FIOS INVISÍVEIS: GOVERNANÇA CIBERNÉTICA E ESTRATÉGIAS DE SOBERANIA

Marta Brescovici Scosi[1]

RESUMO

Este trabalho aborda a cibersegurança como um elemento estratégico nas Relações Internacionais, destacando o ciberespaço como um novo domínio de contenção e conflito. A pesquisa utiliza os conceitos de teoria dos jogos de Thomas Schelling, como dissuasão e coerção, para analisar a defesa cibernética como uma ferramenta tanto para prevenir ataques quanto para projetar poder de forma ofensiva. São explorados atores estatais e não estatais, com destaque para a China, que se destaca em campanhas de ciber espionagem e sabotagem estratégica. Além disso, discute-se a vulnerabilidade de infraestruturas críticas e o uso de métodos como engenharia social para reconhecimento e ataque. O estudo conclui que o fortalecimento de legislações, estratégias securitárias e cooperação internacional são indispensáveis para mitigar os riscos cibernéticos e garantir estabilidade no sistema internacional.

Palavras chaves: Cibersegurança, Ciberespaço, Defesa, Espionagem, China.

1 INTRODUÇÃO

O ciberespaço emergiu como um novo e dinâmico domínio nas relações internacionais, reconfigurando estratégias de poder e segurança em escala global. Desde suas origens em iniciativas militares e acadêmicas durante a Guerra Fria, a internet tornou-se uma infraestrutura essencial para governos, empresas e indivíduos. Contudo, com o aumento da interdependência digital, surgem novos riscos, como crimes cibernéticos transnacionais, espionagem e ataques a infraestruturas críticas, desafiando a capacidade das normas tradicionais do direito internacional de responder a essas ameaças.

Este trabalho analisa como o direito internacional se adapta a essas demandas, explorando os limites da Convenção de Budapeste como marco inicial na governança cibernética e o impacto da proposta de um novo tratado da ONU, impulsionado por China e Rússia. Particular atenção é dada ao papel estratégico da China, cuja abordagem assimétrica e soberanista molda a dinâmica do ciberespaço, destacando a tensão entre segurança estatal e cooperação internacional.

Diante de um ambiente assimétrico, onde o anonimato dificulta a atribuição de responsabilidades e favorece estratégias ofensivas, o estudo busca compreender como o ciberespaço desafia paradigmas tradicionais, exigindo a criação de instrumentos legais mais inclusivos, éticos e eficazes. Ao abordar questões como dissuasão cibernética, espionagem e direitos humanos, este trabalho visa contribuir

[1] Discente do curso de Relações Internacionais - Unilasalle, matriculada na disciplina de Trabalho de Conclusão de Curso II, sob orientação do Prof. Fabricio Pontin. E-mail: fabricio.pontin@unilasalle.edu.br. Data de entrega: 15 de dez. 2024.

para o debate sobre a necessidade de uma governança internacional adaptada à complexidade do mundo digital.

2 DAS REDES PRIVADAS ATÉ A CRIAÇÃO DA INTERNET: SEGURANÇA DIGITAL E A CONVENÇÃO DE BUDAPESTE

Para entender a preocupação com o uso da internet na comunidade internacional é importante destacar o alto envolvimento securitário e militar na rede, que dentre diversas utilidades, é usada como ferramenta estratégica dentro de conflitos. Já na origem da rede, encontramos esse uso no contexto da Guerra Fria: a necessidade de descentralizar a rede de comunicação norte-americana no evento de um ataque soviético em território doméstico levou o Departamento de Defesa dos Estados Unidos, por meio da Agência de Projetos de Pesquisa Avançada (ARPA) a investir em pesquisas acadêmicas e militares focadas na criação de redes fechadas para a transmissão de informação confidencial entre diferentes pontos focais estratégicos-militares no país - essa iniciativa leva a criação da ARPANET que garante a comunicação estratégica entre os órgãos militares e comunidade científica.

A ARPANET, no seu início, consistia em uma tecnologia de computação de dados, envio de dados por diferentes rotas até o destino do pacote, tornando a rede mais robusta e segura, capaz de comunicar seus “nós” sem a centralização de uma fonte de controle, estes processos foram desenvolvidos a partir de protocolos capazes de transformar pulsos telefônicos em sinais digitais que são transmitidos de ponto a ponto, e depois de-codificados no computador de destino. Esses protocolos, chamados de TCP-IP, possibilitaram redes de encriptação e desencriptação de dados que vão evoluir da transmissão de códigos e textos para a transmissão de imagens, vídeos e todo tipo de informação. Assim, a evolução desse novo meio de comunicação foi inicialmente lenta, cara, e segmentada nos setores acadêmicos e militares. No entanto, a partir da década de 80, com a popularização dos computadores pessoais, e baixa do preço dos custos de decodificadores de sinal TCP-IP, chamados de “modems”, redes de comunicação privadas, sem nexo com o setor de segurança, foram criadas, inicialmente através do uso de redes de comunicação peer-to-peer, chamadas BBS, e, no início da década de 90, com a criação do protocolo de hipertexto (HTTP), de forma pública, com o surgimento da World Wide Web (WWW). A popularização das redes públicas com informações disponíveis em servidores de fácil acesso, chamados “sites”, foi uma revolução na lógica de transmissão e consolidação de informação, e se tornou um marco na história da comunicação por ser pioneiro no fornecimento de informações por um sistema de pesquisa. Castells, em 1996, identifica nesse processo de criação da rede mundial de computadores, iniciada na década de 60 com os primeiros computadores militares, consolidada na década de 1970 com a ARPANET e com a criação dos protocolos TCP-IP, a apoteose de uma nova revolução industrial - e o início de um paradigma de comunicação informacional que reestrutura a lógica da comunicação em massa na internet.

Conforme o uso da internet se torna mais prevalente, também o tipo de informação disponível na rede e a sua acessibilidade se tornam mais diversificados. Desde o início das trocas de informação em rede, os riscos eram conhecidos e considerados nos cálculos estratégicos militares referente à segurança da informação, entretanto o papel militar foi diminuindo proporcionalmente ao crescimento em quantidade de usuários e domínios, levando a uma onda de crimes

cibernéticos nos anos 90, principalmente na Europa. Dois exemplos de grande impacto foram o roubo de dados do banco Citibank, que gerou um prejuízo de 10 milhões de dólares em 1995. O ataque contra o banco expôs a falta de um fórum internacional para legislar problemas transfronteiriços que liderasse uma reação conjunta dos países para essa fragilidade dentro da internet. E em 1998, os crimes cibernéticos atravessam a barreira virtual por meio do hacktivismo, definido por como “o uso não violento de ferramentas [tecnológicas] ilegais ou legalmente ambíguas em busca de fins políticos” (Samuel, 2004, p 2), contra o conflito do Kosovo, mais especificamente o uso de força da OTAN, se tornando o primeiro conflito geopolítico com impacto na esfera cibernética, que apesar de não ter freado a ofensiva do bloco, se mostra como um episódio simbólico e político. O ataque se deu por meio da sobrecarga de servidores da OTAN e de todo veículo de mídia e empresa apoiadora do bombardeio no Kosovo. Os dois exemplos demonstram a fraqueza na estrutura crítica dos sistemas governamentais e privados contra ataques, incitando a cooperação internacional unificada para combate ao crime organizado dentro de uma plataforma ainda carente de legislações e acordos internacionais.

A falta de legislações internacionais que punisse os cibercrimes dificultou aspectos como a extradição de criminosos que cometiam seus crimes de forma transfronteiriça em virtude das diferentes leis exercidas em cada Estado, impedindo uma resposta rápida e coordenada bem como atrasando a investigação do ocorrido. A partir desse contexto, o Conselho da União Europeia inicia a elaboração do que vem a ser em 2001 a Convenção de Budapeste, também conhecida como a Convenção sobre o crime cibernético. Este foi o primeiro tratado internacional endereçando temas de segurança cibernética, que tinha como objetivo a criminalização de ciberataques contra a “confidencialidade, integridade e disponibilidade de sistemas informáticos, redes e dados informáticos” (Convenção de Budapeste, 2001).

Assim, a redação da convenção propõe uma cooperação mais dinâmica entre os países signatários, com a ambição de construir um aparato judicial capaz de combater e investigar os crimes no contexto digital, permitindo meios de investigação e servindo de base para facilitar a cooperação internacional no combate de crimes cometidos dentro do ciberespaço. A convenção, como veremos, além de ter um caráter jurídico também estabelece as terminologias do fórum de discussão para assuntos de cibersegurança, para minimizar os erros de tradução.

A formação de um acordo comum entre as nações reflete a institucionalização de um novo campo de batalha no ciberespaço, uma arena emergente que, até então, carecia de um marco regulatório global capaz de unificar as normas sobre crimes cometidos na rede global de comunicações. A Convenção de Budapeste representa um esforço de articulação entre os Estados ao criar uma linguagem jurídica compartilhada para regular as atividades ilícitas no ciberespaço, um espaço por definição descentralizado e de difícil governança, o tratado promove uma cooperação transnacional, viabilizando mecanismos legais para uma vigilância colaborativa além das fronteiras territoriais. As discussões referentes à redação da Convenção foram feitas dentro do Conselho da União Europeia, fora de órgãos de discussão da ONU, com a participação de Estados não membros, posteriormente. Neste contexto, duas grandes potências, não foram convidadas a subscrever à Convenção: Rússia e China. Veremos no próximo capítulo suas reservas em relação à governança coletiva desse novo domínio, e a atual redação de uma nova convenção contra cibercrimes liderada por estes países.

A Convenção de Budapeste sobre o Cibercrime é um instrumento legislativo que tipifica infrações cibernéticas e cria procedimentos investigatórios comuns entre os países signatários, com o objetivo de promover uma cooperação internacional eficaz na investigação e processamento de crimes cibernéticos. Ela estabelece um arcabouço jurídico harmonizando legislações nacionais e facilitando a assistência jurídica mútua, a troca de informações e a extradição em casos de crimes digitais. A convenção também prevê mecanismos como a preservação de dados, busca e apreensão de dados eletrônicos, e a coleta de dados em tempo real. Além disso, tipifica crimes como acesso ilegal a sistemas, fraudes digitais e pornografia infantil, garantindo a proteção dos direitos humanos e da privacidade durante as investigações. Desenvolvida por especialistas e representantes de vários países, incluindo membros do Conselho da Europa e Estados como os EUA e Japão, a convenção prevê a cooperação internacional obrigatória dos países para enfrentar o problema dos crimes digitais.

É crucial entender a complexidade dos instrumentos de cooperação internacional previstos na Convenção de Budapeste. Os artigos 16 e 17 da Convenção de Budapeste (2001) garantem a preservação de dados armazenados, impedindo alterações ou exclusões, e autorizam autoridades a solicitar a retenção de informações sobre tráfego de comunicações, como IPs e registros de atividades em investigações de crimes cibernéticos. Além disso, o Artigo 19 introduz a possibilidade de busca e apreensão de dados como provas em processos legais. Os Artigos 20 e 21 tratam de crimes em tempo real, permitindo a coleta e a interceptação de dados de conteúdo. Todos esses elementos se entrelaçam nos Artigos 23 e 25, que estabelecem a assistência jurídica mútua, promovendo a troca de informações e a colaboração entre países no combate a crimes cibernéticos transnacionais.

3 POSICIONAMENTO DOS ESTADOS

A Convenção de Budapeste, ou convenção sobre o cibercrime, foi elaborada pelo Conselho da Europa para proteger a segurança nacional dos países do continente diante do crescente número de crimes no ambiente digital. Essa convenção visa enfrentar ameaças transnacionais por meio da criação de uma plataforma de cooperação internacional que mitiga as disparidades legislativas entre os Estados membros e uniformizar os meios de resposta e investigação de delitos que ocorrem simultaneamente em diferentes países. O Conselho buscou assegurar, por meio da cooperação internacional, o mesmo tratamento de rigor e seriedade que os crimes no mundo físico nos crimes digitais, considerando que a natureza fluida das fronteiras no ciberespaço dificulta a penalização dos criminosos, em contraste com as fronteiras geopolíticas tradicionais.

Os Estados Unidos é uma peça chave na cibersegurança, berço dessa tecnologia, visualizando o aumento do número de usuários em 1986 criou a Lei Fraude e Abuso de Computador, como medida preventiva a possíveis atividade criminais utilizando um computadores, a lei foi uma tentativa de regulamentar o uso de computadores, estabelecendo definições sobre o que constitui ações realizadas na rede e como essas ações devem ser julgadas. O Estado se absteve de tomar a iniciativa de um tratado internacional que unificasse os esforços de combate ao cibercrime, mas sua falta de protagonismo não impediu que o país ausentasse sua hegemonia, participou ativamente das discussões para a redação da convenção, e a retificou, provando sua preocupação e emergência para com a cibersegurança.

No outro extremo, a Rússia, a sua não adoção à Convenção de Budapeste não é uma surpresa, alegando não ter auxiliado na redação do tratado e que ele feria a soberania russa no que diz respeito à colaboração contra crimes cibernéticos que ocorrem de maneira transfronteiriça. Outro tema muito importante de ser ressaltado é a falta de consentimento entre as partes no que tange à terminologia no ciberespaço, um exemplo claro seria a definição de “Guerra Cibernética” que para o ocidente descreve ataques cibernéticos conduzidos por atores estatais contra infraestruturas digitais, integrados a uma campanha governamental, o conceito no texto russo amplia esse entendimento, incluindo ataques realizados por Estados, coalizões de países ou grupos políticos organizados, que têm como alvo infraestruturas cibernéticas dentro do contexto de uma campanha militar. A "soberania da internet" é uma área de discordância, com a Rússia e outros países defendendo o controle nacional sobre os recursos da internet dentro de suas fronteiras, aplicando suas leis locais.

Em 1994, na China, o Conselho de Estado publicou seu primeiro decreto sobre a segurança dos "sistemas de informação por computador", com ênfase nos sistemas relacionados a "assuntos estatais, desenvolvimento econômico, defesa nacional e avanços científicos e tecnológicos". O decreto, enraizado na lógica de controle estatal sobre o ciberespaço, proibiu o uso de sistemas de computadores que comprometessem o interesse nacional, o bem coletivo, os direitos dos cidadãos ou a própria segurança dos sistemas. A não adesão da China à Convenção de Budapeste reflete o mesmo princípio de Moscou: a defesa intransigente da soberania nacional. As definições impostas pela convenção colidem com os interesses do Estado chinês, principalmente no que tange ao compartilhamento de informações confidenciais em investigações internacionais. Para a China, a exigência de uma cooperação linear entre os países signatários da convenção sem a devida participação na sua redação ameaça a autonomia estatal. Assim, o país busca alternativas fora da ordem ocidental, propondo junto com a Rússia um novo modelo de regulação cibernética, que reforça o controle estatal sobre a internet, alinhado aos seus valores políticos e de soberania.

4 CIBERDEFESA ENQUANTO INSTRUMENTO DE CONTENÇÃO VS INSTRUMENTO DE AGRESSÃO

Compreendida a questão jurídica e o posicionamento dos Estados mais envolvidos na ciberdefesa, o próximo passo para delinear um cenário completo dessa nova esfera de estudo é a exposição teórica. Este capítulo busca explorar a abordagem teórica das Relações Internacionais no contexto digital, analisando a ciberdefesa tanto como um meio de contenção quanto como uma ferramenta de agressão no espaço cibernético. Para isso, considera-se a dinâmica de poder e os conflitos jurídicos e diplomáticos que emergem das relações entre os Estados em um ambiente de extrema assimetria e estratégias diferenciadas.

O ciberespaço, por sua mutabilidade, apresenta características únicas que diferem significativamente dos espaços tradicionais de conflito. Como afirma Gregory J. Rattray em Strategic Warfare in Cyberspace: “Montanhas e oceanos são difíceis de mover, mas partes do ciberespaço podem ser ligadas e desligadas com um clique.” Essa fluidez transforma o ambiente cibernético em um domínio estratégico onde barreiras físicas perdem relevância, ampliando as possibilidades de ação ofensiva e defensiva. Além disso, o anonimato no ciberespaço torna os desafios de segurança ainda mais complexos, já que a atribuição de ataques é

frequentemente dificultada, favorecendo Estados e atores que buscam estratégias de segurança ofensiva.

Thomas Schelling em seu livro "*Arms and influence*" de 1966 define dissuasão como "a ameaça de dano, ou de mais dano por vir, que pode fazer alguém ceder ou se conformar." (Schelling, 1966, p.3) e coerção como uma estratégia que precisa de um entendimento entre as partes envolvidas, fazendo com que a parte passiva à coerção "esteja em uma situação melhor ao fazer o que queremos — e pior ao não fazer o que queremos — quando ele considera a penalidade ameaçada" (Schelling, 1966, p 19). Estes termos popularizados por autores como Schelling e Mearsheimer, em seu livro "*A Tragédia da Política de Grandes Potências"* (2001), são amplamente utilizados dentro das Relações Internacionais, eles explicam a desescalada de conflitos, como em 1962 em que a dissuasão evitou um conflito físico na crise dos mísseis em Cuba. Tradicionalmente, a integridade territorial é o principal objeto de ameaça em estratégias de dissuasão e coerção, pois o território físico é essencial para a segurança nacional. Preocupado em proteger sua integridade territorial e manter sua estratégia nacional, o Estado ameaçado tende a se submeter aos termos impostos pela estratégia de outro Estado ou entidade.

Podemos compreender que o objetivo final dos países que enfrentam a dissuasão ou a coerção é proteger a soberania estatal, e mais que isso, assegurar que seu status quo se mantenha estável por meio da segurança territorial, econômica e social. O território físico é uma parte importante na análise da segurança internacional tradicional, para a coesão e dissuasão possam ser exercidas de forma eficaz é fundamental que o Estado tenha conhecimento de quem é a parte a ser dissuadida ou coagida, para que possa tomar uma ação resposta, como embargos econômicos e o direito de legítima defesa previsto pelo artigo da carta das Nações Unidas de 1945, que curiosamente não prevê esse direito em casos de ataques cibernéticos. Isso por si já representa uma ruptura entre segurança tradicional e cibernética, onde o anonimato se apresenta cada vez mais como um desafio para os Estados atingidos, favorecendo aos Estados que buscam uma segurança ofensiva.

Em 2007, a Estônia sofreu um ataque cibernético ao sistema do governo, instituições bancárias e à mídia, e por 22 dias impactou diretamente os cidadãos do país que depende extensivamente da infraestrutura cibernética, felizmente para os estonianos o ataque não teve um impacto significativo devido a um time estatal especializado em emergências no mundo virtual. Investigações posteriores ao ataque apontaram para a fonte de ataques advindos do território russo, que se recusou a ajudar a atribuir os ataques cibernéticos às partes culpadas, permitindo dentro da legislação internacional a responsabilidade atribuída para a Rússia, o que leva a discussão para a assimetria mencionada no início deste parágrafo: como a Estônia poderia responder a esse ataque? Os indivíduos responsáveis não foram culpabilizados e ficaram impunes de seus crimes, e a Rússia não possui a mesma dependência de sistemas virtuais como a Estónia, o que transforma um contra-ataque num esforço de resposta que seria em vão. Este episódio apresenta a contenção na dificuldade de resposta punitiva contra um adversário com menor dependência digital, nesse caso a Rússia. Este episódio nos apresenta duas questões distintas, primeiro podemos notar os exemplos práticos de agressão, defesa e contenção, que são vistos respectivamente no ataque ao sistema de redes da Estônia, o trabalho de frear o ataque por uma equipe de controle especializada em crimes cibernéticos, e a culpabilização do ataque à Rússia após recusar ajudar

nas investigações que apontavam para o território do Estado. A segunda questão que podemos perceber é a dependência digital reduzida que a Rússia possui em relação à Estônia, que embora também tenha avançado em tecnologia, Moscou depende menos de sistemas digitais para operações críticas, especialmente no governo e em setores estratégicos, mantendo redundâncias analógicas para segurança.

O estudo da estratégia ofensiva dentro das relações internacionais cibernéticas é ainda relativamente embrionário, Joseph Nye em seu artigo *Cyber Powe*r (2010) aponta essa falta de material de estudo como "pouco é declarado publicamente sobre doutrinas cibernéticas ofensivas", ele argumenta que os Estados não divulgam suas capacidades a fim de não reduzir o "valor estratégico" de um ataque surpresa. Ele ainda analisa que os Estados realizam uma espécie de reconhecimento de campo ao invadirem os sistemas cibernéticos uns dos outros para se prepararem para possíveis conflitos, que participam de atividades de espionagem a fim de obter informações como a capabilidade do seu alvo, e também participam de operações disruptivas contra um sistema de informação.

Além dos Estados, corporações transnacionais e grupos criminosos desempenham papéis crescentes no ambiente digital. Empresas como Amazon, Google e Microsoft possuem recursos financeiros e tecnológicos que rivalizam com os de muitos governos, exercendo grande influência global. Os grupos criminosos, por sua vez, frequentemente colaboram com Estados para realizar ataques cibernéticos enquanto negam formalmente a autoria. Segundo o relatório Virtual Criminology Report da McAfee (2009): "As habilidades de hackers podem torná-los aliados naturais para Estados que buscam aumentar suas capacidades enquanto negam envolvimento direto em ataques cibernéticos." Por fim, a dependência de sistemas SCADA (Supervisory Control and Data Acquisition), uma tecnologia usada para monitorar e controlar processos industriais e infraestrutura crítica em tempo real, para o funcionamento de indústrias e serviços essenciais torna a infraestrutura crítica um alvo vulnerável e de alto impacto. Ataques cibernéticos podem causar danos físicos severos, como exemplificado: "Se um hacker ou governo desligasse o fornecimento de eletricidade em uma cidade do norte como Chicago ou Moscou no meio de fevereiro, a devastação poderia ser mais custosa do que bombas." Esse cenário reforça a importância de investir em cibersegurança e cooperação internacional para mitigar riscos associados à disrupção de infraestruturas críticas. Para tanto, o estudo securitário das relações internacionais no espaço cibernético é fundamental para compreender as falhas no sistema e como contorná-las, com soluções legislativas e securitárias.

Essas dinâmicas, que envolvem desde colaborações estratégicas entre Estados e atores não estatais até ataques direcionados a infraestruturas críticas, destacam o papel central de estratégias ofensivas como a espionagem no ciberespaço, um termo em comum que surge em grande parte do material pesquisado referente a parte securitária, citada por Thomas Rid (2012) em seu artigo "Cyber War Will Not Take Place" (A Guerra Cibernética não vai acontecer - tradução própria) como uma das três estratégias ofensivas possíveis dentro do ciberespaço além da sabotagem, que é a "tentativa deliberada de enfraquecer ou destruir um sistema econômico ou militar" (Rid 2012) e da subversão, a manipulação de informações com a finalidade de enfraquecer ou derrubar uma ordem estabelecida, termos esses que, infelizmente, não irei explorar com profundidade neste artigo. A espionagem é o primeiro passo para outras ações securitárias, como um ataque hacker, que busca por meio da espionagem, técnica

ou social, uma brecha na segurança de um sistema para a finalidade buscada pelo Estado ou organização que realiza o ataque.

4.1. Mais sobre a estratégia de espionagem

O Professor Jon R. Lindsay considera que “a ubiquidade da tecnologia da informação anuncia uma nova era dourada para a espionagem” em seu artigo sobre espionagem no livro *The Oxford Handbook of Cyber Security,* permitindo que o uso da estratégia de espionagem dentro do ciberespaço possa ter diversos propósitos como a obtenção de informações que auxiliam a tomada de decisões de um país, monitoramento e rastreamento, apoiar operações militares dentre outras funcionalidades estratégicas. Elucidando em seu texto também que a ciber espionagem difere da convencional, que precisa de agentes, no que diz respeito aos riscos de uma operação tradicional a uma cibernética, enquanto a primeira precisa do deslocamento de agentes, treinamento dentre outros, está suscetível a se tornar um escândalo diplomático se descoberto, a espionagem virtual possui menos custos e menos risco, porque frente a uma crise diplomática, a ciber espionagem encara consequências como a perda do acesso à rede, onde ele pode simplesmente tentar novamente com outro método.

No artigo “The Coming of Cyber Espionage Norms” o autor e professor Martin Libicki esclarece que

> Oficiais americanos, (assim como de países aliados) argumentaram que, embora a ciberespionagem fosse um comportamento estatal aceitável, desde que realizada para proteger a segurança nacional, não era um comportamento aceitável se motivada economicamente. (Libicki, 2017)

Configurando o cenário de estudo da espionagem como uma área cinzenta entre o aceitável e o inaceitável para Estados, uma vez que a violação da confidencialidade de sistemas é considerada uma prática criminosa dentro da Convenção de Budapeste, como visto no artigo 2 que criminaliza o acesso não autorizado a sistemas de computador. Frente a esse problema, o ex-diretor da NSA (Agência de Segurança Nacional Americana) idealiza a formação de zonas de desmilitarização para redes cibernéticas sensíveis “como a rede elétrica e as redes financeiras, que estariam fora dos limites para ataques de Estados-nação” (Zetter, 2010), um passo largo se considerarmos que ainda existe o problema da responsabilização de ataques e espionagens patrocinadas por Estados.

Jon Lindsay aborda essa questão de forma bastante didática, comparando diferentes formas de ciberespionagem com crimes convencionais, como roubos a banco. Assim, a espionagem convencional, feita por qualquer hacker sem ligação com Estados, é comparada com o assalto qualquer, onde a oportunidade “fez” o ladrão - hackers exploram servidores vulneráveis ou desprotegidos, da mesma forma que um ladrão procura uma oportunidade de abordagem de uma pessoa distraída na rua. No entanto, a espionagem ligada à inteligência seria comparável com um crime mais sofisticado, como o roubo a um banco específico, com aplicação de métodos de reconhecimento e estudos, como a engenharia social a fim de ter acesso ao sistema e estudá-lo antes de poder atacar. Para Lindsay, isso implica em diferentes estratégias de defesa, já que “A defesa cibernética deve buscar combater o propósito e a direção de uma operação cibernética ofensiva, e não apenas a tecnologia utilizada em sua implementação” (Lindsay, 2016)

Estas comparações entre a espionagem cibernética convencional e as operações mais sofisticadas revelam a complexidade das ameaças cibernéticas, onde os intervenientes estatais utilizam táticas sofisticadas para atingir os seus objetivos de exploração de uma forma notável. Na espionagem cibernética estatal, a China destaca-se como um dos principais intervenientes, utilizando exatamente estes métodos de exploração e aprendizagem para obter planos críticos. No próximo capítulo, examinaremos como o governo chinês emprega sistematicamente essas táticas, exacerbando a ameaça da espionagem cibernética global.

5 PAPEL CHINÊS NO JOGO GLOBAL

Para a finalidade dessa pesquisa a China é um objeto de importante estudo securitário, no campo tradicional é igualmente uma figura complexa como no cenário das redes, é preciso compreender o papel protagonista chinês e seu extenso impacto na estratégia de países conhecidos por serem “imbatíveis” como os Estados Unidos. No começo de 2024, o Escritório do Diretor de Inteligência Nacional (ODNI) publicou a Avaliação de ameaças de 2024, uma das ameaças é a que se lê a seguir:

> A China permanece como a ameaça cibernética mais ativa e persistente ao governo dos EUA, ao setor privado e às redes de infraestrutura crítica. Se Pequim acreditasse que um grande conflito com os Estados Unidos fosse iminente, consideraria operações cibernéticas agressivas contra infraestruturas críticas e ativos militares dos EUA [...]”

A China adotou uma abordagem tática mais ofensiva a fim de explorar as vulnerabilidades de infraestruturas críticas e redes estratégicas, utilizando o ciberespaço tanto para dissuasão quanto para coerção. Este capítulo analisa as estratégias cibernéticas chinesas, com enfatizando a assimetria de suas capacidades e o impacto dessas ações na segurança internacional, utilizando como ator coadjuvante os Estados Unidos, sendo o Estado que mais securitiza a China.

No ciberespaço, a lógica das operações é favorável ao ataque em vez da defesa. Como apontado no Quadrennial Defense Review (2010) dos EUA, “a velocidade dos ataques cibernéticos e o anonimato no ciberespaço favorecem grandemente a ofensiva” (Hjortdal, 2011). Estratégias ofensivas são particularmente atraentes para Estados como a China, que reconhecem o ciberespaço como uma oportunidade assimétrica para equilibrar o poder militar e tecnológico dos EUA.

> Ao agir de forma agressiva, os Estados podem aumentar o risco de acusações de estarem conduzindo ataques cibernéticos, o que paradoxalmente pode beneficiar países como a China. Isso porque o aspecto dissuasório de possuir capacidades cibernéticas avançadas pode não ser detectado ou amplamente conhecido de outra forma. (Hjortdal, 2011)

Utilizando de seu poderio cibernético como uma forma de coesão, um aviso para a comunidade internacional das capacidades chinesas, mantendo simultaneamente uma incerteza de seu real arsenal e intenção, reforçando a dissuasão, uma estratégia descrita por Schelling em seu livro como essencial para evitar ações hostis.

Hjortdal relata que em suas conversas com estrategistas militares chineses capacidades cibernéticas foram definidas como “uma poderosa oportunidade

assimétrica em uma estratégia de dissuasão" (Hjortdal, 2011 p.5). Um exemplo dessa abordagem é o uso de Computer Network Attack (CNA) como "a ponta de lança da dissuasão" para elevar os custos de um conflito para adversários, a ponto de tornar a continuação de um conflito inviável. Essa estratégia visa não apenas interromper operações críticas, mas também demonstrar poder sem recorrer a confrontos tradicionais, porque, segundo Schelling o poder coercitivo é mais eficaz quando os custos infligidos são altamente visíveis e disruptivos, evitando dessa forma um conflito direto, que poderia significar a destruição mútua assegurada.

Um caso emblemático de coerção foi o ataque às redes elétricas dos EUA em 2009, que revelou que partes da infraestrutura poderiam ser desligadas à vontade dos invasores. Esse ataque, atribuído à China, exemplifica o potencial devastador da coerção cibernética: "uma interrupção massiva poderia deixar os EUA sem energia por seis meses, permitindo à China ocupar Taiwan" (Hjortdal, 2011). Além disso, a dissuasão cibernética opera sob a lógica de incerteza estratégica. Como apontado por Hjortdal (2011), "as capacidades cibernéticas raramente são divulgadas, mas sua existência pode amplificar a dissuasão, mesmo sob o risco de acusações internacionais". A China utiliza extensivamente o ciberespaço para espionagem industrial e militar, buscando acelerar seu desenvolvimento em áreas-chave. Entre os alvos documentados está o programa Joint Strike Fighter, que teve dados críticos copiados, o que gerou especulações quando a China lança seu caça J-20, muito similar ao F-35 americano. Esses incidentes refletem como a espionagem cibernética não apenas fortalece capacidades militares chinesas, mas também reduz sua dependência de tecnologia estrangeira.

Embora altamente eficaz, o uso agressivo do ciberespaço apresenta riscos significativos para a própria China, que possui uma alta dependência do espaço cibernético para exercer suas funções militares e civis. Essa vulnerabilidade exige um equilíbrio estratégico entre a demonstração de força e a proteção de suas próprias infraestruturas para que o Estado consiga se proteger de uma possível retaliação de outro Estado. Hjortdal (2011) ressalta que os atores ocidentais tendem a superestimar as capacidades chinesas para justificar investimentos em programas de defesa , levando a uma discussão mais nebulosa para com o real poderio cibernético da China, que recebe ataques frequentes em seus servidores, provocando o rastreamento de ataques para servidores chineses, o que pode muitas vezes ser apenas uma ponte para o real culpado. Aqui podemos fazer mais uma vez uma referência ao trabalho clássico de Schelling, que identifica a contenção como uma forma de moldar o comportamento de adversários - nessa leitura, o ciberespaço permite à China criar um novo equilíbrio de poder, limitando a capacidade de ação de seus oponentes. O ciberespaço, assim, não é apenas um domínio técnico, mas um espaço estratégico central para a contenção e projeção de poder no século 21, que apresenta uma dicotomia acadêmica extensiva.

6 DIREITO INTERNACIONAL CIBERNÉTICO

A frase "apagar pessoas que apagam bits" (Goodman, 2010 - do original "*Kill people who kill bits*"), é usada pelo autor em seu artigo sobre ciber dissuasão para questionar o uso da segurança convencional dentro do espaço cibernético. Conforme analisado no capítulo anterior, o poder cibernético é exercido de forma assimétrica, isso se percebe na vantagem que a estratégia ofensiva possui no ciberespaço, que desestabiliza sistemas críticos retardando uma resposta ao

ataque, levando também a implicações políticas como a falta de confiança nos sistemas estatais e a perda econômica para a restauração desses sistemas. Will Goodman é assertivo em sua ponderação, levando a discussão de qual seria a resposta apropriada para um ataque cibernético - certamente responder um ataque de inteligência com força seria brutal e injustificável, mas essa mesma lógica se aplica se o sistema afetado for o de um hospital, por exemplo?

Aqui retornamos para a questão do anonimato, apesar de termos hoje uma forma de culpabilizar um Estado, como no caso da Estônia em que a Rússia foi a culpada do ataque realizado por não ter auxiliado nas investigações, é irresponsável autorizar um ataque a um país que somente talvez seja o culpado. A dinâmica complexa do ciberespaço não está coberta pela Convenção de Budapeste, que encontra em assuntos como a espionagem uma dicotomia de opiniões perigosa sendo considerada crime a invasão de redes dentro da Convenção, mas se cria uma tradição entre Estados de permitir que esse tipo de ação ocorra desde que para proteger o próprio Estado e que não crie vantagens comerciais, abrindo novamente um espaço para discussões referente à seriedade ao qual se leva a Convenção.

A Convenção de Budapeste possui diversas lacunas e não aborda adequadamente questões relacionadas à cibersegurança atual, uma temática que está em constante mudança e evolução juntamente com a tecnologia dessa esfera, seguindo as mesmas legislações base desde 2001. Cada vez mais vemos estudos que apontam as falhas desse sistema, clamando por mais coordenação internacional nas regras do tabuleiro internacional cibernético. Nesse cenário, uma nova Convenção vem sendo discutida, muito apoiada pela China e Rússia, para se tornar a primeira estrutura legal global para crimes cibernéticos, sendo estruturada dentro da ONU, diferente da atual Convenção que é um acordo internacional iniciado pela e na União Europeia. Essa proposta enfatiza a necessidade da cooperação jurídica internacional, sem deixar de lado a soberania estatal, deixando a decisões como a de compartilhar dados armazenados em seu país por conta do Estado.

Um passo importante para o desenvolvimento de um tratado com maior representação, uma vez que a redação do texto teve participação dos 193 Estados membros, diferente da Convenção de Budapeste que é liderada pelo Conselho da Europa. Apesar de estar ganhando força, o Tratado tem recebido críticas negativas, o artigo 22 do tratado permite que um Estado que sinta sua segurança nacional ameaçada pode exercer jurisdição em outro país, (Scher-Zagier, 2024). Ao mesmo tempo em que o tratado aumenta o escopo de criminalização de atividades ilegais também dentro da esfera cibernética, como lavagem de dinheiro e tráfico de pessoas, grupos de defensores de direitos humanos criticam a falta de garantias dos direitos humanos, colocando em cheque o bem-estar e a privacidade da população. A proposta de uma nova Convenção é um reflexo claro de todo o exposto relativo a estratégia chinesa nessa pesquisa, o alto foco na soberania, que a fez optar por não assinar a Convenção de Budapeste, aparece como proposta dentro da redação do texto do Tratado.

Dentro dessa discussão complexa, a pergunta que segue sem resposta é: Como podemos garantir que a retaliação seja direcionada, ética e não cause escaladas descontroladas no ciberespaço? Tomamos o exemplo do ataque contra a Estônia de 2007, a culpa foi atribuída a Rússia pela falta de colaboração para a investigação dos culpados, mas é difícil dizer com certeza se o ataque foi mandado pelo Estado Russo, ou se foi uma ação independente por um grupo contra o Estado

da Estônia. Mesmo confirmada a culpabilidade, a retaliação por meio de redes cibernéticas não teria o mesmo efeito que o ataque teve na Estônia, isso porque Moscou não possui a mesma dependência das redes que Talín possui. Esse anonimato não dificulta apenas a retaliação de um Estado, mas dificulta a aplicação de normas internacionais contra os agressores, que podem não ser estatais, mas grupos independentes que operam dentro do território nacional de algum Estado.

Existem preocupações que transcendem ambos os tratados, como a impunidade e a violação dos Direitos Humanos. A impunidade fortalece os ataques ao não demonstrar uma consequência ao descumprimento de regras que, como analisamos acima, não estão bem estabelecidas. Essa impunidade também fortalece a violação dos Direitos Humanos, aqui se torna mais fácil analisar o descumprimento do direito à privacidade e à proteção de dados, mas poderíamos citar também que facilita crimes que extrapolam completamente os limites da internet para o mundo tangível, como o tráfico de pessoas e a venda de ilícitos. A impunidade pode ser explicada pela falta de um consenso estratégico de defesa dentro das redes globais, entendemos neste trabalho que a espionagem é necessária para compreender e prevenir um ataque, mas também sabemos que essa prática vai contra os princípios da Convenção de Budapeste, tornando-a apenas um instrumento de *soft power* para demonstrar valores políticos.

7 CONSIDERAÇÕES FINAIS

O ciberespaço transformou-se em um campo estratégico essencial para a dinâmica das relações internacionais, trazendo desafios sem precedentes para o direito internacional. Este trabalho evidenciou como as características únicas do ciberespaço — sua natureza assimétrica, anônima e transnacional — exigem uma adaptação das normas jurídicas globais para lidar com questões como a soberania digital, a cibersegurança e a proteção de direitos humanos.

A análise destacou as limitações da Convenção de Budapeste, que, apesar de pioneira, não abrange adequadamente temas contemporâneos, como a espionagem cibernética e o impacto de ataques a infraestruturas críticas. Por outro lado, a proposta de um novo tratado pela ONU, apoiada por países como China e Rússia, representa um avanço em termos de inclusão global, mas também gera preocupações quanto à proteção de direitos fundamentais, dada sua ênfase na soberania estatal.

O papel da China no cenário cibernético ilustra a complexidade das disputas no ciberespaço, combinando dissuasão, espionagem e estratégias de influência para moldar as normas emergentes. Essa abordagem reforça a necessidade de uma governança global mais equilibrada, que proteja as populações vulneráveis e promova a cooperação internacional sem comprometer valores democráticos e direitos humanos.

Diante da rápida evolução tecnológica, conclui-se que um arcabouço jurídico adaptável e colaborativo é indispensável para enfrentar os desafios do ciberespaço. Estudos futuros devem explorar como tecnologias emergentes, como inteligência artificial e computação quântica, podem impactar o direito internacional, contribuindo para a criação de um ciberespaço mais seguro, ético e inclusivo.

REFERÊNCIAS

BATSELL G., Stephan; RAO S., Nageswara; SHANKAR, Mallikarjun. **Distributed Intrusion Detection and Attack Containment for Organizational Cyber Security**. 2012. Estados Unidos. Disponível em: https://www.sos-vo.org/node/3579. Acesso em: 12 out. 2024.

CASTELLS, Manuel. **A Sociedade em Rede**. Editora Paz e Terra, 2002.

COMPUTER User Sentenced. New York Times, 1 mai. 1984. Disponível em: https://www.nytimes.com/1984/05/01/us/computer-user-sentenced.html. Acesso em: 6 set. 2024.

CONSELHO DA EUROPA. **Convenção sobre cibercrime**. 23 nov. 2001. Budapeste. Disponível em: https://rm.coe.int/16802fa428. Acesso em: 23 ago. 2024.

CRAIG, Anthony; VALERIANO, Brandon. Realism and Cyber Conflict: Security in the Digital Age. **E-International Relations**, 2018. Estados Unidos. Disponível em: https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/. Acesso em: 20 out. 2024.

CREEMERS, Rogier. The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy. **Journal of Contemporary China**, 33(146), 173–188, 2023. Disponível em: https://doi.org/10.1080/10670564.2023.2196508. Acesso em: 2 set. 2024.

EAST WEST INSTITUTE. **Critical Terminology Foundations** Volume 2 - Russia - U.S. Bilateral on Cybersecurity. Information Security Institute, 2024. Russia. Disponível em: http://www.iisi.msu.ru/UserFiles/File/Terminology%20IISI%20EWI/Russia-U%20S%20%20bilateral%20on%20terminology%202.pdf. Acesso em: 2 set. 2024.

GIER, Keir. Russia and Cybersecurity. **Revista Nação e Defesa**, 2012. Disponível em: http://hdl.handle.net/10400.26/42460. Acesso em: 6 set. 2024.

GILES, Keirs; HAGESTAD II, William. Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. **NATO CCD COE Publication**, 2013. Estônia. Disponível em: https://ccdcoe.org/uploads/2018/10/22_d3r1s1_giles.pdf. Acesso em: 6 set. 2024.

GOLD, John. The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'. **NATO CCD COE Publication**, 2020. Estonia. Disponível em: https://ccdcoe.org/library/publications/the-five-eyes-and-offensive-cyber-capabilities-building-a-cyber-deterrence-initiative/. Acesso em: 23 nov. 2024.

GOODMAN, Will. Cyber Deterrence: Tougher in Theory than in Practice?. **Strategic Studies Quarterly**, Vol. 4, No. 3, pp. 102-135, 2010. Disponível em: https://www.jstor.org/stable/26269789?seq=2. Acesso em: 13 out. 2024.

GORMAN, Siobhan. Electricity Grid in U.S. Penetrated By Spies. **The Wall Street Journal**, 2009. Disponível em: https://www.wsj.com/articles/SB123914805204099085. Acesso em: 15 nov. 2024.

HARMON, Amy. Hacking Theft of $10 Million From Citibank Revealed. **Los Angeles Times**, 19 ago. 1995. Estados Unidos. Disponível em: https://www.latimes.com/archives/la-xpm-1995-08-19-fi-36656-story.html. Acesso em: 6 set. 2024.

HJORTDAL, Magnus. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. **Journal of Strategic Security**, Vol. 4, No. 2, 2011. Disponível em: https://www.jstor.org/stable/26463924. Acesso em: 15 nov. 2023.

KAMIMURA MURATA, Ana Maria; RITZMANN TORRES, Paula. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora?. **Boletim IBCCRIM**, 31(368), 2023. Brasil. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575. Acesso em: 20 out. 2024.

LIBICKI, Martin. The Coming of Cyber Espionage Norms. **NATO CCD COE Publications**, 2017. Estônia. Disponível em: https://ccdcoe.org/uploads/2018/10/Art-01-The-Coming-of-Cyber-Espionage-Norms.pdf. Acesso em: 19 out. 2024.

LINDSAY, Jon. Cyber Espionage. **The Oxford Handbook of Cyber Security**, Chapter 14, 2021.

MEARSHEIMER, John. **The Tragedy of Great Power Politics**. Norton & Company, 2001. Estados Unidos.

NYE, Joseph. Cyber Power. **Belfer Center for Science and International Affairs, Harvard Kennedy School,** 2010. Estados Unidos. Disponível em: https://www.belfercenter.org/publication/cyber-power. Acesso em: 20 out. 2024.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. **Annual Threat Assessment of the U.S. Intelligence Community**. 2024. Disponível em: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3787-2024-annual-threat-assessment-of-the-u-s-intelligence-community. Acesso em: 3 nov. 2024.

RID, Thomas. Cyber War Will Not Take Place. **Journal of Strategic Studies**, 2011. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939. Acesso em: 31 out. 2024.

SCHELLING, Thomas C. **Arms and Influence**. Yale University Press, 1966.

SCHELLING, Thomas. **The Strategy of Conflict**. Pickle Partners Publishing, 2015.

SCHER-ZAGIER, Eli. The New UN Cybercrime Treaty Is a Bigger Deal Than Even Its Critics Realize. **Lawfare**, 2024. Disponível em: https://www.lawfaremedia.org/article/the-new-un-cybercrime-treaty-is-a-bigger-deal-than-even-its-critics-realize. Acesso em: 30 nov. 2024.

SHABRINA, Syarah; AZMI, Agus Nilmada. Challenges of Universal Adoption of The Budapest Convention on Cybercrime. IN: **PROCEEDING ICTESS** (International Conference on Technology, Education and Social Sciences), 2024. Indonesia. Disponível em: https://ejurnal.unisri.ac.id/index.php/proictss/article/view/10254. Acesso em: 6 set. 2024.

U.S.- CHINA ECONOMIC REPORT AND SECURITY REVIEW COMMISSION STAFF. **China and International Law in Cyberspace**. Estados Unidos. Disponível em: https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf. Acesso em: 1 set. 2024.

UNITED NATIONS. **United Nations**: Member States finalize a new cybercrime convention, 2024. Disponível em: https://www.unodc.org/unodc/en/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html. Acesso em: 22 nov. 2024.

VAN WIE DAVIS, Elizabeth. Shadow Warfare - **Cyber Policy in The United States, Russia, and China**. Rowman & Littlefield, 2021. Estados Unidos.

ZETTER, Kim. **Former NSA Director**: Countries Spewing Cyberattacks Should Be Held Responsible. Wired, 2010. Disponível em: https://www.wired.com/2010/07/hayden-at-blackhat/. Acesso em: 25 out. 2024.