RUMO A UM REGIME GLOBAL DE SEGURANÇA CIBERNÉTICA

DOI: 10.61623/cpe.v11n16.a10

Marcel Furtado Garcia[1]

Resumo

A crescente dependência das sociedades modernas em redes digitais vem aumentando a vulnerabilidade às ameaças cibernéticas, que vão desde erros humanos até ataques maliciosos patrocinados pelo Estado. Esta dissertação examina o potencial de um regime global de segurança cibernética que contribua para a paz e a segurança internacionais. Por meio de uma pesquisa qualitativa que analisa a literatura sobre segurança cibernética, documentos governamentais e resoluções da ONU, o trabalho avalia os desafios geopolíticos decorrentes do espaço cibernético, a conveniência de uma estrutura de segurança cibernética para enfrentá-los e sua viabilidade. Um regime global poderia promover a estabilidade no domínio cibernético e, embora existam obstáculos significativos para isso, os esforços internacionais sugerem que o progresso é possível.

Palavras-chave: Cibersegurança; Equilíbrio de poder; Relações Internacionais; Segurança Internacional.

1 Primeiro-Secretário da carreira diplomática, atualmente lotado na Missão Permanente do Brasil junto às Nações Unidas em Nova York. Foi subchefe da Divisão de Defesa e Segurança Cibernética do Itamaraty entre 2023 e 2025. Este artigo foi apresentado como dissertação de mestrado em Relações Internacionais (especialização em segurança cibernética) na King's College London. As opiniões contidas neste trabalho são de exclusiva responsabilidade do autor e não representam necessariamente as posições do Ministério das Relações Exteriores.

TOWARDS A GLOBAL CYBERSECURITY REGIME

Abstract

The increasing dependence of modern societies on digital networks has heightened their vulnerability to cyber-threats, ranging from human error to state-sponsored malicious attacks. This dissertation examines the potential of a global cybersecurity regime to contribute to international peace and security. Through qualitative research analysing cybersecurity literature, governmental documents, and UN resolutions, it assesses geopolitical challenges stemming from cyberspace, the desirability of a cybersecurity framework to address them, and its feasibility. A global regime could foster stability in the cyber-domain, and, while significant obstacles towards it exist, international efforts suggest progress is possible.

Keywords: Cybersecurity; Balance of Power; International Relations; International Security.

HACIA UN RÉGIMEN MUNDIAL DE CIBERSEGURIDAD

Resumen

La creciente dependencia de las sociedades modernas de las redes digitales ha aumentado su vulnerabilidad ante las ciberamenazas, que van desde los errores humanos hasta los ataques maliciosos patrocinados por Estados. Esta tesis examina el potencial de un régimen mundial de ciberseguridad para contribuir a la paz y la seguridad internacionales. A través de una investigación cualitativa que analiza la bibliografía sobre ciberseguridad, documentos gubernamentales y resoluciones de las Naciones Unidas, evalúa los retos geopolíticos derivados del ciberespacio, la conveniencia de un marco de ciberseguridad para abordarlos y su viabilidad. Un régimen global podría fomentar la estabilidad en el ciberespacio y, aunque existen obstáculos importantes para su consecución, los esfuerzos internacionales sugieren que es posible avanzar.

Palabras clave: Ciberseguridad; Equilibrio de poder; Relaciones internacionales; Seguridad internacional.

Introdução

A transformação digital das sociedades modernas tem sido um motor de desenvolvimento e bem-estar. Ao mesmo tempo, as sociedades têm se tornado cada vez mais dependentes do funcionamento constante e correto dos sistemas de redes de informações digitais, da mesma forma que dependem amplamente, por exemplo, da disponibilidade de eletricidade. Essa dependência implica vulnerabilidades a falhas herdadas, erros humanos, acidentes ou ações maliciosas que podem afetar negativamente esses sistemas.

Essa vulnerabilidade não é novidade. Ao longo da história, os sistemas de informação vêm apresentando desafios. Muito antes do surgimento das redes eletrônicas, os avanços na tecnologia de comunicação foram explorados por "hackers". Já em 1834, criminosos violaram o sistema de telégrafo francês no intuito de transmitir informações ocultas sobre o mercado financeiro nacional e obter lucro (Standage e Stevenson, 2018). O nascimento do espaço cibernético ocorreu 135 anos depois, com a primeira conexão de computador estabelecida entre a Universidade da Califórnia e a Universidade de Stanford (Singer e Friedman, 2014, p. 16-18). No início da década de 1970, já havia esforços para lidar com as vulnerabilidades dos sistemas eletrônicos (U.S. Cyber Command, 2024). O primeiro ataque cibernético com consequências físicas significativas pode ter ocorrido em 1982, quando o oleoduto Urengoy-Surgut--Chelyabinsk na Rússia explodiu, supostamente devido a uma sabotagem de *software* pela CIA (Rid, 2013, p. 4-5). Começavam a surgir uma nova fonte e um novo meio de conflito e poder internacionais.

Recentemente, o mundo foi lembrado da extensão da vulnerabilidade cibernética atual. Em meados de julho de 2024, o caos se instalou após um erro humano desativar sistemas digitais em todo o mundo, incluindo serviços essenciais como bancos, saúde e viagens aéreas (Plummer e Gerken, 2024). Isso foi resultado de falhas nas atualizações do *software* de segurança baseado em nuvem da CrowdStrike, utilizado pelas principais plataformas da Microsoft. Embora esse evento não tenha sido intencional, talvez tenha sido o último aviso em grande escala do possível escopo e alcance dos danos que uma operação cibernética ofensiva poderia causar, mundialmente e com efeitos imediatos, especialmente quando realizada com objetivos geopolíticos.

Questão da pesquisa

Esse incidente renovou o apelo para alertar essa nova via global e digital para ações maliciosas. Nesse contexto, esta dissertação se concentrará no

conflito interestatal no espaço cibernético e nas formas de evitá-lo e manter a estabilidade, sob a questão principal "até que ponto um regime global de cibersegurança poderia contribuir para a paz e a segurança internacionais?" Como será visto a seguir, a questão central terá como base duas perguntas secundárias, a primeira relacionada ao contexto em que ela se encontra e a segunda relacionada à viabilidade de tal regime.

Abordagem e estrutura

Esta dissertação é baseada em uma pesquisa qualitativa com foco tanto na literatura sobre segurança cibernética quanto na análise de fontes primárias, incluindo documentos governamentais e discursos oficiais em fóruns multilaterais, além de resoluções e relatórios das Nações Unidas. Juntos, esses materiais oferecem uma base teórica e empírica abrangente para compreender os desafios e os avanços relacionados à construção de um marco internacional de conduta responsável dos Estados no espaço cibernético, bem como para avaliar as perspectivas de um regime global de segurança nessa dimensão, com o objetivo de mitigar as ameaças à paz e à segurança internacionais.

Após essa introdução, três capítulos discutirão os diferentes aspectos envolvidos nessa perspectiva. O Capítulo 1, "Desafios da segurança cibernética", apresentará o pano de fundo para responder à questão principal. Primeiro, ele avaliará o cenário estratégico internacional derivado da natureza do espaço cibernético, em especial como ele afeta o poder dos Estados e a rivalidade geopolítica, tornando-se uma fonte de instabilidade internacional. Depois, com o objetivo de explorar formas sistêmicas de mitigar os desafios da segurança cibernética, o capítulo analisará as suposições e avaliações institucionalistas liberais dos regimes internacionais, como estruturas de incentivos que podem mitigar as ameaças à paz e à segurança. Esses incentivos não são vistos como inequívocos ou inevitáveis, mas podem ser eficazes para evitar conflitos interestaduais violentos.

O Capítulo 2, "Regime desejável", abordará mais diretamente a questão principal. Primeiro, ele abordará as opções nacionais para lidar com ameaças cibernéticas e suas prováveis consequências internacionais. Em seguida, ele as comparará com as possíveis contribuições de um regime global de cibersegurança, argumentando que o último oferece incentivos preferíveis, apesar de suas limitações. Em especial, a definição e o esclarecimento das normas de comportamento do Estado no espaço cibernético, se amplamente compartilhados, reduziriam as ambiguidades e evitariam percepções errôneas. Ao combinar isso com os esforços globais para a resiliência cibernética mediante

o desenvolvimento de capacidades, um regime poderia proporcionar influência forte o suficiente para alterar as percepções de custo-benefício, desencorajando as operações cibernéticas maliciosas patrocinadas pelo Estado e favorecendo a estabilidade na dimensão digital.

Entretanto, um regime global de segurança cibernética enfrentaria limitações significativas. Para que ele contribua para a paz e a segurança internacionais, é necessário avaliar o quão viável e eficaz ele seria. Além dos desafios enfrentados pelos regimes em geral, um regime de segurança cibernética encontraria novas camadas de dificuldades para seu estabelecimento e funcionamento, tanto técnicas quanto políticas. Essas dificuldades serão exploradas no Capítulo 3, "Viabilidade de um regime". Este capítulo argumentará que, apesar de sua magnitude, elas não são intransponíveis e foram abordadas, com certo grau de sucesso, pela comunidade internacional. Embora o surgimento de um regime global de segurança cibernética não seja inevitável e exija ainda mais esforços significativos, a Assembleia Geral da ONU (AGNU) já deu passos importantes nessa direção.

1. Desafios da segurança cibernética

Este capítulo apresentará, primeiramente, os desafios internacionais derivados do espaço cibernético e, em seguida, fará uma revisão da perspectiva institucionalista liberal sobre a teoria do regime. Ele delineará a estrutura teórica para os próximos capítulos, fornecendo o pano de fundo para avaliar a questão principal desta dissertação.

Segurança internacional e espaço cibernético

Esta seção analisará brevemente a natureza do espaço cibernético, pois ele se distingue dos domínios "tradicionais" da rivalidade geopolítica. Com essa finalidade, ela apresentará uma definição e um contexto do espaço e do poder cibernéticos, além de avaliar como estes afetam o ambiente de segurança internacional.

Definição e contexto

Para os fins deste trabalho, o espaço cibernético será entendido como o domínio virtual criado pelo homem e formado por três camadas mutuamente dependentes: física (*hardware* e infraestrutura associada); lógica (dados, *software* e protocolos); e cognitiva/social (relacionada à interação de usuários

humanos). Esta dissertação usará o termo "espaço cibernético" como sinônimo de "ambiente de tecnologia da informação e comunicação (TIC)".

Como todos os sistemas humanos (financeiro, de comunicação, militar e assim por diante) passam a depender da disponibilidade constante de infraestrutura digital e *software*, as operações cibernéticas maliciosas poderiam, em princípio, interromper qualquer sistema cibernético em qualquer lugar. Nesse sentido, um "laptop pode produzir consequências globais" (Kissinger, 2014, p. 345). Embora o incidente da CrowdStrike mencionado na Introdução não tenha sido intencional, vários outros demonstraram a capacidade das operações cibernéticas maliciosas de infligir danos significativos, inclusive com objetivos políticos.

Há dois marcos particularmente ilustrativos. No final de 2009, o malware "Stuxnet" afetou as centrífugas da usina de enriquecimento nuclear iraniana em Natanz e causou um grave retrocesso no programa nuclear do país (Kello, 2013, p. 19-20). No final de abril de 2022, a Costa Rica tornou-se o primeiro país a declarar estado de emergência após ataques cibernéticos em massa que desativaram vários serviços nacionais essenciais. Os responsáveis pelos ataques pediram a derrubada do governo federal (Burgess, 2022). Esses e outros incidentes demonstraram que o espaço cibernético se tornou uma dimensão do conflito internacional (Clarke e Knake, 2010, p. 6-30).

As possibilidades de ações maliciosas no espaço cibernético, ou a partir dele, através de suas múltiplas camadas, abriram caminhos sem precedentes para a condução de rivalidades geopolíticas interestaduais. Esse é um resultado direto das principais características dessa dimensão: anonimato e opacidade (e consequente negação das operações); intangibilidade das capacidades; supressão virtual de distâncias e tempo; e alcance global (Betz e Stevens, 2011, p. 9-10). O espaço cibernético oferece um conjunto de possibilidades para ações hostis, incluindo espionagem, monitoramento, subversão, interrupção e sabotagem (Belk e Noyes, 2012, p. 5).

Diferentes estudiosos consideram as capacidades cibernéticas dos Estados como "alavancas estratégicas", dada a sua capacidade de aumentar os instrumentos convencionais de poder (Nye, 2011, p. 123; Sheldon, 2011, p. 104; Kissinger, Schmidt e Huttenlocher, 2021, p. 150). Essas capacidades tornam-se, elas próprias, recursos de poder (Nye, 2011, p. 123), que podem ser instrumentalizados para manipular o ambiente de segurança e produzir "resultados preferenciais" dentro ou fora do espaço cibernético (Nye, 2014, p. 5).

Ambiente de segurança

As rivalidades geopolíticas estão mudando da dimensão cinética para a virtual (Kissinger, 2014, p. 347), e os Estados reconheceram que as ferramentas cibernéticas podem ameaçar sua segurança. O Conceito Estratégico da OTAN de 2022 afirma que "[o] espaço cibernético é contestado em todos os momentos" (OTAN, 2022, p. 5), o que pode fazer com que os membros da Aliança recorram ao Artigo 5 do Tratado da OTAN (*ibid*., p. 7). Os Estados membros da ONU expressaram preocupação com relação ao desenvolvimento de capacidades cibernéticas "para fins militares" e seu possível uso em conflitos futuros, reconhecendo que as ameaças provenientes do espaço cibernético podem ser uma fonte de volatilidade internacional (Assembleia Geral das Nações Unidas, A/RES/75/240, 2020). O último deriva dos desafios de defesa e ataque que o espaço cibernético gera, que alteram os cálculos estratégicos dos Estados.

Desafios de defesa

As premissas de defesa contra ataques cibernéticos são muito diferentes daquelas contra ataques cinéticos. As operações virtuais ofensivas são imprevisíveis, e o defensor pode não estar ciente das vulnerabilidades que poderiam ser exploradas pelas capacidades cibernéticas intangíveis e desconhecidas dos rivais (Kello, 2017, p. 68-69). Há um alto grau de incerteza com relação à identidade do invasor (*ibid*., p. 129-130). Por fim, o conflito cibernético é marcado por uma mudança crucial de paradigma, da defesa territorial contra invasão para a suposição de que o inimigo cibernético já está instalado, sem ser detectado (*ibid*., p. 6).

Outro desafio central diz respeito ao problema do limite. Há uma falta de referência sobre quando um ataque cibernético equivaleria a um ataque cinético. Assim, os invasores podem se envolver em uma série de agressões cibernéticas de baixo nível, testando as reações de um defensor e colhendo benefícios enquanto tentam evitar o desencadeamento de uma resposta importante (Mazarr, 2018, p. 10; Kello, 2022, p. 13).

Desafios relacionados às operações onfensivas no espaço cibernético

Nesse cenário, alguns estados estabeleceram políticas de "ataque preventivo". Os Estados Unidos, por exemplo, reconhecem que têm "interrompido ativamente a atividade cibernética maliciosa antes que ela possa afetar a pátria dos EUA" (United States of America, 2023, p. 1). Os ataques preventivos também podem buscar garantir que, em uma situação futura de hostilidade aberta, um estado será capaz de penetrar e interromper os sistemas digitais de um rival (Andres, 2012, p. 94-95).

Essas políticas, no entanto, aumentam o espaço para erros, acidentes e escalonamento inadvertido, enquanto as reações e contrarreações digitais rápidas ou automáticas podem desacelerar as oportunidades de redução de escalonamento (Eilstrup-Sangiovanni, 2018, p. 387). Além disso, as atividades cibernéticas maliciosas que visam à futura interrupção de um sistema digital podem desativá-lo imediatamente, e os malwares podem se espalhar mais do que o planejado originalmente (Andres, 2012, p. 94-95). Essas políticas preventivas também contribuem para um cenário maior de volatilidade sistêmica, pois contornam o direito internacional, que disciplina e limita o uso da força a casos muito específicos[2].

Panorama estratégico

Desafios como esses geram problemas significativos para avaliações estratégicas e dinâmicas de equilíbrio de poder. Se antes o poder de uma nação podia ser avaliado por uma combinação de fatores como população, solidez econômica e equipamento militar (Kissinger, 2014, p. 344), os cálculos de poder relativo hoje são complicados pela falta de transparência das capacidades cibernéticas (Eilstrup-Sangiovanni, 2018, p. 390). Como Kissinger, Schmidt e Huttenlocher alertam, "quando o cálculo do equilíbrio se torna incerto, ou quando as nações chegam a cálculos fundamentalmente diferentes de poder relativo, o risco de conflito por erro de cálculo atinge seu auge" (Kissinger, Schmidt e Huttenlocher, 2021, p. 151).

Tal volatilidade é acompanhada pela indefinição da fronteira entre guerra e paz no espaço cibernético. Kello cunhou o termo "unpeace" para caracterizar esse estado de coisas. Ele o define como uma "rivalidade de espectro médio que se encontra abaixo do limiar fisicamente destrutivo da violência interestatal, mas cujos efeitos prejudiciais ultrapassam muito o nível tolerável de competição em tempos de paz e, possivelmente, até mesmo de guerra" (Kello, 2017, p. 78).

Enquanto o espaço cibernético se torna "estrategicamente indispensável" (Kissinger, 2014, p. 346), há uma grave falta de compreensão não apenas em relação às "regras do jogo" da rivalidade cibernética (Hurwitz, 2013-2014, p. 21-22), mas, principalmente, em relação à mudança do próprio cenário de segurança internacional (Kissinger, 2014, p. 344). Esse cenário priva os Estados das suposições e referências comuns necessárias para conduzir um conflito contido (Kello, 2013, p. 31).

2 Ver, por exemplo, os arts. 2.4 e 51 da Carta da ONU.

Como lidar com essa nova realidade? A teoria do regime argumenta, entre outros pontos, que os Estados podem, por meio de instituições internacionais, conseguir reduzir a incerteza e as percepções de vulnerabilidade. A literatura acadêmica sobre isso será abordada na próxima parte deste capítulo.

Teoria do regime

Os defensores dos regimes internacionais argumentam que os Estados podem se beneficiar mutuamente das instituições. Esta dissertação aplicará esse argumento ao espaço cibernético para avaliar até que ponto um regime global poderia enfrentar os desafios que surgem dessa nova dimensão da rivalidade interestatal.

Com esse intuito, esta seção (1) explicará brevemente o foco teórico desta dissertação; (2) analisará a principal literatura sobre regimes internacionais; e (3) apresentará a aplicação das premissas da teoria do regime ao espaço cibernético, que será mais explorada nos próximos capítulos.

Foco teórico

Estados. Embora os atores não estatais também possam empregar ferramentas virtuais para infligir danos consideráveis na dimensão cibernética e a partir da mesma, esta dissertação se concentrará nos Estados que (ainda) são os principais atores na estrutura de segurança internacional, inclusive no espaço cibernético (Goodman, 2010, p. 105).

Institucionalismo liberal. A teoria do regime pressupõe que o conflito interestatal não é inevitável. Essa visão é mais bem desenvolvida pela escola do institucionalismo liberal das Relações Internacionais (RI), que será aplicada neste trabalho. Uma abordagem alternativa seria adotar a perspectiva construtivista da formação de normas e da influência no comportamento do Estado (Fazal, 2024). No entanto, o desenvolvimento das chamadas "normas de comportamento responsável do Estado no espaço cibernético"[3] deriva das negociações dos Estados e se concentra nas ameaças às capacidades materiais destes, especialmente à infraestrutura crítica. Além disso, a natureza opaca do espaço cibernético acrescenta uma camada extra de dificuldade na observação da formação de normas por meio da interação social, bem como na forma como elas podem realmente afetar o comportamento do Estado (Checkel, 1998, p. 340). Embora essas dificuldades também imponham desafios à perspectiva do institucionalismo liberal sobre a formação de regimes, a escolha de adotar essa abordagem deriva do material fértil fornecido pelas discussões da AGNU

3 Adotado oficialmente pela Resolução 71/28 da AGNU (dezembro de 2016).

sobre essas mesmas normas e sobre um futuro mecanismo permanente e universal dedicado à segurança cibernética.

Regime de segurança cibernética "global". A palavra "global" foi escolhida para enfatizar a universalidade em termos de adesão e alcance de tal regime, em oposição a outros mais limitados que também são internacionais (por exemplo, regionais, inter-regionais, etc.). Crucialmente, isso indica a necessidade de ter estados rivais interagindo sob regras e procedimentos mutuamente acordados.

Institucionalismo liberal e críticas

Krasner define regimes como "conjuntos de princípios, normas, regras e procedimentos decisórios implícitos ou explícitos em torno dos quais as expectativas dos atores convergem em uma determinada área das relações internacionais" (Krasner, 1982, p. 186). Para Keohane, os Estados seguem esses princípios, normas, regras e procedimentos, abdicando de parte de sua liberdade de ação, porque esperam obter ganhos mútuos, mesmo na ausência de uma autoridade superior para supervisionar ou garantir a conformidade com o regime (Keohane, 1982, p. 332). Os regimes são benéficos porque fornecem uma estrutura para reduzir os custos de transação, criando "um ambiente institucional mais favorável para a cooperação do que existiria de outra forma", facilitando assim as negociações e legitimando as ações do Estado (Krasner, 1982, p. 334-338; Keohane, 1984, p. 244; Nye, 2014, p. 5). De acordo com Nye, os Estados já obtêm benefícios das normas existentes no âmbito digital, que, por exemplo, sustentam o funcionamento da Internet (Nye, 2014, p. 5-7).

A visão do institucionalismo liberal sobre os regimes está longe de ser consensual. Susan Strange afirma que os regimes internacionais tendem a servir como "instrumentos da estratégia estrutural e da política externa do Estado ou Estados dominantes" (Strange, 1982, p. 484), de tal forma que as lentes do regime são "tendenciosas para o *status quo*" (*ibid*., p. 488). Na mesma linha, Mearsheimer afirma que Estados poderosos podem apoiar a construção de regimes, mas somente para manter ou aumentar seu próprio poder (Mearsheimer, 1994-1995, p. 13). Ademais, ele destaca a incerteza derivada da possibilidade de burlar as regras e normas estabelecidas (*ibid*.).

Mesmo os defensores dos regimes reconhecem os limites e os desafios enfrentados pelos regimes internacionais. Keohane aponta, por exemplo, sua fragilidade quando em comparação com as regras e normas nacionais. Isso se deve à natureza descentralizada, anárquica e de autoajuda do sistema internacional (Keohane, 1984, p. 62). Embora esse reconhecimento seja

convergente com alguns dos argumentos levantados pelos críticos dos regimes, os institucionalistas liberais enfatizam que a teoria do regime não desconsidera "poder e interesses" nem pretende "constituir uma panaceia para conflitos violentos". Em vez disso, seu objetivo é esclarecer quando e como os regimes podem afetar o comportamento do Estado (Keohane e Martin, 1995, p. 50). Um exemplo é o fornecimento de informações de alta qualidade que, entre outras coisas, reduziriam a incerteza ao desencorajar fraudes e a desconfiança mútua (*ibid*., p. 49).

Regimes e paz e segurança internacionais

Os regimes poderiam contribuir para a estabilidade do sistema internacional, por exemplo, evitando o chamado "dilema da segurança", uma circunstância dinâmica em que a melhoria da segurança de uma nação é percebida como uma ameaça por um rival. Essa percepção de vulnerabilidade deriva da incerteza em relação às intenções de um Estado quanto a outros em um sistema anárquico.

Uma situação de dilema de segurança pode resultar em uma corrida armamentista e em uma intensificação descontrolada (Jervis, 1978, p. 169--170). Jervis adverte que "a concorrência desenfreada pode prejudicar todos os atores", pois "as ações individualistas não são apenas caras, mas também perigosas" (Jervis, 1982, p. 358). O espaço cibernético está sujeito aos mesmos riscos. Kissinger alerta contra a "natureza autodestrutiva da conduta nacional irrestrita" nesse domínio (Kissinger, 2014, p. 346). Para ele, "na ausência de alguma articulação de limites e de um acordo sobre regras mútuas de restrição, é provável que surja uma situação de crise, mesmo que não intencional" (*ibid*.).

O estabelecimento de qualquer regime, no entanto, é um esforço complexo. Jervis examinou essas dificuldades no campo da segurança, agravadas pelo dilema da segurança. Em sua opinião, isso faz com que os regimes de segurança internacional sejam tanto desejável (dados os riscos de ações individuais e reações resultantes) quanto difíceis (uma vez que "o medo de que o outro esteja violando ou venha a violar o entendimento comum é um forte incentivo para que cada Estado ataque por conta própria, mesmo que prefira que o regime prospere") (Jervis, 1982, p. 358). Os próximos capítulos abordarão essas características (conveniência e dificuldade) relacionadas a um possível regime de segurança cibernética.

Conclusão parcial

Este capítulo definiu e contextualizou o espaço cibernético como um domínio de rivalidade interestatal, propenso a dinâmicas voláteis sem precedentes que podem resultar em riscos à paz e à segurança internacionais. Embora os ataques cibernéticos tenham demonstrado o quanto podem ser prejudiciais, faltam padrões para que os Estados avaliem tanto a alteração do ambiente estratégico quanto as regras do jogo da rivalidade cibernética.

Por sua vez, os institucionalistas liberais apontaram como os regimes podem ser de benefício mútuo para os Estados, evitando a dinâmica do dilema de segurança, por exemplo, estabelecendo normas e promovendo a convergência do comportamento esperado. Para esses estudiosos, embora os regimes de segurança não sejam uma panaceia, eles apoiam a estabilidade e podem evitar conflitos internacionais violentos.

Os próximos capítulos aplicarão essa visão à dimensão cibernética. Seguindo a avaliação de Jervis sobre os regimes de segurança como sendo desejáveis e difíceis, eles avaliarão a conveniência (Capítulo 2) e a viabilidade (Capítulo 3) de estabelecer um regime global de segurança cibernética.

2. Regime desejável

Este capítulo será dividido em duas seções. Primeiro, tratará das principais abordagens nacionais contra as ameaças cibernéticas e seus impactos na segurança internacional. Em seguida, avaliará como um regime global poderia contribuir para a segurança cibernética internacional, apontando o que constituiria seus pilares centrais. Esta segunda seção argumentará que um regime global poderia aumentar com sucesso a segurança cibernética sistêmica, evitando as deficiências das opções ofensivas. Também serão consideradas algumas limitações de tal regime.

Abordagens domésticas

Os estudiosos apontam diferentes opções para tratar das ameaças cibernéticas à paz e à segurança internacionais. Embora algumas políticas e estratégias nacionais possam lidar com essas ameaças, algumas delas podem incitar a desconfiança e a rivalidade dentro e através do espaço cibernético, sendo elas próprias uma fonte de instabilidade sistêmica.

Ao avaliar os desafios impostos pelas operações cibernéticas hostis patrocinadas pelo Estado abaixo do limiar da guerra, Kello afirma que as

possíveis soluções "devem ser encontradas não essencialmente nas leis e normas atuais, mas em [...] descobrir como responder à atividade – a fim de impedir sua recorrência" (Kello, 2022, p. 16). Ele argumenta que a atual estrutura internacional de normas não conseguiu impedir a rivalidade entre os Estados no espaço cibernético e pede que os países ocidentais desenvolvam uma "nova doutrina" que evite colocar "a ordem internacional à mercê dos atores mais ansiosos para desafiá-la" (*ibid*., p. 25).

Essa visão converge com argumentos que apoiam o fortalecimento da dissuasão cibernética, especialmente com políticas retaliatórias unilaterais (ou "dissuasão por punição"). A OTAN, por exemplo, tem uma política desse tipo em vigor que abrange, e potencialmente atravessa, todas as dimensões estratégicas, inclusive o espaço cibernético (OTAN, 2022, p. 6). Entretanto, a dissuasão por punição envolve desafios significativos, inclusive a necessidade de um Estado ter a capacidade e a vontade de retaliar os agressores (Mazarr, 2018, p. 10). Essa abordagem é particularmente complicada pela natureza opaca das operações cibernéticas e as dificuldades resultantes da descoberta dos autores por trás delas. Até mesmo Kello admite que o problema de atribuição "enfraquece a dissuasão ao reduzir as expectativas de um agressor quanto a penalidades inaceitáveis" (Kello, 2013, p. 33). Além disso, as políticas de dissuasão por meio de punição podem alimentar a rivalidade geopolítica e gerar dinâmicas de escalada, devido aos limites pouco nítidos entre operações defensivas e ofensivas, à falta de clareza sobre o que constituiria uma retaliação proporcional e à determinação de alguns países de punir em todos os domínios (OTAN, 2022, p. 6). Como adverte Mazarr, "as estratégias de dissuasão baseadas em ameaças podem dar tragicamente errado e provocar os exatos conflitos que se pretende evitar" (Mazarr, 2018, p. 5).

Por sua vez, a "dissuasão por negação" difere profundamente de sua prima retaliatória. Como visto, os ataques cibernéticos tendem a ser imprevisíveis e indetectáveis. Conforme demonstrado por Stuxnet, um malware pode entrar em um sistema digital independentemente de suas defesas e isolamento (Clarke e Knake, 2010, p. 292; Kello, 2017, p. 197-198). Isso não quer dizer que a dissuasão por negação não tenha valor. O Stuxnet também demonstrou que infectar um sistema complexo e bem protegido exige um nível de recursos disponível apenas para um número limitado de atores internacionais. As políticas de negação que visam a aumentar a taxa de fugacidade de possíveis ataques são, portanto, valiosas (Goodman, 2010, p. 106). Elas estão diretamente relacionadas à resiliência do sistema e dependem da disponibilidade de recursos de defesa, incluindo habilidades humanas, da vítima em potencial (Nye, 2016-2017, p. 56-57). Apesar de serem imperfeitas e incertas, as políticas de

negação evitam as deficiências sistêmicas derivadas das abordagens ofensivas, inclusive as "preventivas" (Capítulo 1). Pelo contrário, as primeiras trazem benefícios sistêmicos, já que os ataques cibernéticos podem ter ramificações internacionais (Kello, 2017, p. 6). Por esse motivo, as políticas de negação são um elemento fundamental em um regime global de segurança cibernética.

Isoladamente, essas abordagens domésticas só podem ter resultados limitados, de acordo com Nye. Para serem eficazes, elas precisariam ser complementadas com uma estrutura internacional de várias camadas destinada a impedir ações cibernéticas maliciosas (Nye, 2016-2017, p. 62). Nesse sentido, a próxima seção avaliará as mais importantes dessas camadas, que constituiriam os principais pilares de um regime global de segurança cibernética.

Contribuições de um regime global

Outros estudiosos concordam com Nye no sentido de que uma estrutura internacional de políticas e estratégias em várias camadas poderia combater com eficácia as ameaças sistêmicas à paz e à segurança decorrentes do espaço cibernético (Goodman, 2010, p. 109; Mazarr, 2018, p. 11). Da mesma forma, esta dissertação argumentará que a combinação de normas globais, políticas de capacitação e a alteração resultante das percepções de custo-benefício das operações cibernéticas maliciosas poderiam criar uma arquitetura de incentivos influente o suficiente para moldar o comportamento dos Estados e manter a estabilidade no espaço cibernético.

Normas globais

O estabelecimento de um regime global de segurança cibernética, conforme definido por Krasner (Capítulo 1), exigiria que os Estados concordassem com as "regras do jogo" em torno de expectativas convergentes.

O estabelecimento de limites claros para o comportamento do Estado permitiria uma rivalidade geopolítica contida no domínio digital (Eilstrup-Sangiovanni, 2018, p. 383-384), evitando, por exemplo, políticas unilaterais que correm o risco de atrair "o caos na determinação de uma resposta adequada a ataques cibernéticos" ou atrair "adversários para sondar" participando de operações ofensivas abaixo do limiar da guerra (Patrick, 2018).

Fundamentalmente, as ameaças sistêmicas decorrentes da natureza do espaço cibernético exigem um esforço global para estabelecer regras do jogo que sejam amplamente compartilhadas. Embora iniciativas internacionais restritas possam ser valiosas para aumentar a conscientização e iniciar discussões sobre questões complexas específicas, elas não têm, por definição, universalidade, e

apresentam uma lacuna de legitimidade inerente. Elas correm o risco de alienar os principais participantes e alimentar a rivalidade e a desconfiança geopolíticas já existentes. Um exemplo recente é o chamado "Processo de Pall Mall", focado em "combater a proliferação e o uso irresponsável de recursos comerciais de intrusão cibernética" (Reino Unido, 2024). Segundo a declaração conjunta aprovada em sua primeira reunião, os parceiros do Pall Mall "participariam de um diálogo contínuo e globalmente inclusivo, complementar a outras iniciativas multilaterais". Isso ainda não foi confirmado, já que a lista de participantes é formada principalmente por estados ocidentais desenvolvidos e entidades não governamentais.

Por outro lado, os esforços para estabelecer normas de segurança cibernética devem ter como objetivo minimizar a ambiguidade globalmente, se quiserem reduzir os riscos de percepções e cálculos equivocados (Hurwitz, 2013-2014, p. 20-21). A comunidade internacional deu passos importantes nessa direção. Em 2015, a AGNU endossou uma estrutura de "Normas, regras e princípios para o comportamento responsável dos Estados" (Assembleia Geral das Nações Unidas, A/70/174, 2015) e, em 2021, essas normas foram desenvolvidas (Assembleia Geral das Nações Unidas, A/76/135, 2021). Embora não seja vinculativa, a estrutura foi endossada por consenso[4], conferindo-lhe um peso político significativo.

Apesar dessa conquista, ainda há muito a ser feito em relação à ambiguidade no espaço cibernético. Há uma falta fundamental de entendimento comum até mesmo sobre como as regras internacionais obrigatórias já em vigor se aplicam a esse domínio. Alguns países têm publicado posições unilaterais sobre essa questão, mas as perspectivas nacionais ainda são muito amplas e vagas. Os EUA, por exemplo, afirmaram que o direito à autodefesa pode ser acionado "por atividades cibernéticas que equivalem a um [...] ataque armado", sem nenhuma referência sobre como chegar a essa conclusão (Assembleia Geral das Nações Unidas, A/76/136, 2021, p. 137). Nesse contexto, o Brasil recomendou a "atualização [do] entendimento multilateral sobre quais atos equivalem ao uso da força e à agressão, de modo a incluir casos de ataques cibernéticos" (*ibid*., p. 19).

Uma ambiguidade central está relacionada à relação entre o princípio da soberania e a natureza estratificada e transfronteiriça do espaço cibernético. Para Israel, embora "os Estados ocasionalmente realizem atividades cibernéticas que transitam e têm como alvo redes e computadores localizados em outros Estados [...] de acordo com o direito internacional, não está claro se esse tipo

4 Os documentos foram endossados pelas Resoluções 70/237 e 76/19 da AGNU, respectivamente.

de ação é uma violação da regra da soberania territorial" (Schöndorf, 2021, p. 403).

A controvérsia vai além. Os Estados diferem em seu entendimento sobre o próprio conceito de soberania em relação ao espaço cibernético. Essa questão divide até mesmo os aliados da OTAN. Para o Reino Unido, "o conceito geral de soberania por si só [não fornece] uma base suficiente ou clara para extrapolar uma regra específica ou uma proibição adicional para a conduta cibernética que vá além da não intervenção" (Assembleia Geral das Nações Unidas, A/76/136, 2021, p. 117). Por sua vez, o Canadá considera que "[é] axiomático que o princípio da soberania se aplique no espaço cibernético, assim como em qualquer outro lugar" (Canadá, 2024).

Em tese, para que os Estados evitem percepções errôneas, erros de cálculo e volatilidade no espaço cibernético, é necessário considerar bases comuns e estabelecer normas globais para suas operações, especialmente no que diz respeito aos conceitos e princípios básicos que sustentam as relações interestatais pelo menos desde os tratados da Vestefália. A comunidade internacional reconheceu, pelo menos desde 2010, que "a ausência de um entendimento comum em relação ao comportamento aceitável do Estado pode criar o risco de instabilidade e percepção errônea" (Assembleia Geral das Nações Unidas, A/65/10, 2021, par. 7).

Desenvolvimento de capacidade

O desenvolvimento de capacidades é fundamental para a resiliência cibernética nacional e geral. "Capacidade", nesse contexto, está relacionada à maturidade institucional, bem como à disponibilidade de recursos nacionais adequados, incluindo uma força de trabalho qualificada, para se preparar e responder a incidentes cibernéticos (Hurel, 2022, p. 70). A capacidade nacional tem influência direta sobre a segurança cibernética coletiva devido à possível natureza transfronteiriça dos incidentes, em especial os riscos para as cadeias de suprimentos transnacionais. O incidente CrowdStrike de meados de 2024 (Introdução) é uma evidência desses riscos globais.

A comunidade internacional reconhece a importância do desenvolvimento de capacidades para a segurança cibernética. O Grupo de Trabalho Aberto (OEWG) em andamento sobre segurança das tecnologias de informação e comunicação e seu uso, encarregado pela AGNU de abordar os desafios da segurança cibernética (Assembleia Geral das Nações Unidas, A/RES/75/240, 2020, par. 1), reafirmou recentemente que a capacitação é transversal a diferentes desafios do espaço cibernético e contribui para a construção de

uma ciberdimensão segura e pacífica (Assembleia Geral das Nações Unidas, A/79/214, 2024, p. 6).

Algumas iniciativas regionais ilustram os esforços internacionais para promover o desenvolvimento de capacidades e a resiliência coletiva. O "CSIRTAmericas", da Organização dos Estados Americanos (OEA), oferece a seus membros uma plataforma para troca de informações, assistência técnica e treinamento para especialistas, ajudando os países a melhorar sua preparação institucional contra ameaças cibernéticas (Organização dos Estados Americanos, 2024). O "Centro de Excelência em Segurança Cibernética ASEAN-Singapura" (ASCCE) realiza atividades de pesquisa e treinamento, facilitando a comunicação e o compartilhamento de experiências e informações relacionadas a ameaças cibernéticas e melhores práticas (Cyber Security Agency of Singapore, 2021).

As experiências regionais poderiam inspirar um mecanismo de resiliência multilateral. Algumas medidas já foram tomadas nessa direção. O OEWG aprovou, em 2023, princípios para orientar as atividades internacionais de capacitação (Assembleia Geral das Nações Unidas, A/78/265, 2023, anexo C). Em maio de 2024, ele convocou uma primeira reunião global de alto nível sobre capacitação na sede da ONU. Diferentes partes interessadas tiveram a oportunidade de compartilhar opiniões sobre formas de mobilizar e otimizar o uso de recursos para ações internacionais sustentáveis de capacitação (United Nations Institute for Disarmament Research, 2024, p. 17). Por fim, em 2022, a AGNU estabeleceu um "Diretório Global de Pontos de Contato Intergovernamentais sobre o Uso de TICs no Contexto da Segurança Internacional" (Escritório das Nações Unidas para Assuntos de Desarmamento, 2024). O Diretório tem como objetivo facilitar a coordenação e a comunicação entre os estados e oferecer uma plataforma para atividades futuras, incluindo as de capacitação. Ele pode se tornar um primeiro passo institucional em direção a um mecanismo focado em aproveitar, fomentar e dar coerência a diferentes ações internacionais de capacitação. Fundamentalmente, esses desenvolvimentos mostram como as instituições internacionais podem facilitar as negociações e a cooperação interestaduais, conforme enfatizado por Keohane (Capítulo 1).

Paralelamente ao estabelecimento de normas cibernéticas universais, os esforços globais de capacitação poderiam ajudar a reduzir os ganhos esperados de operações maliciosas, ao mesmo tempo em que aumentam seus custos. Essa alteração da percepção de custo-benefício é o terceiro pilar de um regime global eficaz de segurança cibernética.

Percepções sobre custo-benefício

Conforme reconhecido por alguns Estados (Estados Unidos da América, 2023, p. 2) e acadêmicos (Nye, 2016-2017, p. 53; Eilstrup-Sangiovanni, 2018, p. 387; Goodman, 2010, p. 107-108), as percepções influenciam o cálculo de custo-benefício e o comportamento no espaço cibernético. Esse é um aspecto psicológico fundamental influenciado pelos regimes internacionais (Capítulo 1). Derivado do estabelecimento de normas e esforços de capacitação, um regime global de segurança cibernética bem-sucedido alteraria as percepções de custo-benefício de pelo menos duas maneiras.

Primeiro, estabelecer normas e regras claras, globais e legítimas sobre o que é inaceitável, sobre como identificar transgressores e quando e como responder coletivamente aos agressores aumentaria significativamente o custo da fraude. A definição de limites poderia proteger determinados sistemas críticos e criar tabus (Nye, 2016-2017, p. 60-61). Por sua vez, a institucionalização de procedimentos para identificar coletivamente os transgressores e responder a operações maliciosas poderia desencorajar a retaliação unilateral, inclusive ações ofensivas que possam ser consideradas ilegítimas, desproporcionais ou contra o alvo errado (como nos casos de atribuição errônea). Pelo contrário, um regime canalizaria as principais violações para os órgãos multilaterais estabelecidos que têm a legitimidade para resolvê-las em nome da comunidade internacional. O estatuto da Agência Internacional de Energia Atômica (AIEA), por exemplo, determina, entre outras medidas, que a não conformidade ou questões de especial gravidade sejam levadas ao conhecimento do Conselho de Segurança da ONU e da Assembleia Geral (Agência Internacional de Energia Atômica, 1956, art. XII.c).

Uma estrutura clara e amplamente aceita de normas cibernéticas apoiaria o direito internacional em geral, incluindo as regras de autodefesa consagradas na Carta das Nações Unidas (artigos 2.4 e 51). Isso poderia ter um efeito de reforço na própria estrutura das normas cibernéticas, fortalecendo os incentivos contra ações maliciosas no/do espaço cibernético. Os possíveis agressores cibernéticos poderiam ser desencorajados, juntamente com a percepção de vulnerabilidade, que está no centro das preocupações de segurança, incluindo a dinâmica do dilema de segurança (Capítulo 1).

Em segundo lugar, um regime poderia apoiar mecanismos oficiais de cooperação internacional com o objetivo de ajudar os países a se prepararem e responderem a operações cibernéticas maliciosas. Isso também reforçaria as políticas nacionais de dissuasão por negação, aumentando a futilidade de possíveis agressões (Nye, 2016-2017, p. 56). Esse apoio também poderia

favorecer a sustentabilidade da transformação digital nos países, que depende da disponibilidade e do funcionamento correto dos sistemas digitais. Isso é essencial não apenas para o seu desenvolvimento humano, mas também para a resiliência sistêmica. Conforme apontado em um relatório recente do Fórum Econômico Mundial, a desigualdade digital é um "impulsionador do risco do ecossistema", uma vez que "a resiliência geral do ecossistema é frequentemente determinada por seus elos mais fracos" (Fórum Econômico Mundial, 2025, p. 29). Portanto, as percepções de custo-benefício, de um ponto de vista sistêmico, dependeriam da elevação da resiliência coletiva.

Limitações

Naturalmente, um regime global de segurança cibernética encararia limitações e desafios significativos.

Em primeiro lugar, deve-se ter em mente as alegações dos realistas de que os regimes dependem da estrutura de poder internacional (Capítulo 1). Um exemplo é a destituição do primeiro diretor-geral da Organização para a Proibição de Armas Químicas, José Bustani, menos de dois anos depois de ter sido renomeado por unanimidade para esse cargo e um ano antes da invasão do Iraque em 2003 (Stanič, 2004, p. 814). Bustani foi considerado um dos "principais obstáculos à guerra porque [ele] estava propondo métodos não violentos para eliminar os supostos estoques de armas de Saddam" (Stanič, 2004, p. 810). Esse caso relembra a advertência feita por Strange de que os regimes são parciais em relação ao *status quo*, mostrando como seus processos internos podem ser obrigados a garanti-lo.

Em segundo lugar, há desafios específicos e significativos relacionados ao estabelecimento e ao funcionamento de um regime global de segurança cibernética. Esses desafios serão explorados no próximo capítulo.

Conclusão parcial

Os realistas apontam para importantes limitações dos regimes internacionais. O caso Bustani é um lembrete pertinente de que os regimes devem ser aperfeiçoados constantemente, inclusive com o objetivo de mitigar, o máximo possível, a interferência da política de poder e das circunstâncias geopolíticas.

Por outro lado, como os institucionalistas liberais apontaram, os regimes não são concebidos para serem uma panaceia. Este capítulo tentou demonstrar que, como o espaço cibernético é propenso a dinâmicas voláteis que podem

ameaçar a paz e a segurança internacionais, há vantagens em buscar um regime global de segurança cibernética.

As opções domésticas podem não apenas ser insuficientes para lidar com as ameaças cibernéticas, mas também alimentar a rivalidade interestatal e a instabilidade internacional, como no caso de políticas preventivas e baseadas em retaliação. Por sua vez, um regime global que combine normas universais e esforços de capacitação poderia ser influente o suficiente para alterar as percepções de custo-benefício e desencorajar a rivalidade interestatal por meio de operações cibernéticas maliciosas.

Um regime global de segurança cibernética poderia contribuir significativamente para a paz e a segurança internacionais e, dessa forma, é considerado desejável. O estabelecimento das normas de comportamento responsável do Estado e as medidas tomadas pela AGNU para promover os esforços internacionais de capacitação são bem-vindos. Entretanto, o possível estabelecimento e funcionamento de um regime global certamente enfrentaria limitações e desafios fundamentais. O próximo capítulo se concentrará nesses aspectos.

3. A viabilidade de um regime

Se um regime global de segurança cibernética é desejável, é necessário abordar os desafios específicos envolvidos em seu estabelecimento e funcionamento. Este capítulo avalia os principais desafios tecnológicos e políticos. Embora sejam expressivos, esta dissertação argumentará que eles não são intransponíveis. O capítulo será encerrado com um relato de experiências recentes que demonstram o atual engajamento da comunidade internacional nessa tarefa.

Desafios do regime

Como Jervis destaca no Capítulo 1, o estabelecimento de regimes de segurança é um esforço complexo e incerto. A natureza do espaço cibernético acrescenta outros desafios, tanto técnicos quanto políticos.

Desafio técnico

Os principais desafios técnicos de um regime de segurança cibernética decorrem da onipresença e da intangibilidade do espaço cibernético. Essas características resultam em dificuldades críticas para definir os limites das operações maliciosas, estabelecer mecanismos de verificação que investiguem e atribuam ataques e induzir a conformidade com as normas de um regime.

Limite. Como visto (Capítulo 2), há uma ambiguidade significativa em relação às regras do jogo no espaço cibernético, inclusive quando as operações cibernéticas podem atingir o nível de um ataque armado. Esse último é particularmente importante, pois é uma condição necessária para acionar a responsabilidade internacional e o direito à autodefesa. Até o momento, a comunidade internacional só conseguiu fornecer normas gerais de comportamento responsável, inclusive a de que um Estado não deve danificar a infraestrutura essencial por meio de operações cibernéticas.[5]

Verificação. Vários regimes de segurança estabeleceram mecanismos de verificação para aumentar a confiança mútua e desestimular a fraude. Um grande desafio que eles enfrentam é a dupla utilização do material que está sob sua alçada. Em 2023, por exemplo, a AIEA aplicou salvaguardas em 189 países para garantir que eles estejam usando material nuclear de dupla utilização de acordo com suas obrigações legais internacionais (Agência Internacional de Energia Atômica, 2024). No entanto, parece improvável que as técnicas e os conhecimentos desenvolvidos pelos regimes de segurança existentes para verificar a conformidade possam fornecer orientação para um regime de segurança cibernética. O armamento de *software*, que não é apenas de uso duplo, mas também intangível (Nye, 2018, p. 336), parece representar um desafio técnico aparentemente intransponível para o estabelecimento de um mecanismo que desencorajaria a fraude (Nye, 2016-2017, p. 50).

Atribuição. Um desafio semelhante é encontrar o culpado por trás dos ataques cibernéticos. Várias características tornam a atribuição cibernética particularmente problemática, incluindo o considerável grau de anonimato; a dificuldade de identificar o ator humano, mesmo tendo encontrado o endereço IP da máquina usada no ataque; e a facilidade com que os malwares cruzam jurisdições (Kello, 2013, p. 33).

Os Estados que investigam ataques cibernéticos empregam capacidades virtuais e aparatos de inteligência não divulgados, além de raramente fornecerem evidências substanciais de suas descobertas. Isso torna a atribuição "um ato inerentemente político" (Egloff, 2019, p. 55). Alguns estudiosos observaram importantes tendências de viés por trás das políticas de atribuição, devido a interesses geopolíticos (Hurel, 2022, p. 79) e a objetivos comerciais (Oosthoek e Doerr, 2021, p. 309). Isso leva à falta de legitimidade e à contestação da atribuição e da retaliação com base na mesma. Além disso, a possibilidade de atribuição errônea pode ser explorada por agentes mal-intencionados (Hurwitz, 2013-2014, p. 20).

5 Norma "f" das normas de comportamento responsável do Estado.

Os Estados reconheceram esses desafios. A estrutura do comportamento responsável do Estado no espaço cibernético destaca que "as acusações de organização e implementação de atos ilícitos apresentadas contra os Estados devem ser fundamentadas" (Assembleia Geral das Nações Unidas, A/76/135, 2021, p. 18). Além disso, o direito consuetudinário internacional define que um ato internacionalmente ilícito de um Estado consiste em uma ação ou omissão que é atribuível ao Estado de acordo com o direito internacional (Comissão de Direito Internacional, 2001, art. 2.a). Uma atribuição precisa contra um Estado exigiria, portanto, a identificação correta de um endereço de IP e do operador, bem como sua conexão com o governo acusado (*ibid*.; Rid, 2013, p. 144-145; Schmitt e Vihul, 2015, p. 45).

Desafios políticos

O principal desafio político é provavelmente a falta de interesse dos Estados em restringir seu próprio comportamento. Essa relutância decorre principalmente da relativa novidade das operações cibernéticas como alavancas de poder e do sigilo por trás das capacidades cibernéticas dos Estados. Como Schmitt e Vihul enfatizam, "os Estados hesitam em restringir o uso de armas [cibernéticas] que podem lhes proporcionar uma vantagem no campo de batalha até que tenham experiência suficiente que lhes permita pesar os custos e os benefícios das proibições e limitações de seu uso" (Schmitt e Vihul, 2015, p. 45). Além disso, embora grande parte do impacto das capacidades cibernéticas derive de sua natureza oculta (Kissinger, 2014, p. 347), qualquer restrição internacional exigiria um acordo sobre algum grau de definição relacionado ao que deve ser restringido.

Não há perspectivas de negociações globais com relação a essas restrições, já que os Estados estão divididos sobre essa questão (Singer e Friedman, 2014, p. 185-186). Embora a Rússia tenha apresentado um projeto para um tratado global de segurança cibernética (Federação Russa, 2021), vários países ocidentais afirmam que não há necessidade de um novo instrumento internacional vinculativo ou que várias medidas devem ser tomadas antes de considerar essa possibilidade (União Europeia, 2023).

É possível traçar paralelos entre esse cenário e o desenvolvimento do regime nuclear internacional, que começou a tomar forma depois que os países mais avançados se sentiram seguros de sua superioridade tecnológica e só então assumiram um papel de liderança para evitar a proliferação descontrolada (Eilstrup-Sangiovanni, 2018, p. 404-405). Como a corrida pelo desenvolvimento das capacidades cibernéticas mais avançadas ainda está em andamento, as

discussões atuais sobre as normas cibernéticas ainda estão subordinadas à rivalidade entre potências internacionais, "em vez de uma busca unificada por ordem normativa, clareza e previsibilidade" (Tikk, 2021, p. 751).

Abordando os desafios identificados

Um regime emergente de segurança cibernética precisaria enfrentar desafios tecnológicos e políticos específicos da área cibernética, para os quais não existem muitos precedentes que sirvam como guia. Como enfatiza Andres, "no caso das ameaças cibernéticas, o passado não é necessariamente um prólogo" (Andres, 2012, p. 90). Além disso, o ritmo acelerado do desenvolvimento tecnológico provavelmente continuará a apresentar dificuldades sem precedentes, razão pela qual "as leis e regulamentações estão sempre perseguindo um alvo em movimento" (Nye, 2014, p. 6). No entanto, como será visto a seguir, há maneiras de enfrentar os desafios atuais, e a comunidade internacional parece já estar fazendo progressos importantes nessa direção.

Abordando os desafios técnicos

Limite

As definições internacionalmente aceitas na área de segurança podem levar um tempo considerável para surgirem. Por exemplo, o "ato de agressão", mencionado no Capítulo VII da Carta das Nações Unidas, foi definido quase três décadas após a entrada em vigor do instrumento (Assembleia Geral das Nações Unidas, A/RES/3314(XXIX), 1974).

Por sua vez, a AGNU já definiu certos limites que os Estados não devem ultrapassar no espaço cibernético. Por exemplo, a norma "f" das normas de comportamento responsável do Estado afirma que um "Estado não deve conduzir ou apoiar conscientemente atividades de TIC [...] que danifiquem intencionalmente infraestruturas críticas [...]". A norma "i" estabelece que "os Estados devem procurar evitar a proliferação de ferramentas e técnicas maliciosas de TIC e o uso de funções ocultas prejudiciais".

A importante nuance entre a Norma "f", que usa uma linguagem negativa e de proibição, e a Norma "i", que incentiva a adoção de determinadas medidas, indica diferentes graus de preocupação na comunidade internacional que poderiam levar a outros acordos comuns sobre onde os limites ou linhas intransponíveis devem ser traçados.

Verificação e atribuição

Como a tecnologia cibernética é inerentemente de dupla utilização e intangível, as atividades de verificação multilateral provavelmente precisariam

se concentrar em ações maliciosas, em vez de em capacidades, proporcionando um monitoramento ex post-facto. Conforme sugerido por Eilstrup-Sangiovanni, o Sistema de Monitoramento Internacional do Tratado de Proibição Completa de Testes Nucleares (CTBT) pode ser uma fonte de inspiração (Eilstrup-Sangiovanni, 2018, p. 395). Apesar de o CTBT não ter entrado em vigor, seu Comitê Preparatório (CTBTO-PrepCom) conseguiu implementar um sistema impressionante com eficiência comprovada, tendo identificado com rapidez e precisão os testes de explosão nuclear da Coreia do Norte (Comprehensive Nuclear-Test-Ban Treaty Organization, 2024).

A experiência no combate aos crimes cibernéticos demonstrou que a atribuição pode não ser "o desafio intransponível que os modelos teóricos sugerem" (Goodman, 2010, p. 105). A aplicação da lei demonstrou que a perícia é essencial para coibir o crime cibernético e processar os criminosos, e que os esforços para obter evidências eletrônicas podem se beneficiar da cooperação internacional (Kello, 2017, p. 199).

No entanto, a perícia digital continua presa na camada lógica do espaço cibernético. Embora a aplicação da lei possa ser capaz de localizar endereços de IP e os infratores por trás deles, a investigação sobre sua possível ligação com os Estados permanece consideravelmente complexa. Para enfrentar esse desafio, alguns especialistas argumentaram a favor do estabelecimento de um mecanismo multilateral de natureza técnica dedicado e responsável pela investigação de ataques cibernéticos (Eilstrup-Sangiovanni, 2018, p. 394-395; Clarke e Knake, 2010, p. 252; Manshu, 2022, p. 31; Chuanying, 2022, p. 48).

Se, como argumenta Nye, "atribuição é uma questão de grau" (Nye, 2016-2017, p. 51), a atribuição coletiva por um órgão multilateral mandatado, em oposição à atribuição unilateral, aumentaria a credibilidade das investigações cibernéticas e de suas descobertas, bem como a legitimidade de impor consequências preestabelecidas para os perpetradores.

Um sistema multilateral de atribuição/verificação de segurança cibernética também poderia apoiar o regime geral de outras maneiras. Em primeiro lugar, ele incluiria todas as medidas bem-sucedidas tomadas para estabelecer normas e limites claros. Em segundo lugar, ele poderia fornecer um mecanismo eficiente para o compartilhamento de informações de qualidade, dos Estados e de suas próprias investigações internas. Em terceiro lugar, poderia estabelecer regras sobre como lidar com casos inconclusivos, especialmente ataques em grande escala contra infraestruturas essenciais, inclusive sobre quando encaminhá-los a órgãos internacionais encarregados de avaliar ameaças à paz e à segurança internacionais. Em quarto lugar, permitiria um processo de aprendizado institucional (Nye, 2016-2017, p. 51), o autoaperfeiçoamento do regime e o

acúmulo de conhecimento especializado. Em quinto lugar, essa experiência poderia ser canalizada para auxiliar os esforços de resiliência cibernética dos países, bem como estimular sinergias com programas de capacitação existentes, economizando recursos e fomentando processos de aprendizagem cruzada.

Abordando os desafios políticos

A experiência das discussões sobre segurança cibernética na ONU demonstra que há pelo menos duas circunstâncias duradouras que poderiam diminuir as resistências políticas: os incentivos sistêmicos existentes e o papel desempenhado pelos "países intermediários".

Incentivos sistêmicos

A informalidade das normas cibernéticas internacionais existentes as torna aceitáveis para os países que atualmente não estão dispostos a se comprometer com regras internacionais obrigatórias (Sukumar *et al.*, 2024, p. 11). O fato de os Estados-membros da ONU terem reconhecido que o direito internacional se aplica ao espaço cibernético – e, portanto, vincula suas atividades cibernéticas – não é prova do contrário, pois essa aplicação ainda é ambígua (Capítulo 2). Como resultado, há uma informalidade de fato em relação às obrigações internacionais que restringem as ações do Estado no espaço cibernético. Esse cenário parece evitar uma forte resistência contra o desenvolvimento da estrutura de normas existente, buscada pelo OEWG. Nesse sentido, a informalidade não é um ponto fraco. Como mostram outras experiências na área de segurança, os regimes podem começar com medidas voluntárias e ganhar impulso em direção a uma institucionalização mais forte das normas de comportamento do Estado (Nye, 2018, p. 337).

Além disso, o potencial cada vez maior de perturbação por armas cibernéticas incentiva regras mais claras do jogo. A norma consensual que proíbe ataques contra infraestruturas críticas é uma evidência de que a comunidade internacional é capaz de concordar com essas regras. Embora informais e não vinculantes, as normas existentes ainda podem exercer uma influência poderosa sobre os Estados (Nye, 2016-2017, p. 61), além de fornecer um modelo para um regime futuro.

"Países intermediários"

Nas discussões sobre segurança cibernética da AGNU, a grande maioria dos Estados está em algum lugar no meio do espectro de interesses e perspectivas que separam os atuais rivais geopolíticos globais. Esses Estados são identificados às vezes como "países intermediários" (Buchan e Devanny, 2024).

Eles desempenham um papel ativo e influente, superando as divisões geopolíticas e apoiando a estabilidade sistêmica baseada na capacitação. Muitos deles se lembram dos dois processos paralelos (e potencialmente conflitantes) estabelecidos entre 2019 e 2021 no âmbito da AGNU com um mandato semelhante para abordar a segurança cibernética. Há um risco de que essa duplicação ocorra novamente depois que o mandato do atual OEWG expirar em meados de 2025. Em 2022 e 2023, a França e a Rússia apresentaram e conseguiram aprovar resoluções concorrentes da AGNU sobre o assunto. Em 2023, alertando contra a divisão e a "duplicação prejudicial de esforços" que esse cenário causa, o Brasil propôs uma moratória sobre tais resoluções, a fim de apoiar o trabalho consensual dentro do OEWG, em particular com relação às negociações sobre o futuro mecanismo que o sucederá (Brasil, 2023). A iniciativa brasileira obteve apoio e, em 2024, uma única resolução sobre segurança cibernética foi apresentada e aprovada pelo Primeiro Comitê da AGNU (United Nations General Assembly, A/RES/79/237, 2024).

Outro exemplo de influência vem de um grupo informal de 14 países latino-americanos, segundo o qual a capacitação é fundamental para enfrentar os desafios gerais da segurança cibernética (ver, a título de exemplo, Argentina, 2021). Esses Estados conseguiram influenciar as discussões do OEWG, afastando-se da suposição de que a segurança cibernética é um fim em si mesma, aproximando-os da visão de que ela é um instrumento para o desenvolvimento sustentável. Como visto no Capítulo 2, a capacitação está agora no centro das considerações de segurança cibernética da ONU.

Evidência empírica

Os relatórios anuais do OEWG refletiram essa influência latino-americana, inclusive dando à capacitação um papel central em um futuro mecanismo permanente de diálogo institucional regular (RID) interestadual de segurança cibernética da AGNU (Assembleia Geral das Nações Unidas, A/79/214, 2024, anexo C, parágrafos 9-10). A negociação desse mecanismo talvez seja a principal evidência empírica da atual disposição dos Estados-membros da ONU em avançar para um regime global de segurança cibernética.

Caso seja aprovado, o mecanismo RID representará um marco importante na estrutura global de abordagem de questões relacionadas ao espaço cibernético e à paz e segurança internacionais. De acordo com o último relatório do OEWG, "os Estados recomendam o estabelecimento do futuro mecanismo permanente" e destacaram sua disposição de "garantir uma transição perfeita do OEWG

para o futuro mecanismo permanente" (Assembleia Geral das Nações Unidas, A/79/214, 2024, par. 58).

Isso é significativo. Primeiro, poderia ser o reconhecimento de que a segurança cibernética merece – ou impõe a necessidade de – um diálogo interestadual ininterrupto, desvinculado de mandatos específicos e com prazo determinado, como nos GGEs e OEWGs anteriores. Em segundo lugar, isso evitaria a renegociação desses novos mandatos. Em terceiro lugar, evitaria a possibilidade de ter, mais uma vez, fóruns paralelos em vigor com um mandato semelhante.

O ritmo atual do processo é digno de nota. Em 2023, os Estados aprovaram um primeiro projeto para esse mecanismo (Assembleia Geral das Nações Unidas, A/79/214, 2024, parágrafos 55-57). Em 2024, ele foi desenvolvido ainda mais, com princípios gerais de orientação, funções e escopo, estrutura, modalidades e um processo de tomada de decisão (Assembleia Geral das Nações Unidas, A/79/214, 2024, anexo C, par. 10). É importante ressaltar que se espera que o mecanismo tenha como foco (1) o desenvolvimento de normas voluntárias e a compreensão de como o direito internacional se aplica ao espaço cibernético; e (2) o desenvolvimento de capacidades, "permitindo que os Estados protejam as TICs e garantam seu uso pacífico" (*ibid*.).

Conclusão parcial

O Capítulo 2 argumentou que um regime global de segurança cibernética é desejável. No entanto, seu possível estabelecimento e funcionamento precisariam ser viáveis. A experiência mostra que os regimes de segurança podem precisar de décadas para surgir e amadurecer. Este capítulo argumentou que, embora os desafios técnicos e políticos sejam significativos, eles não são insuperáveis.

A experiência recente na AGNU é uma prova de que a comunidade internacional está disposta a enfrentar esses desafios. De fato, a discussão de um mecanismo global de RID, no âmbito da AGNU, ganhou impulso, apesar das atuais circunstâncias geopolíticas. Isso se deve, em grande parte, aos incentivos sistêmicos (informalidade da estrutura normativa e urgência em lidar com as ameaças cibernéticas) e ao trabalho do OEWG, em especial dos "países intermediários", que conseguiu fazer um progresso notável por consenso.

Resta saber se o momento atual levará a AGNU a aprovar um mecanismo permanente de RID para substituir o OEWG no final de seu mandato, em meados

de 2025. O cenário geopolítico pode se deteriorar ainda mais, complicando um acordo. Além disso, os desafios técnicos existentes ainda precisam ser enfrentados, juntamente com possíveis novos obstáculos derivados de novos desenvolvimentos tecnológicos.

No entanto, o progresso feito até agora pela comunidade internacional – estabelecendo uma estrutura de normas para o comportamento responsável do Estado e um projeto para um mecanismo de RID - demonstra a viabilidade e o apetite por um regime global de segurança cibernética com o objetivo de promover "um ambiente de TIC aberto, seguro, estável, acessível, pacífico e interoperável" (Assembleia Geral das Nações Unidas, A/79/214, 2024, anexo C, parágrafo 4b).

Conclusão

O objetivo desta dissertação foi trazer a questão "até que ponto um regime global de segurança cibernética poderia contribuir para a paz e a segurança internacionais?" Essa pergunta é relevante porque o espaço cibernético se tornou outro domínio de rivalidade interestatal. Casos anteriores de incidentes cibernéticos demonstraram a ameaça que eles representam, dando origem a desafios de defesa e ataque e alterando o ambiente de segurança internacional. Faltam padrões tanto para os Estados avaliarem a alteração do cenário estratégico quanto para as "regras do jogo" da interação interestatal na dimensão cibernética. Essa situação é propensa a uma dinâmica volátil sem precedentes que pode gerar uma situação de dilema de segurança e uma escalada descontrolada.

Nesse cenário, este trabalho explorou a teoria do regime institucionalista liberal a fim de buscar formas de mitigar a instabilidade internacional decorrente do espaço cibernético. Conscientes do papel que a política de poder desempenha no sistema internacional, seus teóricos enfatizam que, embora os regimes internacionais não sejam uma panaceia, eles ainda têm valor para evitar conflitos internacionais violentos.

Nesse sentido, este trabalho argumentou que um regime global de segurança cibernética é desejável. Uma estrutura de incentivos contra o comportamento malicioso do Estado poderia proporcionar estabilidade sistêmica se fosse baseada em normas amplamente acordadas e em esforços de capacitação destinados a aumentar a resiliência cibernética sistêmica. Esses dois pilares alterariam significativamente as percepções de custo-benefício e desestimulariam as operações cibernéticas maliciosas. Em comparação, as

opções domésticas ofensivas poderiam levar a uma dinâmica de dilema de segurança de movimento, particularmente perigosa devido à opacidade das capacidades cibernéticas e à dependência das sociedades do funcionamento constante e correto dos sistemas digitais.

Esta dissertação também argumentou que um regime global de segurança cibernética é viável. Entretanto, duas limitações não devem ser ignoradas. Primeiro, as críticas dos realistas aos regimes devem ser levadas em conta. A política de poder desempenha um papel central na influência dos sistemas de segurança internacional, sem falar nos regimes de segurança. Como visto, o poder pode influenciar seus mecanismos e superar a legitimidade internacional.

Em segundo lugar, um regime de segurança cibernética enfrentaria importantes desafios técnicos e políticos em seu estabelecimento e funcionamento, derivados da natureza do espaço cibernético. Os obstáculos técnicos exigirão um envolvimento significativo da comunidade internacional para chegar a entendimentos comuns sobre questões complexas, como limites para operações cibernéticas consideradas inaceitáveis e mecanismos globais com legitimidade para investigar incidentes cibernéticos, encontrar culpados e responder a violações. Os obstáculos políticos, como a resistência dos Estados em reduzir sua autonomia, podem ser atenuados por circunstâncias duradouras, como a informalidade da estrutura das normas de comportamento do Estado e o número crescente de ataques cibernéticos e os danos causados por eles. Além disso, a influência dos "países intermediários" poderia ajudar os rivais globais a chegar a acordos sobre questões delicadas e mudar o foco de um possível regime para a resiliência cibernética.

Por fim, este trabalho argumentou que a comunidade internacional, por meio do OEWG/UNGA, deu passos importantes em direção a um regime de segurança cibernética. Em 2015, a estrutura do comportamento responsável do Estado foi estabelecida por consenso. Nos últimos dois anos, esses desenvolvimentos ganharam impulso com a elaboração de um projeto de um mecanismo permanente de RID, dedicado à segurança cibernética, no âmbito da AGNU e aberto a todos os estados-membros da ONU. Adotando a definição de regimes de Krasner, 2025 pode ser um marco crítico no caminho para uma segurança cibernética global.

Em suma, esta dissertação afirma que um regime global de segurança cibernética não só é viável, mas também poderia proporcionar uma influência forte o suficiente para desencorajar operações cibernéticas maliciosas patrocinadas pelo Estado e favorecer a estabilidade no domínio cibernético, contribuindo de forma significativa para a paz e a segurança internacionais.

Outras pesquisas sobre esse tópico podem envolver áreas relacionadas que estão além do escopo deste trabalho. Isso inclui o impacto sobre o cenário internacional das tecnologias emergentes (especialmente inteligência artificial e computação quântica) e seu rápido desenvolvimento, bem como o papel dos atores não estatais, principalmente as big techs. Outros estudos, partindo de diferentes perspectivas de RI, provavelmente contribuirão para a forma como os atuais desenvolvimentos institucionais e as forças por trás deles afetam os fenômenos internacionais.

Bibliography

ANDRES, Richard. The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence. In: REVERON, Derek (ed.). *Cyberspace and National Security:* Threats, Opportunities, and Power in a Virtual World. Washington: Georgetown University Press, 2012, p. 89-104.

ARGENTINA. Capacity Building on Behalf of a Group of LAC Countries. *United Nations Office for Disarmament Affairs*, 2021. Disponível em: <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/JS_Capacity_building_on_behalf_of_a_group_of_LAC_Countries_-_ENGLISH_VERSION.pdf>. Acesso em: 2 maio 2025.

BELK, Robert; NOYES, Matthew. On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy. *Science, Technology, and Public Policy Program*, Belfer Center, mar. 2012.

BETZ, David; STEVENS, Tim. *Cyberspace and the State:* Toward a Strategy for Cyber-Power. London: Routledge, 2011.

BRASIL. *First Committee Statement by the Brazilian Delegation on Cluster 5* – "Other Disarmament Measures and International Security". First Committee of the United Nations General Assembly, 24 out. 2025. Disponível em: <https://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com23/statements/24Oct_Brazil.pdf>. Acesso em: 15 jul. 2025.

BUCHAN, Russell; DEVANNY, Joe. Cyber Diplomacy in the Middle Ground. *Carnegie Endowment for International Peace,* [s.d.]. Disponível em: <https://carnegieendowment.org/programs/technology-and-international-affairs/cyber-diplomacy-in-the-middle-ground>. Acesso em: 22 out. 2024.

BURGESS, Matt. Conti's Attack Against Costa Rica Sparks a New Ransomware Era. *Wired*, 12 jun. 2022. Disponível em: <https://www.wired.com/story/costa-rica-ransomware-conti/>. Acesso em: 2 maio 2025.

CANADA. International Law Applicable in Cyberspace, [s.d.]. Disponível em: <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng>. Acesso em: 28 set. 2024.

CHECKEL, Jeffrey. The Constructive Turn in International Relations Theory. *World Politics*, v. 50, p. 324-348, jan. 1998.

CHUANYING, Lu. A Chinese Perspective on Public Cyber Attribution. In: LEVITE, Ariel *et al*. (ed.). *Managing US-China Tensions Over Public Cyber Attribution*. Washington: Carnegie Endowment for International Peace, 2022, p. 43-63.

CLARKE, Richard; KNAKE, Robert. *Cyber War:* The Next Threat to National Security and What to Do About it. New York: HarperCollins Publishers, 2010.

COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION. *Detecting nuclear tests*, [s.d.]. Disponível em: <https://www.ctbto.org/our-work/detecting-nuclear-tests>. Acesso em: 27 out. 2024.

CYBER SECURITY AGENCY OF SINGAPORE. A*SEAN-Singapore Cybersecurity Centre of Excellence*. Última modificação em 6 out. 2021. Disponível em: <https://www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence>. Acesso em: 2 maio 2025.

EGLOFF, Florian. Contested Public Attributions of Cyber Incidents and the Role of Academia. *Contemporary Security Policy*, v. 41, n. 1, p. 55-81, 2019.

EILSTRUP-SANGIOVANNI, Mette. Why the World Needs an International Cyberwar Convention. *Philosophy & Technology*, v. 31, n. 3, p. 379-407, set. 2018.

UNIÃO EUROPEIA. EU statement – UN Open-Ended Working Group on ICT in International Law. *European External Action Service*, 24 maio 2023. Disponível em: <https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-open-ended-working-group-ict-international-law-1_en>. Acesso em: 2 maio 2025.

FAZAL, Tanisha. The Power of Principles: What Norms are Still Good for. *Foreign Affairs*, jun. 2024. Disponível em: <https://www.foreignaffairs.com/ukraine/power-principles-norms-tanisha-fazal>. Acesso em: 2 maio 2025.

GOODMAN, Will. Cyber Deterrence: Tougher in Theory Than in Practice? *Strategic Studies Quarterly*, v. 4, n. 3, p. 102-135, 2010.

HUREL, Louise. Interrogating the Cybersecurity Development Agenda: A Critical Reflection. *The International Spectator*, v. 57, n. 3, p. 66-84, 2022.

HURWITZ, Roger. Keeping Cool: Steps for Avoiding Conflict and Escalation in Cyberspace. *Georgetown Journal of International Affairs*, p. 17-28, 2013–2014.

INTERNATIONAL ATOMIC ENERGY AGENCY. *Safeguards Implementation Report for 2023*. 7 jun. 2024. Disponível em: <https://www.iaea.org/sites/default/files/24/06/20240607_sir_2024_part_ab.pdf>. Acesso em: 2 maio 2025.

INTERNATIONAL ATOMIC ENERGY AGENCY. *Statute of the International Atomic Energy Agency*. 23 out. 1956. Disponível em: <https://www.iaea.org/sites/default/files/statute.pdf>. Acesso em: 2 maio 2025.

INTERNATIONAL LAW COMMISSION. *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. 2001. Disponível em: <https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf>. Acesso em: 2 maio 2025.

JERVIS, Robert. Cooperation Under the Security Dilemma. *World Politics*, v. 30, n. 2, p. 168-214, jan. 1978.

JERVIS, Robert. Security Regimes. *International Organization*, v. 36, n. 2, p. 357-378, primavera 1982.

KELLO, Lucas. The Meaning of the Cyber Revolution. *International Security*, v. 38, n. 2, p. 7-40, 2013.

KELLO, Lucas. *Striking Back:* The End of Peace in Cyberspace – And How to Restore it. New Haven: Yale University Press, 2022.

KELLO, Lucas. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2017.

KEOHANE, Robert. The Demand for International Regimes. *International Organization*, v. 36, n. 2, p. 325-355, 1982.

KEOHANE, Robert. *After Hegemony*: Cooperation and Discord in the World Political Economy. Princeton: Princeton University Press, 1984.

KEOHANE, Robert; MARTIN, Lisa. The Promise of Institutionalist Theory. *International Security*, v. 20, n. 1, p. 39-51, 1995.

KISSINGER, Henry; SCHMIDT, Eric; HUTTENLOCHER, Daniel. *The Age of AI*: And Our Human Future. New York: Little, Brown and Company, 2021.

KISSINGER, Henry. *World Order*. New York: Penguin Press, 2014.

KRASNER, Stephen. Structural Causes and Regime Consequences: Regimes as Intervening Variables. *International Organization*, v. 36, n. 2, p. 185-205, 1982.

MANSHU, Xu. Beyond Public Cyber Attribution: Reflections and Response. In: LEVITE, Ariel *et al*. (ed.). *Managing US-China Tensions Over Public Cyber Attribution*. Washington, DC: Carnegie Endowment for International Peace, 2022, p. 25-32.

MAZARR, Michael. Understanding Deterrence. *RAND*, 19 abr. 2018. Disponível em: <https://www.rand.org/pubs/perspectives/PE295.html>. Acesso em: 15 jul. 2025.

MEARSHEIMER, John. The False Promise of International Institutions. *International Security*, v. 19, n. 3, p. 5-49, 1994-1995.

NORTH ATLANTIC TREATY ORGANIZATION. *NATO 2022 Strategic Concept*. 29 jun. 2022. Disponível em: <https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf>. Acesso em: 2 maio 2025.

NYE, Joseph. Deterrence and Dissuasion in Cyberspace. *International Security*, v. 41, n. 3, p. 44-71, Winter 2016/2017.

NYE, Joseph. Normative Restraints on Cyber Conflict. *Cyber Security: A Peer--Reviewed Journal*, v. 1, n. 4, p. 331-342, 2018.

NYE, Joseph. The *Regime Complex for Managing Global Cyber Activities*. Global Commission on Internet Governance. London: Chatham House, 2014.

NYE, Joseph. *The Future of Power*. New York: PublicAffairs, 2011.

OOSTHOEK, Kris; DOERR, Christian. Cyber Threat Intelligence: A Product Without a Process? *International Journal of Intelligence and CounterIntelligence*, v. 34, n. 2, p. 300-315, 2021.

ORGANIZATION OF AMERICAN STATES. *CSIRTAmericas Network*. Disponível em: <https://csirtamericas.org/en>. Acesso em: 29 set. 2024.

PATRICK, Stewart. *NATO's Deterrence Problem*: An Analog Strategy for a Digital Age. Council on Foreign Relations, August 2018. Disponível em: <https://www.cfr.org/blog/natos-deterrence-problem-analog-strategy-digital-age>. Acesso em: 2 maio 2025.

PLUMMER, Robert; GERKEN, Tom. CrowdStrike and Microsoft: What We Know about Global IT Outage. *BBC*, 19 jul. 2024. Disponivel em: <https://www.bbc.com/news/articles/cp4wnrxqlewo>. Acesso em: 15 jul. 2025.

RID, Thomas. *Cyber War Will Not Take Place*. Oxford: Oxford University Press, 2013.

RUSSIAN FEDERATION. *Updated Concept of the Convention of the United Nations on Ensuring International Information Security*. United Nations Office for Disarmament Affairs, 2021. Disponível em: <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_convention_on_ensuring_international_information_security.pdf>. Acesso em: 2 maio 2025.

SCHMITT, Michael; VIHUL, Liis. The Emergence of International Legal Norms for Cyberconflict. In: ALLHOFF, Fritz *et al*. (ed.). *Binary Bullets*: The Ethics of Cyberwarfare. Oxford: Oxford University Press, 2015. p. 34–55.

SCHÖNDORF, Roy. Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. *International Law Studies*, v. 97, n. 395, p. 395-406, 2021.

SHELDON, John. Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly*, v. 5, n. 2, p. 95-112, 2011.

SINGER, P.W.; FRIEDMAN, Allan. *Cybersecurity and Cyberwar*: What Everyone Needs to Know. Oxford: Oxford University Press, 2014.

STANDAGE, Tom; STEVENSON, Seth. *Human insecurity*. Secret History of the Future, 3 out. 2018. Podcast, 30 min. Disponível em: <https://slate.com/technology/2018/10/what-an-1834-hack-of-the-french-telegraph-system-can-teach-us-about-modern-day-network-security.html>. Acesso em: 13 abr. 2024.

STANIČ, Ana. Bustani v. Organisation for the Prohibition of Chemical Weapons. Judgment No. 2232. *The American Journal of International Law*, v. 98, n. 4, p. 810-814, out. 2004.

STRANGE, Susan. Cave! Hic Dragones: A Critique of Regime Analysis. *International Organization*, v. 36, n. 2, p. 479-496, 1982.

SUKUMAR, Arun *et al*. The Pervasive Informality of the International Cybersecurity Regime: Geopolitics, Non-State Actors and Diplomacy. *Contemporary Security Policy*, v. 45, n. 1, p. 7-44, 2024.

TIKK, Eneken. Future Normative Challenges. In: CORNISH, Paul (ed.). *The Oxford Handbook of Cyber Security*. Oxford: Oxford University Press, 2021, p. 751-768.

UNITED KINGDOM. *The Pall Mall Process:* Tackling the Proliferation and Irresponsible Use of Commercial Cyber-Intrusion Capabilities. Disponível em: <https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities>. Acesso em: 27 out. 2024.

UNITED NATIONS GENERAL ASSEMBLY. *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: Report of the Group of Governmental Experts*. A/76/135, 14 jul. 2021. Disponível em: <https://undocs.org/a/76/135>. Acesso em: 23 jul. 2025.

UNITED NATIONS GENERAL ASSEMBLY. *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. A/RES/73/266, 22 dez. 2018. Disponível em: <https://documents.un.org/doc/undoc/gen/n18/465/01/pdf/n1846501.pdf>. Acesso em: 15 jul. 2025.

UNITED NATIONS GENERAL ASSEMBLY. *Definition of Aggression*. A/RES/3314(XXIX), 14 dez. 1974. Disponível em: <https://undocs.org/A/RES/3314(XXIX) >. Acesso em: 15 jul. 2025.

UNITED NATIONS GENERAL ASSEMBLY. *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/70/237, 30 dez. 2015. Disponível em: <https://undocs.org/A/RES/70/237>. Acesso em: 15 jul. 2025.

UNITED NATIONS GENERAL ASSEMBLY. *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/73/27, 11 dez. 2018. Disponível em: <https://undocs.org/A/RES/73/27>.

UNITED NATIONS GENERAL ASSEMBLY. *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/75/240, 31 dez. 2020. Disponível em: <https://undocs.org/A/RES/75/240>. Acesso em: 15 jul. 2025.

UNITED NATIONS GENERAL ASSEMBLY. *Developments in the Field of Information and Telecommunications in the Context of International Security, and Advancing Responsible State Behaviour in the Use of Information and Communications Technologies*. A/RES/76/19, 8 dez. 2021. Disponível em: <https://undocs.org/A/RES/76/19>. Acesso em: 15 jul. 2025.

UNITED NATIONS GENERAL ASSEMBLY. *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/77/36, 12 dez. 2022. Disponível em: <https://undocs.org/A/RES/77/36>. Acesso em: 15 jul. 2025.

UNITED NATIONS GENERAL ASSEMBLY. *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/78/237, 5 dez. 2023. Disponível em: <https://undocs.org/A/RES/78/237>.

UNITED NATIONS GENERAL ASSEMBLY. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/65/10, 30 jul. 2010. Disponível em: <https://undocs.org/a/65/201>. Acesso em: 15 jul. 2025.

UNITED NATIONS GENERAL ASSEMBLY. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174, 22 jul. 2015. Disponível em: <https://undocs.org/A/70/174>. Acesso em: 15 jul. 2025.

UNITED NATIONS GENERAL ASSEMBLY. *Official Compendium of Voluntary National Contributions on How International Law Applies to the Use of Information and Communications Technologies by States*. A/76/136, 13 jul. 2021. Disponível em: <https://undocs.org/A/76/136>. Acesso em: 15. jul. 2025.

UNITED NATIONS GENERAL ASSEMBLY. *Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025 Established Pursuant to General Assembly Resolution 75/240*. A/RES/79/237, 24 dez. 2024. Disponível em: <https://undocs.org/A/RES/79/237>. Acesso em: 25 jul. 2025.

UNITED NATIONS GENERAL ASSEMBLY. *Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security*. A/RES/77/37, 12 dez. 2022. Disponível em: <https://undocs.org/A/RES/77/37>. Acesso em: 25 jul. 2025.

UNITED NATIONS GENERAL ASSEMBLY. *Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security*. A/RES/78/16, 5 dez. 2023. Disponível em: <https://undocs.org/A/RES/78/16>. Acesso em: 25 jul. 2025.

UNITED NATIONS GENERAL ASSEMBLY. *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/79/214, 10 jul. 2024. Disponível em: <https://undocs.org/A/79/214>. Acesso em: 25 jul. 2025.

UNITED NATIONS GENERAL ASSEMBLY. *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/78/265, annex C. 1 ago. 2023. Disponível em: <https://undocs.org/A/78/265>. Acesso em: 25 jul. 2025.

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH. *Accelerating ICT Security Capacity Building: Take-Aways from the Global Roundtable on ICT Security Capacity Building,* jun. 2024. Disponível em: <https://unidir.org/wp-content/uploads/2024/06/UNIDIR_Accelerating_ICT_Security-Capacity_Building_Take_Aways_from_the_Global_Roundtable_on_ICT_Security_Capacity_Building.pdf>. Acesso em: 25 jul. 2025.

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS. *Programme of Action on Cybersecurity*. Disponível em: <https://poc-ict.unoda.org>. Acesso em: 25 jul. 2025.

UNITED STATES CYBER COMMAND. *Our History*. Disponível em: <https://www.cybercom.mil/About/History/>. Acesso em: 25 jul. 2025.

UNITED STATES OF AMERICA. *2023 Cyber Strategy of the Department of Defense*, 12 set. 2023. Disponível em: <https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF>. Acesso em: 25 jul. 2025.

WORLD ECONOMIC FORUM. *Global Cybersecurity Outlook 2025*. Disponível em: <https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf>. Acesso em: 25 jul. 2025.