

Além disso, o ataque permitiu abrir precedentes: vários países e estados passaram a invadir em capacidade ofensiva cibernética, e o uso de armas digitais passou a ser considerado como uma parte de estratégia militar convencional. Após isso, as tensões cibernéticas entre o Irão, EUA, Israel e outros países aumentaram, levando a uma real corrida ao armamento digital.

2.4 Ataque à Infraestrutura da Estónia (2007)

Em abril e maio de 2007, uma das sociedades mais digitalizadas do mundo, na Estónia, ocorreu um ataque cibernético coordenado massivo, que afetou o país na sua totalidade.

Este foi considerado o primeiro caso de ciberataque nacional de grande escala, o momento evidenciou como o Ciberespaço podia ser usado para destabilizar um Estado moderno, sem o uso de recursos extra como o armamento típico.

Os ataques realizaram-se no âmbito de uma crise diplomática entre a Estónia e a Rússia, depois da decisão do governo estoniano sobre a remoção de uma estatua soviética, O Soldado de Bronze, de Tallinn, algo que foi entendido como uma afronta pela comunidade russa local pelas autoridades de Kremlin. Em retaliação, foi lançada uma serie de ataques DDoS contra os principais websites e redes do país.

Figura 1

Alvos do ataque:	**Características do ataque:**
Serviços governamentais e do parlamento	Coordenado, prolongado e com múltiplos vetores de ataque
Sistemas bancários	Utilizou *botnets* globais
Empresas de comunicação e meios de imprensa	Investigações apontaram para grupos nacionalistas russos, com indícios de apoio tático ou encorajamento estatal
Infraestruturas de internet	

Fonte: criação da autora – Catarina Silva

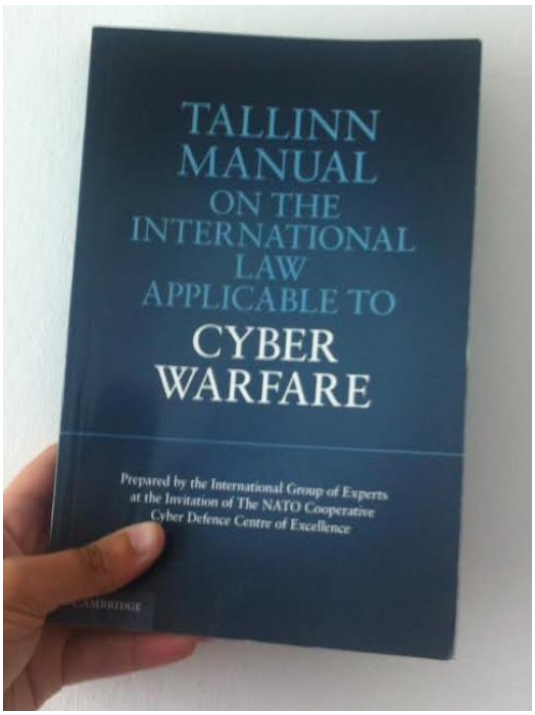
Neste caso, foi possível revelar a fragilidade das democracias digitais, mesmo quando inseridos em tempos de paz e fez com que questões relevantes sobre a preparação dos Estados atuais para lidar com guerras não convencionais. A Estónia, sendo dependente de tecnologias eletrónicas para a sua própria governança, saúde, finanças e educação, acabou por tornar-se vulnerável precisamente pela sua hiperconectividade - um bom exemplo do chamado paradoxo da inovação digital.

A reação da Estónia foi exemplar e revolucionaria. O país tornou-se um modelo internacional de ciberdefesa, criando assim o CCDCOE em Tallinn, que atualmente lidera a pesquisa, treino e doutrina em segurança cibernética para os países aliados.

Mais do que um simples caso isolado, o ataque à Estónia de 2007, provocou um alerta mundial para uma nova forma de confrontação entre Estados, e foi um catalisador para o desenvolvimento de doutrinas militares cibernéticas dentro da NATO e em vários outros Estados.

O *Tallinn Manual* apresenta 95 "regras de letra negra" que tentam aplicar normas tradicionais do Direito Internacional à guerra cibernética, expondo onde as normas falham ou ficam ambíguas.

Figura 2



Fonte: Tallinn Manual (NATO CCDCOE, Cambridge University Press, 2013)

2.5 Ciberataques na Guerra Rússia-Ucrânia (2014-2024)

O conflito entre a Rússia e a Ucrânia terá iniciado com a anexação da Crimeia em 2014 e foi intensificado com a invasão em grande magnitude em 2022, o que é extensamente considerado o primeiro grande exemplo de uma guerra híbrida sustentada com forte inserção de ações cibernéticas ofensivas. A Ucrânia tem funcionado como um "laboratório de testes" para a Rússia aplicar e modificar táticas de guerra cibernética, impactando não só o campo de batalha local, como também o panorama mundial de segurança tecnológica.

Fase inicial (2014-2016): espionagem e sabotagem

Depois da ocupação da Crimeia, a Ucrânia defrontou uma serie de ataques digitais especificamente direcionados para as instituições governamentais, meios de comunicação e infraestruturas essenciais. A maior parte destes ataques foram organizados para recolher dados estratégicos, desorganizar as diversas estruturas administrativas e corroer a confiança das autoridades ucranianas. Das quais destacam-se o uso do *malware BlackEnergy* para infetar sistemas industriais e organizar o terreno para ações futuras mais fatais e ciberataques simultâneos a sistemas de voto eletrónico e comunicações militares.

2.6 Ataques à infraestrutura critica

Um dos ataques mais marcantes aconteceu em dezembro de 2015 e 2016, quando alguns ataques cibernéticos interromperam o fornecimento de energia elétrica em várias zonas da Ucrânia, deixando assim, centenas de milhares de pessoas às escuras. As operações foram outorgadas, ao grupo *Sandworm*, associado ao serviço GRU, utilizando *malwares* como *Industroyer e KillDisk* (Lee, Assante & Conway, 2016).

Esses episódios demonstraram que a guerra cibernética pode originar efeitos físicos devastadores, desorganizando a vida dos civis e afetando a moral nacional. Foram os primeiros ataques comprovadamente bem-sucedidos a uma infraestrutura elétrica em tempo de paz, e mais tarde, em contexto de guerra aberta.

Fase da guerra total (2022-2024): ofensiva cibernética massiva

Com a invasão em fevereiro de 2022, a Rússia lançou uma campanha digital ofensiva e complexa pois utilizava o *malware HermeticWiper*, que procurava apagar dados de computadores e agências governamentais ucranianas antes da invasão, foi realizado um ataque à rede de satélites *Viasat*, que desativou modems de comunicação militares e civis na Ucrânia e entre outros países europeus e foram realizadas campanhas de desinformação massiva e guerra psicológica digital, com o uso de *bots, deepfakes* e manipulação das redes sociais para criar pânico, danificar a credibilidade do governo ucraniano e justificar a agressão russa.

Simultaneamente, a Ucrânia aprimorou as suas defesas cibernéticas, tornando-as notavelmente eficazes, com a ajuda de parceiros internacionais, empresas privadas (como a Microsoft e a google) e especialistas voluntários, organizados em estruturas como a *IT Army of Ukraine*.

Quanto ao seu impacto global e militarização do ciberespaço, o conflito demonstrou que a guerra cibernética não é apenas acessória, é também parte essencial do planeamento estratégico, o Ciberespaço tornou-se um novo campo de batalha, sem fronteiras, em que o governo, civis, empresas e infraestruturas críticas são e serão alvos e o apoio de atores privados e a cooperação internacional em tempo real são atualmente centrais na defesa cibernética.

Esse conflito redefiniu os paradigmas de segurança internacional, exibindo que nenhum país está imune, e que a dissuasão típica é ineficaz contra-ataques tecnológicos silenciosos, diversas vezes anónimos e persistentes.

2.7 Interferência nas Eleições dos EUA (2016 e 2020)

A interferência cibernética nas eleições presidenciais dos Estados Unidos, principalmente, em 2016, determinou um novo patamar na utilização da guerra cibernética como instrumento de influência política internacional. Este episódio demonstrou como as tecnologias digitais podem ser utilizadas por atores estrangeiros para perturbar democracias, sem disparar uma única bala.

Eleição de 2016: Operações de influência e ciberespionagem

Várias agências de inteligência norte-americanas, como a CIA, NSA e o FBI, chegaram à conclusão com alto grau de confiança que a Rússia organizou uma campanha cibernética e de influência com o objetivo de favorecer a eleição de Donald Trump e tornar mais fraca a candidata Hilary Clinton.

Figura 3

Tipos de ataque:	**Características do ataque:**
Ciberesiponagem	Grupos ligados ao serviço GRU, como o *Fancy Bear* (APT28), invadiram os servidores do Partido Democrata e da campanha de Clinton, obtendo e-mails e documentos internos, que foram posteriormente divulgados pelo WikiLeaks em momentos estratégicos.
Desinformação e manipulação social	A IRA, sediada em São Petersburgo, operou milhares de contas falsas em redes sociais (Facebook, Twitter, Instagram, Youtube), propagando conteúdos políticos polarizadores, *fake news* e teorias da conspiração. Essa operação atingiu milhões de eleitores norte-americanos, alimentando divisões raciais, ideológicas e sociais.
Testes em sistemas eleitorais	Embora não tenha havido manipulação direta de votos, houve tentativas de intrusão em registos de eleitores e sistemas eleitorais estaduais, incluindo em Illinois e na Flórida.

Fonte: criação da autora – Catarina Silva

Esse caso mostrou a eficácia de operações psicológicas digitais *(psyops*) no espaço digital, capazes de enfraquecer a confiança pública nas instituições e na integridade dos processos democráticos.

Eleição de 2020: Continuidade e resiliência

Nas eleições de 2020, as autoridades dos Estados Unidos aumentaram as medidas de Cibersegurança, com acompanhamento diário, cooperação entre agências federais (como o DHS e a CISA) e parcerias com algumas empresas privadas. Ainda assim, foram novamente identificadas algumas tentativas de divulgar falsas narrativas sobre fraude eleitoral, inclusivamente com a participação de *bots* automatizados, aumentar a desinformação sobre o processo de votação, especialmente nas comunidades latinas e afro-americanas e infiltração de hackers iranianos e russos em sistemas de governos locais e partidos políticos.

No entanto, de acordo com o relatório da CISA não existiu interferência técnica significativa na contagem de votos ou nos resultados finais da eleição de 2020.

No que diz respeito a implicações para a segurança internacional, as interferências nas eleições norte-americanas revelou que: o Ciberespaço é uma ferramenta estratégica de guerra assimétrica, permitindo os Estados mais pequenos ou revisionistas (como Rússia ou o Irão) influenciem potências globais, a linha entre guerra e paz tornou-se difusa, com ataques Cibernéticos ocorrendo em tempos de "paz formal" e a proteção da democracia digital tornou-se uma questão de segurança nacional. Estes episódios conduziram a uma mudança intensa nas doutrinas de segurança eleitoral, promovendo reformas em sistemas de votação, campanhas de alfabetização mediática e novas leis sobre a integridade social.

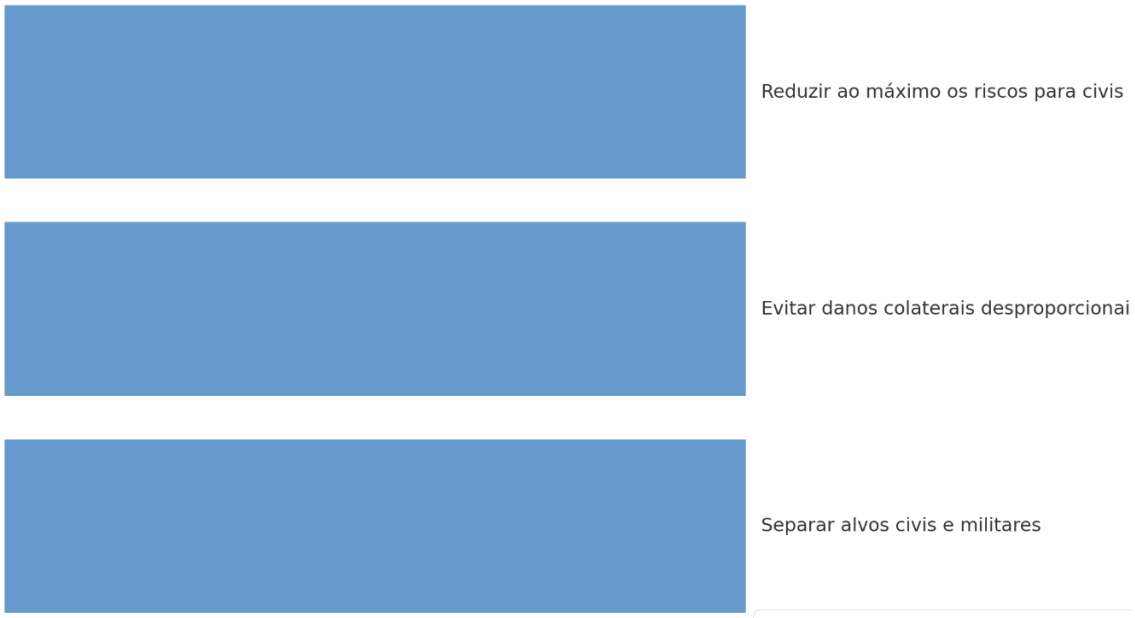
Capítulo 3- Desafios Jurídicos e Perspetivas Futuras

A guerra cibernética provoca diversos e preocupantes desafios ao Direito Internacional, sobretudo pela dificuldade de aplicar regras existentes a um domínio marcado pela ambiguidade, anonimato e velocidade. Este capítulo explora as limitações jurídicas atuais, os obstáculos na atribuição de responsabilidades e as possíveis vias para fortalecer a cooperação e a regulamentação global em matéria de Cibersegurança.

3.1 Direito internacional Humanitário no Contexto da Guerra Cibernética

O Direito Humanitário Internacional, também conhecido como Direito dos Conflitos Armados, estabelece um conjunto de normas internacionais que procuram limitar os efeitos dos conflitos armados, protegendo as pessoas que não participam diretamente e restringe os meios e métodos de combate. Contudo, com o aparecimento da Guerra Cibernética como uma nova forma de conflito, surgem dúvidas sobre como e em que medida esse corpo jurídico tradicional pode ser aplicado a operações conduzidas no Ciberespaço.

Figura 4



Fonte: Elaboração da autora – Catarina Silva, com base no CICV, 2020

Esta figura resume os três princípios fundamentais do Direito Internacional Humanitário — distinção, proporcionalidade e precaução — e como se aplicam a operações cibernéticas ofensivas.

Vários organismos internacionais, incluindo o CICV, afirmam que o DIH permanece aplicável às operações cibernéticas, desde que estas ocorram em contexto de conflito armado- seja internacional ou não- e desde que os seus atos possam ser equiparados aos resultantes de meios convencionais de guerra. Isto quer dizer, se um ataque cibernético

causa, por exemplo, a paralisação de um hospital, danos materiais significativos ou mesmo mortes indiretas, ele pode ser interpretado como um ato sujeito à regulação humanitária existente.

Dessa forma, os princípios essenciais do DIH continuam válidos no espaço cibernético. O princípio da diferença obriga os Estados e combatentes a diferenciar alvos militares de civis e evitar propositadamente ataques a pessoas e bens civis. O princípio da proporcionalidade proíbe ataques que posam causar danos colaterais desproporcionais em relação à vantagem militar obtida. Por outro lado, o princípio da precaução coloca a obrigação de tomar todas as medidas possíveis e minimizar os riscos para civis durante operações agressivas. Assim, os ataques digitais que visem, intencionalmente ou com negligencia, as infraestruturas civis como centrais elétricas, sistemas hospitalares ou redes de abastecimento de água, poderão constituir violações do DIH.

Contudo, a aplicação do DIH a situações cibernéticas encara obstáculos práticos e conceituais consideráveis. Um dos maiores obstáculos foca-se na dificuldade de atribuição: por exemplo, identificar com precisão a origem de um ataque digital, os seus autores e os seus vínculos estatais é um trabalho tecnicamente complexo e politicamente sensível. Isso pode dificultar não só apenas a responsabilização, mas também a aplicação efetiva de normas humanitárias.

Ademais, muitos ciberataques não provocam danos físicos imediatos ou visíveis, mas sim perdas económicas, roubo de dados, sabotagem informacional ou manipulação da opinião pública. Isso ergue uma questão crucial: todos esses ataques configuram o uso da força à luz do direito internacional? Em que momento essas ações cibernéticas, muitas vezes, silenciosas e persistentes, ultrapassam o limiar necessário para que se aplique o DIH?

A falta de tratados específicos sobre a guerra cibernética piora ainda mais esse cenário. Apesar de iniciativas como o Manuel de *Tallin,* realizado por especialistas sob a coordenação de CCDCOE, terem tentado esclarecer e compreender o DIH e outras regras internacionais à luz das novas tecnologias, tais documentos não tem caracter vinculativo. Por exemplo, o Manual de *Tallinn* 2.0, oferece orientações importantes, mas mantem uma compilação de opiniões jurídicas, e não de normas obrigatórias.

Em suma, mesmo que os princípios do DIH possam, em tese, ser aplicados à guerra cibernética, na prática, há um espaço vazio normativo e operacional significativo. Este vácuo abre margem para abusos, ações encobertas e violações dos direitos fundamentais

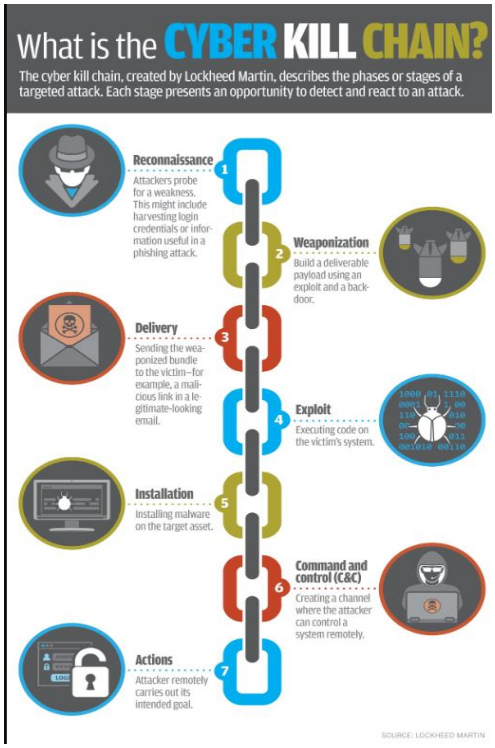
durante conflitos modernos. Perante o exposto, aumenta o consenso entre especialistas e organismos internacionais sobre a necessidade de desenvolver instrumentos jurídicos mais claros e adaptados à realidade dos conflitos cibernéticos, a fim de preservar os princípios humanitários em todas as áreas da guerra contemporânea.

3.2 Atribuição de Responsabilidade e Dificuldades Legais

Um dos principais problemas jurídicos na regulação da guerra cibernética é a atribuição de responsabilidade. Em conflitos tradicionais, a origem de um ataque militar costuma ser transparente e localizável. Contudo, no espaço digital, identificar com clareza quem está por trás de um ataque cibernético é extremamente complicado, tanto do ponto de vista técnico quanto jurídico. Essa incerteza compromete a aplicação de sanções, o direito de retaliação e o funcionamento eficaz do Direito Internacional.

O modelo em 7 fases da *Cyber Kill Chain*, desenvolvido pela Lockheed Martin, ilustra os pontos críticos onde a identificação e rastreamento do agente se tornam mais difíceis — especialmente após o estágio de 'exploração'.

Figura 5



Fonte: CSO Online, com base no modelo original da Lockheed Martin

Os ciberataques podem ser facilmente escondidos devido a técnicas de dissimulação e encobrimento, como o uso de servidores de países terceiros, redes *proxy, bots* automatizados ou até mesmo códigos utilizados em ataques anteriores. Aliás, os grupos não estatais, como hackers mercenários ou organizações ideologicamente motivadas, podem agir com ou sem suporte explicito do Estado, o que dificulta ainda mais a identificação do autor verdadeiro do ataque.

Mesmo com indícios claros de envolvimento por parte do Estado, os países raramente assumem responsabilidade. Em muitos dos casos, os governos desmentem o envolvimento, alegando que os ataques foram efetuados por "atores independentes", servindo-se do princípio da negação plausível *("plausible deniability"*). Isso aconteceu, por exemplo, no ataque *WannaCry* (2017), maioritariamente atribuído ao grupo *Lazarus*, ligado à Coreia do Norte, mas nunca oficialmente reconhecido por *Pyongyang.*

A falta de mecanismos internacionais eficazes para investigar, julgar e responsabilizar ataques cibernéticos representa um desafio principal. Embora a Carta das Nações Unidas, no seu artigo 2(4), proíba o "uso da força" sob o Direito Internacional.

Fora disso, não existem tribunais internacionais com jurisdição clara sobre ciberconflitos, o que agrava a lacuna de responsabilizações.

Outra dificuldade importante é o vazio normativo: a falta de até a data, não existir um tratado internacional específico e vinculativo que regule os atos hostis no espaço digital.

Várias tentativas de criar marcos normativos, como as discussões na área do GGE ou do OEWG, têm crescido lentamente, devido a desentendimento entre potencias digitais como os EUA, China e Rússia, sobre temas como a soberania tecnológica e liberdade na internet.

Resumidamente, a dificuldade de atribuir responsabilidade jurídica dos ataques cibernéticos favorece a impunidade e incentiva o crescimento de operações ofensivas por parte de Estados e atores não estatais. Essa fragilidade institucional afeta a estabilidade internacional e reforça a urgência de estabelecer instrumentos legais e mecanismos cooperativos para lidar com esse novo tipo de ameaça global.

3.3 Ataque *WannaCry* (2017) e a Dificuldade de Responsabilização da Coreia do Norte

O ataque cibernético célebre conhecido como *WannaCry,* ocorrido em maio de 2017 é um dos exemplos mais simbólicos nos problemas que a comunidade internacional enfrenta, na atribuição da responsabilidade jurídica entre conflitos no Ciberespaço.

O acontecimento implicou a difusão global de um *ransomware* - um tipo de *malware* que encripta dados e exige pagamento em criptomoedas para reparar o acesso- prejudicando milhares computadores em mais de 150 países. Hospitais do NHS no Reino Unido, empresas como FedEx e Renault, ministérios e instituições públicas, foram drasticamente impactados.

O *WannaCry* averiguou uma fraqueza no sistema operacional Windows reconhecida como EternalBlue, aparentemente desenvolvida pela NSA e partilhada por um grupo hacker chamado Shadow Brokers. A veloz propagação do ataque mostrou não só, a dependência tecnológica global, onde falhas em software geralmente utilizado podem produzir efeitos destruidores, mas também a fragilidade de infraestruturas críticas diante ameaças tecnológicas.

Apesar de várias agências de inteligência, englobando os Estados Unidos, Japão e o Reino Unido, tenham vindo a publico com a atribuição do ataque ao grupo Lazarus, associado ao governo da Coreia do Norte, nenhuma acusação oficial e concreta foi colocada em tribunais internacionais. As provas congregadas basearam-se particularmente em analises de código, comportamento e ações de rede e parecenças com ataques já realizados pelo mesmo grupo- critérios técnicos que, contudo, não cumprem plenamente os padrões jurídicos internacionais de prova.

Este exemplo revela uma das maiores fraquezas do sistema internacional atualmente: A dificuldade de responsabilizar de forma legal um Estado por ações cibernéticas ofensivas, mesmo com fortes indícios técnicos e consenso político. A Coreia do Norte, por sua vez, negou qualquer envolvimento no caso, utilizando o princípio da negação plausível, e não existiram consequências jurídicas diretas ou responsabilização protocolar nos foros internacionais.

3.4 Estratégias para a Cooperação Internacional e Cibersegurança Global

Perante o aumento da sofisticação dos ataques cibernéticos e da falta de Barreiras no Ciberespaço, fica claro a necessidade de maior cooperação internacional forte, resistente, coordenada e organizada para debater os desafios da cibersegurança. A dependência eletrónica entre Estados, indivíduos e empresas, demanda respostas plurilaterais eficazes, baseadas em confiança mútua, clareza, transparência e normas partilhadas.

Presentemente, não há um documento global que se específico que ajuste de forma geral a guerra cibernética ou defina, de maneira definitiva, regras internacionais de conduta no espaço digital. Entretanto, diversos projetos e fóruns plurilaterais têm procurado criar princípios e normas orientadoras. Entre os mais importantes está o trabalhado do UN GGE, que desde 2004 vem desenvolvendo diálogos sobre como o Direito Internacional se aplica ao uso das tecnologias de informação e comunicação no contexto da segurança internacional.

Ao mesmo tempo, projetos como UIT e GFCE tem realizado um papel importante no apoio a competências técnicas e jurídicas de Estados em desenvolvimento, principalmente, na luta contra o cibercrime e na proteção de infraestruturas importantes.

A NATO ao mesmo tempo reconheceu o Ciberespaço como um "domínio operacional" e aumentou as próprias competências cibernéticas defensivas, incentivado a cooperação entre os seus membros, nomeadamente através do CCDCOE, com base na Estónia. Sendo o próprio Manual de Tallinn, criado nesse contexto, e sendo ele uma referência crucial para a interpretação jurídica de operações cibernéticas em tempos de guerra.

No entanto, existem algumas adversidades que tornam a cooperação internacional, mas complicada como a ausência de consenso sobre as definições-chave, como é o caso de "ataque cibernético" ou "uso da força digital", a hesitação na partilha de informações sensíveis, diferenças políticas e ideológicas sobre a governança da internet e a falta de mecanismos eficientes de responsabilização e *enforcement.*

Nesse domínio, vários especialistas reforçam a necessidade de investir em cibereducação, resiliência digital e cooperação técnica Sul-Sul, fortalecer as redes regionais de cibersegurança (como a ENISA na União Europeia e a OEA na América Latina).

Portanto, a melhoria e o anúncio da ideia de uma cultura de ciberpaz e diplomacia digital é, assim, importante para impedir a escalada de tensões e garantir um ambiente tecnológico estável, seguro e com base no respeito recíproco entre humanos, à soberania e ao Estado de Direito.

Conclusão

A guerra cibernética simboliza uma das maiores dificuldades da área da Segurança Internacional atualmente, revelando-se especialmente pela sua natureza assimétrica, fronteiriça e invisível. Enquanto as infraestruturas críticas as sociedades e as instituições públicas ficam cada vez mais digitalizadas, os Estados vão enfrentando vulnerabilidades inéditas no domínio do Ciberespaço.

Como demonstrado aos longo deste trabalho, os conflitos tecnológicos vão para além do cibercrime ou do ciberterrorismo, colocando-se em um novo paradigma estratégico em que os atores não estatais e estatais utilizam o Ciberespaço como meio de influência, sabotagem ou até mesmo dissuasão. Exemplo disso são alguns dos casos referidos como o ataque *Stuxnet*, eventos na Estónia em 2007 ou até mesmo os ciberataques no contexto da guerra Rússia-Ucrânia, demonstram como as ofensivas digitais podem por vezes, ter impactos reais na soberania, estabilidade e na segurança de Estados-Nação.

Contudo, apesar do aumento deste tipo de ameaça, a estrutura jurídica internacional ainda é limitada, fragmentada e, muitas das vezes, ineficaz para lidar e resolver desafios como os da atribuição da responsabilização e da prevenção de conflitos cibernéticos. A falta de mecanismos plurilaterais robustos agrava esse mesmo cenário, permitindo assim a impunidade e o uso político das operações digitais.

Perante isto, revela-se extremamente urgente reforçar a cooperação internacional, promover a confiança entre Estados e investir no desenvolvimento de regras e instituições capazes de regulamentar o comportamento no Ciberespaço. A diplomacia digital, o diálogo multilateral e a educação cibernética devem ser usadas como pilares de uma estratégia mundial de segurança cibernética.

Por fim, a guerra cibernética não é só uma questão técnica, mas sim profundamente política, ética e estratégica. Para enfrentá-la requer uma abordagem transversal, que junte tecnologia, diplomacia, direito e sobretudo, responsabilidade internacional, preservando valores democráticos e a segurança coletiva em um mundo cada vez mais interconectado.

Bibliografia

Centro Nacional de Cibersegurança. (2024). https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercncs.pdf *Relatório sobre riscos e conflitos cibernéticos em Portugal.* CNCS.

Clarke, R. A., & Knake, R. K. (2010). https://www.harpercollins.com/products/cyber-war-richard-a-clarke-robert-knake *Cyber war: The next threat to national security and what to do about it.* Ecco.

Coleman, G. (2014). https://www.versobooks.com/products/1656-hacker-hoaxer-whistleblower-spy *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous.* Verso Books.

Council of Europe. (2001). https://rm.coe.int/1680081561 *Convention on Cybercrime (Budapest Convention).*

Cybersecurity and Infrastructure Security Agency. (2021). https://www.cisa.gov/rumorcontrol *Election security: Rumor vs. reality.* U.S. Department of Homeland Security.

Farwell, J. P., & Rohozinski, R. (2011). https://doi.org/10.1080/00396338.2011.555586 Stuxnet and the future of cyber war. *Survival, 53*(1), 23–40.

Greenberg, A. (2018/2019). https://www.penguinrandomhouse.com/books/597684/sandworm-by-andy-greenberg/ *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers.* Doubleday.

Hathaway, O. A., Crootof, R., Levitz, P., Perdue, W., & Spiegel, A. (2012). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134932 The law of cyber-attack. *California Law Review, 100*(4), 817–885.

Hultquist, J. (2019). https://www.mandiant.com/sites/default/files/2021-09/rpt-apt38-2018-web_v5-1.pdf *APT38: The rise of North Korea's cyber operations.* FireEye.

International Committee of the Red Cross. (2020). https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf *International humanitarian law and cyber operations during armed conflicts.* ICRC.

International Committee of the Red Cross. (2021). https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf *International humanitarian law and cyber operations during armed conflicts.* ICRC.

Kello, L. (2017). https://yalebooks.yale.edu/book/9780300236147/the-virtual-weapon-and-international-order/ *The virtual weapon and international order.* Yale University Press.

Lee, R. M., Assante, M., & Conway, T. (2016). https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt6a77276749b76a40/607f235992f0063e5c070fff/E-ISAC_SANS_Ukraine_DUC_5%5B73%5D.pdf *Analysis of the cyber attack on the Ukrainian power grid.* E-ISAC/SANS Institute.

Libicki, M. C. (2012). https://www.cambridge.org/core/books/conquest-in-cyberspace/7A0E6DEB32ACE50B76C06DE42A3B4000 *Conquest in cyberspace: National security and information warfare.* Cambridge University Press.

Lin, H. (2012). https://www.cambridge.org/core/journals/international-review-of-the-red-cross/article/cyber-conflict-and-international-humanitarian-law/9B46D09CEBCB12B453E594243AC5799F Cyber conflict and international humanitarian law. *International Review of the Red Cross, 94*(886), 515–531.

Melzer, N. (2011). https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf *Cyberwarfare and international law.* UNIDIR.

MetaCompliance. (n.d.). https://www.metacompliance.com/blog/security-awareness-training/what-is-cyber-warfare What is cyber warfare? *MetaCompliance Blog.*

Microsoft. (2022). https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Defending-Ukraine-Early-Lessons-from-Cyber-War.pdf *Defending Ukraine: Early lessons from the cyber war.* Microsoft Digital Security Unit.

Mueller, R. S. (2019). https://www.justice.gov/storage/report_volume1.pdf *Report on the investigation into Russian interference in the 2016 presidential election* (Vols. 1–2). U.S. Department of Justice.

Nakashima, E. (2015, June 4). https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/ Chinese breach data of 21.5 million in second U.S. government hack. *The Washington Post.*

Nocetti, J. (2015). https://www.cogitatiopress.com/mediaandcommunication/article/view/808/498 Russia's "cyber power": Between domestic control and global geopolitics. *Politics & Governance, 3*(2), 48–62.

Ottis, R. (2008). https://ccdcoe.org/uploads/2010/01/LP_Proceedings_2010-2.pdf Analysis of the 2007 cyber attacks against Estonia from the information-warfare perspective. In *Proceedings of the 7th European Conference on Information Warfare and Security* (pp. 163–172). Academic Publishing.

Rid, T. (2013). https://global.oup.com/academic/product/cyber-war-will-not-take-place-9780199330638 *Cyber war will not take place.* Oxford University Press.

Rid, T., & Buchanan, B. (2015). https://www.tandfonline.com/doi/full/10.1080/01402390.2014.977382 Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37.

Rid, T. (2020). https://us.macmillan.com/books/9780374287269/activemeasures *Active measures: The secret history of disinformation and political warfare.* Farrar, Straus and Giroux.

Sanger, D. (2012). https://www.penguinrandomhouse.com/books/211438/confront-and-conceal-by-david-e-sanger/ *Confront and conceal: Obama's secret wars and surprising use of American power.* Crown.

Schmitt, M. N. (Ed.). (2013). https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/1A6E70B53178208A2AACB54841931505 *Tallinn manual on the international law applicable to cyber warfare.* Cambridge University Press.

Schmitt, M. N. (Ed.). (2017). https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/5F2869964E4C2CF2A334AEC1FD80E017 *Tallinn manual 2.0 on the international law applicable to cyber operations.* Cambridge University Press.

Segal, A. (2016). https://publicaffairsbooks.com/titles/adam-segal/the-hacked-world-order/9781610394154/ *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age.* PublicAffairs.

Singer, P. W., & Friedman, A. (2014). https://global.oup.com/academic/product/cybersecurity-and-cyberwar-9780199918119 *Cybersecurity and cyberwar: What everyone needs to know.* Oxford University Press.

Taddeo, M., & Floridi, L. (2018). https://www.nature.com/articles/d41586-018-04602-6 Regulate artificial intelligence to avert cyber arms race. *Nature, 556*(7701), 296–298.

Tikk, E., Kaska, K., & Vihul, L. (2010). https://ccdcoe.org/uploads/2010/01/LP_Proceedings_2010-2.pdf *International cyber incidents: Legal considerations.* CCDCOE.

Tikk, E., & Kerttunen, M. (2022). https://ccdcoe.org/uploads/2022/04/Policy-Brief_Cyber-operations-in-the-Russia-Ukraine-conflict.pdf *Cyber operations in the Russia–Ukraine conflict* (Policy Brief). CCDCOE.

Tsagourias, N., & Buchan, R. (2015). https://www.e-elgar.com/shop/usd/research-handbook-on-international-law-and-cyberspace-9781789904246.html Cyber war and international law. In N. Tsagourias & R. Buchan (Eds.), *Research handbook on international law and cyberspace* (pp. 206–223). Edward Elgar.

United Nations. (2013, 2015, 2021). https://www.un.org/disarmament/ict-security/ *Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security (GGE reports).* UN ODA.

U.S. Senate Select Committee on Intelligence. (2019–2020). https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4 *Report on Russian active measures campaigns and interference in the 2016 U.S. election* (Vols. I–V). U.S. Government Printing Office.

Weber, M. (1919). https://archive.org/download/weber_max_1864_1920_politics_as_a_vocation/weber_max_1864_1920_politics_as_a_vocation.pdf Politics as a vocation. In *From Max Weber: Essays in sociology* (H. H. Gerth & C. W. Mills, Eds.). Oxford University Press.

Zetter, K. (2014). https://www.penguinrandomhouse.com/books/240915/countdown-to-zero-day-by-kim-zetter/ *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon.* Crown.

TI Inside. (2023, abr.). https://pt.linkedin.com/pulse/explos%C3%A3o-das-guerras-cibern%C3%A9ticas-5-formas-de-proteger-o-setor A explosão das guerras cibernéticas: 5 formas de proteger o setor de serviços financeiros contra-ataques de Estados-nação. *LinkedIn Pulse.*