UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SOCIOECONÔMICO (CSE)
PROGRAMA DE PÓS-GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

Danniel Garcia Barbosa de Figueiredo

Governança de Sistemas Ciber-Físicos:
os jogos de poder, interesses e segurança no ciberespaço

Florianópolis - SC
2024

Danniel Garcia Barbosa de Figueiredo

Governança de Sistemas Ciber-Físicos:

os jogos de poder, interesses e segurança no ciberespaço

Dissertação submetida ao Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de Mestre em Relações Internacionais.

Orientador(a): Prof.(a) Danielle Jacon Ayres Pinto, Dr.(a)

Florianópolis - SC

2024

Figueiredo, Danniel Garcia Barbosa de
Governança de Sistemas Ciber-Físicos : os jogos de poder, interesses e segurança no ciberespaço / Danniel Garcia Barbosa de Figueiredo ; orientadora, Danielle Jacon Ayres Pinto, 2024.
159 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Socioeconômico, Programa de Pós-Graduação em Relações Internacionais, Florianópolis, 2024.

Inclui referências.

1. Relações Internacionais. 2. Governança do Ciberespaço. 3. Sistemas Ciber-Físicos. 4. Internet das Coisas . 5. Estados Nacionais. I. Pinto, Danielle Jacon Ayres. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Relações Internacionais. III. Título.

Danniel Garcia Barbosa de Figueiredo

Governança de Sistemas Ciber-Físicos:
os jogos de poder, interesses e segurança no ciberespaço

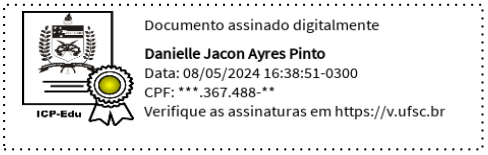
O presente trabalho em nível de Mestrado foi avaliado e aprovado, em 22 de março de 2024, pela banca examinadora composta pelos seguintes membros:

Prof.(a) Cristina Soreanu Pecequilo, Dr.(a)
Universidade Federal de São Paulo (UNIFESP)

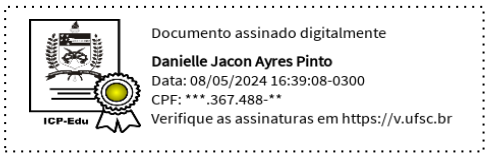
Prof.(a) Graciela de Conti Pagliari, Dr.(a)
Universidade Federal de Santa Catarina (UFSC)

Prof. Italo Barreto Poty, Dr.
Universidade Federal Fluminense (UFF)

Certificamos que esta é a versão original e final do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestre em Relações Internacionais.



Coordenação do Programa de Pós-Graduação



Prof.(a) Danielle Jacon Ayres Pinto, Dr.(a)
Orientador(a)

Florianópolis, 2024.

Ao céu estrelado, companheiro das noites acordado
que possibilitaram a escrita desta dissertação.

AGRADECIMENTOS

Agradeço à Universidade Federal de Santa Catarina e ao Programa de Pós-Graduação em Relações Internacionais pela oportunidade de realizar gratuitamente um mestrado de qualidade ímpar, com um corpo docente extremamente qualificado. O aprendizado durante esse período vai para muito além dessa dissertação e me faz ter a certeza de que o campo das RI está muito bem representado a nível nacional para os próximos anos.

Agradeço à minha orientadora, Profª Drª Danielle Jacon Ayres Pinto, por toda a paciência, compreensão e apoio, não só ao longo do processo de construção desta dissertação, mas ao longo de toda a minha trajetória acadêmica. Aprender e conviver com Danielle é um privilégio e uma experiência extremamente enriquecedora.

Agradeço ao GEPPIC (Grupo de Pesquisa em Estudos Estratégicos e Política Internacional Contemporânea) por despertar em mim a paixão pela pesquisa da política envolvendo as relações cibernéticas na sociedade contemporânea, e aos companheiros de pesquisa que me acompanharam durante minha trajetória no grupo.

Agradeço aos meus pais por todo o apoio ao longo de toda a minha vida e por me proporcionarem a oportunidade de ter morado em Florianópolis e ter podido cursar minha graduação e pós-graduação na UFSC.

Agradeço aos meus companheiros de trabalho da Politize! - Instituto de Educação Política, pelo apoio e compreensão das dificuldades do processo de conciliar trabalho e pesquisa.

E agradeço, por fim, a minha companheira de vida, Carla da Silva Oliveira, por todo o amor proporcionado desde o primeiro dia em que a conheci, e em especial nas noites que precisaram ser viradas para que eu pudesse concluir essa dissertação. Seu sorriso e seus olhos brilhando foram o combustível que me manteve de pé e a motivação para que eu pudesse ir além do meu melhor na construção desta dissertação. Muito obrigado, eu amo você!

“I think that technologies are morally neutral until we apply them. It's only when we use them for good or for evil that they become good or evil.”

(William Gibson; 23 novembro de 1994)

RESUMO

A governança global da internet está em um momento de inflexão, no qual decisões estratégicas precisam ser tomadas, pois impactarão significativamente não só o ambiente cibernético, mas também a economia e a segurança global. Este momento é marcado, entre outros aspectos, pela iminente consolidação dos sistemas ciber-físicos, que se conectam aos ambientes real e virtual simultaneamente. Enquanto abrem uma série de possibilidades para a melhoria da qualidade de vida de seus usuários e possuem grande potencial econômico, esses sistemas também trazem riscos que devem ser considerados pela sociedade e pelos Estados Nacionais. Diante desses riscos, analisa-se, por meio de bibliografia e documentos oficiais, como as cinco principais potências cibernéticas apontadas pelo National Cyber Power Index 2022 (Estados Unidos, China, Rússia, Reino Unido e Austrália), estão se posicionando em relação à governança da internet, no geral, e a aos sistemas ciber-físicos em específico e que tipos de disputas podem ser observadas a partir disso.

Palavras-chave: governança da internet; internet das coisas; sistemas ciber-físicos.

ABSTRACT

Global internet governance is at a turning point, where strategic decisions must be made as they will significantly impact not only the cyber environment but also the global economy and security. This moment is marked, among other things, by the imminent consolidation of cyber-physical systems, which connect to both the real and virtual environments simultaneously. While they open a range of possibilities for improving the quality of life for their users and have great economic potential, these systems also introduce risks that must be considered by society and National States. In light of these risks, an analysis is conducted through literature and official documents on how the top five cyber powers identified by the National Cyber Power Index 2022 (United States, China, Russia, United Kingdom, and Australia) are positioning themselves in relation to internet governance in general, and cyber-physical systems in particular, and what kind of disputes can be observed from this.

Keywords: internet governance; internet of things; cyber-physical systems.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ASEAN	Associação das Nações do Sudeste Asiático
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICTs	Information and Communication Technologies
IOT	Internet of Things (Internet das Coisas)
ISO	International Standards Organization
ITU	União Internacional de Telecomunicações (UIT)
NATO	North Atlantic Treaty Organization (OTAN)
NIST	National Institute of Standards and Technology
PSTI	Product Security and Telecommunications Infrastructure
UK	United Kingdom (Reino Unido)
UN GGE	Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security
UNIDIR	United Nations Institute for Disarmament Research
UN OEWG	Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security
WCIT	World Conference on International Communications
WGIG	Working Group on Internet Governance
WSIS	World Summit on the Information Society

SUMÁRIO

INTRODUÇÃO: DA CASA NOVA DE PORCHAT AOS RUMOS DA ECONOMIA E SEGURANÇA GLOBAIS

1.1 POR QUE FALAR DE SISTEMAS CIBER-FÍSICOS?

Era uma sexta-feira quando ao ligar a televisão em horário nobre, na TV Globo, maior emissora do Brasil, milhões de brasileiros puderam assistir uma interação entre os atores e humoristas Fábio Porchat e João Vicente Castro. A interação se deu dentro da casa nova de Fábio Porchat, que recebe a visita de João Vicente. Enquanto Porchat vai se arrumar para sair, João com um comando de voz ativa a playlist do amigo e, em seguida, explorando a casa, abre a geladeira e come um pedaço de bolo com a boca diretamente do prato, acreditando na garantia do anonimato do mundo no qual cresceu. Ao voltar, contudo, Porchat aponta em seu celular como a casa capturou a cena, espelha a cena diretamente na televisão e, posteriormente, do próprio celular, envia o vídeo capturado para toda a equipe do Porta dos Fundos (portal de humor brasileiro do qual ambos os atores fazem parte) através de um comando de voz.

Essa interação, em tom de esquete humorístico, é um dos quatro episódios da campanha “Casa nova, vida Smart”, lançada pela gigante coreana Samsung para divulgar sua tecnologia “*SmartThings*”, feita para utilização nas chamadas *Smart Houses* (casas inteligentes). Nas palavras da diretora de marketing da campanha, Ana Karina Pinto, “A ideia da campanha é mostrar às pessoas que ter uma ‘casa inteligente’ é mais simples do que muitos podem imaginar [...] a tecnologia [...] traz facilidades que vão desde o controle de dispositivos e a otimização das rotinas diárias, até a possibilidade de transformar os ambientes da casa de acordo com suas necessidades e preferências”[1]. A matéria sobre a campanha segue na linha dos benefícios, apontando a “facilidade em controlar ambientes da casa, além de dispositivos como TV, ar-condicionado, robô aspirador, lava e seca, entre outros produtos de forma simples e rápida” (SAMSUNG, 2023).

Uma propaganda como essa, exibida em canal aberto, é representativa e símbolo de um mundo em transformação, onde os objetos físicos tendem a ser cada vez mais conectados a ambientes virtuais. E, da mesma forma em que a Samsung

[1] Vídeo disponível em: https://news.samsung.com/br/samsung-lanca-campanha-com-fabio-porchat-e-joao-vicente-para-mostrar-os-beneficios-de-uma-vida-conectada-com-smartthings. Acesso em: 01 jan. 2024.

demonstra como sua tecnologia vem para facilitar a vida de seus consumidores, provavelmente sem intenção, também aponta para um dos principais problemas que essa hiperconexão carrega: a privacidade dos usuários e seus dados. A mesma câmera que, intencionalmente, captura a imagem de João Vicente e rapidamente pode transmitir essa imagem a outras telas via *smartphone*, se invadida poderia capturar imagens não intencionais, e rapidamente transmiti-las a um invasor. Ou ainda, poderia ser utilizada para monitoramento em tempo real da casa e mesmo para transmitir mensagens não intencionais. Um exemplo é o hackeamento de um "*baby monitor"* no qual o invasor o usa para gritar com a criança e, posteriormente, com seu pai.[2]

No episódio quatro da campanha, por sua vez, também em tom humorístico, e não com esse intuito[3], a Samsung apresenta outro risco fundamental: o da invasão de dispositivos. No esquete, Porchat altera intencionalmente as condições da casa (temperatura, iluminação), liga e desliga a televisão rapidamente, finge não ter controle sobre seu robô aspirador, entre outros, no intuito de passar a mensagem ao seu amigo que era hora de que ele fosse embora da casa. Por mais que ali Porchat tivesse controle de tudo, os riscos ficam evidentes no caso de controle externo dos dispositivos: elevação ou diminuição brusca da temperatura, mal funcionamentos de dispositivos, tornando-os perigosos e, no caso de a fechadura da casa também ser *smart,* um cenário extremo poderia ser de pesadelo ao morador. O que um dia foi parte apenas de cenas de filmes de ficção científica futurista hoje já não é tão distante assim.

Esse exemplo ilustra o caso de um indivíduo com poder aquisitivo relativamente alto, num cenário de uma *Smart House* completa. À primeira vista, pode-se pensar: tudo bem, é um risco, mas ainda não é um risco tão grande assim, afinal são poucas as pessoas que poderão ter uma casa desse tipo em um futuro próximo. Cabe lembrar, contudo, que a conexão das "coisas" vai muito além disso. De acordo com o portal de dados *statista*, em 2023 foram mais de 15 bilhões de dispositivos conectados a chamada "Internet das Coisas" e a previsão é de que, até 2030, esse número dobre,

[2]Reportagem sobre o caso mencionado. Disponível em: https://www.mirror.co.uk/news/world-news/man-hacks-10-month-olds-baby-monitor- 3468827. Acesso em: 01 jan. 2024.
[3] Quarto episódio da campanha. Disponível em: https://www.youtube.com/watch?v=OdkZiPgYRBM. Acesso em: 01 jan. 2024.

se aproximando dos 30 bilhões. (STATISTA, 2023)[4]. Estudos recentes, contudo, já apontam que esse número pode chegar na casa dos 27 bilhões ainda em 2025 (PACETE, 2022). Ou seja, os dados mostram uma média superior a 3 aparelhos por habitante e, consequentemente, um elevado número de potenciais alvos para ataques cibernéticos.

Ao tratar de dados nessa escala de números, por mais que as questões e riscos individuais continuem relevantes, é preciso pensar para além dos indivíduos e abordar a questão sob uma ótica de sociedade. Sobretudo quando já existem exemplos, como o Mirai Botnet, feitos para infectar esses tipos de dispositivos. Trautman et al. (2019) apontam que o Mirai Botnet chegou a infectar 600.000 dispositivos conectados à Internet das Coisas, de roteadores a monitores de qualidade de ar e câmeras de segurança. No caso do ataque, em 2016, a principal consequência foi deixar usuários sem acesso à internet. Mas não é preciso ir muito longe na imaginação para pensar em outros tipos de risco, como no próprio exemplo citado anteriormente. Ao pensar em sociedade, e também em governança e segurança social, não há como não pensar em Estados Nacionais.

Diante disso, nasce a pergunta: “por que fazer uma dissertação sobre essa temática?” A relevância dessa pesquisa reside na abordagem e na conexão entre três aspectos relevantes para a sociedade e para as Relações Internacionais no presente e no futuro: a crescente presença e desenvolvimento de sistemas ciber-físicos; as discussões sobre a governança do espaço cibernético; e o papel que os Estados Nacionais exercem e devem exercer no Sistema Internacional.

Ao falar de sistemas ciber-físicos, estamos tratando de tecnologias que agregam componentes do mundo real e do mundo digital simultaneamente. Desse modo, podem ser acessadas virtualmente, mas possuem presença física e, consequentemente, capacidade de interação com pessoas e objetos materiais (DENARDIS, 2020). Mais especificamente, Laura DeNardis resgata como definição da ciência da informação que “Um sistema ciber-físico consiste em uma coleção de dispositivos de computação se comunicando uns com os outros e interagindo com o mundo físico por meio de sensores e atuadores em um loop de feedback”[5]

[4] Dados do Statista sobre dispositivos de IoT. Disponível em: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. Acesso em: 01 jan. 2024.

[5] Original: ”A cyber-physical system consists of a collection of computing devices communicating with one another and interacting with the physical world via sensors and actuators in a feedback loop.”

(DENARDIS, 2020, p.27). A escolha de DeNardis pelo uso do termo “sistemas ciber-físicos”, ao invés do termo “Internet das Coisas”, parte pelo fato de Internet das Coisas já possuir uma conotação mais voltada para o mercado de consumo, o que pode ofuscar fenômenos maiores em setores como defesa, transporte, agricultura (DENARDIS, 2020), embora entenda que o termo “Internet das Coisas” é uma forma coloquial de chamar os sistemas ciber-físicos (DENARDIS, RAYMOND, 2017). A escolha de termo de DeNardis é mantida no título da dissertação e como termo central deste trabalho. Contudo, o termo Internet das Coisas também será utilizado pois, como veremos, tende a ser mais comum dentro dos documentos dos Estados.

Em sua obra, DeNardis traz grandes preocupações sobre o impacto desses sistemas em questões de segurança e privacidade. O caráter econômico dos mesmos, contudo, não deve ser desconsiderado. Isso porque, conforme pesquisa da *Markets and Markets*, essa indústria deverá movimentar US$650 bilhões (seiscentos e cinquenta bilhões de dólares) até 2026 (BRANDÃO, 2022). Controlá-la, ou ao menos se inserir dentro dela, é uma questão fundamental para se fazer presente no topo da economia global.

Definições à parte, a questão principal tratada aqui é que, estando conectados ao mundo físico, os sistemas ciber-físicos passam a representar riscos de segurança e preocupações geopolíticas, uma vez que “um ataque na Internet não é mais apenas para interromper os sistemas de comunicação que conectam as pessoas, mas para interromper o mundo real, a infraestrutura material necessária para o funcionamento social básico*”* [6] (DENARDIS, RAYMOND, 2017, p. 475). Um exemplo ilustrativo trazido por DeNardis é o dos carros autônomos:

> Uma distinção que os teóricos fizeram entre a guerra cibernética e a “guerra do mundo real” é que o conflito cibernético não resulta em morte humana. Essa distinção entra em colapso à medida que um número crescente de sistemas críticos do mundo real se tornam cibernéticos. Por exemplo, embora os veículos autônomos salvem vidas porque muitos acidentes decorrem de erro humano, as redes digitais controlam esses veículos e os hackers em qualquer lugar do mundo podem sabotá-los ou interrompê-los, resultando potencialmente em morte humana. (DENARDIS, 2020, p. 20)[7]

[6] Original: “an attack on the Internet is no longer merely about disrupting communication systems connecting people, but about disrupting real world, material infrastructure necessary for basic societal functioning.”

[7] Original: “One distinction theorists have made between cyber war and “real-world war” is that cyber conflict does not result in human death. This distinction collapses as an increasing number of critical real-world systems become cyber embedded. For example, while autonomous vehicles will save lives because so many accidents arise from human error, digital networks control these vehicles, and hackers anywhere in the world can potentially sabotage or disrupt them, potentially resulting in human death.”

Contudo, para além desse exemplo, estamos falando de sistemas de saúde, indústria, infraestruturas críticas e até mesmo aparelhos que estarão (ou já estão) presentes no dia a dia das pessoas, em suas "*smart houses*", como a de Porchat.

Dado esse contexto, o debate acerca dos sistemas ciber-físicos dialoga e necessita estar presente nos debates sobre a governança do espaço cibernético *per* si, na busca de normas, regras e princípios para eles. Embora de forma sucinta, os relatórios de 2021 do *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (UN GGE) e do Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (UN OEWG), dois dos principais grupos dentro das Nações Unidas a discutirem questões de governança cibernética reforçam essa questão. Para o UN GGE:

> Tecnologias novas e emergentes estão expandindo as oportunidades de desenvolvimento. No entanto, suas propriedades e características em constante evolução também expandem a superfície de ataque, criando novos vetores e vulnerabilidades que podem ser explorados por atividades maliciosas de TIC. Garantir que vulnerabilidades na tecnologia operacional e nos dispositivos, plataformas, máquinas ou objetos de computação interconectados que constituem a Internet das Coisas não sejam explorados para fins maliciosos tornou-se um sério desafio. (UNGGE, 2021, p.7, grifo do autor)[8]

Já o UN OEWG trouxe que:

> Os Estados reconheceram que, mesmo que os avanços tecnológicos e os novos aplicativos possam oferecer oportunidades de desenvolvimento, eles também podem expandir as superfícies de ataque, amplificar vulnerabilidades no ambiente de TIC ou ser aproveitados para novas atividades maliciosas. Tendências e desenvolvimentos tecnológicos específicos foram destacados a esse respeito, incluindo progresso em aprendizado de máquina e computação quântica; a ubiquidade dos dispositivos conectados ("Internet das Coisas"); novas formas de armazenar e acessar dados por meio de livros contábeis distribuídos e computação em nuvem; e a expansão de big data e dados pessoais digitalizados. (UNOEWG, 2021, p.18, grifo do autor)[9]

[8] Original: "New and emerging technologies are expanding development opportunities. Yet, their ever-evolving properties and characteristics also expand the attack surface, creating new vectors and vulnerabilities that can be exploited for malicious ICT activity. Ensuring that vulnerabilities in operational technology and in the interconnected computing devices, platforms, machines or objects that constitute the Internet of Things are not exploited for malicious purposes has become a serious challenge."

[9] Original: "States recognized that even as technological advances and new applications may offer development opportunities, they may also expand attack surfaces, amplify vulnerabilities in the ICT

Mueller e Badiei (2020) também seguem nessa linha de percepção de relevância, ao finalizarem sua retrospectiva histórica sobre a governança da internet apontando como desafio futuro a questão da Internet das Coisas e como isso impactaria o próprio uso do termo “internet governance” para elas. Assim sendo, o olhar para os sistemas ciber-físicos dialoga diretamente com debates atuais no campo da governança cibernética.

E onde entra a questão do Estado nisso tudo? Em primeiro lugar, cabe retornar aos riscos de segurança trazidos pelos sistemas ciber-físicos. Bruce Schneier, do *Center for Internet and Society,* de Harvard resume bem a questão em entrevista ao *Atlantic Council,* quando diferencia os riscos dos sistemas ciber-físicos dos demais sistemas de tecnologia da informação ao apontar que “A IoT é onde a “security” (segurança a nível militar) encontra a segurança (integridade física). Planilhas inseguras podem comprometer seus dados. Dispositivos IoT inseguros podem comprometer sua vida.*”* (ATLANTIC COUNCIL, 2022)[10]. Assim sendo, se tratando de riscos securitários, com potencial de impacto físico e econômico, o Estado, enquanto tradicional “guardião” da segurança nacional, não pode ser desconsiderado. Embora seja inegável a relevância de empresas privadas no debate sobre governança e segurança no ciberespaço, com destaque para as iniciativas comandadas pela Microsoft (HUREL, LOBATO, 2020), quando falamos de sistemas ciber-físicos DeNardis lembra bem que “em áreas como privacidade e segurança, pode haver pouco incentivo para fabricantes de dispositivos ou provedores de sistemas IoT cuidarem totalmente da segurança, considerando a necessidade de lançar rapidamente produtos no mercado e criar rapidamente novos produtos.”*[11]* (DENARDIS, RAYMOND, 2017, p. 495). Desse modo, na medida em que os riscos de segurança aumentaram, é importante observar como os Estados se colocam, e qual sua real capacidade de ação no modelo *multistakeholder* que se desenvolveu na governança cibernética.

---

environment or be **leveraged for novel malicious activities**. Particular technological trends and developments were highlighted in this regard, including progress in machine learning and quantum computing; **the ubiquity of connected devices (“Internet of Things”)**; new ways to store and access data through distributed ledgers and cloud computing; and the expansion of big data and digitized personal data.”

[10] Original: “the IoT is where security meets safety. Insecure spreadsheets can compromise your data. Insecure IoT devices can compromise your life”.

[11] Tradução: “in areas such as privacy and security, there may be little incentive for device manufacturers or IoT system providers to fully take care of security, considering the need to quickly bring products to market and quickly create new product [...]”

Além disso, cabe observar a própria vontade dos Estados em se fazerem mais presentes. No livro "*Power and Authority in internet governance: return of the state?*", Haggart; Tusikov e Scholte (2021) destacam uma fala do presidente francês, Emmanuel Macron, no Fórum de Governança da Internet (IGF) de 2018, onde Macron apresenta a existência de um modelo "Californiano" de governança da internet, constituído por atores privados fortes, com pouco "accountability"; um modelo "Chinês", baseado em controle autoritário do Estado, protecionismo e violação de direitos humanos; e advoga por um terceiro modelo, com maior envolvimento de Estados democráticos, voltado para o interesse público e direitos humanos (HAGGART; TUSIKOV e SCHOLTE, 2021). O quanto essas percepções de necessidade de envolvimento tendem a crescer em meio aos sistemas ciber-físicos também é algo interessante.

E em terceiro lugar, olhar para como os Estados se colocam em meio aos sistemas ciber-físicos é relevante em termos de reflexões sobre o que queremos enquanto sociedade. No documento "*Governance Principles for a Society Based on Cyber-Physical Systems*", um grupo de experts voluntários de países membros do G7 lembra os riscos de um acúmulo de poder na arquitetura de sistemas ciber-físicos tanto por parte de empresas privadas, que poderiam preservar seus interesses em detrimento do bem estar social, quando por parte de governos (sobretudo em países autoritários) que poderiam usá-los para monitorar comportamentos e restringir liberdades no ciberespaço e no espaço físico (INATANI et al., 2023). É em meio a esse contexto, de dilemas econômicos, de segurança, de privacidade, envolvendo atores diversos, que essa dissertação se localiza.

Diante disso, ao longo desta dissertação será observada a abordagem que está sendo dada aos sistemas ciber-físicos a partir dos cinco Estados mais poderosos no *Cyber Power Index 2022,* elaborado anualmente pelo Belfer Center[12]*.* Embora o índice seja alvo de ataques de alguns dos países que aborda, como a Rússia, que o aponta como baseado em especulações falsas (FEDERAÇÃO RUSSA, 2022), ele é um dos principais e mais completos índices desse tipo e, por isso, está sendo adotado como critério de escolha. A premissa é que, na impossibilidade de analisar todos os Estados de uma só vez no âmbito desta dissertação, a análise de cinco Estados relevantes no campo cibernético pode trazer elementos que contribuirão com a pesquisa da temática

[12]A versão de 2022 do Índice encontra-se disponível em: https://www.belfercenter.org/publication/national-cyber-power-index-2022. Acesso em: 01 jan.2024.

e poderão dar uma ideia geral de cenário para embasar pesquisas futuras. Também parte-se da premissa que, entre os Estados escolhidos, existem perspectivas diferentes, o que permite comparação entre essas perspectivas e contribui para a investigação de se os posicionamentos de Rússia e China se aproximam ou se distanciam dos países do Ocidente observados, dentro desse tema.

A divisão da estrutura se dá da seguinte forma: esta introdução busca justificar a relevância do tema e apresentar, de forma breve, os conceitos de ciberespaço e poder cibernético. Em seguida, o primeiro capítulo traz uma revisão objetiva da temática da governança do ciberespaço e quais os principais marcos históricos e as discussões recentes em torno desse tema. Aqui, busca-se pontuar um processo de securitização da governança cibernética, de um momento em que se tratava a internet como um espaço mais livre e "*multistakeholder*" até o momento em que ele também é percebido como um espaço fundamental para o exercício de segurança.

O segundo capítulo, por sua vez, discorre sobre o conceito de sistemas ciber-físicos e algumas das implicações trazidas por eles. Busca-se aqui compreender como esses sistemas contribuem para um processo de securitização da temática, e o que eles trazem de novo para esse debate.

O terceiro capítulo foca na análise dos posicionamentos a respeito de governança da internet e de sistemas ciber-físicos por parte dos cinco Estados analisados. Para tanto, serão observados os documentos oficiais dos Estados presentes no *"Cyber Policy Portal"* da UNIDIR (*United Nations Institute for Disarmament Research*)[13], acompanhados de outros documentos específicos sobre a temática encontrados ao longo da pesquisa. Por fim, parte-se para a discussão sobre o quanto os sistemas ciber-físicos estão ou não sendo percebidos como ameaças de segurança, e quais são os pontos de destaque em meio às abordagens por parte dos Estados. A partir disso, são estabelecidas as considerações finais. Os resultados da pesquisa são apresentados de forma qualitativa, visando contribuir com a compreensão e com o debate do fenômeno social abordado.

A partir dessa estrutura, busca-se compreender como os sistemas ciber-físicos estão se encaixando nos debates sobre a governança do ciberespaço, a partir da

[13] O portal da UNIDIR tem o objetivo de servir como um repositório internacional de documentos cibernéticos dos países, a fim de fomentar medidas de transparência e confiança. Assim, olhar para os documentos que estão ali é uma forma de confiar nesse processo. O mapa interativo do portal e os documentos ali presentes estão disponíveis em:: https://cyberpolicyportal.org/. Acesso em: 1 de jan. de 2024.

perspectiva dos Estados Nacionais analisados. A resposta dessa pergunta poderá levantar novas perguntas de pesquisa e contribuir para análises futuras de possibilidades de acordos, legislações e conflitos futuros neste campo. Em paralelo a isso, a dissertação também visa: 1. Analisar historicamente e criticamente o debate sobre a governança do ciberespaço; 2. Compreender os Estados observados estão abordando a governança do ciberespaço; 3. Evidenciar as estratégias, preocupações e propostas internas e externas para a governança de sistemas ciber-físicos dos Estados observados.

Investiga-se a hipótese de que o desenvolvimento de sistemas ciber-físicos aumenta os riscos e vulnerabilidades de segurança nacional atrelados ao ciberespaço. Desse modo, os Estados Nacionais tenderão a assumir um papel ainda mais presente no debate e na agenda de governança, no geral, e dos sistemas ciber-físicos em específico, buscando preservar seus interesses securitários e garantir sua sobrevivência e isso deverá se manifestar em seus discursos, documentos e posicionamentos.

O falseamento da hipótese se dará através da avaliação da existência ou não de discursos e práticas favoráveis à governança digital por parte dos governos em questão. Ou seja, em seus documentos os Estados apontam os sistemas ciber-físicos como um risco que requer medidas preventivas por parte desses Estados ou não?

Havendo posicionamentos na linha de maiores preocupações e que visem englobar os sistemas ciber-físicos sob o guarda-chuva dos Estados Nacionais, a hipótese se mostra verdadeira. Não havendo posicionamentos, ou havendo posicionamentos favoráveis à governança desses sistemas permanecer sob o predomínio de empresas privadas, a hipótese se mostra falsa. Independentemente do resultado, a pesquisa abre margem para maior compreensão e estudos futuros acerca do tema.

1.2 CONCEITOS RELEVANTES

A seguir, são apresentados os conceitos de espaço cibernético e de poder cibernético, a fim de contextualizar as discussões posteriores.

1.2.1 Ciberespaço: definições e peculiaridades

> "Tudo o que eu sabia sobre a palavra "ciberespaço" quando a criei era que parecia uma palavra da moda eficaz. Parecia evocativo e essencialmente sem sentido. Sugeria alguma coisa, mas não tinha nenhum significado semântico real, mesmo para mim, conforme vi emergir na página" (William Gibson, autor da ficção Neuromancer, onde o termo ciberespaço aparece pela primeira vez. Declaração retirada de MUELLER, 2017, p. 418)[14]

Quando pensamos em ciberespaço, elementos fundamentais de se considerar são: ele é extremamente recente em termos históricos de sociedade e, em pouquíssimo tempo, cresceu a ponto de se tornar fundamental para ela. Esses dois elementos, o "ser recente" e "crescer em importância ao longo do tempo" são indissociáveis quando se pensa nesse espaço em si e, consequentemente, em todas as derivações que surgem dele, como os próprios sistemas ciber-físicos.

Isso porque a relação dos seres humanos com a cibernética em si é bem recente na história humana, e boa parte das transformações provocadas por ela ainda estão em processo. A origem do termo cibernética, conforme aponta Rid (2016), data da década de 1940, através do matemático do MIT, Norbert Wiener, que se baseou no termo grego *kybernian,* que significa dirigir, governar, controlar.

Em 1948, a obra *"Cybernetics; or Control and Communication in the Animal and the Machine"* inaugura esse termo em larga escala, dando origens a um debate que se prolongaria por todo o restante do século XX sobre como deveria ser a relação humana com as máquinas, sobre se seria possível construir máquinas pensantes ou mesmo modificar os corpos humanos a partir de interações com máquinas[15]. Esse debate inspirou a ficção, com obras como o Exterminador do Futuro (1969) e o clássico *Neuromancer,* na década de 1980, onde o termo *ciberespaço* aparece pela primeira vez - representando um espaço dentro das máquinas, acessível aos protagonistas, imaginado por William Gibson.

Apesar de não ser exatamente da forma como Gibson imaginou, o ciberespaço gerou um novo espaço acessível às pessoas, para troca de informações e conteúdo em escala nunca antes vista. Uma forma didática de compreender esse espaço cibernético é através de sua definição em três camadas, conforme apontam Libicki

[14] Original: All I knew about the word 'cyberspace' when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page."

[15] Uma boa ilustração a respeito disso foi publicada na revista Life, em 1960, sob o título de *Man Remade to Live in Space*. Ali, tem-se dois cyborgs (organismos cibernéticos), representando seres humanos modificados para viverem no espaço. Segundo Thomas Rid (2016), o autor da ideia, Manfred Clynes, teve essa imagem em seu escritório por anos.

(2009), assim como a recente *Allied Joint Doctrine for Cyberspace Operations*, da OTAN (2020). Para a OTAN, o ciberespaço é composto por: uma camada física, uma camada lógica (chamada de sintática por Libicki), e uma camada *cyber-persona* (chamada de semântica por Libicki).

Em essência, a camada física se refere às infraestruturas, sem as quais o ciberespaço não consegue existir. Afinal, diferente dos demais espaços, que existem naturalmente, o ciberespaço é um espaço que foi criado pelos seres humanos, através de cabos, satélites, servidores, etc. Essas infraestruturas têm o diferencial de serem materiais, possuindo localizações geográficas. Bons exemplos para visualizar essa questão são o *Submarine Cable Map*[16] e o *Data Centers World Map* [17], que trazem a localização geográfica de algumas delas. Para tornar ainda mais visual, vejamos um exemplo mais palpável. Em 2023, a construção de uma usina de dessalinização em Fortaleza foi motivo de debate no Brasil. Isso porque havia riscos de a obra afetar o relevo oceânico e, consequentemente, movimentar e até mesmo romper algum dos 17 cabos submarinos que passam pela região. Caso isso acontecesse, a rede brasileira poderia ficar mais lenta ou, até mesmo, cair. (SILVA, 2023)

A segunda camada, chamada de lógica/sintática é marcada por instruções e protocolos, que permitem a comunicação entre as máquinas no ciberespaço. É o componente mais técnico. É aqui onde é administrado, por exemplo, o famoso Internet Protocol (IP), que atribui endereços aos elementos da web. Conforme aponta a OTAN:

> Entidades na camada lógica são elementos manifestados em código ou dados, como firmware, sistemas operacionais, protocolos, aplicativos e outros componentes de software e dados. A camada lógica não pode funcionar sem a camada física e as informações fluem através de redes com fio ou do espectro eletromagnético. A camada lógica, juntamente com a camada física, permite que a persona cibernética se comunique e aja. (OTAN, 2020, p.3)[18]

Por fim, a terceira camada é a dos usuários, onde circula o conteúdo. De todas as camadas, essa é a mais utilizada pelo usuário comum. É aqui onde ocorrem, por

[16] Submarine Cable Map Disponível em: https://www.submarinecablemap.com/. Acesso em: 01 jan.2024.

[17] Data Centers World Map Disponível em: https://map.datacente.rs/. Acesso em: 01 jan.2024.

[18] Original: ”Entities at the logical layer are elements manifested in code or data, such as firmware, operating systems, protocols, applications, and other software and data components. The logical layer cannot function without the physical layer and information flows through wired networks or the electromagnetic spectrum. The logical layer, along with the physical layer, allows the cyber-persona to communicate and act.”

exemplo, as movimentações de conteúdo das redes sociais. A figura abaixo, extraída de Canabarro (2014, p. 68) ilustra bem essa distribuição.

Figura 1 - A Distribuição da Internet em Camadas

Fonte: Originalmente publicada em KURBALIJA; GELBSTEIN, 2005, p. 37. Retirada, para fins deste trabalho, de CANABARRO, 2014a, p.68.

Uma reflexão interessante de se fazer, observando essas três camadas, é o quanto os sistemas ciber-físicos se encaixam diretamente dentro da camada de conteúdo e aplicações. Isso porque, como veremos mais à frente, a partir de sua definição, esses sistemas possuem um componente de atuação prática no mundo real. Um sistema que dirige um carro autônomo possui sua camada infraestrutural e de padronização, mas é diferente na aplicação, por exemplo, de uma página web, por conta de seu caráter físico. Embora não seja o objetivo desta dissertação, acredita-se que uma possível quarta camada física, ou uma reestruturação conceitual da terceira camada seja importante para os rumos desse debate.

Voltando a linha de raciocínio anterior, em relação ao elemento de “crescer em importância ao longo do tempo”, enquanto a relação humana com as máquinas era pensada e debatida, tanto em círculos sociais como na ficção, a ciência também avançava e o primeiro computador eletrônico datado surge em 1946.

Pouco tempo depois, a ARPANET, primeira conexão entre computadores, originada através de pesquisas no departamento de defesa dos Estados Unidos,

surge em 1969. A *World Wide Web* surge em 1989 e a internet, como conhecemos hoje, começa a se propagar na década de 1990. Dali para frente, o crescimento foi exponencial. Conforme aponta Nye (2010, p.3, tradução do autor) “em 1992, havia somente um milhão de usuários na internet; dentro de quinze anos, esse número cresceu para um bilhão”.

E, quando olhamos para dados mais atuais, de acordo com [19], em 2021, cerca de 67,9% da população mundial (mais de 5,3 bilhões de pessoas) está conectada à internet. Esse grande volume de usuários em tão pouco tempo, acompanhado da interconexão cada vez maior da sociedade com o ciberespaço, o torna um espaço cada vez mais estratégico a ser observado por uma série de atores, entre eles os Estados Nacionais, a partir de uma perspectiva securitária. Mueller (2017), capta bem a percepção de riscos gerada pelo ciberespaço, apesar de ter uma visão crítica sobre o conceito de cibersegurança ser utilizado de forma a ser sinônimo de segurança nacional.

> Muitos na comunidade de segurança cibernética, refletindo suas raízes governamentais e militares, tendem a igualar a segurança cibernética e a segurança nacional. Ao fazê-lo, eles estão se conformando com o entendimento tradicional do papel do Estado como garantidor da segurança pública, o que os leva a ver a segurança coletiva no ciberespaço como responsabilidade dos Estados-nação. Essa perspectiva tradicional raramente se concentra no fato de que o ciberespaço é globalmente interoperável, mas existem quase 200 estados-nação diferentes, muitas vezes hostis ou rivais no mundo, em grande parte em um estado de anarquia quando se trata de questões de segurança global (MUELLER, 2017, p.7)[20]

Se, por um lado, com o advento do ciberespaço, tem-se crescimento de oportunidades econômicas - com possibilidade de movimentação de cerca de US$ 3,5 trilhões de dólares apenas com e-commerce em 2025 (FORBES, 2021), além de ganhos em comunicação, e transmissão e difusão de informações - por outro, a interconexão cada vez maior com esse espaço também traz uma série de riscos de segurança, que tendem a crescer ao longo do tempo, sobretudo quando

[19] Internet World Stats. Disponível em: https://www.internetworldstats.com/stats.htm. Acesso em: 01 jan. 2024.

[20] Original: “Many in the cybersecurity community, reflecting their governmental and military roots, tend to equate cyber security and national security. In doing so, they are conforming to the traditional understanding of the state’s role as guarantor of public security, which makes them see collective security in cyberspace as the responsibility of nation-states. This traditional perspective rarely dwells on the fact that cyberspace is globally interoperable but there are nearly 200 different, often hostile or rivalrous nation-states in the world, largely in a state of anarchy when it comes to global security matters.”

infraestruturas críticas, entendidas como serviços essenciais para o funcionamento das sociedades, como plantas hidrelétricas, sistemas bancários, de comunicação, entre outros (FONSECA, ROCHA, 2019) se encontram cada vez mais conectadas ao ciberespaço.

Cabe ressaltar, contudo, algumas diferenças fundamentais que o espaço cibernético possui em relação aos demais espaços de exercício de poder, que o tornam ainda mais necessário de atenção pelos Estados. Medeiros e Goldoni (2020) assim o fazem através da ferramenta que chamaram de *Fundamental Conceptual Trinity of Cyberspace.* A ferramenta busca mostrar como o ciberespaço desafia 3 dos pilares fundamentais das Relações Internacionais: a soberania baseada na territorialidade, o monopólio de poder do Estado, e a *accountability* entre atores internacionais. Dessa forma, o ciberespaço seria caracterizado por i) deterritorialidade, ii) multiplicidade de atores, iii) incerteza.

A deterritolialidade é marcada por conta da imaterialidade da camada não-infraestrutural do ciberespaço. Diferente de outros domínios, esse espaço transcende fronteiras e, uma vez em movimento, os dados se tornam indistinguíveis. É o que permite que possamos acessar dados e informações de quaisquer cantos do mundo, rompendo com a ideia de fronteira e território nacional, e permite a formação de redes globais, de comércio, finanças, crimes, entre outros, dentro desse espaço. Dentro dessa deterritolialidade, contudo, controlar o que entra e o que sai se torna muito difícil, e os Estados se tornam mais vulneráveis a ataques.

A multiplicidade de atores é caracterizada pelo grande volume de usuários da internet. Se inicialmente a ARPANET era uma ferramenta militar, hoje ela está nas mãos de mais da metade da população mundial. Essa ubiquidade, aliada ao baixo custo de entrada nesse espaço, permite uma difusão de poder entre os atores existentes, sobretudo se possuírem boa capacidade de expertise técnica. Essa difusão coloca em risco a segurança nesse espaço, se somada a

> facilidade em desenvolver e distribuir armas cibernéticas, ou seja, códigos de computador com o objetivo de explorar vulnerabilidades e/ou causar algum dano direto ou indireto, contribui para a busca de capacidades cibernéticas cada vez mais agressivas por diversos atores. (MEDEIROS, GOLDONI, 2020, p.42)[21]

[21] Original: “the ease in developing and distributing cyber weapons, that is, computer code with the aim of exploiting vulnerabilities and/or causing some direct or indirect damage, contributes to the pursuit of increasingly aggressive cyber capabilities by different actors [...]”

Já a incerteza pode ser caracterizada por quatro elementos: i) a ausência da permanência dos objetos no ciberespaço, para além da camada física, uma vez que podem ser criados, excluídos, modificados dentro da camada virtual com certa facilidade. Em um exemplo simples, um vírus de computador pode ser modificado inúmeras vezes, dificultando as defesas contra eles. ii) a velocidade, uma vez que a velocidade de ação dentro desse espaço é bem maior do que nos demais, diminuindo as janelas de tomada de decisão. iii) a ausência de formas de mensurar sucesso, uma vez que efeitos de ações cibernéticas nem sempre são facilmente percebidos e quantificados e, às vezes, podem ser estrategicamente ocultados. iv) a anonimidade, advinda da multiplicidade de atores e da dificuldade em identificar quem são.

Essas características apresentam desafios aos Estados nacionais, que historicamente vem tendo controle em torno dos espaços de poder. Ironicamente, o *kybernian* (controle) que deu origem ao termo cibernética, é mais incerto do que certo dentro do universo cibernético. Diante disso, o estabelecimento de "regras de convivência" no ciberespaço, e para seus componentes ciber-físicos, se torna essencial e, por isso, é importante se falar de governança. Mas, antes disso, outro conceito que cabe ser bem compreendido é o de poder nesse espaço. Vejamos um pouco mais sobre isso.

1.2.2 Poder no âmbito cibernético

Sendo um espaço estratégico, tanto em termos de oportunidades, quanto em termos de segurança, o ciberespaço vem seguindo o caminho dos outros domínios (terrestre, aéreo, marítimo e espacial) em ganhar destaque entre as prioridades estatais. Uma vez que se entende o espaço cibernético como um domínio, passamos a compreendê-lo como um espaço de exercício de poder. Tal poder, segundo Nye, pode ser classificado como:

> a capacidade de obter resultados preferenciais por meio do uso de recursos de informação eletronicamente interconectados do domínio cibernético. Em uma definição amplamente utilizada, o poder cibernético é "a capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais e através dos instrumentos de poder". O poder cibernético pode ser usado para produzir resultados preferidos no ciberespaço ou pode usar instrumentos cibernéticos para produzir resultados

> preferidos em outros domínios fora do ciberespaço" (NYE, 2010, p.4, grifo do autor)[22]

Ou seja, um novo ambiente no qual pode-se utilizar dos recursos existentes para buscar vantagens e resultados estratégicos aos atores que exercem esse poder. Partindo dessa lógica, quanto maior a capacidade de exercer poder nesse ambiente, maior a capacidade de obter resultados estratégicos a partir dele. Essa perspectiva é interessante para quem exerce o poder, assim como é arriscada para aqueles sobre os quais o poder é exercido. Se olharmos sob essa perspectiva, fica mais fácil entender a disputa de narrativas entre China, Rússia e o Ocidente sobre a forma como o espaço cibernético deve ser regido.

Uma outra definição que dialoga com essa é a presente no *National Cyber Power Index 2022,* que define 8 objetivos, cada um com uma série de indicadores e, a partir deles, entende o poder cibernético como "a implantação efetiva de capacidades cibernéticas por um estado para atingir seus objetivos nacionais" (BELF CENTER, 2023, p.7)[23]. É com base nisso que se chega à classificação tomada aqui como critério de seleção para a escolha dos países a serem observados. Parte-se da premissa de que os Estados mais "poderosos" terão maior capacidade de agência em relação aos sistemas ciber-físicos, caso tenham isso como objetivo.

Adam Segal, no excelente "The *Hacked World Order*", também reflete sobre o tema e traz alguns componentes relevantes que percebe entre os mais poderosos no campo cibernético: o tamanho da economia; capacidade tecnológica (poder econômico e tecnológico); instituições públicas conectadas com instituições privadas; militares e agências de inteligência vorazes; e uma narrativa atrativa sobre o ciberespaço (SEGAL, 2016, p.34). Vejamos como o autor aborda esses componentes no quadro abaixo:

---

[22] Original: "the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain. In one widely used definition, cyber power is "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power." Cyber power can be used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace."

[23] Original: "."the effective deployment of cyber capabilities by a state to achieve its national objectives,"

Quadro 1 - Elementos de poder no campo cibernético segundo Adam Segal

Elementos	Descrição
Poder econômico e tecnológico	• Derivado de empresas com capacidade de desenvolver elementos centrais ao funcionamento e interações no ciberespaço (servidores que carregam os dados da internet, telefones e computadores usados para comunicação, aplicativos e serviços web que servem de *gateways* para a internet*.)*
Tamanho da economia[24]	• Estamos falando de número de usuários e, consequentemente, capacidade de consumo desses usuários e a influência que isso exerce nas empresas que disputam os mercados.
Instituições públicas conectadas com instituições privadas	• Está relacionado a habilidade do governo de trabalhar em conjunto com empresas privadas locais, sobretudo em termos de defesa, dado que as empresas privadas "possuem a grande maioria das redes de telecomunicações, energia e transporte*"* (SEGAL, 2016, p.36)[25] e em campos de espionagem, dado que "Quanto mais informações as empresas de tecnologia coletavam, mais atraentes se tornavam para a NSA e outras agências, tanto como alvos quanto como parceiros relutantes*"*. (SEGAL,2016,p.36)[26] • E também está relacionado a conseguir alinhar interesses estatais quando se pensa em comércio e políticas de comércio. "O desafio para os governos que desejam aproveitar a energia e a inovação do setor privado é que as empresas de tecnologia cada vez mais realizam mais negócios no exterior do que em seu próprio país. As empresas são fundamentais para qualquer solução, mas seus incentivos econômicos muitas vezes as levam a tentar encontrar um meio-termo entre os governos." (SEGAL, 2016, p.37)[27]
Militares e agências de inteligência vorazes	• Está ligado à capacidade de inteligência, análise, pesquisa e desenvolvimento, capaz de criar impacto significativo em caso de ataques. Aqui entra um elemento econômico, relacionado à capacidade de investimento do Estado nessa linha, mas também o quão intensa é a competição militar que serve de incentivo à inovação nesse campo. Também se considera a vontade política e a criatividade para usar o potencial militar em momentos estratégicos.
Narrativa atrativa	• Fala da capacidade de estabelecer uma narrativa internacional sobre os propósitos da rede e a forma como ela deve ser administrada.

Fonte: Elaborado pelo autor com base em Segal (2016).

[24] Segal não trata esse tópico separadamente. Ele o aborda dentro do bloco de "Poder econômico e tecnológico". A separação no quadro deriva da interpretação do autor, numa tentativa de facilitar a esquematização.
[25] Original: "own the vast majority of telecom, energy, and transportation networks."
[26] Original: "The more information technology companies collected, the more attractive they became to the NSA and other agencies as both targets and reluctant partners".
[27] Original: " The challenge for governments wanting to harness the energy and innovation of the private sector is that technology companies increasingly do more business abroad than they do at home. Companies are critical to any solutions, but their economic incentives often lead them to try and find the middle ground between governments"

Olhando para cada um deles separadamente, em relação ao poder econômico, Segal traz como exemplo que um elevado percentual dos sites mais acessados na Índia, África do Sul e Brasil são controlados por empresas americanas (Google, Facebook, Twitter, LinkedIn, etc.). Da mesma forma:

> Um e-mail enviado do Brasil para o Peru, por exemplo, pode viajar para Brasília, sair de Fortaleza pela costa através de um cabo submarino, entrar nos Estados Unidos através de Miami, passar pela Califórnia e depois seguir de volta pelo Pacífico até Lima. (SEGAL, 2016, p. 35)[28]

O autor parte da premissa da existência de um grau de influência dos Estados Nacionais sobre as empresas com sede em seu território. Tal premissa não é descartável quando lembramos das revelações trazidas por Edward Snowden, sobre espionagem internacional a partir de dados obtidos por empresas americanas.

Por outro lado, Segal traz o contraponto de inovações tecnológicas como fontes de vulnerabilidade. Segundo ele “novos motores de crescimento econômico e oportunidade - a Internet das Coisas, carros autônomos, cidades inteligentes - estão abertos a ataques cibernéticos destrutivos. O progresso traz uma exposição maior.” [29](SEGAL, 2016, p. 35).

A isso, poder-se-ia argumentar que, por mais que seja um risco considerável, uma vez que se controle o mercado de inovações e seus padrões, esse risco poderia ser diluído e as vulnerabilidades poderiam se tornar uma vantagem em termos de acesso a dados de produtos em outros Estados a partir delas, dependendo de quem as encontre primeiro. Segal entende que, em termos de sofisticação tecnológica, os Estados Unidos teriam uma capacidade única de poder e (consequentes) riscos, mas também aponta que, futuramente, a China enfrentaria o mesmo dilema.

Quando falamos em números de usuários, Segal aponta para um futuro asiático, já que a Ásia possui 42% da população mundial e ainda possui baixos índices de penetração interna, apesar de já possuir, em números absolutos, o maior volume de usuários por região. Ou seja, ainda há um grande mercado a ser explorado pelas empresas que nele se destacarem.

---

[28] Original: “An e-mail sent from Brazil to Peru, for example, might travel to Brasilia, leave Fortaleza on the coast via submarine cable, enter the United States through Miami, pass by California, and then head back down the Pacific to Lima.”

[29] Original: "new engines of economic growth and opportunity—the Internet of Things, self-driving cars, smart cities—are open to destructive cyberattacks. Progress brings greater exposure.”

Em relação à conexão de público-privada, Segal aponta os incentivos econômicos de mercados, como o chinês, como dificuldade e enxerga que Estados menores, e com boa capacidade tecnológica, como Israel, poderiam ter vantagem nesse aspecto, por conta da maior familiaridade, além de relações mais próximas entre os agentes de segurança e as empresas.

Cabe acrescentar que aqui poderíamos dialogar com o ponto anterior, do tamanho econômico. Empresas que possuem maiores laços com seus governos em mercados estratégicos, como as companhias chinesas, poderiam ter maiores vantagens em explorar esses mercados e fortalecer esse aspecto de poder. O contraponto, contudo, é que essa proximidade pode ser observada como um risco de segurança em outros países e acarretar banimentos, como no caso do banimento da Huawei e da ZTE do mercado dos Estados Unidos (POSSA, 2022).

Na linha das capacidades militares, novamente nos deparamos com um elemento econômico, mas também podemos relacionar com a proximidade público-privada. Havendo maior controle sobre a informação, a inovação e os padrões que derivam internacionalmente da inovação, há uma maior capacidade de se antecipar em termos de ataque e defesa nesse campo.

Por fim, a classificação de estórias/narrativas que Segal traz é interessante, pois é nela que conseguimos ver de forma mais clara uma disputa de poder no que tange a governança e padrões no ciberespaço. Disputas sobre como, em que locais, e com quais atores a governança deve ser abordada passam muito por uma disputa de controle sobre qual narrativa prevalece: a de um ciberespaço *multistakeholder*, com decisões conjuntas entre diferentes atores, ou a de um ciberespaço soberano, governado e administrado sob o cetro de Estados Nacionais.

Considerando esses critérios, Segal vê China e Estados Unidos como os únicos *superpowers* em termos cibernéticos, com a Rússia atrás, com uma menor capacidade de inovação e competição tecnológica no longo prazo. (SEGAL, 2016, p.40)

Dessa forma, a partir dos autores aqui abordados, podemos observar o poder cibernético como a habilidade de usar o ciberespaço para obter vantagens esperadas (dentro e fora dele) e conseguimos observar alguns critérios para analisar esse poder que, na visão de Segal, não são alcançáveis a todos os atores dentro do ecossistema. Ele acaba se limitando aos Estados Nacionais, com poucos deles tendo capacidades de se tornar superpotências. Partindo da premissa da existência de poder no campo

cibernético, este também pode ser percebido como um espaço de disputas de poder. Veremos um pouco mais dessas disputas ao longo dos capítulos desta dissertação.

2 GOVERNANÇA DO ESPAÇO CIBERNÉTICO

> Em nenhum momento de todas essas deliberações [orçamentárias] sequer foi considerado fazer cortes em nossos gastos com cibersegurança... navios, aviões, forças terrestres, muitas outras coisas foram deixadas de lado; não a cibersegurança. (Ashton Carter, então vice-secretário de Defesa dos Estados Unidos, em reunião de especialistas em segurança cibernética em São Francisco em fevereiro de 2012. Citado em SEGAL, 2016. p15)[30]

"Governos do Mundo Industrial, vocês gigantes aborrecidos de carne e aço, eu venho do Ciberespaço, o novo lar da Mente. Em nome do futuro, eu peço a vocês do passado que nos deixem em paz. Vocês não são bem-vindos entre nós. Vocês não têm nenhuma soberania onde nos reunimos. [...]" (BARLOW, 1996). O texto de John Barlow, um dos fundadores da *Electronic Frontier Foundation,* na famosa carta da Declaração de Independência do Ciberespaço, de 1996, trazia uma visão do ciberespaço como livre de qualquer jurisdição estatal. Uma utopia autônoma e anárquica, que prometia ser o ápice da liberdade humana.

Quase trinta anos depois, as coisas estão longe do que Barlow imaginou. Reconhecido em uma série de documentos como um espaço de poder - e conflito - o ciberespaço vem ganhando cada vez mais atenção por parte dos Estados Nacionais sob um aspecto securitário. Ao mesmo tempo, ele se tornou um espaço que movimenta gigantescas quantias financeiras e está no centro do desenvolvimento econômico global para as próximas décadas.

Diante do surgimento e da consolidação um espaço com capacidade para mudar não só as telecomunicações, mas de mudar a forma como a própria sociedade está configurada, em termos de comércio, organização da economia, em termos de configuração da informação, em termos de desenvolvimento tecnológico e em termos de segurança, não há como não surgir perguntas como: como esse espaço deve ser organizado? Que regras deve ter? Quem deve ser envolvido? Como será o futuro de tudo isso?

Perguntas como essas vem movimentando o debate em torno da governança do ciberespaço ao longo das últimas décadas. E é com isso que esse capítulo visa dialogar. Parte-se de uma definição do conceito de governança cibernética para, em

[30]Original: "No moment in all those [budget] deliberations was it even considered to make cuts in our cyber expenditures . . . ships, planes, ground forces, lots of other things on the cutting room floor; not cyber"

seguida, abordar a configuração por trás dessa governança e os debates que a envolvem. Posteriormente, faz-se uma breve recapitulação dos principais momentos históricos que envolvem a governança da internet para, por fim, apresentar alguns dos debates que ainda persistem no tema.

2.1 CONCEITUAÇÃO DE GOVERNANÇA CIBERNÉTICA

Uma das primeiras definições mais sólidas de governança da internet advém do World Summit on Information Society, em 2005, onde o artigo 34 da "*Tunis Agenda for Information Society*" traz que:

> uma definição funcional de governança da Internet é o desenvolvimento e a aplicação pelos governos, setor privado e sociedade civil, em suas respectivas funções, de princípios, normas, regras, procedimentos de tomada de decisão e programas compartilhados que moldam a evolução e o uso da Internet. (WSIS, 2005, grifo do autor)[31]

Essa definição, por si, já traz alguns dos aspectos importantes dos debates sobre o espaço cibernético. Por mais que o espaço sem nenhum tipo de controle defendido por Barlow não estivesse mais em voga, a definição apresentada destacava a presença de um tripé que considerava os governos nacionais, mas também o setor privado e a sociedade civil. Esse modelo, que divide as responsabilidades e papéis dentro do espaço cibernético ficaria conhecido como *multistakeholderismo.*

Canabarro (2018), por sua vez, traz uma definição com elementos mais técnicos e políticos. Para ele, a governança passa por administrar padrões globais para os dispositivos da rede (a nível mais estrito) e administrar tensões relacionadas a fluxos globais e infraestruturas, usuários e provedores territoriais (a nível mais amplo):

> Em um sentido estrito, a governança global da Internet diz respeito ao endereçamento numérico e alfanumérico dos dispositivos computacionais terminais e nucleares que integram a Internet e às tarefas de transmissão, roteamento e comutação de pacotes de dados de uma ponta à outra da Rede. Em um sentido mais amplo, a governança da Internet diz respeito à inevitavelmente a tensão existente entre, de um lado, o caráter global de fluxos e transações que ocorrem por meio da Internet, e, de outro, a

[31] Em inglês: "a working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."

> vinculação territorial da infraestrutura, dos usuários e dos provedores de bens e serviços relativos à Internet. (CANABARRO, 2018, p.74)

Em seu “Internet Governance Project”[32], por sua vez, Milton Mueller simplifica a definição em “regras, políticas, padrões e práticas que coordenam e moldam o ciberespaço global” [33], apontando também que:

> Enquanto a conectividade à Internet gerou novos serviços inovadores, capacidades e formas sem precedentes de compartilhamento e cooperação, também criou novas formas de crime, abuso, vigilância e conflito social. A governança da Internet é o processo pelo qual os participantes do ciberespaço resolvem conflitos sobre esses problemas e desenvolvem uma ordem viável." (INTERNET GOVERNANCE PROJECT, 2023, s.p.)[34]

Partindo dessas três definições, conseguimos inferir pontos interessantes. O primeiro deles é que, assim como em outros conceitos que envolvem o ciberespaço, é difícil estabelecer um conceito único para a governança cibernética. Dependendo do momento e do local onde a definição for feita, ela destaca alguns aspectos em detrimento de outros e também representa uma disputa de interesses. A definição do WSIS, por exemplo, conforme apontado por DeNardis e Raymond (2013), é fruto de um contexto histórico específico, no qual havia a preocupação relacionada ao controle unilateral da internet por parte dos Estados Unidos, por meio da relação de seu departamento de comércio com o ICANN. Assim, a declaração traz o elemento dos “governos”, numa tentativa de deixar claro o caráter multilateral do ciberespaço. O *Working Group on Internet Governance* (WGIG), que chegou a essa definição, inclusive, não contou com a participação dos Estados Unidos, que optou por não participar.[35] Segundo os autores, a própria criação do Fórum de Governança da Internet (IGF) parte de uma tentativa de diminuir a coordenação do ciberespaço por parte dos Estados Unidos:

> Também às vezes é esquecido que a convocação do Fórum de Governança da Internet das Nações Unidas (IGF), realizado pela primeira vez em Atenas, Grécia, em 2006, foi um compromisso decorrente de um impasse sobre os

[32] Internet Governance Project. Disponível em: https://www.internetgovernance.org/what-is-internet-governance/. Acesso em:01 jan.2024.
[33] Original: "rules, policies, standards and practices that coordinate and shape global cyberspace.”
[34]Original: [...] while Internet connectivity generated innovative new services, capabilities and unprecedented forms of sharing and cooperation, it also created new forms of crime, abuse, surveillance and social conflict. Internet governance is the process whereby cyberspace participants resolve conflicts over these problems and develop a workable order."
[35] O grupo contou com a participação de 40 membros, com predomínio de governos, mas também com alguns representantes do setor privado e sociedade civil. Para mais informações, verificar o relatório do Working Group. Disponível em: https://www.wgig.org/docs/WGIGREPORT.pdf.

> apelos das Nações Unidas e dos governos para a diminuição da coordenação dos Estados Unidos de certas funções administrativas da Internet e a resistência americana a essas recomendações (DENARDIS, 2013, p.8)[36]

O segundo ponto a observar é a percepção da necessidade da definição de uma série de padrões, regras e processos a nível global para permitir o funcionamento da rede, que está longe de ser tarefa simples. Canabarro apresenta o principal deles, do endereçamento numérico e alfanumérico, mas para além desse, existem uma série de outros. Em um esforço de mapear esses processos, DeNardis e Raymond (2013, p.4) dividem a Governança da Internet em seis grandes áreas, cada uma com uma série de tarefas, totalizando 44 tarefas no total. I. Controle de recursos críticos da internet[37]; II. Definição dos padrões da internet[38]; III. Coordenação de Acesso e Interconexão[39]; IV. Governança da Cibersegurança[40]; V. Intermediação da informação[41]; VI. Aplicação de direitos de propriedade intelectual *"Architecture based"*[42]. Esse grande volume de tarefas é realizado por uma série de organizações públicas e privadas. Cabe lembrar que, na medida em que novas tecnologias surgem e se aperfeiçoam dentro desse espaço, como no caso dos sistemas ciber-físicos, regras, padrões e processos precisam ser criados para englobá-los. Ou seja, os processos mapeados pelos autores em 2013 tendem a estar mais complexos ou com forte tendência a se complexificar atualmente.

---

[36] Original: Also sometimes lost is that the convocation of the United Nations Internet Governance Forum (IGF), first held in Athens, Greece in 2006, was a compromise emanating from an impasse over United Nations and governmental calls for a diminishment of United States coordination of certain Internet administrative functions and American resistance to these recommendations.

[37] Tarefas previstas: Central Oversight of Names and Numbers; Technical Design of IP Addresses; New Top-Level Domain Approval; Domain Name Assignment; Oversight of Root Zone File; IP Address Distribution (allocation/assignment); Management of Root Zone File; Autonomous System Number Distribution; Operating Internet Root Servers; Operating Internet Root Servers.

[38] Tarefas previstas: Protocol Number Assignment; Designing Core Internet Standards; Designing Core Web Standards; Establishing Other Communication Standards;

[39] Tarefas previstas: Facilitating Multilateral Network Interconnection; Peering and Transit Agreements to Interconnect; Setting Standards for Interconnection (e.g. BGP); Network Management (Quality of Service); Setting End User Access and Usage Policies; Regulating Access (e.g. Net Neutrality).

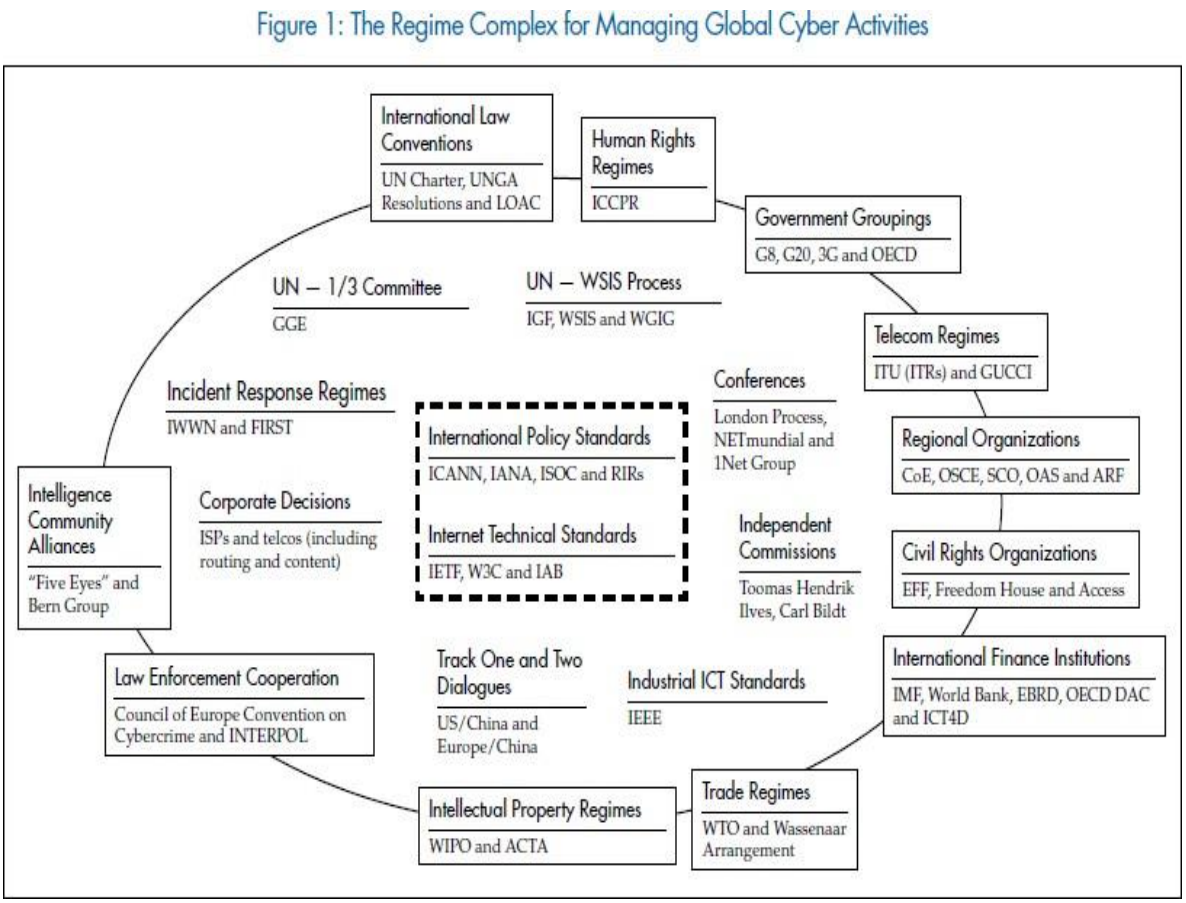
[40] Tarefas previstas: Securing Network Infrastructure; Designing Encryption Standards; Cybersecurity Regulation/Enforcement; Correcting Software Security Vulnerabilities; Software Patch Management; Securing Routing, Addressing, DNS; Responding to Security Problems; Responding to Security Problems.

[41] Tarefas previstas: Commercial Transaction Facilitation; Mediating Government Content Removal Requests (Discretionary Censorship); App Mediation (Guidelines, Enforcement); App Mediation (Guidelines, Enforcement); Responding to Cyberbullying and Defamation; Regulating Privacy, Reputation, Speech; Mediating Govt. Requests for Personal Data.

[42] Tarefas previstas: Domain Name Trademark Dispute Resolution; Removal of Copyright Infringing Content; Algorithmic Enforcement (e.g. Search Rankings); Algorithmic Enforcement (e.g. Search Rankings); Domain Name System IPR Enforcement; Regulating Online IPR Enforcement; Standards-Based Patent Policies; Enacting Trade Secrecy in Content Intermediation.

Nye (2014) seguiu um esforço semelhante em mapear os processos e atores, e tentou dividi-los em blocos de discussão, com variados graus de interação entre si, no que chamou de "*Regime Complex for Managing Global Cyber Activities*". A figura abaixo ilustra o modelo de Nye.

Figura 2 - O Regime cibernético de Nye



Fonte: NYE, Joseph S. et al. **The regime complex for managing global cyber activities**. USA: Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, 2014, p.8

Dentro do modelo conseguimos visualizar uma série de discussões e processos que acontecem concomitantemente, envolvendo diferentes atores. Conforme aponta o autor, o esforço é uma tentativa de ampliar a visualização da governança para além da disputa multilateralismo x *multistakeholderismo* - que, como veremos posteriormente, ainda é um ponto importante na discussão:

> O mapa oval das atividades de governança cibernética mistura normas, instituições e procedimentos, alguns dos quais são de grande escala, enquanto outros são relativamente pequenos; alguns são bastante formais e

> outros muito informais. O oval não foi projetado para mapear todas as atividades de governança no ciberespaço (o que é uma empreitada massiva) e, portanto, é deliberadamente incompleto. Como todas as heurísticas, distorce a realidade ao simplificar. No entanto, é um corretivo útil para a habitual dicotomia ONU versus *multistakeholder* como uma abordagem para a governança cibernética, e situa a governança da Internet dentro do contexto maior da governança cibernética. (NYE, 2014)[43]

Um terceiro ponto que precisamos levar em consideração, a partir da percepção desse volume de diferentes atores que estão envolvidos na prática nos processos, por fim, é o de que, conforme aponta Canabarro em sua definição, a governança envolve tensões entre os atores. Olhando mais diretamente para esses atores, Madeline Carr (2015) destaca jogos de poder dentro do espaço cibernético. A autora parte de uma ótica que considera o ciberespaço como um espaço de projeção de poder:

> A governança da Internet está envolta em política, interesses e legitimidade contestada. Isso não se deve, como alguns podem argumentar, ao envolvimento indevido dos governos. Em vez disso, é porque a Internet é um mecanismo para a projeção de poder - poder suave através da dominação cultural e linguística, poder duro através de ataques cibernéticos como o Stuxnet, coleta de inteligência e ganho comercial [...] (CARR, 2015, p. 643)[44]

Ou seja, dentro desse espaço, existem uma série de decisões técnicas, mas que também possuem implicações políticas que não podem ser ignoradas. Quando se parte desse ponto, cabe considerar qual das alternativas melhor atende aos interesses políticos dos atores envolvidos. Um modelo *multistakeholder*, com uma miríade de atores estatais, privados e da sociedade civil possuindo algum grau de poder decisório; um modelo multilateral, que foca em Estados Nacionais no sentido clássico Westphaliano ou um modelo supranacional, onde uma organização, como a ITU, poderia delimitar as regras de governança. (CARR, 2015). Esses modelos vão e voltam dentro dos debates e narrativas dos atores envolvidos nos debates.

---

[43] Original: The oval map of cyber governance activities [...] mixes norms, institutions and procedures, some of which are large in scale, while others are relatively small; some are quite formal and some very informal. [...] The oval is not designed to map all governance activities in cyberspace (which is a massive undertaking) and, thus, is deliberately incomplete. Like all heuristics, it distorts reality as it simplifies. Nonetheless, it is a useful corrective to the usual UN versus multistakeholder dichotomy as an approach to cyber governance, and it locates Internet governance within the larger context of cyber governance.

[44] Original: Internet governance is mired in politics, interests and contested legitimacy. This is not, as some might argue, because governments have undue involvement. Rather, it is because the Internet is a mechanism for the projection of power – soft power through cultural and linguistic dominance, hard power through cyber attacks like Stuxnet, intelligence gathering and commercial gain [...]

Partindo das definições abordadas e considerando - a partir das reflexões aqui trazidas - a governança cibernética como um esforço constante de administrar e buscar equilibrar poder e interesses dos vários atores envolvidos, enquanto se estabelece, se mantém e se atualizam os padrões, regras e processos que tornam o ciberespaço possível, vejamos uma breve recapitulação desse esforço ao longo dos últimos anos.

2.2 UM BREVE HISTÓRICO DA GOVERNANÇA DA INTERNET

O foco desta seção, conforme aponta seu título, está em observar o histórico da governança. Para isso, primeiramente parte-se de uma divisão em blocos históricos, utilizando como base Muller e Badie (2020), com destaque para o processo de securitização percebido por eles. Posteriormente, alguns dos principais marcos em torno da governança do ciberespaço são adicionados em um quadro de linha do tempo.

2.2.1 Fases da governança

Mueller e Badiei (2020) dividem a governança da internet em 4 fases, sistematizadas no quadro abaixo, a partir da observação das pesquisas e debates produzidos sobre o tema desde seu surgimento.

Quadro 2 - As fases da governança da internet (continua)

Fase	Principais acontecimentos
Fase 1(1993–1997) Discovery *and Exceptionalism*	• Emergência da internet como um meio de massas; • Início da utilização de termos como “cyberspace”, “internet”, “the Net”; “governance”, “law”, de forma associada; • Início do discurso do ciberespaço como espaço “excepcional”, que deveria regras e instituições próprias, independente de governos nacionais; • Foco das produções em um campo de “legal studies” e predominantemente nos Estados Unidos.

Quadro 2 - As fases da governança da internet (conclusão)

Fases	Principais acontecimentos
Fase 2 (1996–2003): ICANN Über Alles	• Surgimento do termo “internet governance” atrelado a formação do ICANN, focado na coordenação do DNS e dos endereços IP. • Maior parte da literatura do período tratado dos debates em torno do ICANN e suas atribuições, além de sua relação com o governo dos Estados Unidos.
Fase 3 (2003–2009): *World Summit on the Information Society* e *Internet Governance Forum*	• Realização do World Summit on the Information Society (WSIS 2002 - 2005), por meio do UN Working Group on Internet Governance (WGIG); • Definição de “governança da internet” desenvolvida no WSIS indo além do escopo do ICANN, consolidando a posição de atores não estatais no debate, e preservando o modelo “multistakeholder” • Crescimento de plataformas de mídias sociais (Facebook, Twitter, Google) • Criação do Fórum de Governança da Internet, em caráter multistakeholder, em 2006. • Criação do Global Internet Governance Academic Network (GigaNet) em 2006. • Debates sobre direitos autorais e de propriedade na rede.
Fase 4 (2010–): *Surveillance, Securitization, and Alignment*	• Questões de vigilância, privacidade e segurança cibernética passando a predominar nas produções e debates; • Processo de securitização do espaço cibernético, com aproximação da governança da internet dos Estados Nacionais; • Ciência política e Relações Internacionais entrando no debate da governança, com seus respectivos temas (guerras, espionagem, dissuasão, grupos terroristas, ameaças a infraestruturas críticas; • Caso Snowden; • Tech-nacionalismo, com empresas de tecnologia sendo barradas de Estados, sob acusação de espionagem para outro Estado (ex. Huawei).

Fonte: Elaborada pelo autor, com base em Mueller e Babiei (2020)

A partir das quatro fases dos autores, podemos perceber uma tendência de aproximação do debate, de um campo anteriormente mais técnico para um campo mais político, com maior conexão com os Estados Nacionais. Cabe dar um foco especial para quarta fase, de securitização, que se estende até hoje. É justamente nessa fase que os sistemas ciber-físicos - abordados no capítulo seguinte - surgem e podem contribuir ainda mais para essa tendência securitária. Não só pela complexidade crescente que adicionam, mas por adicionarem novas brechas de

segurança para coletas de dados, e mesmo eventuais ciberataques, como o caso do Mirai botnet[45].

Tudo isso pesa em uma balança securitária que já se encontrava pesada após as revelações do "Caso Snowden", sobre atividades de vigilância e monitoramento realizado pela NSA - a *National Security Agency*, dos Estados Unidos que acentuaram as tensões entre Estados, e evidenciaram a presença (visível ou não) dos Estados em meio à governança do ciberespaço. Em um âmbito mais visível, após Snowden, aconteceram reações diplomáticas importantes. O próprio Brasil foi protagonista ao questionar a posição dos Estados Unidos sobre o ICANN (CANABARRO, 2014), pauta que, historicamente, já vinha sendo questionada por China e Rússia. Mas, mais do que isso, esse acontecimento contribuiu como evidência para diminuir a confiança entre os Estados num campo onde a confiança já é um elemento difícil. Conforme aponta Nye:

> Os Estados Unidos reclamaram da espionagem cibernética chinesa que rouba propriedade intelectual e levantaram a questão na cúpula entre o presidente dos EUA, Barack Obama, e o presidente da República Popular da China, Xi Jinping, em junho de 2013. No entanto, o esforço dos EUA para criar uma norma que diferencie a espionagem para ganho comercial de todas as outras espionagens foi perdido no barulho criado pelas revelações de extensa vigilância da Agência de Segurança Nacional (NSA) divulgadas por Snowden. (NYE, 2014, p.10)[46]

A percepção de securitização do processo de governança da internet e do ciberespaço também é percebida em trabalhos como o de Segal (2016), Louise Marie Hurel (2016) e Mueller (2017). Segal enxerga o período entre o meio do ano de 2012 e o meio do ano de 2013 como um marco ("ano zero") nesse processo, apontado que, a partir dali, caiu por terra o resquício de utopia livre da geopolítica que ainda pairava sobre o ciberespaço.

> Foi em 2012 que os estados-nação ao redor do mundo reafirmaram visivelmente seu controle sobre o fluxo de dados e informações em busca de poder, riqueza e influência, finalmente sepultando o já abalado mito do

[45] Para entender mais sobre o ataque, ver: https://olhardigital.com.br/2016/11/29/seguranca/mega-ataque-deixou-quase-1-milhao-de-pessoas-sem-internet-na-alemanha/.

[46] Original:" The United States has complained about Chinese cyber espionage that steals intellectual property, and raised the issue at the summit between US President Barack Obama and President of the People's Republic of China Xi Jinping in June 2013. However, the US effort to create a norm that differentiates spying for commercial gain from all other spying has been lost in the noise created by the revelations of extensive National Security Agency (NSA) surveillance released by Snowden."

> ciberespaço como uma utopia digital, livre de geopolítica convencional. (SEGAL, 2016, p.1)[47]

Para o autor, os dois principais pontos que culminaram nesse processo foram: o Stuxnet (primeiramente detectado em 2010) e a complexidade nele envolvida, que apontava para o envolvimento de um Estado intencionalmente utilizando o ciberespaço para causar dano a outro, inaugurando uma nova era de ataques cibernéticos patrocinados por Estados, e de maiores investimentos em capacidades cibernéticas ofensivas e defensivas dentro deles; o outro critério é o próprio caso Snowden que, ao expor o modelo de vigilância em massa que os Estados Unidos vinham adotando, mina a confiança entre os Estados e acende neles sinais de alerta.

Hurel (2016), apesar de perceber e advogar por uma abordagem mais integrada e colaborativa, aponta como os campos da governança da internet e da cibersegurança vem competindo por recursos, legitimidade e influência.

Mueller (2017), por sua vez, também percebe a existência de uma tendência, dentro da comunidade de cibersegurança, de trazer o debate mais para o escopo dos Estados Nacionais sobre a própria justificativa dos riscos nele envolvidos.

> O mundo da cibersegurança contém muitos defensores da governança multissetorial, mas se olharmos de perto para as pessoas e instituições que avançam essas ideias em contextos de cibersegurança, descobrimos que quase sempre vêm do mundo da governança da internet. No mundo da cibersegurança como um todo, o discurso, os valores e os modelos de governança são muito mais inclinados à direita (ou seja, em direção a modelos centrados no estado). Em alguns dos casos mais extremos, intelectuais da área de ciber segurança citam explicitamente preocupações com a cibersegurança para rejeitar a governança da internet multissetorial por atores não estatais. **(**MUELLER, 2017, p. 417, grifo do autor**)**[48]

Um exemplo direto trazido pelo autor é o de que grupos conservadores dentro dos Estados Unidos argumentaram que a transição IANA, que retirou o controle contratual dos Estados Unidos sobre o ICANN, abria margem para que China e Rússia obtivessem maior controle sobre o ICANN no âmbito das Nações Unidas.

---

[47] Original: “it was in 2012 that nation-states around the world visibly reasserted their control over the flow of data and information in search of power, wealth, and influence, finally laying to rest the already battered myth of cyberspace as a digital utopia, free of conventional geopolitics.”

[48] Original: The cybersecurity world contains many advocates of multistakeholder governance, but if one looks closely at the people and institutions that advance these ideas in cybersecurity contexts, one finds that they almost always come from the world of internet governance. In the cybersecurity world as a whole, the discourse, values and governance models are much more skewed to the right (i.e., toward state-centric models). In some of the more extreme cases, cyber intellectuals explicitly cite cybersecurity concerns to reject multistakeholder internet governance by nonstate actors.

Embora a transição do ICANN para uma organização independente tenha ocorrido - apesar de quaisquer protestos - começando em 2013 e terminando em 2016, no que Canabarro (2018) chamou de “longo 2014”, o ambiente do ciberespaço ainda está longe de uma harmonia e consenso em termos de governança.

Pijovic (2021) enxerga a existência de uma competição entre um bloco Sino-Russo e o “Five Eyes” (Estados Unidos, Reino Unido, Austrália, Canadá e Nova Zelândia), no tocante à como as normas que regem o ciberespaço devem ser moldadas. Entre os principais pontos de divergência, está a diferença conceitual entre “*cyber security*”, mais presente em documentos do Ocidente, e “*information security*”, mais presente em China e Rússia: “para o Five Eyes, a segurança cibernética é principalmente sobre a integridade dos sistemas que fornecem as informações e, apenas por extensão, as próprias informações” (p. 224)[49], o que é percebido de uma forma diferente pelo outro grupo.

O segundo ponto é o da “soberania cibernética”, que aparece nas narrativas sino-russas.

> Em abril de 2015, o acordo da China e da Rússia "sobre cooperação para garantir a segurança internacional da informação" formalizou o bloco sino-russo de segurança cibernética. O acordo deixou clara a preocupação primordial do bloco com a soberania cibernética ao enfatizar que “o Estado tem o direito soberano de definir e implementar políticas públicas em matéria de TIC e internet”.. (PIJOVIC, 2021, p. 225)[50]

A terceira grande diferença, por sua vez, está na visão de a partir de onde o ciberespaço deve ser governado. O famoso debate *multilateralismo x multistakeholderismo*, que embora seja apontado como uma simplificação excessiva por Nye (2014), não pode ser desconsiderado ao se tratar de governança. China e Rússia partem de uma agenda reformista, que busca trazer para a ONU o debate, desafiando o modelo *multistakeholder* tradicional do ICANN, defendido pelo Ocidente.

> A agenda sino-russa de reforma da governança da Internet é ampla, buscando aprimorar o papel da ONU reformando a Corporação da Internet para Atribuição de Nomes e Números (ICANN) e substituindo a Convenção de Budapeste por um novo tratado de crimes cibernéticos da ONU. A China

[49] Original: “for the Five Eyes, cyber security is primarily about the integrity of the systems delivering the information, and only by extension the information itself”

[50] Original: “In April 2015, China and Russia’s agreement ‘on cooperation in ensuring international information security’ formalized the Sino-Russian cyber security bloc. The agreement made clear the bloc’s primary concern with cyber sovereignty by emphasizing that ‘the state has the sovereign right to define and implement public policies on matters relating to’ ICT and the internet [...].”

> vai “pressionar pela reforma institucional do Fórum de Governança da Internet da ONU para permitir que ele desempenhe um papel maior na governança da Internet” e “promover vigorosamente a reforma da ICANN para torná-la uma instituição internacional verdadeiramente independente, aumentar suas representações e garantir maior abertura e transparência em sua tomada de decisão e operação” (MFAPRC 2017). A Rússia vê o transnacionalismo da Convenção de Budapeste como uma violação dos "princípios da soberania do Estado e da não-interferência"[...] (PIJOVIC, p.226)[51]

China e Rússia vêm se destacando nas últimas décadas como representantes de uma perspectiva na qual as telecomunicações devem ser governadas a partir de um predomínio dos Estados, com menor relevância para o modelo de *multistakeholder*, no qual atores e instituições não estatais possuem maior relevância. (NOCETTI, 2015). Os dois países vêm desenvolvendo uma narrativa, presente em seus documentos de defesa, que apresenta o espaço cibernético como um espaço de ameaça, que exige maior controle por parte dos Estados e deve estar sob sua soberania. A Cyberspace Security Strategy (2016) da China, por exemplo, traz como um de seus princípios:

> “(1) Respeitar e proteger a soberania no ciberespaço: Nenhuma violação da soberania no ciberespaço será tolerada, os direitos de todos os países de escolher independentemente seu caminho de desenvolvimento, método de gerenciamento de rede e política pública da Internet, bem como de participar igualmente na governança internacional do ciberespaço serão respeitados.” (CHINA, 2016)[52]

Já a Rússia, apesar de não usar o termo “cyber”, demonstra por diversas vezes preocupação com a segurança da informação em seus documentos de defesa. Na Doutrina de Segurança da Informação (2016), por exemplo, aparece que:

> 29. Os principais impulsos para garantir a segurança da informação no campo da estabilidade estratégica e parceria estratégica igualitária são os seguintes: proteger a soberania da Federação Russa no espaço da informação por meio de políticas independentes e de propriedade nacional para perseguir seus

[51] Original: “The Sino-Russian internet governance reform agenda is wide, seeking to enhance the UN’s role by reforming the Internet Corporation for Assigned Names and Numbers (ICANN) and replacing the Budapest Convention with a new UN cyber crime treaty. China will ‘push for institutional reform of the UN Internet Governance Forum to enable it to play a greater role in Internet governance’ and ‘vigorously promote the reform of ICANN to make it a truly independent international institution, increase its representations and ensure greater openness and transparency in its decision-making and operation’ (MFAPRC 2017). Russia views the Budapest Convention’s transnationalism as violating ‘principles of state sovereignty and non-interference’[...]”

[52] Traduzido do inglês: “(1) Respecting and protecting sovereignty in cyberspace: No infringement of sovereignty in cyberspace will be tolerated, the rights of all countries to independently choose their development path, network management method and Internet public policy, as well as to equally participate in international cyberspace governance will be respected. [...]”

> interesses nacionais na esfera da informação" (FEDERAÇÃO RUSSA, 2016)[53]

Veremos um pouco mais dessas divergências de visões e posicionamentos no capítulo 4. Por ora, o que vale ressaltar é que embora tenha partido de um princípio mais técnico, com menor grau de envolvimento Estatal em suas discussões, o ciberespaço e a governança têm se tornado um ambiente de disputas de poder e de narrativa. Apesar disso, não é um ambiente de conflito declarado pois, ao mesmo tempo em que os países se posicionam de forma diferente, e apresentam alguns impasses, também se colocam abertos a processos de diálogo em uma série de mecanismos estabelecidos para esse fim. A linha do tempo, trazida na sequência, busca apresentar um pouco dessa dualidade que marca a governança do ciberespaço.

2.2.2 Linha do tempo de principais acontecimentos

Olhando sob uma ótica de linha do tempo, o quadro abaixo representa alguns dos principais destaques relacionados à governança nas últimas duas décadas. O quadro busca ser completo, mas, obviamente, não consegue abordar todos os acontecimentos dos múltiplos fóruns regionais que abordam governança da internet. Dá-se um enfoque maior aos processos dentro do âmbito das Nações Unidas.

[53] Traduzido do Inglês: "The main thrusts of ensuring information security in the field of strategic stability and equal strategic partnership are the following: protecting the sovereignty of the Russian Federation in information space through nationally-owned and independent policy to pursue its national interests in information sphere [...]"

Quadro 3 - Linha do tempo dos principais acontecimentos relacionados à governança (continua)

Ano	Acontecimento	Relevância do acontecimento
1999	Início dos debates sobre segurança cibernética na ONU, a partir da adoção da resolução A/RES/53/70, de 4 de janeiro de 1999[54]	Com base em proposta elaborada pela Rússia em setembro de 1998, o ano de 1999 marca os primeiros debates sobre o tema no âmbito das Nações Unidas, que continue até os dias atuais
2003 - 2005	Processo do WSIS na ONU[55]	Processo de diálogo que culminou com a definição clássica de governança da internet
2006	Criação do Fórum de Governança da Internet (IGF)[56]	Criado para ser o principal fórum de debate *multistakeholder* sobre governança da internet do mundo, o IGF realiza reuniões anuais e produz relatórios e recomendações a partir delas. As sedes das reuniões variam ano a ano.
2010	Relatório do UN Governamental Group of Experts (GGE) sobre segurança cibernética[57]	O relatório foi aprovado em consenso pelos membros, trazendo uma série de recomendações para aumentar o diálogo entre os Estados para diminuir riscos e estabelecer infraestruturas críticas nacionais e internacionais seguras; também se falava em medidas de geração de confiança; elaboração de termos comuns; e troca de informações sobre legislações e capacidades nacionais sobre o tema.
2012	Conferência Mundial sobre a Regulamentação das Telecomunicações Internacionais (WCIT)	Prevista para atualizar *International Telecommunications Regulation* (ITR), no âmbito da UIT, incluindo a internet, a conferência foi marcada pelo seu fracasso em atingir um consenso. No fim, a internet não foi mencionada no texto da ITR.

[54] A resolução pode ser acessada em: https://digitallibrary.un.org/record/265311
[55] O relatório final pode ser encontrado em: https://www.wgig.org/docs/WGIGREPORT.pdf.
[56] Site oficial: https://www.intgovforum.org/en. Acesso em: 01 jan. 2024.
[57] Mais informações em: https://dig.watch/resource/un-gge-report-2010-res-a65201.

Quadro 3 - Linha do tempo dos principais acontecimentos relacionados à governança (continuação)

Ano	Acontecimento	Relevância do acontecimento
2013	O caso Snowden	O caso Snowden muda a tônica dos debates sobre governança, gerando uma série de questionamentos sobre o papel dos Estados Unidos enquanto guardião da internet
2013	Relatório do UN GGE reconhecendo que a Lei Internacional se aplica ao espaço cibernético [58]	Também adotado em consenso, o documento marca o reconhecimento de que a Lei Internacional e a Carta da ONU se aplicam ao ciberespaço. De lá para cá, no entanto, ainda não houve consenso em termos de mecanismos de atribuição de ataques cibernéticos que justifiquem retaliações dentro da Lei Internacional.
2013	Anúncio da Transição IANA	Em meio à pressão internacional, os Estados Unidos anunciam que seu Departamento de Comércio deixaria a supervisão das funções IANA.
2014	Realização da NETMundial (Encontro Multissetorial sobre o futuro da governança da internet)	Realizado em parceria entre o Brasil e a 1NET, o fórum ganhou relevância em meio aos debates pós-caso Snowden, mas se enfraqueceu após o anúncio da transição IANA, conforme aponta Canabarro (2018). Apesar disso, foi elaborada a Declaração Multissetorial de São Paulo[59]
2015	Relatório do UN GGE com introdução de 11 princípios de governança cibernética [60]	Também adotado em consenso, o documento estabelece uma série de princípios que deveriam ser adotados para se pensar a governança cibernética.

[58] Relatório do UN GGE reconhecendo que a Lei Internacionalse aplica ao espaço cibernético. Disponível em: https://dig.watch/wp-content/uploads/A_68_98_E.pdf.Acesso em: 01 jan. 2024.
[59] Declaração Multissetorial de São Paulo. Disponível em: https://www.cgi.br/media/docs/publicacoes/4/Documento_NETmundial_pt.pdf. Acesso em: 01 jan. 2024.
[60] Relatório do UN GGE com introdução de 11 princípios degovernança cibernética. Disponível em: https://dig.watch/wp-content/uploads/2022/08/UN-GGE-2015-report.pdf. Acesso em: 01 jan. 2024.

Quadro 3 - Linha do tempo dos principais acontecimentos relacionados à governança (continuação)

Ano	Acontecimento	Relevância do acontecimento
2015	Proposição de Código de Conduta por Rússia, China, Quirguistão, Cazaquistão, Tadjiquistão e Uzbequistão[61]	Os países citados propuseram uma versão atualizada de um Código de Conduta para segurança da informação, anteriormente submetido em 2011. O documento é citado em documentos dos países como sugestão de caminho a ser tomado para estabelecimento de uma legislação própria para o tema, no âmbito da ONU.
2016	Finalização da transição IANA	Se completa o processo iniciado em 2013
2018	Estabelecimento do UN OEWG[62]	Em meio a impasses para novos consensos no UN GGE, um grupo paralelo, organizado dentro da Assembleia Geral da ONU, foi criado. O OEWG reconheceu todos os relatórios adotados em consenso pelo UN GGE e, até 2021, funcionou em paralelo a ele.
2020	Renovação do UN OEWG para 2021-2025	Ao final de seu primeiro mandato 2019 - 2021, o OEWG ganhou uma renovação por mais 4 anos e é, atualmente, o principal espaço de discussão sobre governança da internet dentro da ONU.
2021	Relatório final do primeiro UN OEWG[63]	Encerrando o primeiro ciclo do OEWG, o relatório traz elementos sobre normas, ameaças, medidas de geração de confiança e lei internacional. Esse padrão de tópicos se mantém nas discussões do atual OEWG.

[61]Mais informações em: https://ccdcoe.org/incyder-articles/an-updated-draft-of-the-code-of-conduct-distributed-in-the-united-nations-whats-new/. Acesso em: 01 jan. 2024.
[62] Estabelecimento do UN OEWG. Disponível em: https://dig.watch/wp-content/uploads/2022/08/UN-GA-2018-OEWG.pdf. Acesso em: 01 jan 2024.
[63] Relatório final do primeiro UN OEWG. Disponível em: https://dig.watch/wp-content/uploads/2022/08/OEWG-Report.pdf. Acesso em: 01 jan. 2024.

Quadro 3 - Linha do tempo dos principais acontecimentos relacionados à governança (conclusão)

Ano	Acontecimento	Relevância do acontecimento
2021	Relatório final do último UN GGE [64]	O relatório reforça discussões anteriores e marca o fim das discussões dentro do UN GGE.
2022	Adoção da resolução do Program of Action[65]	Proposto, de forma conjunta, por 40 países, incluindo Austrália, Reino Unido e Estados Unidos, e com oposição da Rússia, o Program of Action tem a narrativa de se tornar o fórum permanente na ONU para discussões sobre uso de ICTs em âmbito de segurança internacional após o encerramento do UN OEWG, em 2025.

Fonte: Elaborado pelo autor, com base em referências como <https://dig.watch/processes/un-gge>; <https://www.internetgovernance.org/what-is-internet-governance/> e Canabarro (2018)

De forma geral, o centro dos debates de governança do ciberespaço no âmbito dos últimos relatórios dos grupos dentro da ONU gira em torno de cinco grandes temas: 1. As ameaças existentes e emergentes; 2. Normas, regras e princípios para o comportamento dos Estados; 3. A aplicação da Lei Internacional ao ciberespaço; 4. Medidas de geração de confiança; 5. Cooperação internacional e assistência em segurança e criação de capacidades em ICTs. Dentro desses temas, os fóruns têm sido o espaço de apresentar e debater visões, com os países submetendo seus posicionamentos. Embora ricos em caráter informativo e de diálogo, os fóruns encontram dilemas políticos.

Enquanto ocorreram em paralelo, o UN GGE e o UN OEWG concorreram enquanto espaço de discussão, com o primeiro tendo a prevalência dos Estados Unidos e seus aliados e o segundo com a prevalência da Rússia (PJOVIC, 2021). Após a finalização do UN GGE, essa tendência não demorou a retornar com a adoção do *Programe of Action*. Essa percepção é apontada pela própria Rússia, que, em seu documento de visões sobre o *Program of Action*, apresentado no OEWG, traz que:

> As discussões no OEWG mostram que até mesmo os defensores do PoA não têm uma posição comum sobre seus parâmetros específicos, mais importante

[64] Relatório final do último UN GGE. Disponível em:https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf. Acesso em: 01 jan.2024.
[65] Adoção da resolução do Program of Action. Disponível em: https://digitallibrary.un.org/record/3991743?ln=en. Acesso em: 01 jan. 2024.

> ainda, sobre o procedimento de tomada de decisão. Vale ressaltar que os países ocidentais atribuem um significado político muito específico ao Programa de Ação, eles o promovem publicamente para antagonizar a Rússia. Eles justificam a necessidade de estabelecer o PoA pelas supostas atividades maliciosas de nosso país no espaço da informação, incluindo no contexto da operação militar especial na Ucrânia (esses argumentos foram mencionados, especificamente, pelos representantes franceses na OSCE). Tal causa anti-russa não pode servir de base para uma interação construtiva entre Estados no IIS. Isso contradiz o espírito da Carta da ONU e, especificamente, seu Artigo 1 sobre igualdade e relações amigáveis entre Estados. Nessas circunstâncias, espera-se que o PoA seja usado pelos países ocidentais para impor regras e padrões não vinculativos de seus interesses, substituindo assim as normas do direito internacional - em consonância com o conceito de ordem baseada em regras promovido pelos EUA. (FEDERAÇÃO RUSSA, 2023, P.2)[66]

Desse modo, mesmo quase 10 anos após a transição IANA, o componente político da governança da internet persiste e é em meio a ele que temos novas tecnologias surgindo no ecossistema global. Entre elas, os sistemas ciber-físicos. Veremos um pouco mais sobre suas implicações no capítulo seguinte.

2.3 CONCLUSÃO DO CAPÍTULO

O capítulo buscou, primeiramente, apresentar e contextualizar a governança cibernética. Embora recente, com avanços em definições e propostas praticamente todos centralizados no século XXI, a governança da internet é complexa sobretudo por envolver interesses de uma grande variedade de atores, para além dos atores tradicionais geopolíticos. O funcionamento da rede, embora longe do que queria John Barlow, conta com atores da sociedade civil e empresariais em uma grande variedade de funções, e conta com espaços para a manifestação das visões desses atores, seja em momentos como o WSIS e o WICT, seja no próprio IGF ou espaços próprios desses atores.

---

[66] Traduzido do Inglês: Discussions in the OEWG show that even the PoA proponents do not have a common position on its specific parameters, most importantly, on the decision-making procedure [...] It is worth noting that Western countries attach very specific political meaning to the Programme of Action, they publicly promote it to antagonize Russia. They justify the need to establish the PoA by alleged malicious activities of our country in information space, including in the context of the special military operation in Ukraine (these arguments were voiced, namely, by the French representatives at the OSCE). Such anti-Russian cause cannot serve as a basis for constructive interaction of States on IIS. It contradicts the spirit of the UN Charter and, specifically, its Article 1 on equality and friendly relations between States. In these circumstances, the PoA is expected to be used by Western countries to impose non-binding rules and standards of their interests, thus replacing the norms of international law – in line with the US-promoted rules-based order concept.
.

Apesar disso, a internet não é um espaço isolado da geopolítica global e os acontecimentos da segunda década do século XXI, sobretudo pós-Snowden, vêm reforçando esse ponto, com a segurança cibernética entrando de vez no radar dos Estados Nacionais, uma vez que percebem seus potenciais impactos nocivos. E o debate securitário encontra eco em narrativas divergentes sobre como e onde as decisões devem ser tomadas. Se já havia a disputa histórica entre um bloco *multilateral* (China, Rússia) e um bloco *multistakeholder* (majoritariamente representado pelos Estados Unidos), acerca de quem devem ser os atores envolvidos - e com poder de voto - nas principais discussões da rede, cada vez mais se consolida também um debate sobre onde as principais discussões devem ser realizadas, com o *Program of Action* já sendo lançado sob fortes protestos da Rússia.

É nesse cenário, que já é complicado geopoliticamente, que estão surgindo novas tecnologias com grande potencial econômico, e com potenciais riscos securitários diferentes dos riscos até então presentes nos tradicionais ataques cibernéticos. Mais do que roubo de dados e interrupções de serviços, com danos majoritariamente econômicos, tecnologias como os sistemas ciber-físicos possuem potencial de dano físico.

Ao mesmo tempo em que se inserem em um debate já existente, essas tecnologias trazem elementos novos aos quais os atores desse ecossistema precisam reagir e se adaptar. A grande questão por trás dessa adaptação é o grau de envolvimento por parte dos Estados no controle desse tipo de tecnologia. Antes de entrar nessa questão, tema do capítulo 4, vamos entender um pouco melhor o que, de fato, representam os sistemas ciber-físicos.

3 SISTEMAS CIBER-FÍSICOS

> Os ataques cibernético-físicos diferem dos ataques cibernéticos pelo fato de ameaçarem diretamente sistemas físicos: infraestrutura, estruturas civis e pessoas. Os ataques cibernético-físicos podem causar mortes e danificar instalações físicas que podem levar meses para serem reparadas. (WOLF, 2020, p.1)[67]

Um dos argumentos de Thomas Rid (2012), no famoso artigo "*Cyber war will not take place*" para justificar que uma guerra cibernética não aconteceria, partindo da concepção de guerra de Clausewitz, é o do caráter violento da guerra. Segundo ele "se um ato não é potencialmente violento, não é um ato de guerra [...] Um verdadeiro ato de guerra é sempre potencialmente ou realmente letal, pelo menos para alguns participantes de pelo menos um dos lados." (RID, 2012, p.7).[68] Até aquele momento, na visão do autor, os ataques cibernéticos não possuíam esse potencial de violência.

Passados pouco mais de dez anos do artigo, contudo, temos um cenário um pouco diferente. O desenvolvimento e popularização de dispositivos que podem ser invadidos via espaço cibernético, mas possuem interação com o mundo físico torna esse potencial de violência mais palpável e, consequentemente, reforça as preocupações securitárias que já vinham crescendo ao longo da última década.

Diante disso, neste capítulo é apresentada a definição de sistemas ciber-físicos, alguns dos riscos trazidos por eles e que tipo de discussão eles levantam. Espera-se com isso apresentar um contexto dessa discussão para, a partir dele, observar como os Estados Nacionais selecionados estão lidando com a questão (tema do capítulo 4).

3.1 O QUE SÃO SISTEMAS CIBER-FÍSICOS?

Primeiramente, é preciso reforçar que, para fins dessa dissertação, o termo "sistemas ciber-físicos" está sendo usado como sinônimo de "internet das coisas". Essa premissa se baseia em De Nardis (2020), onde a autora adota os termos como

[67] Original: Cyber-physical attacks differ from cyber attacks in that they directly threaten physical systems: infrastructure, civil structures, and people. Cyber-physical attacks can kill people and cause damage to physical plants that can take months to repair.
[68] Original: "if an act is not potentially violent, it's not an act of war [...] A real act of war is always potentially or actually lethal, at least for some participants on at least one side."

sinônimos, preferindo o uso de “sistemas ciber-físicos” devido ao caráter econômico e comercial atrelado à “internet das coisas”. Para ela, é preciso haver o cuidado para explorar o tema para além de seus aspectos comerciais, dado que, como ela sustenta em sua argumentação e o próprio título do livro defende, os sistemas ciber-físicos estão e estarão em todos os aspectos da vida humana.

Apesar dessa preferência, contudo, o termo “internet das coisas” ainda é amplamente utilizado para se referir ao conceito de dispositivos com componentes físicos e virtuais. Em alguns dos países observados, como veremos no capítulo a seguir, os dois termos aparecem, com leves diferenciações entre eles, geralmente adotando um caráter mais industrial aos sistemas ciber-físicos. Termos como “industrial internet”, “dispositivos conectáveis”, “internet de veículos”, “internet das coisas industrial”, e termos com prefixo “smart” (*smart houses, smart cities*, etc.) também aparecem aos montes na literatura e nos debates relacionados. Em trabalhos futuros, um olhar mais apurado para a terminologia, para os aspectos técnicos que podem resultar nessas variações de terminologia, e para como os *stakeholders* usam a terminologia em diferentes contextos podem ser bem ricos ao debate. Esse, contudo, não é o objetivo aqui. Dessa forma, quando um dos termos for utilizado nesta dissertação, tenha em mente a premissa de que ele está sendo usado como um sinônimo do outro.

Dito isso, em que consiste, de fato, a internet das coisas (sistemas ciber-físicos)? Quando olhamos para a ITU, a definição que existe é relacionada a Internet das Coisas, que é apontada como:

> [...] uma infraestrutura global para a sociedade da informação, possibilitando serviços avançados ao interconectar coisas (físicas e virtuais) com base em tecnologias de informação e comunicação interoperáveis existentes e em evolução (TIC). Através da exploração de capacidades de identificação, captura de dados, processamento e comunicação, a IoT faz pleno uso das 'coisas' para oferecer serviços a todos os tipos de aplicativos, garantindo ao mesmo tempo que os requisitos de segurança e privacidade sejam atendidos. [...] coisas são objetos do mundo físico (coisas físicas) ou do mundo da informação (mundo virtual) que são capazes de serem identificados e integrados em redes de comunicação. [...] Coisas físicas existem no mundo físico e são capazes de serem sentidas, ativadas e conectadas. Exemplos de coisas físicas incluem o ambiente circundante, robôs industriais, bens e equipamentos elétricos. Coisas virtuais existem no mundo da informação e são capazes de serem armazenadas, processadas e acessadas. Exemplos

> de coisas virtuais incluem conteúdo multimídia e software de aplicativos. (SECTOR STANDARDIZATION 2012, p.2)[69]

Por sua vez, a ISO (*International Standard Organization*) trabalha com a definição de “sistemas ciber-físicos”, colocando a Internet das Coisas dentro deste guarda-chuva, ao lado da robótica e carros autônomos:

> Os sistemas ciberfísicos integram componentes computacionais (processamento de informações) com processos físicos, que interagem por meio de uma rede. Avanços tecnológicos na 'Internet das Coisas', 'Robótica' e 'Veículos Autônomos' são a base para tornar os sistemas ciberfísicos possíveis, e hoje existem exemplos de sistemas ciberfísicos bem-sucedidos em todos os lugares... desde trens sem condutor, até edifícios inteligentes, eletrodomésticos e itens do dia a dia, como robôs de limpeza, dispositivos de fitness vestíveis ou bicicletas elétricas. (ISO, 2023)[70]

Definições semelhantes sobre Internet das Coisas aparecem em outros autores, como Minerva, Biru e Rotondi (2015) e Koniagina (2023). Laura DeNardis (2020), por sua vez, amplia a definição para outros aspectos, incluindo dispositivos no corpo humano. Para ela, os sistemas ciber-físicos fazem com que as fronteiras físicas e não físicas colapsem.

> Os tropos relacionados à Internet das Coisas frequentemente são centrados no consumidor, incluindo eletrodomésticos e outros sistemas domésticos ou objetos pessoais, como o carro de um indivíduo. Além desses objetos de consumo cotidiano, a indústria e os governos locais são uma importante base de operação de ambientes ciberfísicos. Por exemplo, as cidades operam sistemas de controle de tráfego, utilidades, iluminação pública, aplicativos de transporte e outros sistemas conectados diretamente à Internet pública ou indiretamente via redes proprietárias com um gateway para a Internet pública. Os sistemas ciberfísicos, é claro, existem nas vastas infraestruturas que sustentam os setores industriais [...] O "objeto" na Internet das Coisas

---

[69] Original: [...] a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT). Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of "things" to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled. [...] things are objects of the physical world (physical things) or of the information world (virtual world) which are capable of being identified and integrated into communication networks. [...] Physical things exist in the physical world and are capable of being sensed, actuated and connected. Examples of physical things include the surrounding environment, industrial robots, goods and electrical equipment. Virtual things exist in the information world and are capable of being stored, processed and accessed. Examples of virtual things include multimedia content and application software.

[70] Original: Cyber-physical systems integrate computational components (information processing) with physical processes, which interact through a network. Technological advances in the ‘Internet of Things’, ‘Robotics’, and ‘Autonomous vehicles’ are the foundation for making cyber-physical systems possible, and today there are examples of successful cyber-physical systems everywhere… from driver less trains, to smart buildings, to household appliances and everyday items such as cleaning robots, wearable fitness devices or electric bikes.

> abrange os sistemas biológicos de uma pessoa por meio de tecnologias vestíveis, dispositivos de identificação biométrica e sistemas digitais de monitoramento médico para verificar temperatura, frequência cardíaca ou nível de glicose no sangue. Sistemas de diagnóstico e tratamento médico também dependem de dispositivos conectados à Internet." (DENARDIS, 2020, p. 24) [71]

Ou seja, em essência, estamos falando de dispositivos que são capazes de existir simultaneamente no mundo físico e virtual, realizando uma comunicação entre esses dois mundos e movimentando dados entre eles. Essa definição é um guarda-chuva que engloba uma grande variedade de dispositivos e, por si só, já dá uma ideia do desafio que é lidar com esse tipo de sistema. Até que ponto, por exemplo, os padrões de segurança de um carro autônomo podem ser os mesmos de um dispositivo inteligente atrelado ao corpo humano para medir automaticamente os níveis de glicose de uma pessoa?

O governo de New South Wales (2021), estado da Austrália, em *seu Internet of Things (IoT) Policy Guide*, criou um mapa mental simples, mas objetivo, que ajuda a visualizar essa variedade. Vejamos esse mapa na figura abaixo:

[71] Original: Tropes related to the Internet of things are often consumer-centric, including home appliances and other domestic systems or an individual's car or other personal object. Beyond these everyday consumer objects, industry and local governments are an important constituency operating cyber-physical environments. For example, cities operate traffic control systems, utilities, street lights, transportation apps, and other systems connected directly to the public Internet or indirectly via proprietary networks with a gateway to the public Internet. Cyber-physical systems, of course, exist in the vast infrastructures underlying industrial sectors [...] The "thing" in the Internet of things encompasses a person's biological systems via wearable technologies, biometric identification devices, and digital medical monitoring systems for checking temperature, heart rate, or blood glucose level. Medical diagnostic and treatment systems similarly rely on Internet-connected devices"

Figura 3 - Mapa de aplicações da Internet das Coisas

Fonte: Retirado de New South Wales (2021, p.2)

Para além da definição em si, é importante entender como esses sistemas funcionam. O quadro abaixo, baseada em De Nardis (2020), traz algumas das características dos sistemas ciber-físicos. Em seguida, temos a Figura 4, também retirada de DeNardis (2020), que representa visualmente o funcionamento de um sistema ciber-físico.

Quadro 4 - Características dos sistemas ciber-físicos (continua)

Característica	Explicação	Implicações
Direct Physical-Virtual Interaction	Diferente dos sistemas de informação, os sistemas ciber-físicos devem levar em conta preocupações e práticas de engenharia tanto para os processos do mundo físico quanto para o mundo digital.	Muda a natureza política dos sistemas, pois, diferente dos sistemas de informação, esses sistemas estão sujeitos a ataques, interrupções, roubos, e precisam se preocupar por padrão com a segurança física do consumidor e com informações críticas tangíveis. Expande as expertises necessárias para seu desenho, somando tecnologia da informação a aspectos hidráulicos e pneumáticos
Transduction	É a conversão de uma forma de energia em outra, por meio de sensores e atuadores. Os sensores capturam informações no mundo físico, os convertendo em sinais elétricos, que transmitem para a rede digital. Os atuadores, por sua vez, convertem sinais elétricos recebidos em energia mecânica que gerará uma ação no mundo real. A Figura 4, retirada de De Nardis (p.62) , ilustra essa dinâmica.	Esses espaços de transdução são novos espaços que têm potencial para melhorar a sociedade e a economia, mas também são pontos de vulnerabilidade para manipulação, vigilância e ataques.
Autonomy and Machine Learning	É o processo em que os sistemas diminuem a necessidade humana nos processos. Alguns deles são desenhados para não precisarem de intervenção humana e interagirem apenas com outras máquinas. Outros são semi autônomos, precisando apenas de algumas intervenções humanas. O aprendizado das máquinas, por sua vez, deriva de interação constante com os dados e mudanças no ambiente, através dos sensores e atuadores, gerando ajustes no processo. “A autonomia também envolve a capacidade dos objetos cibernéticos aprenderem, se adaptarem, mudarem e melhorarem, com base em um feedback contínuo dos dados coletados” (p.65)[72]	Pensando em questões políticas, agora é preciso considerar, para além das pessoas, conteúdos e instituições, a tecnologia e sua dinâmica evolutiva. Questões de responsabilidade e accountability precisam ser pensadas a partir disso, assim como riscos e eventuais limites.
Constrained Architectures	Geralmente os dispositivos possuem um desenho arquitetônico mais limitado, focado nas atividades específicas que exercem	Limites arquitetônicos criam limites políticos, uma vez que legislações e padrões de privacidade e segurança podem acabar gerando a necessidade de redesenhar os sistemas para dar a eles mais poder de memória e processamento.

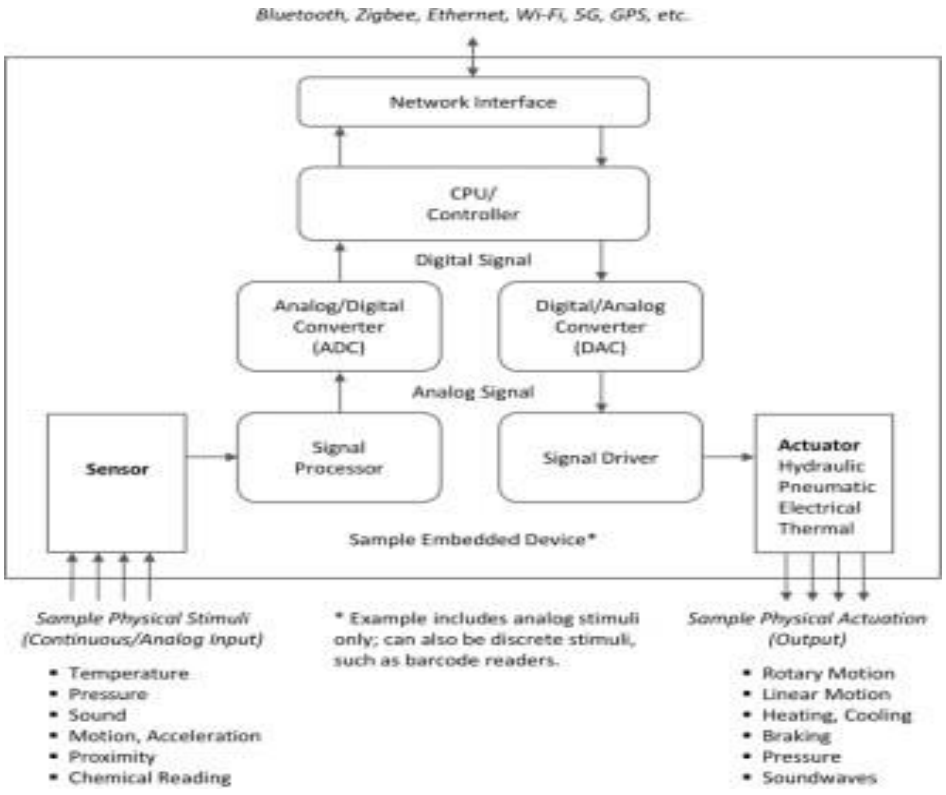
[72] Original: “Autonomy also involves the ability for cyber-embedded objects to learn, adapt, change, and improve, based on a continuous feedback of collected data.”

Quadro 4 - Características dos sistemas ciber-físicos (conclusão)

Característica	Explicação	Implicações
Network Architecture Heterogeneity	Os dispositivos são capazes de se conectar a uma rede para se comunicar entre si, de diferentes maneiras, assim como dispositivos de informação baseados em telas. Alguns estão conectados diretamente à internet, e outros não se conectam diretamente, mas os dados que coletam passam pela internet pública, mesmo quando estão em redes privadas. Não há um padrão técnico universal consistente, mesmo na Internet das Coisas para consumo.	Os sistemas ciber-físicos desafiam a premissa de uma internet universal, com padrões abertos? Os sistemas ciber-físicos devem ser fragmentados em outras redes, que não as globais, para fins de segurança?
Embedded Identification—Only on a Massive Scale	Os dispositivos não seguem necessariamente um padrão comum de identificação, como o caso do IP. Alguns possuem endereço IP, mas outros estão conectados a outros protocolos.	Levando em conta o crescimento desses dispositivos para a casa dos bilhões, mecanismos de identificação e segurança precisam ser pensados.

Fonte: Elaborado pelo autor com base em De Nardis (2020 p. 44-55)

Figura 4 - Funcionamento de um Sistema Ciber-Físico



Fonte: Retirado de De Nardis (2020), p.47.

Cabe lembrar que, assim como o conceito de governança da internet, aqui também falamos de um conceito vivo e ainda mais recente, que tenderá a ser modificado ao longo dos anos, até que se chegue a um padrão universal. Dessa forma, compreender o funcionamento dos dispositivos e as questões que os envolvem é importante para que os conceitos que se consolidem sejam os mais efetivos possíveis em termos de legislação. E tão importante quanto compreender o funcionamento, é compreender os riscos envolvidos na implementação desses sistemas. Vejamos um pouco mais sobre isso.

3.2 RISCOS DE SEGURANÇA DOS SISTEMAS CIBER-FÍSICOS

> "[...] O design e controle de objetos físicos conectados é um terreno emergente e de alta importância na política global da Internet. A cibersegurança tornou-se agora uma das questões mais consequentes da era moderna, necessária para a segurança humana, privacidade, infraestrutura crítica e segurança nacional, assim como para a segurança econômica, democracia, direitos de expressão e acesso ao conhecimento." (De Nardis, 2020, p.7)[73]

Para pensar os riscos de segurança desses sistemas, podemos olhar sob duas perspectivas: a primeira é a do funcionamento dos equipamentos em si, e a segunda é a de sua vulnerabilidade a ataques. O quão, de fato, estamos dispostos a confiar nossas vidas a eles? Esse debate vem se solidificando no início de 2024, em meio às investigações do caso de Hans von Ohain, que pode ser considerado a primeira vítima de um acidente envolvendo um carro 100% autônomo, acontecido em 2022.

De acordo com a apuração do jornal *The Washington Post*, von Ohain utilizava um modelo da Tesla - empresa famosa por seu desenvolvimento de carros autônomos - e estava bêbado em seu carro, supostamente utilizando a tecnologia “Full-Self Driving”, lançada para 400.000 utilizadores, quando o carro bateu em uma árvore e explodiu. O jornal aponta que há registros de problemas envolvendo o “Autopilot”, uma tecnologia anterior, recomendada para trajetos mais simples, mas a promessa do *Full-Self Driving* era a de garantir a segurança em qualquer percurso.

[73] Original: “[...] the design and control of connected physical objects is an emerging and high-stakes terrain of global Internet policy. Cybersecurity has now become one of the most consequential issues of the modern era, necessary for human safety, privacy, critical infrastructure, and national security, asmuch as for economic security, democracy, speech rights, and access to knowledge.”

> Os proprietários de Tesla têm se queixado há muito tempo do comportamento ocasionalmente errático do software dos carros, incluindo frenagem repentina, falta de reconhecimento de marcações de estrada e colisões com veículos de emergência estacionados. Desde que os reguladores federais começaram a exigir que os fabricantes de automóveis relatassem acidentes envolvendo sistemas de assistência ao motorista em 2021, mais de 900 incidentes foram registrados em Teslas. Uma análise do The Washington Post encontrou pelo menos 40 acidentes que resultaram em ferimentos graves ou fatais. A maioria envolveu o Autopilot, que é projetado para uso em rodovias de acesso controlado. Nenhum acidente fatal foi definitivamente vinculado ao sistema mais sofisticado de Condução Autônoma Completa, que é programado para guiar o carro em quase todos os lugares, desde estradas suburbanas tranquilas até ruas movimentadas de cidades.". (THADANI et al., 2024)[74]

Sendo ou não comprovado o envolvimento do sistema no acidente, a essência da discussão está tanto na questão da qualidade do software, quanto da mensagem passada através dele. A viúva de Hans, Nora Bass, captou a questão da mensagem ao trazer que "Independentemente de quão embriagado Hans estivesse, Musk afirmou que este carro pode se autoconduzir e é essencialmente melhor do que um humano [...] nos foi vendida uma falsa sensação de segurança." (THADINI et al, 2024).[75] O quanto, de fato, em meio à corrida para inovar e colocar um produto no mercado, a segurança é analisada nos mínimos detalhes? Essa questão pode ser observada nesse trecho, onde o próprio Elon Musk aponta essa tecnologia como a essência do valor da Tesla:

> Embora ainda em fase beta, a tecnologia é "a diferença entre a Tesla valer muito dinheiro e valer basicamente zero", disse Musk, observando o entusiasmo de seus clientes - e investidores - por um carro totalmente autônomo. Muitos fabricantes de automóveis estavam desenvolvendo tecnologia avançada de assistência ao motorista, mas a Tesla foi mais agressiva em lançar recursos sofisticados para um público ávido. (THADINI et al, 2024)[76]

---

[74] Original: "Tesla owners have long complained of occasionally erratic behavior by the cars' software, including sudden braking, missed road markings and crashes with parked emergency vehicles. Since federal regulators began requiring automakers to report crashes involving driver-assistance systems in 2021, they have logged more than 900 in Teslas. A Post analysis found at least 40 crashes that resulted in serious or fatal injuries.Most involved Autopilot, which is designed for use on controlled-access highways. No fatal crash has been definitively linked to the more sophisticated Full Self-Driving, which is programmed to guide the car almost anywhere, from quiet suburban roads to busy city streets."

[75] Original: "Regardless of how drunk Hans was, Musk has claimed that this car can drive itself and is essentially better than a human [...] We were sold a false sense of security."

[76] Original: Though still in its beta phase, the technology is "the difference between Tesla being worth a lot of money and being worth basically zero," Musk has said, noting his customers' — and investors' — enthusiasm for a fully autonomous car. Many major automakers were developing advanced driver-assistance technology, but Tesla was more aggressive in pushing sophisticated features out to an eager public.

Seguindo nessa linha, de acordo com levantamento da McKinsey, embora para 61% dos consumidores de produtos de Internet das Coisas considerem o elemento da “Confiança Digital” como crítico em sua decisão de compra (observando elementos de segurança), só 31% dos fornecedores consideram esse elemento como essencial no desenho dos produtos. No caso das preocupações em relação à privacidade do produto, esse valor é de 61% para consumidores e apenas 47% para fornecedores (CASO et. al, 2023). Esse dado corrobora com a percepção de DeNardis (2020) de que, na busca por ganhos de mercado, a iniciativa privada tende a não dar o foco necessário às questões de segurança no desenho de seus produtos. Koniagina et al. (2023) também reforçam esse ponto ao trazer que a abordagem securitária para dispositivos de Internet das Coisas não tem sido nem reativa nem proativa historicamente, fazendo que vulnerabilidades de segurança surjam desde os estágios de desenho e desenvolvimento dos produtos.

Para além de questões de mal funcionamento, aqui cabe observar os sistemas ciber-físicos dentro de um ecossistema cada vez mais crescente em termos de ataques cibernéticos. Um primeiro ponto a ser colocado nessa linha é o do volume de dispositivos. Se considerarmos as previsões que falam em crescimento exponencial de dispositivos ciber-físicos para os próximos anos, estamos falando de bilhões de dispositivos passíveis de serem atacados nos próximos anos, seja como alvos em si, ou seja como meios para um alvo maior.

A Cisco (2017), em seu relatório de riscos cibernéticos de 2017 apontou para o risco do uso de dispositivos de Internet das Coisas para ataques de negação de serviço (DDoS).

> No último ano, também observamos adversários empregando dispositivos da Internet das Coisas (IoT) em ataques de negação de serviço distribuído (DDoS). A atividade de botnets no espaço da IoT sugere que alguns operadores podem estar focados em estabelecer as bases para um ataque de grande alcance e alto impacto que poderia potencialmente interromper a própria Internet (CISCO, 2017, p.1)[77]

O Mirai Botnet é o exemplo mais conhecido nessa linha. Criado por estudantes que conheceram ataques DDoS por meio do jogo Minecraft e a partir disso se

[77] Original: “Within the past year, we have also observed adversaries employing Internet of Things (IoT) devices in DDOS attacks. Botnet activity in the IoT space suggests some operators may be focused on laying the foundation for a wide-reaching, high impact attack that could potentially disrupt the Internet itself.”

especializaram nesse tipo de ataque (SHAPIRO, 2023), o Mirai tem a peculiaridade de atacar dispositivos de internet das coisas (por exemplo, câmeras inteligentes) ao invés de computadores. O *malware* buscava por aparelhos com segurança frágil (por exemplo, nomes e senhas padrão) e, uma vez tendo infectado milhares de aparelhos, os utilizava para fazer o DDoS. Na França, em 2016, a empresa OVH sofreu um ataque de DDoS que era 100 vezes maior do que estavam acostumados até então. No mês seguinte, a Dyn, provedora de DNS, também sofreu um ataque semelhante, que afetou cerca de 175.000 sites. Estima-se que o ataque à OVH atingiu um pico de 1TBs. Desde então, variações do Mirai vêm sendo observadas ao longo dos anos. (MALWAREBYTES, 2024).

A CISCO também alerta para as fragilidades de segurança destes dispositivos, e da urgência de se olhar para os riscos de segurança atrelados a eles.

> A Internet das Coisas (IoT) promete grandes avanços para a colaboração e inovação empresarial. Porém, à medida que ela cresce, o risco de segurança também aumenta. A falta de visibilidade é um problema: os defensores simplesmente não estão cientes de quais dispositivos IoT estão conectados à sua rede. Eles precisam agir rapidamente para resolver esse e outros obstáculos à segurança da IoT. Atualmente, atores de ameaças já estão explorando vulnerabilidades de segurança em dispositivos IoT. Esses dispositivos servem como fortalezas para os adversários, permitindo que eles se movam lateralmente pelas redes de forma silenciosa e com relativa facilidade. (CISCO, 2017, p.3)[78]

Mais recentemente, conseguimos perceber que o problema está longe de ter um fim. De acordo com análise do Zscaler ThreatLabz, houve um aumento de 400% focados em dispositivos IoT no primeiro semestre de 2023, em relação ao primeiro semestre de 2022. Foram mais de 300.000 ataques bloqueados, a grande maioria usando o Mirai ou o chamado Gafgyt botnet, e focados em vulnerabilidades já conhecidas há alguns anos. (MCKENDRICK, 2023). E, de acordo com o Global Security Intelligence Report, da BlackBerry, a tendência é de que o risco promovido por esses sistemas permaneça e aumente nos próximos anos.

> [...] a crescente digitalização e integração com a Internet das Coisas (IoT) nos ecossistemas de TI e OT podem apresentar riscos imprevistos. À medida que

[78] Original: The Internet of Things (IoT) holds great promise for business collaboration and innovation. But as it grows, so too does security risk. Lack of visibility is one problem: Defenders are simply not aware of what IoT devices are connected to their network. They need to move quickly to address this and other hurdles to IoT security. Threat actors are already exploiting security weaknesses in IoT devices. The devices serve as strongholds for adversaries, and allow them to move laterally across networks quietly and with relative ease.

> novas tecnologias são adotadas, ameaças cibernéticas sofisticadas certamente seguirão. Além de danificar a infraestrutura, os criminosos cibernéticos também buscam acesso a dados e sistemas." (BLACKBERRY, 2023).[79]

Ao analisar os tipos de riscos promovidos pelos sistemas ciber-físicos, a McKinsey (2023) estabelece um framework de seis dimensões que precisam ser levadas em conta ao pensar esses sistemas. A Confidencialidade (que se divide entre *privacidade* e *acesso*) que pressupõe a proteção dos dados relacionados a esses sistemas e acesso apenas por pessoas autorizadas. A importância disso se ressalta do uso de *IoT* em sistemas altamente regulados, com os relacionados a sistemas de saúde e indústria. A Integridade (que se divide em *confiabilidade* e *conformidade*), devido ao fato de esses sistemas serem cada vez mais autônomos, é preciso ter a certeza de que os dados providos por eles não foram alterados e são precisos; da mesma forma, é importante ter a certeza de que estão atrelados a legislações adequadas. E a Disponibilidade (dividida entre *uptime* e *resiliência*), que diz respeito a garantias de que os dispositivos se mantenham operantes e tenham medidas de segurança que já antevenham possíveis falhas promovidas por interação humana. (MCKINSEY, 2023).

Chegar a padrões de excelência dentro desses critérios, em um cenário onde as empresas buscam colocar os produtos no mercado no menor tempo e com o menor custo possível, é desafiador. Conforme apontam Chen et.al (2018) “as demandas de mercado por custos mais baixos associadas a baixas barreiras de entrada no mercado de IoT significam que atualmente há pouco incentivo para construir dispositivos IoT mais seguros”[80]. Esse cenário securitário se soma a um cenário de grande potencial econômico derivado dos produtos e dos dados por eles gerados, e disputas políticas em campos diversos, como os das padronizações relacionadas a esses produtos. DeNardis (2020) defende que em um cenário onde a presença da internet se conecta a todos os campos da vida, todas as empresas adquirem um elemento de empresas de tecnologia e a segurança dos websites e dados em si se conecta diretamente com

[79] Original: “[...] increasing digitization and integration with the Internet of Things (IoT) in both IT and OT ecosystems can present unforeseen risks. As new technologies are adopted, sophisticated cyberthreats will no doubt follow. In addition to damaging infrastructure, cyber criminals also seek access to data and systems."

[80] Original."market demands for lower costs paired with low barriers to entry in the IoT market mean there is currently little incentive to build more secure IoT devices.”

a segurança da Internet das Coisas. Assim sendo, não há como pensar governança da internet sem considerar a IoT.

3.3 OS SISTEMAS CIBER-FÍSICOS NO DEBATE DA GOVERNANÇA DO CIBERESPAÇO

> Novas inovações e novos atores criam novos desafios de governança em áreas críticas, incluindo segurança cibernética, privacidade e liberdade de expressão. (DENARDIS, 2017)[81]

Em seu artigo de 2017, Laura DeNardis e Mark Raymond levantam a agenda da Internet das Coisas, entendida pelos autores como uma forma coloquial de se falar sobre sistemas ciber-físicos, como essencial de ser debatida por conta de seus impactos significativos na sociedade, e dos riscos que os acompanham. Os autores ressaltam que, embora o tema tenha recebido uma atenção considerável em termos de produtos para consumo, ainda há uma margem importante para avançar em termos de políticas e governança relacionadas aos seus aspectos públicos, tanto por conta de seu volume, quanto por sua presença em setores fundamentais.

> Mais tráfego da Internet já conecta coisas do que pessoas, e as projeções globais do impacto econômico da IoT são potencialmente de onze trilhões de dólares até 2025.9 Também é apropriado porque a expansão da Internet em objetos do cotidiano usados por pessoas cria questões de interesse público sem precedentes sobre como ela também transformará a privacidade e a segurança humana. Essa atenção aos produtos de consumo perde a maior parte de como a Internet se expandiu para objetos do cotidiano. Fora dos aplicativos IoT do consumidor estão os sistemas físicos cibernéticos que fundamentam quase todos os setores industriais [...] Todos os setores econômicos, da agricultura ao varejo, são agora domínios nos quais o ciberespaço toca o mundo material.12 Todas essas redes, embora muitas vezes usem algumas tecnologias proprietárias, também contam com os protocolos subjacentes e equipamentos de rede da Internet ou se conectam à Internet para funções de administração e controle. (DENARDIS, RAYMOND, 2017, p. 477)[82]

---

[81] Original: New innovations and new actors create new governance challenges in critical areas including cyber security, privacy and freedom of expression.

[82] Original: More Internet traffic already connects things than people, and global projections of the economic impact of the IoT is potentially eleven trillion dollars by 2025.9 It is also appropriate because the expansion of the Internet into everyday objects used by people creates unprecedented public interest questions about how it will also transform privacy and human security. This attention to consumer products misses the bulk of how the Internet has expanded into everyday objects. Outside of consumer IoT applications are the cyber physical systems that underlie almost all industrial sectors [...] All economic sectors, from agriculture to retail, are now domains in which cyberspace touches the material world. All of these networks, while often using some proprietary technologies, also rely on the underlying protocols and network equipment of the Internet or connect into the Internet for administration and control functions.

Diante disso, para os autores fica claro que o debate sobre governança global da internet necessita dar mais foco aos sistemas ciber-físicos. Se, por um lado, Milton Mueller e Badiei (2020) refletem sobre se os sistemas ciber-físicos devem ser regulados de forma mais voltada ao seu setor, ““dispositivos médicos, por exemplo, devem ser considerados governança da Internet ou parte da política de saúde? Os veículos autônomos são tratados como governança da Internet ou política de transporte?”[83] (MUELLER, BADIEI, 2020, p.76), DeNardis e Raymond (2017) ressaltam a questão do interesse público que o tema levanta para defender que “A Internet das Coisas não é apenas uma jurisdição local, ou mesmo uma questão doméstica, mas uma preocupação internacional de governança da Internet*”*[84] (DENARDIS, RAYMOND, 2017, p. 477). Ao desenhar um framework de interesses públicos relacionados aos sistemas ciberfísicos, os autores chegam a 5 tópicos principais, resumidos no quadro abaixo:

Quadro 5: Framework de interesses públicos relacionados ao ciberespaço (continua)

Características	**Preocupações**
Critical Internet Resource Constraints (Restrições críticas de recursos da Internet)	Preocupação sobre o quanto a infraestrutura e a legislação da internet atual estão preparadas para se adequar e lidar com os sistemas ciber-físicos.
Privacy complications (Complicações de privacidade)	Preocupação sobre o volume de dados coletado por meio de sistemas ciber-físicos, e sobre como o consentimento para a coleta se torna mais difícil em dispositivos sem o intermédio de uma tela. Há também a preocupação sobre o quanto esse tema está sendo guiado por interesses privados, em um ritmo acelerado. Ainda, reflete-se sobre a relação da privacidade com a segurança humana. O que aumenta consideravelmente os riscos é que uma infiltração de dados em sistemas ciberfísicos pode resultar na perda de vidas humanas e na perda do funcionamento básico do dia a dia, não apenas na perda de dados de comunicação. Agora, a privacidade está relacionada à segurança humana, conforme abordado a seguir. (p.484) [85]

[83] Original: “medical devices, for example, [should] be considered Internet governance or part of health policy? Are autonomous vehicles handled as Internet governance or transportation policy?”
[84] Original: “Internet of Things is not merely a local jurisdiction, or even domestic issue, but an international Internet governance concern.”
[85] “What raises the stakes considerably is that an infiltration of data in cyber physical systems can result in loss of human life and loss of basic day-to-day functioning, not just loss of communication data. Privacy is now related to human security, addressed next” (p. 484)

Quadro 5: Framework de interesses públicos relacionados ao ciberespaço (continuação)

Características	Preocupações
Human security (Segurança humana)	Dialogando com o ponto acima, há preocupações em torno da segurança humana, tanto no sentido de proteção de direitos civis e políticos (até mesmo do próprio Estado) quanto no sentido de proteção física e responsabilização a partir de danos causados por sistemas ciber-físicos: “No caso de falhas de software ou sistemas hackeados serem responsáveis por ferimentos ou morte, por exemplo, pode haver complicações em responsabilizar empresas devido à fragilidade das leis de responsabilidade de software, especialmente quando o software foi adquirido pelo fabricante do dispositivo de uma empresa diferente” (p.486)[86] Há ainda, a preocupação com os riscos humanos atrelados a interrupção de infraestruturas críticas, como redes elétricas, sistemas de saúde e sistemas de transporte.
International Security (Segurança Internacional)	Preocupação com o aumento do número de dispositivos passíveis de serem atacados e como isso afeta o equilíbrio entre ataque e defesa no espaço cibernético. “O efeito geral dos sistemas físicos cibernéticos onipresentes na segurança internacional permanece obscuro. Por um lado, “as vantagens que o software complexo oferece aos invasores diminuem rapidamente nas ‘bordas’ do ciberespaço, onde os computadores são usados para controlar sistemas físicos, porque o conhecimento dos sistemas físicos é necessário para exercer um controle cuidadoso”. Por outro lado, tal tecnologia "expande significativamente a superfície de ataque e borra as fronteiras dos sistemas cuja resiliência precisa ser aprimorada". (p. 489)[87] Preocupação e reflexões sobre como os Estados e governos irão se colocar em meio a esse cenário.

[86] Original: “In the event that software flaws or hacked systems are responsible for injury or death, for example, there may be complications around holding firms responsible given the weakness of software liability laws, especially where the software was purchased by the device manufacturer from a different firm.”

[87] Original: “The overall effect of ubiquitous cyber physical systems on international security remains unclear. On the one hand, “the advantages that complex software offers attackers diminish rapidly at the ‘edges’ of cyberspace, where computers are used to control physical systems, because knowledge of the physical systems is needed to exercise careful control.” On the other hand, such technology “greatly expands the attack surface and blurs the boundaries of the systems whose resilience needs to be enhanced.”

Quadro 5: Framework de interesses públicos relacionados ao ciberespaço (conclusão)

Características	Preocupações
Global Competition Tensions — Innovation and Interoperability Versus Enclosure (Tensões de Competição Global — Inovação e Interoperabilidade versus Fechamento)	Preocupação sobre o quanto regulações nacionais podem inibir a inovação nos sistemas ciber-físicos. Preocupação com como os produtos devem ser construídos (de forma a serem de código aberto ou não) e de sua interoperabilidade (conexão e trabalho em conjunto): Ao visualizar os sistemas físicos cibernéticos através de lentes de relações internacionais, [...] pode ser que a falta de interoperabilidade sirva como uma verificação de vigilância invasiva, ataques generalizados de segurança cibernética e conflito cibernético. Por outro lado, pode-se argumentar que os padrões abertos, que normalmente são desenvolvidos em abordagens mais participativas e cruzadas e que permitem inspeção aberta, podem ter recursos de segurança reforçados e menos vulnerabilidades de protocolo do que especificações proprietárias que são fechadas no desenvolvimento e não abertas para inspeção e ampla supervisão técnica. (p.494)[88] Preocupação sobre confiança nos sistemas: “Os armazenamentos de recursos críticos da Internet acomodarão o crescimento projetado no número de dispositivos interconectados? Até que ponto as violações de segurança cibernética de alto nível, sejam originárias do estado ou de criminosos cibernéticos, corroem a confiança do consumidor e a adoção do mercado na IoT? Como em outras questões de governança da Internet, diferentes conjuntos de valores entram em tensão.” (p.493)[89]

Fonte: Elaborado pelo autor, com base em DENARDIS e RAYMOND (2017)

Diante de todas essas questões, os autores trazem a reflexão sobre até que ponto o Estado e seus representantes permitirão o predomínio privado em relação aos sistemas ciber-físicos.

> Dado o papel tradicional do Estado, não está claro se os governos ou os cidadãos continuarão a tolerar o fornecimento altamente privatizado de segurança cibernética no caso de lesões e perda de vidas causadas pela

[88] “When viewing cyber physical systems through an international relations lens, [...] it may be the case that lack of interoperability can serve as a check on invasive surveillance, widespread cybersecurity attacks, and cyber conflict. Conversely, the argument can be made that open standards, which are typically developed in more participatory, cross-business approaches and which allow for open inspection, can have hardened security features and fewer protocol vulnerabilities than proprietary specifications which are closed in development and not open for inspection and wide technical oversight.”

[89] Original: “Will stores of critical Internet resources accommodate projected growth in the number of interconnected devices? To what extent will high-profile cybersecurity breaches, whether originating with the state or cybercriminals, erode consumer trust and market adoption in the IoT? As with other questions of Internet governance, different sets of values come into tension.”

> interrupção de sistemas físicos cibernéticos críticos se tornarem comuns. (DENARDIS, RAYMOND, 2017, p. 487)[90]

> Até que ponto os líderes percebem os sistemas ciberfísicos como uma fonte de ameaça — seja para a segurança humana ou nacional — eles provavelmente vão insistir em exercer um maior controle sobre essa área de políticas, e potencialmente também em impor controles ou restrições sobre a economia digital. (DENARDIS, RAYMOND, 2017, p. 491)[91]

Somada a essas questões de interesses públicos, há um cenário de disputa econômica crescente promovida pelo potencial desses sistemas. A McKinsey aponta que o mercado de IoT pode chegar na casa dos 600 bilhões de dólares em 2030, com potencial ainda maior no caso de maiores garantias de segurança (MCKINSEY, 2023). E a inserção nesse mercado envolve domínios de uma infraestrutura que já vem sendo disputada econômica e politicamente nos últimos anos, com a questão do 5G. Conforme aponta Chen et al.:

> Os analistas argumentam que a indústria da IoT provavelmente se beneficiará significativamente do contínuo avanço e amadurecimento de outras tecnologias relacionadas, como a computação em nuvem, a tecnologia sem fio de quinta geração (5G) e as redes de área ampla de baixa potência (LPWAN). A computação em nuvem e tecnologias relacionadas (como a computação de névoa e de borda) irão aprimorar o desempenho de sensores, agregadores e utilitários externos implantados em várias partes de uma rede IoT, tornando recursos computacionais mais capazes disponíveis para dispositivos e sensores IoT com capacidade computacional limitada.[92] (CHEN ET AL, 2018)

Cabe destacar também, como veremos no próximo capítulo, que a questão dos padrões técnicos (*standards*) para o funcionamento e segurança dos dispositivos de IoT - último ponto do quadro 5 - também é objeto de disputa política.

Desse modo, o pano de fundo que precisamos observar ao pensar sistemas ciber-físicos passa, em resumo, por um momento histórico que já vinha sendo marcado por preocupações de segurança no ciberespaço, e que tem esse tipo de

---

[90] Original: “Given the traditional role of the state, it is not clear whether governments or citizens will continue to tolerate highly privatized cybersecurity provision in the event that injury and loss of life from disruption of critical cyber physical systems becomes commonplace.”

[91] Original: “To the extent that leaders perceive cyber physical systems as a source of threat — either to human or national security — they are likely to insist on exercising increased control over this policy area, and potentially also to insist on imposing controls or restrictions on the digital economy.”

[92] Original: “Analysts argue that the IoT industry is likely to benefit significantly from the continued advancement and maturation of other related technologies like cloud computing, fifth generation (5G) wireless technology, and low-power wide area networks (LPWAN). Cloud computing and related technologies (such as fog and edge computing14) will enhance the performance of sensors, aggregators, and external utilities deployed in various parts of an IoT network by making more capable computing resources available to IoT devices and sensors with limited onboard computing capacity.”

preocupação acentuado por novas tecnologias que, ao mesmo tempo que possuem um grande potencial econômico, acompanham riscos intrínsecos ao seu processo de desenvolvimento, difíceis de se resolver organicamente. Acrescenta-se a esse quadro, disputas geopolíticas para emplacar a infraestrutura necessária para o bom funcionamento dessas novas tecnologias e, novamente, para colher os benefícios econômicos derivados destas infraestruturas.

3.4 CONCLUSÃO DO CAPÍTULO

O capítulo teve como objetivo apresentar o conceito de sistemas ciber-físicos. Embora longe de ser consensual em meio às definições e debates sobre o tema, o elemento central, pensando no aspecto securitário sob o qual estamos observando a questão, é que ao interagir simultaneamente com o ciberespaço e o mundo físico eles podem, além de serem utilizados para promover ataques cibernéticos DDoS, como no caso do Mirai Botnet, os sistemas ciber-físicos tem potencial de causar danos físicos aos seus usuários, caso invadidos com esse propósito. Quando pensamos na adoção em larga escala desses sistemas em indústrias e setores como saúde e educação, para além do âmbito doméstico, o potencial dano que pode ser derivado de falhas de segurança e ataques direcionados cresce em termos societais.

Assim, as preocupações que derivam da iminência desses sistemas estão muito além do básico, e se espalham por vários macroeixos temáticos, conforme apontado por DeNardis e Raymond (2017) que vão desde questões infraestruturais, a questões de privacidade e segurança humana - derivadas do grande volume de dados que esses sistemas movimentam -, questões de segurança da informação, e disputas globais para sair na frente nas padronizações relacionadas.

Em meio a esse quadro, olhar para como as potências cibernéticas estão lidando com essas questões - e como essas mesmas questões dialogam com as visões dessas potências para a governança do ciberespaço - pode trazer mais elementos para esse debate e ajudar a entender, objetivamente, as disputas e jogos políticas que estamos vivenciando.

4 POTÊNCIAS CIBERNÉTICAS E OS SISTEMAS CIBER-FÍSICOS

Diante dos debates trazidos até aqui, o presente capítulo propõe observar como algumas das principais potências cibernéticas se posicionam em relação ao tema. Para isso, primeiramente faz-se uma recapitulação de como cada país está observando o ciberespaço e os desafios colocados por ele. Em seguida, analisa-se os principais documentos de cada país em busca de menções e iniciativas relacionadas a sistemas ciber-físicos e internet das coisas, para entender como a temática está sendo tratada pelo país. Por fim, faz-se um esforço de observar ações internas específicas dos países sobre o tema. Após a estruturação dos cinco países, têm-se uma breve análise comparativa, e as principais reflexões derivadas da pesquisa.

4.1 ESTADOS UNIDOS

4.1.1 Como os Estados Unidos percebem a governança do ciberespaço?

O primeiro elemento a ser considerado, quando pensamos em Estados Unidos é a percepção clara de uma disputa política no âmbito do ciberespaço. Em sua mais recente Estratégia Nacional de Cibersegurança, o país aponta China, Rússia, Irã e Coreia do Norte como Estados autocráticos e revisionistas, que se utilizam do espaço cibernético para perseguir seus objetivos de forma agressiva, desconsiderando normas internacionais e sendo um risco à segurança nacional dos Estados Unidos. (ESTADOS UNIDOS, 2023b)

Vejamos mais especificamente China e Rússia, que são tratados no âmbito desta dissertação. Os Estados Unidos enxergam a China como seu principal adversário político e deixam claro que a disputa vai para além do ciberespaço. A China é vista como ameaça também por seu potencial de dominar tecnologias críticas ao desenvolvimento global, por sua ideologia e seu potencial de modificar a ordem global. Segundo eles, a China representa:

> A ameaça mais ampla, ativa e persistente tanto para as redes governamentais quanto para as do setor privado e é o único país com a intenção de remodelar a ordem internacional e, cada vez mais, com poder econômico, diplomático, militar e tecnológico para fazê-lo. Nos últimos dez

> anos, expandiu as operações cibernéticas além do roubo de propriedade intelectual para se tornar nosso competidor estratégico mais avançado, com capacidade de ameaçar os interesses dos EUA e dominar tecnologias emergentes essenciais para o desenvolvimento global. Tendo aproveitado com sucesso a Internet como espinha dorsal de seu estado de vigilância e capacidades de influência, a RPC está exportando sua visão de autoritarismo digital, buscando moldar a Internet global à sua imagem e colocando em perigo os direitos humanos além de suas fronteiras. (Estados Unidos, 2023b, p.3, grifo do autor)[93]

A Rússia, por sua vez, é acusada de usar capacidades cibernéticas para desestabilizar adversários políticos por meio de diferentes ameaças cibernéticas, que vão desde espionagem a campanhas de desinformação, prejudicando os Estados Unidos e seus aliados. A guerra na Ucrânia é citada como exemplo de comportamento irresponsável, com consequências para além da própria Ucrânia.

> O governo russo tem utilizado suas capacidades cibernéticas para desestabilizar seus vizinhos e interferir na política doméstica das democracias ao redor do mundo. A Rússia permanece uma ameaça cibernética persistente enquanto aprimora suas capacidades de espionagem, ataques, influência e desinformação cibernética para coagir países soberanos, abrigar atores criminosos transnacionais, enfraquecer alianças e parcerias dos EUA e subverter o sistema internacional baseado em regras. Assim como seu ataque "NotPetya" em 2017, os ciberataques da Rússia em apoio à sua brutal e injustificada invasão da Ucrânia em 2022 resultaram em impactos irresponsáveis que afetaram a infraestrutura crítica civil em outros países europeus. (Estados Unidos, 2023, p.3, grifo do autor)[94]

Diante da percepção de um cenário internacional com rivais cibernéticos relevantes, a Estratégia dedica um de seus pilares exclusivamente para pensar as ações dos Estados Unidos no ciberespaço em âmbito internacional. Sob a narrativa de manter um ciberespaço “aberto, livre, global, interoperável, confiável e seguro”[95]

---

[93] Original: “the broadest, most active, and most persistent threat to both government and private sector networks and is the only country with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do so. Over the last ten years, it has expanded cyber operations beyond intellectual property theft to become our most advanced strategic competitor with the capacity to threaten U.S. interests and dominate emerging technologies critical to global development. Having successfully harnessed the Internet as the backbone of its surveillance state and influence capabilities, the PRC is exporting its vision of digital authoritarianism, striving to shape the global Internet in its image and imperiling human rights beyond its borders.”

[94] Original: “Russian government has used its cyber capabilities to destabilize its neighbors and interfere in the domestic politics of democracies around the world. Russia remains a persistent cyber threat as it refines its cyber espionage, attack, influence, and disinformation capabilities to coerce sovereign countries, harbor transnational criminal actors, weaken U.S. alliances and partnerships, and subvert the rules-based international system. Like its 2017 “NotPetya” attack, Russia’s cyberattacks in support of its 2022 brutal and unprovoked invasion of Ukraine have resulted in irresponsible spillover impacts onto civilian critical infrastructure in other European countries.”

[95] Original: “open, free, global, interoperable, reliable, and secure.”

(p.29), o país deixa claro que irá buscar coalizões para preservar esses interesses e buscar isolar e gerar custos a atores que caminhem na direção contrária. Reconhecendo a relevância de sua participação no UN GGE e no UN OEWG, os EUA apontam que, para além disso, trabalharão com parceiros para enfraquecer a "*dark vision*" do futuro da internet promovida pela China.

A partir disso, são apontados cinco caminhos que refletem a posição Estadunidense em relação ao ciberespaço. Vejamos um resumo de cada um deles no quadro abaixo:

Quadro 6 - Os Caminhos para a Política Cibernética Internacional dos EUA, de Acordo com a Estratégia Nacional de Cibersegurança de 2023 (continua)

Caminho	Principais pontos
1. Construir coalizões para conter ameaças ao ecossistema digital	• Ressaltam a Declaração pelo Futuro da Internet, assinada em 2022 por 60 países; • Destacam também a Freedom Online Coalition, da qual fazem parte; • Deixam claro que estão reunindo parceiros de mentalidade parecida entre países, comunidade de negócios internacional e outros stakeholders, para preservar sua visão de internet que "promove fluxos de dados seguros e confiáveis, respeita a privacidade, promove os direitos humanos e possibilita o progresso em desafios mais amplos. (p.29)[96] • Ressaltam outros mecanismos, como o "Quad" (Quadrilateral Security Dialogue) junto a Índia, Japão e Austrália e uma série de outras iniciativas semelhantes, entre tratados e diálogos multilaterais; • Através dessas parcerias, os Estados Unidos buscam compartilhar informações, princípios de segurança, expertises cibernéticas, entre outros; • Reforçam que parcerias *multistakeholder,* incluindo organizações privadas e da sociedade civil também estão inclusas na estratégia; • Reforçam que trabalharão com aliados para "desenvolver novas colaborações e mecanismos de aplicação da lei para a era digital)" e apoiar a criação de hubs junto aos seus parceiros, para garantir essa efetividade.

[96] Original: "promotes secure and trusted data flows, respects privacy, promotes human rights, and enables progress on broader challenges."

Quadro 6 - Os Caminhos para a Política Cibernética Internacional dos EUA, de acordo com a Estratégia Nacional de Cibersegurança de 2023 (continuação)

Caminho	Principais Pontos
2. Fortalecer a capacidade de parceiros internacionais	Na medida em que solidifica suas alianças, os Estados Unidos buscarão apoiar seus aliados para "proteger redes de infraestrutura crítica, desenvolver capacidades eficazes de detecção e resposta a incidentes, compartilhar informações sobre ameaças cibernéticas, buscar colaboração diplomática, desenvolver capacidade e eficácia de aplicação da lei por meio de colaboração operacional"[97] e, a partir disso, apoiar seus interesses e ao que considera normas de comportamento responsável no ciberespaço; • Para tanto, haverá atuação do Departamento de Justiça, do Departamento de Defesa e do Departamento de Estado, cada qual dentro de sua área de expertise.
3. Aumentar a capacidade dos Estados Unidos de apoiar aliados e parceiros	• Os Estados Unidos delimitarão políticas para estabelecer quando é de interesse nacional apoiar um parceiro e como fazer isso rapidamente; • É dado o exemplo do desenvolvimento da capacidade de resposta a incidentes cibernéticos da OTAN, que está sendo liderada pelos Estados Unidos.

[97] Original: "secure critical infrastructure networks, build effective incident detection and response capabilities, share cyber threat information, pursue diplomatic collaboration, build law enforcementcapacity and effectiveness through operational collaboration"

Quadro 6 - Os Caminhos para a Política Cibernética Internacional dos EUA, de Acordo com a Estratégia Nacional de Cibersegurança de 2023 (conclusão)

Caminho	Principais Pontos
4. Criar coalizões para reforçar as normas globais de comportamento responsável por parte dos Estados	• Relembram que todos os membros da ONU se comprometeram a adotar normas de comportamento responsável no ciberespaço; • Vem e continuará adotando uma diplomacia de posicionamentos de condenação, junto aos seus aliados, em relação a seus adversários que desrespeitarem essas normas; • Buscará, junto aos seus aliados, gerar consequências significativas àqueles que desrespeitarem essas normas. "Esses esforços exigirão o uso colaborativo de todas as ferramentas da diplomacia, incluindo isolamento diplomático, custos econômicos, operações de contra-ciber e aplicação da lei, ou sanções legais, entre outros."[98]
5. Garantir cadeias de suprimento globais seguras para informação, comunicação e tecnologia operacional para produtos e serviços.	• Os Estados Unidos trabalharão para reduzir sua dependência de materiais, componentes, produtos e serviços, pois isso é visto como um risco ao seu ecossistema digital. Esse é um esforço de longo prazo, que exigirá cooperação de setores públicos e privados; • Mencionam que estão trabalhando junto aos seus parceiros de suprimentos segura e confiável para 5G e tecnologias de próxima geração; • Reforçam a colaboração dos EUA com aliados e parceiros, incluindo IPEF e Quad, para melhorar a gestão de risco nas cadeias de suprimento transfronteiriças; • Mencionam esforços focados em redirecionar cadeias de suprimento para parceiros confiáveis; • Mencionam o dep. de Estado impulsionando segurança e diversificação das cadeias de suprimento através de novo fundo para semicondutores e telecomunicações. Implementação de ordens executivas para proteger a segurança nacional contra riscos de TICs controladas por governos adversários.

Fonte: Elaborada com base em Estados Unidos (2023b)

Ou seja, pela Estratégia, os Estados Unidos percebem o ciberespaço como ambiente de clara disputa geopolítica, no qual tentam estabelecer alianças para

[98] "These efforts will require collaborative use of all tools of statecraft, including diplomatic isolation, economic costs, counter-cyber and law enforcement operations, or legal sanctions, among others."

preservar seus valores e visões de mundo, e garantir estruturas que lhe permitam ter vantagens econômicas e minimizar riscos dentro de um ecossistema de disputa pelo controle das novas tecnologias.

A Declaração pelo Futuro da Internet (ESTADOS UNIDOS, 2022a), mencionada na Estratégia Nacional de Cibersegurança, merece um destaque especial também, pois resgata e esclarece pontos centrais na argumentação norte-americana sobre a governança. A declaração foi assinada por 60 países[99], incluindo Reino Unido e Austrália e, naturalmente, não possui as assinaturas de Rússia e China.

Com 3 páginas, ela fala em resgatar a promessa da internet, enquanto espaço aberto e *multistakeholder*, em meio a desafios que vêm sendo apresentados para essa visão nas últimas décadas. Tais desafios incluem governos autoritários, com ferramentas para controlar liberdade de expressão e negar direitos humanos, comportamentos maliciosos no ciberespaço, campanhas de desinformação, crimes cibernéticos, entre outros. Diante disso:

> Nós afirmamos nosso compromisso em promover e sustentar uma Internet que: seja aberta, livre, global, interoperável, confiável e segura; garanta que a Internet reforce princípios democráticos e direitos humanos e liberdades fundamentais; ofereça oportunidades para pesquisa colaborativa e comércio; seja desenvolvida, governada e implementada de forma inclusiva, para que comunidades não atendidas e subatendidas, especialmente aquelas que estão se conectando pela primeira vez, possam navegar com segurança e com proteção à privacidade e dados pessoais; seja governada por processos multissetoriais. Em resumo, uma Internet que possa cumprir a promessa de conectar a humanidade e ajudar as sociedades e democracias a prosperarem. (ESTADOS UNIDOS, 2022a)[100]

Para garantir essa visão, os assinantes da declaração assumem 5 princípios: i) a promoção de direitos humanos e liberdades fundamentais; ii) uma internet global;

---

[99] Albania, Andorra, Argentina, Australia, Austria, Belgium, Belize, Bosnia and Herzegovina, Bulgaria, Cabo Verde, Canada, Chile, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, The European Commission, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Jamaica, Japan, Kosovo, Latvia, Liechtenstein, Lithuania, Luxembourg, Maldives, Malta, Marshall Islands, Micronesia, Moldova, Monaco, Montenegro, Netherlands, New Zealand, Niger, North Macedonia, Norway, Palau, Peru, Poland, Portugal, Republic of Korea, Romania, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Taiwan, Trinidad and Tobago, the United Kingdom, Ukraine, Uruguay.

[100] Original: “We affirm our commitment to promote and sustain an Internet that: is an open, free, global, interoperable, reliable, and secure and to ensure that the Internet reinforces democratic principles and human rights and fundamental freedoms; offers opportunities for collaborative research and commerce; is developed, governed, and deployed in an inclusive way so that unserved and underserved communities, particularly those coming online for the first time, can navigate it safely and with personal data privacy and protections in place; and is governed by multistakeholder processes. In short, an Internet that can deliver on the promise of connecting humankind and helping societies and democracies to thrive.”

iii) acesso à internet de forma exclusiva e acessível; iv) confiança no ecossistema digital; v) governança da internet de forma *multistakeholder.* O primeiro deles é autoexplicativo. Trata-se de promover os direitos presentes na Declaração Universal e derivados no ciberespaço. A implicação mais política disso se encontra no último *bullet point*, que podemos entender que está direcionado aos Estados considerados autoritários. Fala-se em:

> Abster-se de usar ou abusar da Internet ou de ferramentas ou técnicas algorítmicas para vigilância ilegal, opressão e repressão que não estejam alinhadas com os princípios internacionais de direitos humanos, incluindo o desenvolvimento de cartões de pontuação social ou outros mecanismos de controle social doméstico ou detenção e prisão preventivas.[101](ESTADOS UNIDOS, 2022a)

Em relação ao ponto da Internet Global, a narrativa é a de evitar interrupções de internet, bloqueio de conteúdo, entre outros. Novamente fala-se num discurso de coalizão, no qual buscam “promover nosso trabalho para realizar os benefícios do livre fluxo de dados com confiança, baseado em nossos valores compartilhados como parceiros democráticos, de mentalidade semelhante, abertos e voltados para o exterior."[102] O terceiro ponto faz referência a garantir a disponibilidade e as habilidades necessárias para um acesso efetivo à internet globalmente. Mas também reforça sua visão contrária ao controle de informações ao trazer que

> A exposição a conteúdos diversos online deve contribuir para o discurso público pluralista, promover uma maior inclusão social e digital na sociedade, fortalecer a resiliência à desinformação e à informação incorreta, e aumentar a participação nos processos democráticos."[103] (ESTADOS UNIDOS, 2022a)

O quarto ponto traz elementos de combate aos crimes cibernéticos, proteção de dados dos indivíduos baseada na lei e seguindo direitos humanos, estando protegidos dos próprios governos; proteção de consumidores de produtos inseguros vendidos online; proteção de infraestruturas, inclusive a infraestrutura eleitoral, no

[101] Original: “Refrain from misusing or abusing the Internet or algorithmic tools or techniques for unlawful surveillance,oppression, and repression that do not align with international human rights principles, including developing social score cards or other mechanisms of domestic social control or pre-crime detention and arrest.“
[102] Original: “promote our work to realize the benefits of data free flows with trust based on our shared values aslike-minded, democratic, open and outward looking partners”
[103] Original: "Exposure to diverse content online should contribute to pluralistic public discourse, foster greater social and digital inclusion within society, bolster resilience to disinformation and misinformation, and increase participation in democratic processes.”

caso de campanhas de desinformação e manipulação, entre outros pontos nessa mesma linha.

O quinto ponto, por sua vez, reforça o posicionamento histórico dos Ocidente por uma internet *multistakeholder*.

> Proteger e fortalecer o sistema multissetorial de governança da Internet, incluindo o desenvolvimento, implementação e gestão de seus principais protocolos técnicos e outros padrões e protocolos relacionados. [...] Abster-se de minar a infraestrutura técnica essencial para a disponibilidade geral e integridade da Internet. [104] (ESTADOS UNIDOS, 2022a)

Dada essa visão geral de governança, vejamos como os principais documentos estão tratando o elemento dos sistemas ciber-físicos/ Internet das Coisas dentro dele.

4.1.2 Como os Estados Unidos percebem os sistemas ciber-físicos?

O quadro abaixo compila as menções à Internet das Coisas ou sistemas ciber-físicos nos principais documentos recentes relacionados ao ciberespaço. Vale mencionar que, assim como nos demais países, partiu-se dos documentos presentes no portal de *Cyber Policy Portal* da UNIDIR, complementado eventualmente com outros documentos observados ao longo da leitura. Os documentos observados que não apresentaram qualquer tipo de relação com a temática de Internet das Coisas não estão inseridos no quadro. O quadro contribui, mas possivelmente não esgota tudo o que existe em relação ao tema no país.

[104] Original: “Protect and strengthen the multistakeholder system of Internet governance, including the development,deployment, and management of its main technical protocols and other related standards and protocols. [...] Refrain from undermining the technical infrastructure essential to the general availability and integrity of the Internet.”

Quadro 7 - Menções sobre IoT e sistemas ciber-físicos nos documentos dos Estados Unidos (continua)

Documento	**Ano**	**Como aborda sistemas ciber-físicos/IoT?**
National Cybersecurity Strategy (ESTADOS UNIDOS, 2023b)	2023	Dentro da estratégia mais recente dos Estados Unidos, a Internet das Coisas é mencionada algumas vezes. A primeira delas é dentro de uma narrativa de grandes ambições digitais para a década. Dentro disso, o documento aponta que: "Nós vislumbramos uma 'Internet das Coisas' (IoT) em amadurecimento, abrangendo desde bens de consumo até controles industriais digitalizados e constelações de satélites, que aumentarão a eficiência e a segurança, ao mesmo tempo em que fornecerão insights transformadores sobre nosso meio ambiente e economia." (p. 5)[105] A segunda menção vem em um caráter de preocupação atrelado ao avanço tecnológico. O documento aponta que "tecnologias avançadas sem fio, IoT e ativos baseados no espaço [...] acelerarão essa tendência, movendo muitos de nossos sistemas essenciais para a Internet e **tornando os ciberataques inerentemente mais destrutivos e impactantes em nossa vida diária**. (p.6, grifo do autor)."[106] Por fim, o documento dentro de seu terceiro pilar, de *"Shape Market Forces to Drive Security and Resilience"* possui um ponto específico para falar de Internet das Coisas (3.2 Drive the Development of Secure IoT Devices). Dentro dele, a narrativa é de que os dispositivos de IoT não estão totalmente protegidos contra ameaças cibernéticas. Destaque aqui para como os EUA reconhecem que produtos estão sendo colocados no mercado sem as devidas precauções securitárias. Muitos dos dispositivos IoT implantados hoje não estão suficientemente protegidos contra ameaças de cibersegurança. Com muita frequência, eles foram implantados com configurações padrão inadequadas, podem ser difíceis ou impossíveis de corrigir ou atualizar, ou vêm equipados com capacidades avançadas - e às vezes desnecessárias - que permitem atividades cibernéticas maliciosas em sistemas físicos e digitais críticos. Vulnerabilidades recentes de IoT têm mostrado quão facilmente atores mal-intencionados podem explorar esses dispositivos para construir botnets e realizar vigilância." (p. 24, grifo do autor)[107] Dentro disso, o Estado se propõe a coordenar os esforços de segurança e a estabelecer um programa de rotulagem de produtos de IoT, com base em sua cibersegurança.

[105] Original: "We envision a maturing "Internet of Things" (IoT), comprising everything from consumer goods to digitized industrial controls to constellations of satellites, that will increase efficiency and safety while providing game-changing insights into our environment and economy." (p.5)
[106] Original: "advanced wireless technologies, IoT, and space-based assets [...] will accelerate this trend, moving many of our essential systems online and **making cyberattacks inherently more destructive and impactful to our daily lives**."
[107] Original: "many of the IoT devices deployed today are not sufficiently protected against cybersecurity threats. **Too often they have been deployed with inadequate default settings, can be difficult or impossible to patch or upgrade, or come equipped with advanced—and sometimes unnecessary—capabilities that enable malicious cyber activities on critical physical and digital systems.** Recent IoT vulnerabilities have shown just how easily bad actors can exploit these devices to construct botnets and conduct surveillance."

Quadro 7 - Menções sobre IoT e sistemas ciber-físicos nos documentos dos Estados Unidos (continuação)

Documento	**Ano**	**Como aborda sistemas ciber-físicos/IoT?**
National Cybersecurity Strategy Implementation Plano (ESTADOS UNIDOS, 2023c)	2023	Assim como na estratégia, a Internet das Coisas é abordada no terceiro pilar do documento, intitulado “Shape Market Forces to Drive Security and Resilience”, e ganha um ponto próprio, intitulado “*Drive the Development of Secure IoT Devices”.* Dentro desse ponto, são abordadas duas implementações necessárias. A primeira, sob responsabilidade do OMB (Office of Management and Budget), trata da implementação do Federal Acquisition Regulation, prevista no Cibersecurity Improvement Act, de 2020. Também se reforça a necessidade de um esforço de pesquisa e desenvolvimento, compras e análise de risco relacionados à IoT. Na segunda, sob responsabilidade do National Security Council, fala-se sobre uma estruturação do programa de rotulagem de segurança da Internet das Coisas e da busca de uma agência para liderá-lo. (p,29). Podemos entender que esse programa de rotulagem, apesar de não mencionado diretamente no documento, é o US Cyber Trust Mark.
National Security Strategy (ESTADOS UNIDOS, 2022b)	2022	Na mais recente estratégia de segurança nacional, não há menção direta à Internet das Coisas. Há, contudo, uma seção específica para tecnologia, dentro do subtítulo “Shaping the rules of the road”, na qual os Estados Unidos deixam clara sua percepção sobre a necessidade de se olhar com cuidado para as tecnologias que surgirão na década, e garantir que elas atendam aos seus interesses e o de seus aliados. "Na próxima década, tecnologias críticas e emergentes estão preparadas para reestruturar as economias, transformar os militares e remodelar o mundo. Os Estados Unidos estão comprometidos com um futuro em que essas tecnologias aumentem a segurança, prosperidade e valores do povo americano e das democracias com mentalidade semelhante." (p. 33).[108] Essa preocupação é reforçada quando trazem a necessidade de trabalhar com "ampla gama de parceiros para promover a resiliência da infraestrutura de rede em 5G e outras tecnologias avançadas de comunicação, incluindo a promoção da diversidade de fornecedores e a segurança das cadeias de suprimentos." (p.34). [109] Na seção de cibersegurança, há uma preocupação clara com ciberataques, sem determinar alvos específicos a eles. Fala-se "definir padrões para infraestrutura crítica para melhorar rapidamente nossa resiliência cibernética e construir capacidades coletivas para responder rapidamente a ataques." (p.34). [110] Por mais que não se fala em Internet das Coisas, podemos presumir essa temática dentro do guarda-chuva maior de segurança cibernética.

[108] Original: “In the next decade, critical and emerging technologies are poised to retool economies, transform militaries, and reshape the world. The United States is committed to a future where these technologies increase the security, prosperity, and values of the American people and like-minded democracies”

[109] Original: “broad range of partners to advance network infrastructure resilience in 5G and other advanced communication technologies, including by promoting vendor diversity and securing supply chains.” (p.34)

[110] Original: “to define standards for critical infrastructure to rapidly improve our cyber resilience, and building collective capabilities to rapidly respond to attacks” (p.34).

Quadro 7 - Menções sobre IoT e sistemas ciber-físicos nos documentos dos Estados Unidos (continuação)

Documento	**Ano**	**Como aborda sistemas ciber-físicos/IoT?**
CISA (Cybersecurity and Infrastructure Security Agency) Strategic Plan 2023 - 2025 (CISA, 2022)	2022	Nesse documento, a CISA apresenta uma percepção clara dos riscos trazidos pelos sistemas ciber-físicos a diferentes esferas da sociedade. Apontam que "As fronteiras entre a infraestrutura cibernética e física da nação estão cada vez mais borradas. A convergência de tecnologias ciber-físicas e sistemas que entregam nossas funções críticas - desde manufatura até saúde, transporte e além - significa que eventos isolados podem resultar na perda ou degradação de serviços em várias indústrias. A tecnologia operacional (OT) e os sistemas de controle industrial (ICS) apresentam riscos únicos que exigem foco particular devido às consequências ampliadas da interrupção e aos desafios relacionados à implementação de certos controles de segurança em grande escala. Enquanto novas e emergentes tecnologias são impulsionadoras vitais da inovação e oportunidade, elas também podem apresentar riscos não previstos." (p.8, grifo do autor).[111]
Executive Order on Improving the Nation's Cybersecurity (WHITE HOUSE, 2021)	2021	Em meio a uma série de medidas para garantir a segurança da cadeia de suprimentos de software, o documento aponta, nas medidas (s) e (t) o papel do diretor da NIST de atuar sobre um "labeling program" relacionado à produtos de IoT e estabelecer os critérios de segurança cibernética desse programa. "O Diretor do NIST, em coordenação com representantes de outras agências conforme o Diretor do NIST considere apropriado, deve iniciar programas piloto informados por programas de rotulagem de produtos de consumo existentes para educar o público sobre as capacidades de segurança de dispositivos de Internet das Coisas (IoT) e práticas de desenvolvimento de software, e deve considerar formas de incentivar fabricantes e desenvolvedores a participar desses programas." (p.12)[112]

[111] Original: "The boundaries between the nation's cyber and physical infrastructure are therefore increasingly blurred. The convergence of cyber-physical technologies and systems that deliver our critical functions — from manufacturing to healthcare to transportation and beyond — means that single events can manifest in the loss or degradation of service across multiple industries. Operational technology (OT) and industrial control systems (ICS) pose unique risks that demand particular focus due to the heightened consequences of disruption and challenges related to deploying certain security controls at scale. **While new and emerging technologies are vital drivers of innovation and opportunity, they can also present unanticipated risks**"

[112] Original: "Director of NIST, in coordination with the Chair of the Federal Trade Commission (FTC) and representatives of other agencies as the Director of NIST deems appropriate, shall identify IoT cybersecurity criteria for a consumer labeling program [...]. The criteria shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products."

Quadro 7 - Menções sobre IoT e sistemas ciber-físicos nos documentos dos Estados Unidos (continuação)

Documento	**Ano**	**Como aborda sistemas ciber-físicos/IoT?**
National Maritime Cybersecurity Plano (WHITE HOUSE, 2020)	2020	O documento aborda a Internet das Coisas como um dos elementos de tecnologias emergentes, ao lado do 5G, que irá necessitar de medidas de segurança e cooperação para evitar riscos. "O rápido aumento no número de dispositivos conectados à internet, conhecidos como IoT, e o lançamento das redes 5G agregarão opções aprimoradas de conectividade, que exigirão requisitos rigorosos de segurança, integridade e confidencialidade. As ameaças de adversários estatais e não estatais representam uma ameaça particular às cadeias de suprimentos que exigirão colaboração entre partes interessadas privadas, públicas e internacionais."(p. 29)[113]
Federal Cybersecurity Research and Strategic Plan (ESTADOS UNIDOS, 2019)	2019	O documento aborda o termo “Internet das Coisas” e também o termo “Sistemas Ciber-físicos”, com o segundo tendo ligação maior com processos complexos, industriais e ligados a infraestruturas críticas. Há uma preocupação com segurança, uma vez que os dispositivos tendem a estar mais conectados e com menor intervenção humana. "A Internet das Coisas é agora uma realidade, à medida que um número crescente e variado de dispositivos de consumo, eletrodomésticos e sensores usados para transporte e serviços municipais compartilham poder de computação, conectividade de rede e capacidade de serem controlados remotamente. O ambiente IoT é complexo, e seus desafios de segurança são igualmente complexos. Os dispositivos IoT muitas vezes têm recursos limitados de computação, armazenamento de dados, comunicação e energia disponível. As abordagens de autenticação, criptografia e aplicação de políticas e segurança que funcionam para o ambiente de desktop e servidor não serão implantáveis em um dispositivo com recursos limitados. A usabilidade e os fatores humanos também são um desafio para o design seguro da IoT porque os dispositivos têm interfaces de usuário limitadas e o usuário típico de dispositivos de consumo não é treinado em segurança cibernética e pode não tomar decisões confiáveis de segurança e privacidade.(p.22)[114]

[113] Original: “Rapidly increasing numbers of internet-connected devices, known as the IoT, and the rollout of 5G networks will add enhanced connectivity options, which will require strict security, integrity, and confidentiality requirements. Threats from state and non-state adversaries pose a particular threat to supply chains that will require collaboration between private, public, and international stakeholders”

[114] Original: The Internet of Things is now a reality as a growing number and variety of consumer devices, home appliances, and sensors used for transportation and municipal services share compute power, network connectivity, and ability to be controlled remotely. The IoT environment is complex, and its security challenges are just as complex. IoT devices are often limited in computational, data storage, communication, and available power resources. Approaches to authentication, encryption, and security policy enforcement that work for the desktop and server environment will not be deployable to a resource-constrained device. Usability and human factors are also a challenge for the secure design of IoT because the devices have limited user interfaces, and the typical user of consumer devices is not trained in cybersecurity and may not make reliably good security and privacy decisions.”

Quadro 7 - Menções sobre IoT e sistemas ciber-físicos nos documentos dos Estados Unidos (continuação)

Documento	**Ano**	**Como aborda sistemas ciber-físicos/IoT?**
Federal Cybersecurity Research and Strategic Plan (ESTADOS UNIDOS, 2019) Continuação	2019	Abordagens de autenticação, criptografia e aplicação de políticas de segurança que funcionam para o ambiente de desktop e servidor não podem ser implantadas em dispositivos com recursos limitados. Usabilidade e fatores humanos também são um desafio para o design seguro do IoT porque os dispositivos têm interfaces de usuário limitadas, e o usuário típico de dispositivos de consumo não é treinado em cibersegurança e pode não tomar decisões de segurança e privacidade de forma confiável." "Sistemas ciber-físicos (CPS) são sistemas engenheirados que são construídos para e dependem da integração perfeita de componentes de computação e físicos. Exemplos de tais sistemas podem ser vistos em montagens de fabricação "inteligentes", conectadas à Internet, controles de fluxo de tráfego, robôs de resgate, drones de segurança de fronteira e dispositivos médicos para consumidores, entre muitos outros. Avanços em CPS permitirão capacidade avançada, adaptabilidade, escalabilidade, resiliência, segurança e usabilidade que expandirão os horizontes desses sistemas cada vez mais críticos. À medida que os sistemas CPS se tornam mais complexos, a interdependência dos componentes aumenta a vulnerabilidade a ataques e falhas em cascata. Os algoritmos que controlam os CPS podem ser complexos e opacos, e sua segurança pode depender da defesa cibernética autônoma, em vez de intervenção humana, bem como de hardware eletrônico analógico e digital seguro. Além disso, a restauração e resiliência dos sistemas CPS após uma falha ou ataque cibernético podem ser desafiadas pelo potencial sobrecarga nos sistemas físicos." (p.22, grifo do autor)[115]

[115] Original: “Cyber-physical systems (CPS) are engineered systems that are built for and depend upon the seamless integration of computation and physical components. Examples of such systems can be seen in “smart,” Internet-connected manufacturing assemblies, traffic flow controls, rescue robots, border security drones, and consumer medical devices, among a host of others. Advances in CPS will enable advanced capability, adaptability, scalability, resiliency, safety, security, and usability that will expand the horizons of these increasingly critical systems. **As CPS systems become more complex, the interdependence of components increases the vulnerability to attacks and cascading failures**. The algorithms that control CPS may be complex and opaque, and their security may depend on autonomous cyber defense rather than human intervention, as well as on secure analog and digital electronic hardware. Furthermore, restoration and resiliency of CPS systems after a fault or cyber attack may be challenged by the potential overload on the physical systems.”

Quadro 7 - Menções sobre IoT e sistemas ciber-físicos nos documentos dos Estados Unidos (conclusão)

Documento	**Ano**	**Como aborda sistemas ciber-físicos/IoT?**
U.S. Department of Homeland Security Cybersecurity Strategy (ESTADOS UNIDOS, 2018)	2018	O documento aponta a iminência da internet das coisas como fator de risco para ataques cibernéticos, trazendo exemplos de dois ataques de ransomware no qual isso pode ser visível. "A crescente interconexão de sistemas cibernéticos e físicos dentro da infraestrutura crítica também cria o potencial risco para atividades cibernéticas maliciosas resultarem em consequências físicas diretas; por exemplo, a anulação dos controles na rede elétrica ucraniana em dezembro de 2015 resultou em uma perda generalizada de energia. Incidentes de ransomware como WannaCry e NotPetya demonstram como o rápido crescimento da internet das coisas complica ainda mais a ameaça, pois dispositivos cotidianos podem ser alvo de atores cibernéticos maliciosos com consequências potencialmente de grande alcance." (p.4)[116] O documento também aponta para a responsabilidade do Departamento de pensar os aspectos securitários do ciclo de vida de aparelhos da internet das coisas. "O DHS também deve incentivar a melhoria da segurança para infraestrutura de nuvem e ao longo do ciclo de vida dos dispositivos da Internet das Coisas e tecnologias emergentes." (p.25)[117]

Fonte: Elaborada pelo autor, baseada em documentos dos EUA

A partir da análise dos documentos, é possível perceber uma clareza crescente dos Estados Unidos sobre a importância de se preservar os sistemas ciber-físicos. A presença de um tópico específico para eles na estratégia de segurança cibernética de 2023, que inexiste em 2018, demonstra que o termo vem ganhando espaço na visão e na narrativa estratégica estadunidense. E, mais relevante ainda, o documento de 2023 reconhece que os produtos estão chegando ao mercado sem os padrões de segurança adequados. Isso pressupõe uma necessidade maior de fiscalização e padronização de segurança para esses produtos. Assim, por mais que os Estados Unidos se coloquem ativamente como defensores de um modelo *multistakeholder*, em temas que se tornam securitários, como esses, conseguimos perceber um certo grau

[116] Original: “The growing interconnection of cyber and physical systems within critical infrastructure also creates the potential risk for malicious cyber activity to result in direct physical consequences; for example, the December 2015 overriding of controls in the Ukrainian electric grid resulted in widespread loss of power. Ransomware incidents such as WannaCry and NotPetya demonstrate how the rapid growth of the internet-of-things further complicates the threat as everyday devices can be targeted by malicious cyber actors with potentially far-reaching consequences.”

[117] “DHS must also encourage improved security for cloud infrastructure and throughout the life-cycle of internet-of-things devices and emerging technologies.”

de hierarquia onde, apesar de seguirem relevantes no processo, os representantes da iniciativa privada precisarão se adequar a modelos de segurança advindos de cima para baixo.

Para além das menções nesses documentos, os Estados Unidos vêm desenvolvendo políticas e legislações específicas para se estabelecer e se consolidar nesse campo. Vejamos algumas delas.

4.1.3 Como o país vem abordando o tema internamente?

A mais recente iniciativa estadunidense relacionada à Internet das Coisas é o que está sendo chamado de "*US Cyber Trust Mark*". Proposto pela Federal Communications Commission (FCC), o programa que conta com o apoio de gigantes tecnológicas como Amazon e Google[118] basicamente fala em aumentar os requisitos de segurança cibernética para dispositivos inteligentes e adicionar um selo aos produtos que atingirem os critérios estabelecidos. Dessa forma, seria mais fácil aos consumidores identificar os produtos mais seguros no momento do consumo. Fala-se também no estabelecimento de um QR code ligado a um registro nacional de produtos certificados, que permitirá a checagem de informações sobre esses produtos. Além disso, o programa pressupõe a continuidade de esforços na definição de padrões de segurança para produtos de alto risco por parte do NIST (Instituto Nacional de Padrões e Tecnologia), assim como colaboração por parte do Departamento de Energia na definição dos padrões de segurança para dispositivos inteligentes importantes nesse campo. É previsto, ainda, um esforço por parte do Departamento de Estado em harmonizar padrões junto aos aliados e parceiros estadunidenses, na tentativa de somar esforços em iniciativas semelhantes. (WHITE HOUSE, 2023)

Além dessa iniciativa, o esforço para melhorar a segurança dos dispositivos de IoT já vem acontecendo há alguns anos. Em 2020, foi lançada a lei 116-207, que ficou conhecida como '*IoT Cybersecurity Improvement Act of 2020*'. Entre uma série de outros pontos, a lei define o NIST como responsável pela definição dos padrões de segurança a serem adotados pelos dispositivos (ESTADOS UNIDOS, 2020).

[118] Lista de organizações que apoiaram o anúncio: Amazon, Best Buy, Carnegie Mellon University, CyLab, Cisco Systems, Connectivity Standards Alliance, Consumer Reports, Consumer Technology Association, Google, Infineon, the Information Technology Industry Council, IoXT, KeySight, LG Electronics U.S.A., Logitech, OpenPolicy, Qorvo, Qualcomm, Samsung Electronics, UL Solutions, Yale and August U.S.

Há ainda de se trazer que, na ordem executiva EO 14028, sob o título de "*Improving the Nation's Cybersecurity*", a Internet das Coisas é mencionada na seção de "*Enhancing Software Supply Chain Security*", justamente numa linha de implementação de um programa como o Cybertrust Mark, que marcasse produtos de acordo com suas capacidades de segurança, e incentivasse fornecedores a participarem do programa. (ESTADOS UNIDOS, 2021)

Antes disso, ainda em 2016, o Departamento de Estado lançava seus princípios estratégicos para garantir a segurança da Internet das Coisas. (ESTADOS UNIDOS, 2016) e em 2017 o NIST estabelecia um framework para o desenvolvimento de sistemas ciber-físicos (NIST, 2017). Dessa forma, conseguimos perceber por parte dos Estados Unidos uma atenção ao tema e um esforço por se preparar para uma adequação securitária em relação a ele. A iniciativa do US Cybertrust Mark, prevista para 2024, é uma tentativa interessante de se colocar em meio à disputa por mercados. Cabe verificar, para além do mercado interno, o quanto essa prática se legitimará e se consolidará internacionalmente, tanto em termos de padronização quanto em termos de narrativa.

No fim, fica a pergunta a caráter de reflexão: para um cidadão brasileiro que já tem como rotina comprar produtos, por exemplo, na *Shein*, por conta dos preços baixos, será mesmo um selo desse tipo que fará a diferença na escolha entre um produto estadunidense e um chinês? Dependerá do quão forte for a capacidade de cada um de fazer valer seu poder nesse ambiente, e do quanto serão colocadas barreiras aos produtos que não tiverem esse tipo de selo.

4.2 REINO UNIDO

4.2.1 Como o Reino Unido percebe a governança do ciberespaço?

Como mencionado na seção anterior, o Reino Unido é assinante da Declaração para o Futuro da Internet. Disso, subentende-se que o país compactua com os elementos ali apresentados, e já trazidos. Para além da declaração, contudo, cabe ressaltar os pontos trazidos diretamente nos documentos do país. Aqui focaremos na *Cyber Strategy* de 2022.

Dentro dela, o Reino Unido também percebe uma competição de valores dentro do espaço cibernético, entre um bloco liderado majoritariamente por China e Rússia,

que prega por um controle maior do Estado como forma de garantir e um grupo que quer preservar liberdades sistêmicas e sociedades abertas, no qual se inclui. Essa divisão é mencionada duas vezes no documento.

> Os debates sobre as regras que regem o ciberespaço se tornarão cada vez mais um campo de competição sistemática entre grandes potências, com um choque de valores entre países que desejam preservar um sistema baseado em sociedades abertas e competidores sistêmicos como China e Rússia, que estão promovendo um maior controle estatal como a única forma de garantir o ciberespaço. Isso colocará pressão sobre a internet livre e aberta, à medida que os Estados-nação, grandes empresas de tecnologia e outros atores promovem abordagens concorrentes para padrões técnicos e governança da internet. (REINO UNIDO, 2022, p.30, grifo do autor) [119]

> [...] enfrentamos abordagens concorrentes internacionalmente à medida que competidores sistêmicos como China e Rússia continuam a advogar por uma maior soberania nacional sobre o ciberespaço como resposta aos desafios de segurança. A liberdade na internet está diminuindo globalmente e a visão da internet como um espaço compartilhado que apoia a troca de conhecimento e bens entre sociedades abertas corre o risco de ser ameaçada. (REINO UNIDO, 2022, p.23, grifo do autor) [120]

Diante desse cenário, o Reino Unido mais do que preservar um ciberespaço aberto, livre e pacífico, se propõe a liderar os esforços para alcançá-lo e a fortalecer alianças para esse fim. Dentro desse, que é o quarto pilar de sua estratégia, o Reino Unido destaca 3 objetivos. Vejamos no quadro abaixo:

[119] Original: Debates over the rules governing cyberspace will increasingly become a site of systemic competition between great powers, with a clash of values between countries that want to preserve a system based on open societies and systemic competitors like **China and Russia who are promoting greater state control as the only way to secure cyberspace**. This will put pressure on the free and open internet, as nation states, big technology firms and other actors promote competing approaches to technical standards and internet governance

[120] Original: "[...] we face competing approaches internationally as systemic competitors like China and Russia continue **to advocate for greater national sovereignty over cyberspace as the answer to security challenges**. Internet freedom is decreasing globally and the vision of the internet as a shared space that supports the exchange of knowledge and goods between open societies risks coming under threat."

Quadro 8 - Objetivos Estratégicos do Reino Unido

Objetivo	Principais pontos
Fortalecer a segurança cibernética e a resiliência de parceiros e aumentar as ações coletivas para interromper e dissuadir adversários	• O Reino Unido espera que em 2025 tenha parceiros mais preparados para lidar com ameaças cibernéticas e construir resiliência. O país priorizará apoiar países da Europa Oriental, África e Indo-Pacífico, além de continuar com parceiros no Oriente Médio e Américas; • Continuarão trabalhando com organismos multilaterais e ajudarão a desenvolver capacidades em organizações da sociedade civil; • Estabelecerão uma campanha de higiene cibernética internacional, que visará aumentar os custos de atividades maliciosas no ciberespaço; • Consolidação de uma aliança capaz de gerar consequências significativas aos adversários, através de sanções. • Continuarão a apoiar os esforços da OTAN nesse sentido.
Moldar a governança global para promover um ciberespaço livre, aberto, pacífico e seguro	• O Reino Unido quer se colocar proativamente no debate internacional de governança para garantir que sua visão de ciberespaço prevaleça em meio às normas, regras e princípios estabelecidos. Coloca que trabalhará com organizações regionais, como a OSCE, ASEAN, GFCE, além da ONU; • Continuarão a promover a Convenção de Budapeste sobre crimes cibernéticos, trabalhando junto a parceiros para que ela permaneça o acordo internacional central para cooperação nesse campo • Continuarão a promover e participar de esforços *multistakeholder,* como os dentro do ICANN e do IGF; • Ainda, o Reino Unido vê que quanto mais *"middle ground countries"* estiverem de acordo com sua visão, maior a probabilidade de sucesso em conter a influência de Estados autoritários.
Alavancar e exportar as capacidades e a expertise em cibersegurança do Reino Unido para aumentar suas vantagens estratégicas e promover seus interesses mais amplos de política externa e prosperidade.	• Para 2025, o Reino Unido espera que suas atividades tenham promovido estabilidade e protegido o sistema internacional baseado e as sociedades abertas e democráticas onde elas estejam em risco. • Esperam também estar no top 3 de exportadores globais de soluções e expertise cibernética, podendo exportar para governos e grandes clientes comerciais.

Fonte: Elaborado pelo autor, com base em Reino Unido (2022)

Além desses pontos, cabe destacar outros dois pontos presentes na estratégia, no pilar anterior, que dialogam não exclusivamente, mas diretamente com os sistemas ciber-físicos: o desenvolvimento de padrões e a cadeia de suprimentos. Em seu terceiro pilar na estratégia, o Reino Unido trabalha vantagens tecnológicas. E, dentro dessas vantagens, temos o objetivo 3 focado em garantir a segurança da nova geração de tecnologias, diminuindo os riscos cibernéticos da dependência de mercados globais e garantindo uma cadeia de suprimentos confiável. Dentro disso, elementos de segurança no desenho dos produtos são ressaltados, assim como o controle dos padrões internacionais, que também são frisados no ponto seguinte. Junto aos seus aliados, o Reino Unido busca influenciar na definição de padrões internacionais.

> Iremos introduzir e implementar o Projeto de Lei de Segurança de Produtos e Infraestrutura de Telecomunicações para possibilitar a aplicação de padrões mínimos de segurança em todos os novos produtos conectáveis ao consumidor vendidos no Reino Unido. Apoiaremos uma transição cibernética segura para um sistema de energia inteligente e flexível, incluindo pontos de carga para veículos elétricos inteligentes e eletrodomésticos inteligentes. Trabalharemos com organismos de padronização, indústria e parceiros internacionais para influenciar o consenso global sobre padrões técnicos. (REINO UNIDO, 2022, p.86, grifo do autor) [121]

O Reino Unido também se propõe a liderar o desenvolvimento de uma política internacional focada em fornecedores, para garantir que estejam tendo os devidos cuidados em relação aos riscos percebidos. Da mesma forma, se propõe a construir um consenso internacional relacionado a cidades inteligentes, as quais chama de "*connected places*". "Vamos fortalecer a capacidade das autoridades locais e organizações, como portos, universidades e hospitais, para comprar e usar tecnologia de lugares conectados de forma segura."[122] (REINO UNIDO, 2020, p.87). No Objetivo 4 desse mesmo Pilar, o Reino Unido reforça a questão da padronização, se propondo a:

---

[121] Original: We will introduce and implement the **Product Security and Telecommunications Infrastructure Bill** to enable enforcement of minimum security standards in all new consumer connectable products sold in the UK. We will support a cyber secure transition to a smart and flexible energy system, including smart electric vehicle charge-points and energy smart appliances. **We will work with standards bodies, industry and international partners to influence the global consensus on technical standards.**

[122] Original: We will strengthen the capability of local authorities and organizations such as ports, universities and hospitals, to buy and use connected places technology securely"

> Trabalhar com a comunidade multissetorial para moldar o desenvolvimento de padrões técnicos digitais globais nas áreas prioritárias que são mais importantes para defender nossos valores democráticos, garantir nossa segurança cibernética e avançar nos interesses estratégicos do Reino Unido por meio da ciência e tecnologia. [...] Os padrões técnicos digitais globais são uma parte fundamental do funcionamento da internet, das redes de telecomunicações e das tecnologias emergentes. Como eles são desenvolvidos e implementados pode impactar nossos objetivos de segurança cibernética, prosperidade econômica e nossas normas e valores. (p.88)[123]

Dessa forma, podemos perceber um Reino Unido que se propõe a um papel de protagonista na disputa global para estabelecer os padrões futuros para o funcionamento do ciberespaço. A menção aos padrões cibernéticos e a percepção da importância de estar presente nos debates das novas tecnologias são claros na narrativa. Dentro disso, vejamos um pouco mais das menções à IoT.

4.2.2 Como o Reino Unido percebe os sistemas ciber-físicos?

O quadro abaixo aborda menções à Internet das coisas e sistemas ciber-físicos encontradas nos documentos mais recentes do país, com base no portal da UNIDIR.

Quadro 9 - Percepção do Reino Unido acerca de sistemas ciber-físicos (continua)

Documento	**Ano**	**Como aborda sistemas ciber-físicos/IoT?**
National Cyber Strategy (REINO UNIDO, 2022)	2022	A menção à Internet das Coisas está dentro de uma seção intitulada “Technologies vital to Cyber Power”, e aparece ao lado de outras tecnologias, como 5G e 6G, Inteligência Artificial, Blockchain, Semicondutores, Autenticação Criptográfica e Tecnologias Quânticas. “Uma variedade de tecnologias existentes e emergentes será fundamental para o poder cibernético do Reino Unido e precisamos ser capazes de antecipar, avaliar e agir sobre esses desenvolvimentos. Esperamos priorizar uma variedade de tecnologias e aplicações conforme entregamos a estratégia, como as listadas abaixo. [...] Internet das Coisas e tecnologias utilizadas em ambientes de consumo, empresarial, industrial e físico, como lugares conectados. ” (p.80)[124]

[123] Original: Work with the multistakeholder community to shape the development of global digital technical standards in the priority areas that matter most for upholding our democratic values, ensuring our cyber security, and advancing UK strategic interests through science and technology [...] **Global digital technical standards are a core part of the functioning of the internet, telecommunication networks, and emerging technologies**. How they are developed and deployed can impact our cyber security objectives, economic prosperity, and our norms and values.

[124] Original: A variety of existing and emerging technologies will be critical to the UK’s cyber power and we need to be able to anticipate, assess, and act on these developments. We expect to prioritise a

Quadro 9 - Percepção do Reino Unido acerca de sistemas ciber-físicos (continuação)

Documento	Ano	Como aborda sistemas ciber-físicos/IoT?
		Dentro do terceiro objetivo da seção “"Garantir a próxima geração de tecnologias conectadas, mitigando os riscos de segurança cibernética da dependência dos mercados globais e garantindo que os usuários do Reino Unido tenham acesso a fornecedores confiáveis e diversos." Assumindo a liderança nas tecnologias vitais para o poder cibernético”, intitulado “Proteja a próxima geração de tecnologias conectadas, mitigando os riscos de segurança cibernética da dependência dos mercados globais e garantindo que os usuários do Reino Unido tenham acesso a um fornecimento confiável e diversificado”[125] há também uma menção direta ao fortalecimento securitário das “infraestruturas ciber-físicas”. "Iremos identificar aplicações de tecnologia inovadoras e emergentes que tenham o potencial de criar riscos de segurança cibernética, e garantir que o Reino Unido esteja na vanguarda do desenvolvimento seguro dessas tecnologias. À medida que o governo considera opções para uma capacidade no Reino Unido em gêmeos digitais e tecnologia mais ampla de 'infraestrutura ciber-física', garantiremos que a segurança cibernética esteja no centro do processo decisório. E implementaremos um esquema de garantia para garantir que o Reino Unido esteja em uma posição forte para uma ampla variedade de implantações de veículos conectados e automatizados." (p.87)[126] Da mesma forma, como mencionado na seção anterior, o Reino Unido fala em ser protagonista em termos de desenvolvimento de padrões, cadeias de suprimentos, e fala diretamente em cidades inteligentes. Todos esses pontos se relacionam a IoT, ainda que esta não esteja diretamente mencionada.

range of technologies and applications as we deliver the strategy, such as those set out below. [...] Internet of Things and technologies used in consumer, enterprise, industrial and physical environments such as connected places”.

[125] Original: Taking the lead in the technologies vital to cyber power”, intitulado “Secure the next generation of connected technologies, mitigating the cyber security risks of dependence on global markets and ensuring UK users have access to trustworthy and diverse supply”

[126] Original: **We will identify novel and emerging technology applications that have the potential to create cyber security risks**, and ensure the UK is at the forefront of the safe and secure development of these technologies. As the government considers options for a UK capability in digital twin and wider ‘cyber-physical infrastructure’ technology, we will ensure that cyber security is at the heart of decision-making. And we will roll out an assurance scheme to ensure that the UK is in a strong position for a wide range of connected and automated vehicle deployments”

Quadro 9 - Percepção do Reino Unido acerca de sistemas ciber-físicos (continuação)

Documento	**Ano**	**Como aborda sistemas ciber-físicos/IoT?**
National Cyber Security Strategy 2016 - 2021 (REINO UNIDO, 2016)	2016	No documento, a Internet das Coisas é mencionada algumas vezes. A primeira está ligada a uma percepção de aumento das superfícies de ataque no qual, dentro do subtítulo "*An expanding range of devices*", o Reino Unido traz a percepção dos riscos de dano físico possivelmente derivados: "Quando a última Estratégia Nacional de Segurança Cibernética foi publicada em 2011, a maioria das pessoas concebia a segurança cibernética através do prisma de proteger dispositivos como seu computador de mesa ou laptop. Desde então, a Internet se integrou cada vez mais em nossas vidas diárias de formas que em grande parte desconhecemos. A 'Internet das Coisas' cria novas oportunidades para exploração e aumenta o impacto potencial de ataques que têm o potencial de causar danos físicos, ferimentos a pessoas e, no pior dos casos, morte." (p.20, grifo do autor)[127] A conexão da internet das coisas com processos industriais também é destacada: "A implementação rápida da conectividade em processos de controle industrial em sistemas críticos, em uma ampla gama de indústrias como energia, mineração, agricultura e aviação, criou a Internet Industrial das Coisas. Isso abre simultaneamente a possibilidade de dispositivos e processos, que nunca foram vulneráveis a tais interferências no passado, serem hackeados e adulterados, com consequências potencialmente desastrosas." (p.20)[128] E a conclusão desse trecho passa pela percepção de um risco sistêmico promovido por sistemas cada vez mais interconectados "Portanto, não estamos mais apenas vulneráveis aos danos cibernéticos causados pela falta de segurança cibernética em nossos próprios dispositivos, mas também às ameaças aos sistemas interconectados que são fundamentais para nossa sociedade, saúde e bem-estar." (p.20)[129]

[127] Original: When the last National Cyber Security Strategy was published in 2011, most people conceived of cyber security through the prism of protecting devices such as their desktop computer or laptop. Since then the Internet has become increasingly integrated into our daily lives in ways we are largely oblivious to. The 'Internet of Things' creates new opportunities for exploitation and increases the potential impact of attacks **which have the potential to cause physical damage, injury to persons and, in a worst case scenario, death**"

[128] Original: "The rapid implementation of connectivity in industrial control processes in critical systems, across a wide range of industries such as energy, mining, agriculture and aviation, has created the Industrial Internet of Things. This is simultaneously opening up the possibility of devices and processes, which were never vulnerable to such interference in the past, being hacked and tampered with, with potentially disastrous consequences"

[129] Original: "Therefore, we are no longer just vulnerable to cyber harms caused by the lack of cyber security on our own devices but by threats to the interconnected systems that are fundamental to our society, health and welfare"

Quadro 9 - Percepção do Reino Unido acerca de sistemas ciber-físicos (continuação)

Documento	**Ano**	**Como aborda sistemas ciber-físicos/IoT?**
National Cyber Security Strategy 2016 - 2021 (REINO UNIDO, 2016)	2016	Outra perspectiva levantada através da resposta está relacionada aos ganhos econômicos de se utilizar IoT sob um guarda-chuva sólido de segurança cibernética . "A segurança cibernética é fundamental para desbloquear a inovação e expansão, e ao adotar uma abordagem organizacional e centrada em riscos para a segurança cibernética, as organizações podem se concentrar em oportunidades e exploração. Construir confiança em um negócio que opera com sucesso dentro da Internet das Coisas (IoT), e que oferece total suporte e proteção aos indivíduos e seus dispositivos móveis pessoais (desde um simples telefone até um dispositivo de saúde, de eletrodomésticos inteligentes a carros inteligentes), é um diferencial competitivo chave e deve ser uma prioridade." (p.38, grifo do autor)[130] Outra menção aparece dentro do subtítulo "*Promoting Cyber Security Science and Technology*", onde a Internet das Coisas e os Sistemas Cyber-Físicos são colocados como áreas importantes de pesquisa, que deverá ser fruto de incentivo governamental. "O Governo continuará a fornecer financiamento e apoio para os Centros Acadêmicos de Excelência, Institutos de Pesquisa e Centros de Treinamento Doutoral. Além disso, criaremos um novo Instituto de Pesquisa em uma área de assunto estrategicamente importante. [...] Áreas importantes que serão consideradas incluem: análise de grandes dados; sistemas autônomos; sistemas de controle industrial confiáveis; sistemas ciberfísicos e Internet das Coisas; cidades inteligentes; verificação automatizada de sistemas; e a ciência da segurança cibernética." (p. 59)[131]

[130] Original: "Cyber security is key to unlocking innovation and expansion, and by adopting a tailored organisation and risk-centric approach to cyber security, organisations can refocus on opportunities and exploration. Building trust in a business that operates successfully within the Internet of Things (IoT), and that fully supports and protects individuals and their personal mobile devices (from a simple phone to a health care device, from smart appliances to smart cars), **is a key competitive differentiator and must be a priority"**

[131] Original: "The Government will continue to provide funding and support for the Academic Centres of Excellence, Research Institutes and Centres for Doctoral Training. In addition, we will create a new Research Institute in a strategically important subject area.[...] Important areas that will be given consideration include: big data analytics; autonomous systems; trustworthy industrial control systems; cyber-physical systems and the Internet of Things; smart cities; automated system verification; and the science of cyber security"

Quadro 9 - Percepção do Reino Unido acerca de sistemas ciber-físico (conclusão)

Documento	Ano	Como aborda sistemas ciber-físicos/IoT?
National Cyber Security Strategy 2016 - 2021 (REINO UNIDO, 2016)	2016	Dentro do subtítulo "*Effective Horizon Scanning*" é ressaltado o uso de evidências sólidas para embasar as políticas cibernéticas no campo da Internet das Coisas: "Também garantiremos que a formulação de políticas cibernéticas siga uma abordagem baseada em evidências, levando em consideração avaliações de todas as fontes disponíveis. Isso incluirá, por exemplo: evidências técnicas específicas, por exemplo, sobre a Internet das Coisas, ou o papel futuro de materiais avançados [...]" (p. 59) [132] Já o termo "cyber-physical systems" aparece na introdução, na argumentação de que aparelhos da nossa vida cotidiana, ao estarem conectados à internet, passam a representar vulnerabilidades: "A expansão da Internet além de computadores e telefones celulares para outros sistemas ciberfísicos ou 'inteligentes' está estendendo a ameaça de exploração remota a uma série de novas tecnologias. Sistemas e tecnologias que sustentam nossas vidas diárias - como redes elétricas, sistemas de controle de tráfego aéreo, satélites, tecnologias médicas, plantas industriais e semáforos - estão conectados à Internet e, portanto, potencialmente vulneráveis a interferências." (p.11)[133]

Fonte: Elaborado pelo autor, com base em documentos do Reino Unido

É possível perceber uma grande preocupação do Reino Unido com o tema, tanto pelos potenciais positivos que ele traz, quanto pelos riscos atrelados em caso de negligência. As duas estratégias nacionais de segurança são bem ricas nesse sentido, e se conectam com as demais legislações locais presentes no país.

4.2.3 Como o país vem abordando o tema internamente?

O Reino Unido possui uma iniciativa chamada "*Secure by design*"[134] que, por sua própria descrição, dialoga com a "proteção dos cidadãos e negócios das ameaças

[132] Original: "We will also ensure that cyber policy-making follows an evidence-based approach, taking into account assessments from all available sources. This will include, for example: specific technical evidence, for example on the Internet of Things, or the future role of advanced materials [...]"
[133] Original: "The expansion of the Internet beyond computers and mobile phones into other cyber-physical or 'smart' systems is extending the threat of remote exploitation to a whole host of new technologies. Systems and technologies that underpin our daily lives – such as power grids, air traffic control systems, satellites, medical technologies, industrial plants and traffic lights – are connected to the Internet and, therefore, potentially vulnerable to interference"
[134] Secure by design. Disponível em: https://www.gov.uk/government/collections/secure-by-design#legislation. Acesso em: 01 jan. 2024.

representadas por produtos de consumo conectáveis, também conhecidos como IoT ou smart devices"[135]. (REINO UNIDO, 2024)

Dentro dessa macro iniciativa, o país vem estabelecendo alguns documentos e princípios para embasar a Internet das Coisas sob sua jurisdição. O primeiro e mais conhecido deles é o "*Code of Practice for Consumer IoT*", de 2018. O Código foi lançado sob a narrativa de que a segurança dos dispositivos afeta nossa vida física e em meio à percepção de que muitos dos dispositivos presentes no mercado careciam de segurança adequada. Dessa forma, ele é um guia para que os *stakeholders* empresariais possam estabelecer boas práticas de segurança desde a concepção dos produtos, e para que a mentalidade em relação à segurança seja estabelecida entre os fornecedores.

> [...] um número significativo de dispositivos no mercado atualmente foi encontrado sem medidas básicas de segurança. [...] Este Código de Prática estabelece medidas práticas para fabricantes de IoT e outros stakeholders da indústria melhorarem a segurança de produtos IoT para consumidores e dos serviços associados. [...] Este Código de Prática não é uma solução milagrosa para resolver todos os desafios de segurança. Somente ao adotar uma mentalidade de segurança e investir em um ciclo de vida de desenvolvimento seguro, uma organização pode ter sucesso em criar IoT seguros. (REINO UNIDO, 2018, p.2, grifo do autor)[136]

O Reino Unido reforça, ainda, que as recomendações do código surgem em meio a uma cadeia de suprimentos de IoT "complexa e internacional", e que seus esforços com o código são complementares a padrões e recomendações de segurança discutidos internacionalmente. Na prática, o código consiste em 13 recomendações[137], com breves explicações para cada uma delas, e serviu de base para a implementação do ETSI European Standard 303 645[138], lançada em 2020.

---

[135] Texto original: The government is working to protect UK citizens and businesses from the threats posed by poorly secured consumer connectable products (also known as 'IoT' or 'smart' devices.)

[136] Original: [...]a significant number **of devices on the market today have been found to lack basic security measures**. [...] This Code of Practice sets out practical steps for IoT manufacturers and other industry stakeholders to improve the security of consumer IoT products and associated services. [...] This Code of Practice is not a silver bullet for solving all security challenges. **Only by shifting to a security mindset and investing in a secure development lifecycle can an organisation succeed at creating secure IoT**.

[137] 1. No default passwords; 2. Implement a vulnerability disclosure policy; 3. Keep software updated; 4. Secure store credentials; 5. Communicate securely; 6. Minimise exposed attacks surface; 7. Ensure software integrity; 8. Ensure that personal data is protected; 9. Make systems resilient to outages; 10. Monitor systems telemetry data; 11. Make it easy for consumers to delete personal data; 12. Make installation and 13. maintenance of devices easy

[138] ETSI European Standard 303 645. Disponível em: https://www.gov.uk/government/publications/etsi-industry-standard-based-on-the-code-of-practice. Acesso em: 01 jan. 2024.

Inspirado nesses dois documentos, o país vai colocar em vigor, a partir de 29 de abril de 2024, um regime de segurança obrigatório para produtos IoT, baseado em seu PSTI (Product Security and Telecommunications Infrastructure) Act. O PSTI foi lançado em duas partes, uma delas em 2022[139] e a mais recente em 2023[140], com recomendações mais claras e diretas que as presentes no Código de Conduta.

Com essa legislação, o Reino Unido busca se colocar como referência global na temática. Esse posicionamento é claro na própria apresentação da legislação em seu site oficial, no qual o Reino Unido aponta que: “Quando este regime entrar em vigor, consumidores e empresas que adquirirem novos produtos conectáveis se beneficiarão de **proteções de segurança líderes mundiais** contra ameaças de crimes cibernéticos**.**” (REINO UNIDO, 2024, grifo do autor)[141].

Como veremos posteriormente, o Código de Conduta vem servindo de base para outros países, como a Austrália. Caberá verificar, uma vez em prática, o quanto o PSTI seguirá o mesmo caminho.

4.3 RÚSSIA

4.3.1 Como a Rússia percebe a governança do ciberespaço?

Quando pensamos na Rússia, primeiramente é necessário entender a visão que o país possui e coloca no ciberespaço. Figueiredo, Rê e Menezes (2019) e Bartles (2016) apontam como o país de Putin enxerga que o mundo pós Guerra-Fria, no século XXI é marcado pelo uso de sistemas de informação para desestabilizar regimes, gerando desestabilizações internas nos países. Segundo eles:

> o elemento chave que podemos adquirir a partir do texto de Gerasimov é a percepção de que para a Rússia, no mundo pós Guerra-Fria, a soberania de regimes não ocidentais se encontra ameaçada por políticas de controle estadunidense, tais como uso massivo de propaganda, da internet e de mídias sociais. Ou seja, o elemento da informação, já forte na guerra fria, é agora ainda mais relevante na estratégia do Ocidente. Conforme aponta Bartles “A Rússia acredita que o padrão de mudança forçada patrocinada pelos EUA tem sido amplamente substituído por um novo método. Em vez de uma evidente invasão militar, os primeiros atos de um ataque dos EUA vêm

[139] Parte 1. Disponível em: https://www.legislation.gov.uk/ukpga/2022/46/part/1/enacted. Acesso em: 01 jan. 2024.
[140] Parte 2. Disponível em: https://www.legislation.gov.uk/ukdsi/2023/9780348249767. Acesso em: 01 jan. 2024.
[141] Original: "When this regime comes into effect, consumers and businesses who purchase new connectable products will benefit from **world-leading security protections** from the threat of cyber crime.”

> da parcela de uma oposição política através de propaganda estatal (por exemplo, CNN, BBC), a Internet e mídias sociais e organizações não governamentais (ONGs). Após introduzir a dissidência política, o separatismo e/ou o conflito social com sucesso, o governo legítimo tem uma dificuldade crescente em manter a ordem. (FIGUEIREDO, RÊ, MENEZES, 2019,p.2)

Diante disso, em seus documentos, a Rússia prevê a busca pelo que chama de "segurança da informação". O documento mais recente nesse tema é o "*Fundamentals of the state policy of the Russian Federation in the field of international information security*", de 2021, que compila os principais pontos e argumentos que vêm sendo estabelecidos pela Rússia no campo da governança global do ciberespaço nos últimos anos. Vejamos alguns dos principais pontos desse documento.

Primeiramente, cabe entender que segurança da informação a nível internacional, para a Rússia, é "um estado do espaço global de informações no qual, com base em princípios e normas geralmente reconhecidas do direito internacional e em termos de parceria igualitária, é assegurada a manutenção da paz, segurança e estabilidade internacional"[142] (FEDERAÇÃO RUSSA, 2021, tradução Google). Ou seja, em meio a uma percepção de ameaças, busca-se pela paz e estabilidade para manter o próprio regime. Dentre as ameaças citadas, além de extremismo e terrorismo, crimes e ataques a infraestruturas críticas, cabe aqui destacar dois pontos que dialogam com a forma como a qual a Rússia enxerga o ciberespaço e com a Doutrina Gerasimov, mencionada por Figueiredo, Rê e Menezes (2019).

A Rússia frisa como ameaça o uso de tecnologias da informação para infringir a soberania e integridade territorial dos Estados. Para o país, entre as principais ameaças em termos de segurança da informação está:

> O uso de tecnologias de informação e comunicação nos âmbitos militar-político e outros com o propósito de minar (infringir) a soberania, violar a integridade territorial dos Estados e realizar outras ações no espaço global de informações que dificultam a manutenção da paz, segurança e

[142] Traduzido do Inglês: "a state of the global information space in which, on the basis of generally recognized principles and norms of international law and on the terms of equal partnership, the maintenance of international peace, security and stability is ensured."

Original em russo: Международная информационная безопасность представляет собой такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности

> estabilidade internacionais. (FEDERAÇÃO RUSSA, 2021, tradução Google)[143]

Da mesma forma, o risco econômico no campo das tecnologias de informação também é citado. A Rússia manifesta preocupação com monopólios tecnológicos e limites de acesso à tecnologia derivados desses monopólios. Mais especificamente:

> O uso por estados individuais da predominância tecnológica no espaço global de informações para monopolizar o mercado de tecnologias de informação e comunicação, limitar o acesso de outros estados a tecnologias avançadas de informação e comunicação, bem como para fortalecer sua dependência tecnológica dos estados dominantes no campo da informatização e desigualdade de informações. (FEDERAÇÃO RUSSA, 2021, tradução Google)[144]

Dessa preocupação deriva a necessidade, trazida em documentos russos, da autonomia em sua produção tecnológica. Em sua “Estratégia para Desenvolvimento da Sociedade da Informação 2017 - 2030”, por diversas vezes a Rússia traz a necessidade de produzir sua própria tecnologia. Por exemplo, no ponto 29, letra e), o país traz que um dos elementos para o funcionamento estável da infraestrutura de informação russa reside em "substituir equipamentos, software e base de componentes eletrônicos importados por equivalentes russos, garantir independência tecnológica e de produção e segurança da informação." (FEDERAÇÃO RUSSA, 2017, s.p. tradução GPT4).[145] O ponto 30 dessa mesma política, por sua vez, reforça essa

---

[143] Traduzido do Inglês: “the use of information and communication technologies in the military-political and other spheres for the purpose of undermining (infringing) sovereignty, violating the territorial integrity of states, and carrying out other actions in the global information space that impede the maintenance of international peace, security and stability.”

Original em russo: использование информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности

[144] Traduzido do Inglês: “the use by individual states of technological dominance in the global information space to monopolize the market of information and communication technologies, limit the access of other states to advanced information and communication technologies, as well as to strengthen their technological dependence on the dominant states in the field of informatization and information inequality.”

Original em russo: “использование отдельными государствами технологического доминирования в глобальном информационном пространстве для монополизации рынка информационно- коммуникационных технологий, ограничения доступа других государств к передовым информационно-коммуникационным технологиям, а также для усиления их технологической зависимости от доминирующих в сфере информатизации государств и информационного неравенства”

[145] Traduzido do Inglês: “Replace imported equipment, software, and electronic component base with Russian analogs, ensure technological and production independence and information security”

necessidade ao trazer a necessidade de criação de expertise e equipamentos próprios, que possam ser utilizados por cidadãos e pelo governo.

> É necessário: criar software de sistema e de aplicativos gerais russos, equipamentos de telecomunicações e dispositivos de usuário para uso generalizado por cidadãos, entidades de pequenas, médias e grandes empresas, órgãos estatais e órgãos de autogoverno local, incluindo com base no processamento de big data, tecnologias de nuvem e Internet das coisas (FEDERAÇÃO RUSSA, 2017, s.p.)[146]

Voltando à política de 2021, cabe frisar também a percepção russa da necessidade do desenvolvimento de padrões de tecnologia. A ação é destacada no ponto 11.i, da seção IV (Main directions of implementation of state policy in the field of international information security) no qual é trazido o papel da Rússia em:

> Promovendo os padrões nacionais da Federação Russa no campo da segurança da informação na implementação da cooperação internacional e regional no campo da padronização, promovendo sua adoção como padrões internacionais, regionais e interestaduais. (2021, p.4)[147]

Esse mesmo ponto também é reforçado na Estratégia 2017-2030, onde o país aponta que, a nível internacional, é necessário "integrar os padrões russos no campo das tecnologias de informação e comunicação em padrões internacionais correspondentes, bem como garantir a harmonização dos padrões interestaduais e nacionais nesta área" (2017, ponto 34, f, tradução GPT4).[148] Além disso, a Rússia também frisa outros 5 pontos a serem observados a nível internacional, sendo eles: a) a defesa do direito à soberania estatal para que os Estados determinem suas

---

O documento original em russo pode ser encontrado em: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf.

[146] Traduzido do Inglês: "It is necessary to:Create Russian general-system and application software, telecommunication equipment, and user devices for widespread use by citizens, entities of small, medium, and large businesses, state bodies, and local self-government bodies, including based on big data processing, cloud technologies, and the Internet of things." O documento original em russo pode ser encontrado em: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf.

[147] Traduzido do Inglês: "promoting national standards of the Russian Federation in the field of information security in the implementation of international and regional cooperation in the field of standardization, promoting their adoption as international, regional and interstate standards." Original em russo: продвижение национальных стандартов Российской Федерации в области информационной безопасности при осуществлении международного и регионального сотрудничества в сфере стандартизации, содействие их принятию в качестве международных, региональных и межгосударственных стандартов.

[148] Traduzido do Inglês: "to integrate Russian standards in the field of information and communication technologies into corresponding international standards, as well as to ensure the harmonization of interstate and national standards in this area". O documento original em russo pode ser encontrado em: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf.

políticas informacionais, tecnológicas e econômicas relacionadas à internet; b) trabalhar de forma contrária ao uso da internet para fins militares; c) O desenvolvimento de "*humanitarian significance of the Internet*"; d) o desenvolvimento de regulações para um funcionamento seguro da internet ""incluindo questões de jurisdição e determinação dos sujeitos das relações jurídicas, com base na participação igualitária dos membros da comunidade global na gestão da rede de informações globais e seus recursos"[149] e e) a criação de novos mecanismos de parceria "visando, com a participação de todas as instituições da sociedade, desenvolver um sistema de confiança na Internet, garantindo confidencialidade e segurança pessoal dos usuários, bem como a confidencialidade de suas informações."[150]

Quando se pensa no principal fórum para diálogos sobre o assunto, a Rússia frisa o papel das Nações Unidas em seus documentos e busca se colocar ativamente nesses fóruns. Até o momento, no atual processo do UN OEWG 2021 - 2025, por exemplo, entre os países analisados, a Rússia é o que mais submeteu *Statements* ao longo dos anos. Foram 52 submissões, ao lado de 38 da Austrália, 17 do Reino Unido, 7 da China e 5 dos Estados Unidos. Retomando o documento de *Fundamentals for State Policy*, a ONU aparece como mecanismo de diálogo[151], para "os Estados membros das Nações Unidas devem garantir um processo de negociação democrático, inclusivo e transparente sobre questões de segurança no uso de tecnologias da informação e comunicação." (FEDERAÇÃO RUSSA, 2021, tradução Google)[152], e também como o local para firmar a sua proposta de "*Convention of the United Nations on Ensuring International Information Security*" (FEDERAÇÃO RUSSA

[149] Traduzido do Inglês: "including issues of jurisdiction and determination of subjects of legal relations, based on equal participation of members of the global community in managing the global information network and its resources." O documento original em russo pode ser encontrado em: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf.

[150] Traduzido do Inglês: "aimed with the participation of all institutions of society, to develop a trust system in the Internet, guaranteeing confidentiality and personal safety of users, confidentiality of their information".

[151] A Rússia também cita a importância de diálogos com outras organizações, como Commonwealth of Independent States (CIS), BRICS, Collective Security Treaty Organization (CSTO), Shanghai Cooperation Organization (SCO), Association of Southeast Asian Nations (ASEAN) e G20.

[152] Traduzido do Inglês: "UN member states to ensure a democratic, inclusive and transparent negotiation process on security issues in the use of information and communication technologies" Original em russo: содействие организации под эгидой ООН регулярного институционального диалога с участием всех государств – членов ООН для обеспечения демократического, инклюзивного и транспарентного переговорного процесса по вопросам безопасности в сфере использования информационно-коммуникационных технологий.

et al, 2023), cuja versão mais recente data de maio 15 de 2023, lançada em conjunto com Coreia do Norte, Nicarágua, Belarus e Síria.

Essa convenção, por sua vez, é a tentativa do país de avançar em seu esforço histórico de construir um tratado multilateral voltado para o tema dentro do escopo das Nações Unidas. A proposta reforça os pontos presentes na narrativa russa, como os riscos de uso de tecnologias de informação e comunicação para violar e desestabilizar a soberania e a integridade territorial, social e econômica de Estados e os riscos de monopólio tecnológico e o que isso poderia gerar nos Estados e traz algumas colocações interessantes em relação à atribuição de ataques. Em meio à acusações de ser responsável por ataques cibernéticos, presentes inclusive em documentos oficiais de países como Estados Unidos e Reino Unido, o documento problematiza essa questão e aponta como um risco "fazer acusações infundadas por parte de alguns Estados contra outros Estados de organizar e realizar atos ilícitos com o uso de tecnologias da informação e comunicação, incluindo ataques cibernéticos." (FEDERAÇÃO RUSSA et al, 2023, pág. 2)[153] e reforça essa questão da recomendação de uma norma para tornar esse tipo de acusação inadmissível, assim como sanções derivadas dela:

> 6. inadmissibilidade de acusações infundadas de outros Estados de cometer atos ilícitos com o uso de tecnologias da informação e comunicação, incluindo ataques cibernéticos, em particular, com o objetivo de impor restrições, como sanções e outros meios."[154] (FEDERAÇÃO RUSSA et al, 2023, pág. 2)

A narrativa russa, como um todo, parte de um tom legalista e defensivo no ciberespaço, falando muito em cooperação e em desenvolvimento de mecanismos legais de prevenção de conflitos, em meio a um ambiente em que as tecnologias da informação representam oportunidades, mas também riscos significativos à sua soberania. O país tem posições semelhantes às chinesas no tocante à defesa da soberania e do uso das agências da ONU como principal fórum de debate, onde os Estados são os atores principais, com poder de voto, e os demais atores adquirem um caráter consultivo.

---

[153] Traduzido do Inglês: ""Laying unsubstantiated accusations by some States against other States of organizing and carrying out wrongful acts with the use of information and communications technologies, including computer attacks."

[154] Traduzido do Inglês: "6. inadmissibility of unsubstantiated accusations of other States of committing wrongful acts with the use of information and communications technologies, including computer attacks, in particular, with a view to impose restrictions, such as sanctions and other means."

4.3.2 Como a Rússia percebe os sistemas ciber-físicos?

Olhando para os documentos presentes no UNIDIR, o único que de fato menciona a Internet das Coisas diretamente é a Estratégia 2017-2030. Vejamos no quadro abaixo.

Quadro 10 - Percepção da Rússia acerca de sistemas ciber-físicos
(continua)

Documento	**Ano**	**Como aborda sistemas ciber-físicos/IoT?**
Fundamentals of the state policy of the Russian Federation in the field of international information security (FEDERAÇÃO RUSSA, 2021)	2021	Não aborda diretamente, mas possui um ponto relacionado à padronização no campo da *"information security"* que poderia englobar padronização de IoT, como já citado anteriormente Promovendo os padrões nacionais da Federação Russa no campo da segurança da informação na implementação da cooperação internacional e regional no campo da padronização, promovendo sua adoção como padrões internacionais, regionais e interestaduais. (p.4)[155]
Strategy for the Development of the Russian Federation in the field of international information security 2017 - 2030 (FEDERAÇÃO RUSSA, 2017)	2017	O documento aborda, em seu ponto 4, o conceito de Internet das Coisas como "um conceito de rede computacional que conecta coisas (objetos físicos) equipados com tecnologias de informação embutidas para interação entre si ou com o ambiente externo sem participação humana."[156]

[155] Em inglês: "promoting national standards of the Russian Federation in the field of information security in the implementation of international and regional cooperation in the field of standardization, promoting their adoption as international, regional and interstate standards"
[156] Em inglês: "a computing network concept that connects things (physical objects) equipped with built-in information technologies for interaction with each other or with the external environment without human participation"

Quadro 10 - Percepção da Rússia acerca de sistemas ciber-físicos (continuação)

Documento	Ano	Como aborda sistemas ciber-físicos/IoT?
		Em paralelo a isso, traz um segundo conceito interessante, de “industrial internet”, que está relacionado a conexão da internet com equipamentos industriais: "Um conceito para a construção de infraestruturas de informação e comunicação baseadas na conexão com a rede de informações e telecomunicações 'Internet' (a seguir 'Internet') de dispositivos industriais, equipamentos, sensores, sistemas de controle de processos tecnológicos, bem como a integração desses meios de hardware e software entre si sem a participação humana.”[157] Em seguida, o documento coloca a Internet das Coisas como um dos elementos pelos quais a Rússia está trabalhando infraestruturalmente. "Para evitar a substituição, distorção, bloqueio, exclusão, remoção dos canais de comunicação e outras manipulações da informação, o desenvolvimento da infraestrutura de informação da Federação Russa é realizado [...] c) Ao nível das redes de comunicação (linhas e meios de comunicação, infraestrutura do segmento russo da Internet, redes de comunicação tecnológicas e dedicadas, redes e equipamentos da Internet das coisas” [158] “O documento também menciona a Internet das Coisas dentro de uma narrativa de desenvolvimento de softwares e serviços russos para alimentá-la: Para fornecer software e serviços seguros e tecnologicamente independentes, é necessário: a. a) Criar software geral e de aplicativos russos, equipamentos de telecomunicações e dispositivos de usuário para uso generalizado por cidadãos, entidades de pequenas, médias e grandes empresas, órgãos estatais e órgãos de autogoverno local, incluindo com base em processamento de big data, tecnologias de nuvem e Internet das Coisas.”[159] No ponto 36, letra f, a Internet das Coisas é apontada como um dos principais direcionamentos de desenvolvimento das tecnologias de informação e comunicação russas.

[157] Em inglês: “a concept for building information and communication infrastructures based on connecting to the "Internet" information-telecommunication network (hereafter "Internet") industrial devices, equipment, sensors, control systems of technological processes, as well as the integration of these software and hardware means with each other without human participation” (Tradução GPT 4)
[158] Em inglês: “To prevent substitution, distortion, blocking, deletion, removal from communication channels, and other manipulations of information, the development of the information infrastructure of the Russian Federation is carried out [...] c) At the level of communication networks (lines and means of communication, infrastructure of the Russian segment of the Internet, technological and dedicated communication networks, networks and equipment of the Internet of things).” (Tradução GPT 4)
[159] Em inglês: “To provide safe and technologically independent software and services, it is necessary to: a. a) Create Russian general-system and application software, telecommunication equipment, and user devices for widespread use by citizens, entities of small, medium, and large businesses, state bodies, and local self-government bodies, including based on big data processing, cloud technologies, and the Internet of Things.”

Quadro 10 - Percepção da Rússia acerca de sistemas ciber-físicos (conclusão)

Documento	Ano	Como aborda sistemas ciber-físicos/IoT?
		Por fim, o termo é citado no ponto 41, que fala da relação entre Estado e mercado para formar a nova base de tecnologia do país. "As principais tarefas de aplicação de tecnologias da informação na esfera de interação entre o estado e os negócios, formando uma nova base tecnológica na economia são: i) desenvolvimento de medidas destinadas a introduzir tecnologias da informação russas em organizações russas, incluindo em organizações de serviços comunitários e agrícolas, tecnologias da informação russas, incluindo tecnologias para processamento de grandes volumes de dados, computação em nuvem, a Internet das coisas."[160]

Fonte: Elaborado pelo autor com base em documentos russos.

A separação direta entre Internet das Coisas e Internet Industrial é um ponto interessante do documento, pois pode indicar um caminho diferente em termos de legislação para cada uma das frentes. Em paralelo a isso, as preocupações do país com infraestrutura e desenvolvimento de equipamento próprio dialogam diretamente com suas percepções securitárias em relação aos sistemas de informação como um todo. Na Internet das Coisas, assim como em outras tecnologias, a Rússia quer cada vez mais se garantir autonomamente, num esforço de evitar que situações de dependência externa prejudiquem sua estratégia.

4.3.3 Como o país vem abordando o tema internamente?

A Rússia tem poucos documentos específicos sobre Internet das Coisas. De forma geral, o tema pode ser entendido como englobado dentro de outras leis do país e, de certa forma, fragmentado. Konagina et. al (2023) captam bem essa percepção:

> A Rússia mantém suas posições de liderança em número de sensores e dispositivos de controle. No entanto, seu arcabouço regulatório e legal ainda está insuficientemente preparado para os desafios tecnológicos. O documento chave de definição de metas da Federação Russa no campo da

[160] Em inglês: "41. The main tasks of applying information technologies in the sphere of interaction between the state and business, forming a new technological basis in the economy are: i) development of measures aimed at introducing Russian information technologies in Russian organizations, including in organizations of housing and communal services AND agricultural organizations, Russian information technologies, including technologies for processing large volumes of data, cloud computing, the Internet of things"

> cibersegurança é a Doutrina de Segurança da Informação da Federação Russa, aprovada pelo Decreto do Presidente da Rússia em 5 de dezembro de 2016. A Doutrina define ameaças de informação externas e internas para o indivíduo, sociedade e estado, bem como define as principais medidas para preveni-las (Frolova et al. 2018). Um dos principais atos legislativos da Rússia no campo da cibersegurança é a Lei Federal sobre Segurança da Infraestrutura de Informações Críticas da Federação Russa, que entrou em vigor em 1º de janeiro de 2018 (Duma Estatal 2017). O escopo da Lei se estende a infraestruturas de informação críticas (CII), como finanças e comunicações (Zharova 2019). Alguns aspectos de segurança da IoT também são mencionados nas edições atuais do Código Civil, nas Leis Federais sobre Telecomunicações, sobre Informação, Tecnologias da Informação e Proteção, sobre Dados Pessoais, e em muitos outros atos legislativos dos níveis federal e departamental. Pesquisadores admitem que a regulamentação atual da IoT e cibersegurança na Rússia é de certa forma pontual e fragmentada. (Naumov and Arkhipov 2018). (KONAGINA et. al 2023, p. 261, grifo do autor).[161]

Essa percepção é partilhada por Kupstova (2021) que, ao analisar legislações sobre certificações de proteção ou proibições de software estrangeiro, aponta que:

> É difícil dizer de forma definitiva que esses atos legislativos atendem completamente às especificidades da Internet das Coisas, ao seu propósito e características no contexto do funcionamento dos dispositivos interconectados em rede. Por exemplo, falta uma regulamentação jurídica adequada para carros autônomos, tecnologias vestíveis e outros dispositivos semelhantes. Portanto, nesta questão, é importante considerar não apenas as características, mas também as ameaças à segurança da informação do software da IoT. (KUPSTOVA, 2021, tradução GPT4)[162]

---

[161]Traduzido: “Russia maintains its leading positions in the number of sensors and control devices. However, its regulatory and legal framework is still insufficiently prepared for technological challenges. The key goal-setting document of the Russian Federation in the field of cybersecurity is the Doctrine of Information Security of the Russian Federation, approved by the Decree of the President of Russia on December 5, 2016. The Doctrine defines external and internal information threats to the individual, society, and the state, as well as defines the main measures to prevent them (Frolova et al. 2018). One of Russia’s central legislative acts in the field of cybersecurity is the Federal Law on Security of Critical Russian Federation Information Infrastructure, which entered into force on January 1, 2018 (State Duma 2017). The scope of the Law extends to such critical information infrastructure (CII) as finance and communications (Zharova 2019). Some IoT security aspects are also mentioned in the current editions of the Civil Code, in Federal Laws on Telecommunications, on Information, Information Technologies and Protection, on Personal Data, and many other legislative acts of the federal and departmental levels. Researchers admit that current IoT and cybersecurity regulation in Russia is somehow ad hoc and fragmented.”

[162]Traduzido: “It is difficult to unequivocally say that these legislative acts fully meet the specifics of the Internet of Things, their purpose, and features within the functioning of devices networked together. For example, there is insufficient legal regulation of autonomous vehicles, wearable technologies, and other similar devices. Therefore, in this matter, it is important to consider not only the features but also the threats to the information security of IoT software.”

Texto original: Сложно однозначно сказать о том, что данные законодательные акты в полной мере отвечают специфике Интернета вещей, их предназначению и особенностям в рамках функционирования устройств, объединённых в сеть. Например, отсутствует достаточное правовое регулирование автопилотируемых автомобилей, «носимых технологий» и других подобных устройств. Поэтому в данном вопросе важно учитывать не только особенности, но и угрозы информационной безопасности программного обеспечения IoT. (p.227)

Recentemente, contudo, alguns esforços têm sido direcionados para políticas desse tipo. Um exemplo é a "*Order of the Ministry of Communications of Russia of 31.10.2019 No. 637 "On Approval of the Plan (Roadmap) for the Implementation of the Concept of Building and Development of Narrowband Wireless Communication Networks 'Internet of Things' in the Territory of the Russian Federation*" (Ordem do Ministério das Comunicações da Rússia de 31.10.2019 No. 637 "Sobre a Aprovação do Plano -Mapa de Rota- para a Implementação do Conceito de Construção e Desenvolvimento de Redes de Comunicação Sem Fio de Banda Estreita 'Internet das Coisas' no Território da Federação Russa). Conforme apontado por Kuptsova (2019), o documento é:

> Um passo progressivo na área da Internet das Coisas é a aprovação do Plano de Implementação da concepção de construção e desenvolvimento de redes de comunicação sem fio de banda estreita da "Internet das Coisas" no território da Federação Russa. Este plano define os principais padrões e direções para a implementação das tecnologias da Internet das Coisas, incluindo o desenvolvimento de projetos piloto de "casa inteligente", na área da medicina, agricultura, entre outros. (KUPTSOVA, 2021, tradução GPT4)[163]

Olhando mais atentamente para esse plano, ele possui 6[164] grandes pontos relacionados ao tema de "*narrowband wireless IoT*". Dentre esses pontos, há um esforço de identificação de riscos, e desenvolvimento de padrões. No ponto 3.2.1, por exemplo, fala-se no desenvolvimento e promoção de padrões dentro do campo de *narrowband wireless communication networks,* e na defesa desses padrões na ITU.

---

[163] Texto original. Прогрессивным шагом в области Интернета вещей является утверждение Плана реализации концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории РФ. В данном плане определены основные стандарты и направления реализации технологий Интернета вещей, в т.ч. разработаны пилотные проекты «умного дома», в области медицины, сельского хозяйства и др.
Traduzido do Inglês: "A progressive step in the field of the Internet of Things is the approval of the Plan for the implementation of the concept of building and developing narrowband wireless communication networks "Internet of Things" in the territory of the Russian Federation. This plan defines the main standards and directions for implementing Internet of Things technologies, including the development of pilot projects in "smart home", healthcare, agriculture, and more."

[164] 1. Approval of threat models and violators for various systems of narrowband wireless communication networks "Internet of Things"; 2. Conducting pilot projects for the deployment of various identification systems for "Internet of Things" devices; 3. International and national standardization in the field of narrowband wireless communication networks "Internet of Things"; 4. Regulatory and legal support for the construction and development of narrowband wireless communication networks "Internet of Things" on the territory of the Russian Federation. 5. Radio frequency support for narrowband wireless communication networks "Internet of Things"; 6. Development of industry sections of the Concept for the construction and development of narrowband wireless communication networks "Internet of Things" on the territory of the Russian Federation (Tradução GPT4).
Original disponível em: https://digital.gov.ru/ru/documents/7046/. Acesso em 01 de jan. de 2024.

Seria de responsabilidade do Ministério de Desenvolvimento Digital, Comunicações e Mídia de Massas da Rússia[165] a: “Promoção na União Internacional de Telecomunicações e na Comunidade Regional de Comunicação de padrões (recomendações) e outros documentos sobre os temas dos padrões nacionais em desenvolvimento”[166] (FEDERAÇÃO RUSSA, 2019, p.8, tradução GPT4). Da mesma forma, no ponto 3.2.2 é previsto um esforço da Rosstandart para promover esses mesmos padrões em organizações de definições de padrões internacionais. Ela deveria atuar para “Promoção e aceitação de propostas da Federação Russa em padrões internacionais e regionais da ISO, IEC e seus comitês técnicos conjuntos sobre os temas dos padrões nacionais em desenvolvimento”[167] (FEDERAÇÃO RUSSA, 2019, p.8, tradução GPT4). Há também uma preocupação no desenvolvimento de regulações para o tema no país, previstas no ponto 4. Os principais atores com responsabilidades dentro desse documento são os dois aqui mencionados (Ministério de Desenvolvimento Digital, Comunicações e Mídia de Massas e Rosstandart).

Olhando para um aspecto mais securitário, a Rússia vem mapeando e se preparando para ameaças. Conforme apontado por Anna e Vladimir (2021), a segurança da Internet das Coisas no país é de responsabilidade do *Federal Service for Technical and Export Control* (FSTEC) da Rússia, em cooperação com agências governamentais e companhias de cibersegurança no país. Dentro disso, a organização vem mapeando e lidando com riscos.

> Dentro do contexto do IoT, o FSTEC identificou uma série de ameaças específicas para o funcionamento de dispositivos interconectados embarcados: roubo e uso de informações confidenciais e credenciais de usuários, ransomware e ataques de ransomware, instalação de firmware não autorizado, acesso remoto e ataques via dispositivos móveis, interceptação de dados, ataques de homem no meio e exploração de vulnerabilidades em aplicativos. (ANNA, VLADIMIR, 2021, p. 4546)[168]

[165] Original em russo: Минкомсвязь России

[166] Original em russo: “Продвижение в Международном союзе электросвязи и Региональном содружестве в сфере связи стандартов (рекомендаций) и других документов по тематикам разрабатываемых национальных стандартов”

[167] Original em russo: “Продвижение и принятие предложений Российской Федерации в международных и региональных стандартах Международной организации по стандартизации (ИСО), Международной электротехнической комиссии (МЭК) и их совместных технических комитетах по тематикам разрабатываемых 9 национальных стандартов”

[168] Traduzido em Inglês: “Within the framework of the IoT, FSTEC has been identified a number of specific threats to the functioning of embedded interconnected devices: theft and use of confidential information and user credentials, ransomware and ransomware attacks, installation of unauthorized

Anna e Vladimir (2021) também ressaltam um esforço russo de se envolver no desenvolvimento de padrões de segurança de IoT, assim como o de trabalhar para desenvolver tecnologia própria domesticamente. Para eles:

> Uma ameaça característica à segurança do IoT na Rússia é o uso de tecnologias, grande parte das quais pertence a desenvolvedores estrangeiros. Na Federação Russa, a segurança da informação é garantida pelo desenvolvimento de software e padrões domésticos. (ANNA, VLADIMIR, 2021, p. 4548).[169]

Nessa linha de desenvolvimento de padrões, é importante destacar a existência do Technical Committee 194 "Cyber-physical systems"[170]. Também conhecido como *Cyber-physical systems committee of Rosstandart*, o Comitê foi criado em 2017 e também conta com a presença da Russian Venture Company (RVC). Focado em tecnologias-chave para a Rússia, como *"smart manufacturing", "smart energy", "smart cities", "big data",* inteligência artificial e internet das coisas, o comitê vem trabalhando no desenvolvimento de padrões nacionais para Internet das Coisas, tendo, inclusive, apresentado alguns deles para debate público em 2020. (TADVISER, 2024)[171]

Por fim, é preciso entender que o Estado russo vem exercendo um papel importante no desenvolvimento da IoT como um todo. Pankov (2019), com base em fala do então economista chefe do banco mundial, aponta o Estado como motor de desenvolvimento para as tecnologias digitais na Rússia, puxando o setor privado. Da mesma forma, a PWC (2017) vê o Estado apostando nessa tecnologia para áreas estratégicas.

> O governo da Federação Russa está desenvolvendo medidas para a implementação do IoT no complexo agroindustrial. Na saúde, é necessário tanto realizar a subsidiação quanto estimular investimentos privados. O Estado está interessado em reduzir os custos com saúde através do aumento da eficiência das instituições médicas e da implementação da telemedicina. A introdução de tecnologias IoT abre novas oportunidades na área de prestação de serviços públicos à população. As grandes cidades têm o maior

---

firmware, remote access and attacks via mobile devices, data interception, man-in-the-middle attacks, and exploitation of vulnerabilities in applications."

[169] Traduzido em Inglês: "[...] a characteristic threat to IoT security in Russia is the use of technologies, a significant part of which belongs to foreign developers. In the Russian Federation, information security is ensured by the development of domestic software and standards."

[170] Documento disponível em: https://tc194.ru/. Acesso em: 01 jan. 2024.

[171] Ver os padrões apresentados em: https://tadviser.com/index.php/Company:Technical_Committee_of_Cyber-Physical_Systems_(TC_194)#Presentation_of_a_series_of_national_standards_for_public_discussion_IoT.

> potencial para a implementação de tecnologias IoT, como, por exemplo, "sistemas inteligentes de monitoramento" do transporte público, estacionamento, gestão da iluminação de ruas e entradas de prédios, aquecimento, coleta e separação de lixo, telemedicina. O Estado pode realizar projetos piloto e, em seguida, replicar a experiência bem-sucedida em todo o país ou em regiões específicas. (PWC, 2017, p. 52)[172]

Os mesmos autores, contudo, também apontam as dificuldades para o Estado em seguir esse modelo, que pede por investimentos, muitas vezes incertos, em meio a uma infraestrutura frequentemente antiga e desgastada. É justamente esse poderio de investimento e domínio tecnológico que foi apontado por Segal (2016) como limitante para que a Rússia seja considerada uma superpotência. Podemos trazer essa mesma reflexão para o campo da IoT. Diante de dificuldades de investimento que já existem, cabe observar como a Rússia se portará em relação ao tema nos próximos anos, dado o seu cenário de guerra com a Ucrânia que, querendo ou não, consome um grande volume de recursos.

4.4 CHINA

4.4.1 Como a China percebe a governança do ciberespaço?

Conforme mencionado, a China historicamente tem tido um posicionamento favorável a uma governança baseada no multilateralismo, com as principais discussões acontecendo no âmbito das Nações Unidas e, mais especificamente, na ITU (União Internacional das Telecomunicações) (PIJOVÍC, 2021). Esse posicionamento, assim como a defesa do conceito de soberania cibernética, aproxima o país da Rússia em suas colocações sobre esses temas. Recentemente, em comunicado conjunto lançado em 4 de fevereiro de 2022 os dois países reforçaram sua proximidade nos posicionamentos, afirmando querer falar em uma só voz no âmbito do UN OEWG e fortalecer seus laços de cooperação. O comunicado aponta que:

---

[172] Original em russo: Правительство РФ прорабатывает мероприятия по внедрению IoT в агропромышленный комплекс. В здравоохранении необходимо как осуществлять субсидирование, так и стимулировать частные инвестиции. Государство заинтересовано в снижении затрат на здравоохранение за счет повышения эффективности медицинских учреждений и внедрении телемедицины. Внедрение технологий IoT открывает новые возможности в сфере оказания государственных услуг населению. У крупных городов есть наибольший потенциал для внедрения технологий IoT, например «умных систем отслеживания» общественного транспорта, паркинга, управления освещением улиц и подъездов, отоплением, вывозом и сортировкой мусора, телемедицины. Государство может реализовать пилотные проекты и затем тиражировать успешный опыт в масштабах страны или отдельных регионов.

> A Rússia e a China reafirmam o papel-chave da ONU em responder às ameaças à segurança internacional da informação e expressam seu apoio à Organização no desenvolvimento de novas normas de conduta dos Estados nessa área. As partes apoiam a internacionalização da governança da Internet, defendem direitos iguais na sua governança, acreditam que quaisquer tentativas de limitar seu direito soberano de regular os segmentos nacionais da Internet e garantir sua segurança são inaceitáveis, e estão interessadas em uma maior participação da União Internacional de Telecomunicações na abordagem dessas questões. (FEDERAÇÃO RUSSA, CHINA, 2022)[173]

É mencionada ainda a recente Global Data Security Initiative chinesa, estabelecida para definir princípios para a segurança de dados a nível internacional que, a princípio, também conta com apoio russo. Diante disso, para adentrar elementos mais específicos do posicionamento chinês, vejamos a Global Data Security Initiative (GDSI)[174], assim como as menções à governança cibernética nos documentos mais recentes do país.

Lançada em 2020 (e com última atualização datada de 2024), a GDSI faz parte de um esforço de projeção chinês. O país tenta se colocar como um parceiro confiável globalmente, em meio às disputas pela preponderância no fornecimento de novas tecnologias que movimentam grandes quantidades de dados, como o 5G, e à preocupações acerca de vigilância de outros países por parte da tecnologia chinesa (MERICS, 2020). Diante disso, após lançada, a iniciativa vem sendo propagada em diferentes fóruns internacionais, como o IGF, a ASEAN, o G20, BRICS, a Organização de Cooperação de Shangai, entre outros, e já conta com o apoio e já conta com o apoio dos países da ASEAN e da Liga Árabe, além de Equador, Tanzânia, Paquistão e Rússia. (DIGICHINA, 2022a).

O documento em si é bem curto e estabelece 8 pontos, sendo eles: 1. Os países devem trabalhar a governança de dados baseada em fatos, e garantir a

---

[173] Traduzido em Inglês: Russia and China reaffirm the key role of the UN in responding to threats to international information security and express their support for the Organization in developing new norms of conduct of states in this area. [...] The sides support the internationalization of Internet governance, advocate equal rights to its governance, believe that any attempts to limit their sovereign right to regulate national segments of the Internet and ensure their security are unacceptable, are interested in greater participation of the International Telecommunication Union in addressing these issues.

[174] Nome em mandarim: 全球数据安全倡议. Disponível em: https://www.mfa.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/zclc_674645/qt_674659/202010/t20201029_7669146.shtml. Acesso em: 01 jan. 2024.

segurança e estabilidade das cadeias de suprimento globais; 2. Os países não devem usar tecnologias de informação para destruir infraestrutura, roubar dados ou ter comportamentos que prejudiquem a segurança e interesses nacionais de outros países; 3. Estabelece uma oposição ao uso de tecnologias da informação para violar informações pessoais e estabelecer vigilância em larga escala sob cidadãos de outros países; 4. Traz que as empresas devem se adequar à legislação dos países em que estão localizadas, e não devem armazenar dentro do país dados gerados e obtidos no exterior; 5. Frisa o respeito à soberania, jurisdição e segurança de dados dos países, trazendo que não se pode acessar dados em outros países sem a permissão dos mesmos; 6. Aponta que, em caso de necessidade de obtenção de dados transfronteiriços para fins de aplicação da lei, a soberania judicial e segurança dos dados dos países deve ser respeitada. Dessa forma, as questões devem ser resolvidas por meio de canais de assistência judicial ou acordos bilaterais ou multilaterais; 7. Foca nas empresas, apontando que elas não devem estabelecer *backdoors* em seus produtos, que permitam obtenção ilegal de dados ou controle e manipulação de sistemas e equipamentos do usuário; e, por fim, 8. Frisa a necessidade de os fornecedores apontarem falhas e vulnerabilidades de segurança dos produtos, quando essas forem encontradas, e também que estes não devem usar a dependência dos usuários para buscar ganhos ilegítimos (MINISTÉRIO DE RELAÇÕES EXTERIORES DA CHINA, 2024, baseado em tradução Google).

Em paralelo ao seu esforço de dados, o país também lançou em 2023 um documento intitulado "*China 's position on Global Digital Governance*", que dialoga com elementos trazidos em outros posicionamentos chineses, como o "*China's position on international rules making in cyberespace*". O documento, que possui versão oficial em inglês[175], conta com quatro princípios e sete propostas, tem um *timing* interessante quando consideramos o lançamento da Declaração pelo Futuro da Internet, encabeçada pelos Estados Unidos no ano anterior. Embora sem menções diretas, podemos perceber as indiretas do jogo político logo no primeiro parágrafo da declaração, que aponta que "Um certo país politizou a ciência e tecnologia, bem como questões econômicas e comerciais, e as usou como arma e ferramenta para dividir a Internet global, colocando em risco o desenvolvimento e a cooperação digitais

[175]Versão em inglês do Chinas position on Global Digital Governance". Disponível em: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202305/t20230525_11083607.html. Acesso em: 01 de jan. de 2024.

globais."[176] Esse ponto é reforçado no primeiro princípio, que pede por unidade e cooperação no ciberespaço. Ali a China deixa clara a percepção de que existe uma disputa política clara em curso e que envolve aspectos econômicos, de mercados, padrões e cadeias de suprimento no âmbito digital.

> Conforme o Secretário-Geral da ONU nos alertou de forma semelhante, dois mercados, dois conjuntos de padrões e duas cadeias de suprimentos também estão surgindo no domínio cibernético e digital. Traçar linhas ideológicas ou instigar políticas de grupo e confrontos de blocos só criará obstáculos no caminho do desenvolvimento global e do progresso humano. (MINISTÉRIO DAS RELAÇÕES EXTERIORES DA CHINA, 2023)[177]

O princípio seguinte foca na digitalização econômica voltada ao desenvolvimento. Ali, a China frisa a importância da cooperação e pede que seja respeitada a soberania dos Estados para escolher seus próprios caminhos de desenvolvimento, com base em suas condições nacionais. Embora não mencionado diretamente, também podemos subentender que esse tipo de colocação é estratégica para a China em meio ao seu esforço de parcerias econômicas e políticas dentro da sua *Belt and Road Initiative*. Conforme apontado pela The Economist (2020), o lado digital da iniciativa vem crescendo ao longo dos últimos anos e, mais do que simplesmente um esforço por emplacar sua tecnologia, envolve o estabelecimento de normas e padrões que beneficiam a China na disputa envolvendo a preponderância em relação às novas tecnologias:

> Para a China, não se trata apenas de promover líderes mundiais em alta tecnologia. O país também deseja incentivar a adoção mais ampla de normas e padrões cibernéticos desenvolvidos internamente. Por exemplo, marcas de fintech como WeChat Pay e Alipay podem ajudar a internacionalizar o yuan e estabelecer infraestrutura de pagamentos transfronteiriços para competir com o sistema liderado pelos americanos, o swift, que atualmente domina. Cabos submarinos e computação em nuvem podem fornecer dados de usuários em todo o mundo, impulsionando os esforços da China para superar os Estados Unidos em inteligência artificial. (THE ECONOMIST, 2020)[178]

---

[176] Traduzido Inglês: "certain country has politicized science and technology as well as economic and trade issues, and used them as a weapon and tool to divide the global Internet, jeopardizing global digital development and cooperation."

[177] Traduzido Inglês: As the UN Secretary-General has warned us in a similar way, two markets, two sets of standards and two supply chains are also emerging in the cyber and digital domain. Drawing ideological lines or instigating group politics and bloc confrontation will only set obstacles in the way of global development and human progress.

[178] Traduzido Inglês: For China, it is not just a question of fostering world-beaters in high-tech. It also wants to encourage the wider adoption of homegrown cyber norms and standards. For instance, fintech brands like WeChat Pay and Alipay can help to internationalise the yuan and establish cross-

O terceiro princípio dialoga com promoção da imparcialidade e justiça e mostra preocupações com medidas coercitivas e monopólio tecnológico. É um princípio estratégico em meio ao banimento de companhias chinesas, realizado por países como Estados Unidos, Reino Unido, Suécia e França (PODER360, 2022). A China aponta que:

> Os Estados devem promover a cooperação e assistência internacionais, opor-se ao monopólio tecnológico e às medidas coercitivas unilaterais, manter uma cadeia de suprimentos aberta, segura e estável de produtos e serviços digitais globais, e tornar o desenvolvimento digital global mais equitativo, eficaz e benéfico para todos. Os Estados devem fazer esforços para enfrentar os desafios impostos pela economia digital aos grupos vulneráveis, garantindo que pessoas de todos os segmentos da sociedade possam compartilhar os benefícios e dividendos do desenvolvimento digital em igualdade de condições.[179]

Por fim, o quarto princípio, diante dos desafios levantados pelos anteriores, reforça o multilateralismo no âmbito das Nações Unidas enquanto caminho para estabelecer as regras de governança, com destaque para a atuação dos Estados Nacionais. Os demais atores teriam atuação relevante, mas limitada aos seus papéis, sem o voto nas decisões finais.

> Os Estados devem formular regras internacionais por meio da ampla participação e consulta entre todos os Estados membros sob os auspícios da ONU, trabalhar juntos para construir um sistema de governança da Internet internacional caracterizado pelo multilateralismo, democracia e transparência, e garantir a distribuição equitativa e gestão conjunta dos recursos básicos da Internet. Organizações internacionais, empresas de TIC, comunidades tecnológicas, organizações civis e outros interessados podem desempenhar seu papel de acordo com suas funções e responsabilidades.[180]

---

border payments infrastructure to compete with swift, the American-led system which currently dominates. Undersea cables and cloud computing could provide user data around the world, boosting China's efforts to surpass America in artificial intelligence.

[179] Traduzido do Inglês: States should promote international cooperation and assistance, stand against technological monopoly and unilateral coercive measures, maintain an open, secure and stable supply chain of global digital products and services, and make global digital development more equitable and effective and beneficial to all. States should make efforts to address the challenges posed by digital economy to vulnerable groups, ensuring that people from all walks of life can share the benefits and dividends of digital development on an equal footing.

[180] Traduzido do Inglês: States should formulate international rules through wide participation and extensive consultation among all Member States under the auspices of the UN, work together to build an international Internet governance system featuring multilateralism, democracy and transparency, and ensure equitable distribution and joint management of basic Internet resources. International organizations, ICT companies, technology communities, civil organizations and other stakeholders can play their part commensurate with their roles and responsibilities.

Esses princípios são frisados novamente nas propostas. O quadro abaixo resume os principais pontos levantados em cada uma das sete. Cabe destacar o ponto 4, no qual a China busca a defesa dos direitos humanos adequada à sua narrativa, colocando o direito ao desenvolvimento como essencial, e ressaltando o papel do Estado de moderar a rede para garantir a ordem pública e os direitos dos indivíduos. Assim, um ponto geralmente usado para atacá-la se torna um elemento estratégico de sua narrativa. Também é interessante como a questão dos padrões tecnológicos aparece no ponto 2, numa narrativa de evitar fragmentação na internet e é reforçada em outros pontos, como o da inteligência artificial. O "direito ao desenvolvimento" também é bastante reforçado e está bem presente na narrativa chinesa. No "*China's Positions on International Rules-making in Cyberspace*", de 2021, esse ponto já era frisado, com o adendo de que sanções e bloqueios são um obstáculo a esse direito, ponto que é novamente reforçado em 2023.

> O sistema atual de distribuição e gestão dos recursos críticos da Internet é desequilibrado e injusto. O desenvolvimento desigual e a crescente divisão digital entre países e regiões são evidentes. Certos Estados politizam questões de tecnologia e cibersegurança, suprimindo deliberadamente empresas de TIC de outros Estados e impondo barreiras injustas e injustas à cadeia de suprimentos e comércio global de TIC, prejudicando o desenvolvimento e a cooperação globais. (MINISTÉRIO DE RELAÇÕES EXTERIORES DA CHINA, 2021)[181]

Quadro 11 - Propostas da China para a governança global digital (continua)

Proposta	**Principais elementos**
1. Conectar todas as pessoas à internet	Esse ponto dialoga diretamente com a narrativa de direito ao desenvolvimento, com as tecnologias digitais como meio para isso. A China traz que os Estados devem: • Promover acesso justo, razoável e universal à Internet, popularizar tecnologia e diversidade linguística online, e garantir que todos compartilhem os benefícios do desenvolvimento digital, mantendo a segurança, estabilidade e conectividade da Internet global sem prejudicar o direito dos Estados.

[181] Traduzido do Inglês: The current distribution and management system of critical Internet resources is imbalanced and unjust. The unbalanced development and widening digital divide among countries and regions are prominent. Certain States politicize technology and cybersecurity issues, willfully suppress other States' ICT enterprises and impose unfair and unjust barriers on global ICT supply chain and trade, jeopardizing global development and cooperation.

Quadro 11 - Propostas da China para a governança global digital (continuação)

Proposta	**Principais Elementos**
	Fortalecer a capacitação digital, assegurar o direito dos países em desenvolvimento ao uso pacífico de recursos e tecnologias da Internet, e apoiar esses países com assistência, incluindo financiamento e treinamento, visando acesso acessível à Internet e promover inclusão digital para grupos vulneráveis, além de incentivar trocas de conhecimento e políticas de desenvolvimento para apoiar a implementação da Agenda 2030.
2. Evitar a fragmentação da internet	Como mencionado, esse ponto reforça o elemento da padronização, e também a narrativa de multilateralismo chinesa • Os Estados devem se opor a divisões e fragmentações na internet; • Os Estados devem formular regras e padrões comuns e interoperáveis no ciberespaço, com participação ampla de Estados, dentro da ONU, mantendo seu compromisso com multilateralismo, democracia e transparência; • Os Estados devem evitar usar a narrativa de segurança nacional para promover bloqueios nas cadeias de suprimento, e apoiar com que as empresas façam suas próprias escolhas, de forma independente.
3. Proteção de dados	Nesse ponto, a China reforça os elementos de sua DGSI. • Os Estados devem, de forma objetiva e baseada em evidências, garantir a livre circulação de dados, de forma ordenada e de acordo com a lei. • Os Estados devem se opor ao uso de ICTs para roubo de dados de outros Estados, assim como conduzir atividades que afetem interesses nacionais e interesses públicos. • Os Estados devem respeitar a soberania, jurisdição e governança de dados de outros Estados e não obter dados de outros Estados sem permissão, se utilizando de acordos bilaterais ou multilaterais quando for necessário obter dados para fins de aplicação da lei, mas entendendo que acordos bilaterais não podem ferir a soberania de dados de um terceiro Estado. • Os fornecedores de ICTs não devem instalar backdoors para obter dados e vantagens de forma ilegal, e devem informar quando encontrarem vulnerabilidades.

Quadro 11 - Propostas da China para a governança global digital (continuação)

Proposta	**Principais Elementos**
4. Aplicação de direitos humanos online	Nesse ponto, a China constrói uma narrativa estratégica relacionada aos Direitos Humanos. • Defendem o direito ao desenvolvimento como o direito humano básico e primário. Diante disso, os Estados devem estabelecer medidas para facilitar a inovação digital e se opor à medidas coercitivas unilaterais, que diminuem as capacidades de desenvolvimento econômico e a melhora na qualidade de vida das pessoas e constituem uma violação dos Direitos Humanos • Os Estados devem evitar politizar a questão dos direitos humanos ou interferir em assuntos domésticos de outros Estados sob a justificativa de proteção de direitos humanos online • Os Estados devem respeitar os direitos e liberdades de seus cidadãos no ciberespaço, mas também são responsáveis por proteger e regular a transmissão de informações na internet, de forma a prevenir violações de direitos e prejudicar a ordem pública, incitar violência, discriminação e intolerância, ou ameaçar a segurança nacional.
5. Introduzir critérios de responsabilização por conteúdo discriminatório e enganoso	Esse ponto dialoga na relação entre empresas privadas de tecnologia. Traz que: • Os Estados devem adotar medidas apropriadas, incluindo a formulação e aprimoramento do arcabouço legal e regulatório, incentivando organizações de TIC a adotar autodisciplina e códigos de conduta, e aumentar a regulação e supervisão de empresas de TIC para prevenir atos ilícitos na Internet, como ameaças à segurança nacional, incitação à subversão, terrorismo, ódio racial e discriminação, além de violações à reputação, privacidade e direitos de propriedade intelectual. • Devem também incentivar empresas de TIC a estabelecer ou melhorar sistemas para tratar queixas e denúncias do público e proteger os direitos dos consumidores, com as empresas tomando a iniciativa de aceitar supervisão pública, responder a queixas e denúncias de forma tempestiva e oferecer compensação aos usuários por violações de seus direitos e interesses conforme a lei.

Quadro 11 - Propostas da China para a governança global digital (continuação)

Proposta	**Principais Elementos**
6. Promover a regulação da inteligência artificial	Aqui, a China estabelece preocupação com o surgimento da inteligência artificial e desde já pede por cuidados para seu desenvolvimento. Esse é o maior ponto do documento. Os Estados devem: • Promover a criação de um quadro e padrões para a governança internacional da IA assegurando que a IA seja segura, confiável e contribua para o desenvolvimento sustentável global, mantendo uma abordagem centrada nas pessoas e garantindo o direito ao desenvolvimento e uso pacífico das tecnologias por todos os países. • Priorizar a ética na IA estabelecer normas e mecanismos de responsabilização, e adaptar mecanismos de revisão e regulação ética às condições nacionais, melhorando a gestão de segurança e risco da IA. • Exigir que entidades de P&D fortaleçam a autodisciplina, controlem o uso prematuro de tecnologias, garantam a segurança e a controlabilidade dos algoritmos, e busquem a qualidade dos dados, considerando as demandas diversificadas para alcançar a universalidade, justiça e não discriminação dos sistemas de IA. • Proibir o uso de tecnologias de IA que contrariem leis e éticas, fortalecer a monitoração da qualidade e avaliações de produtos e serviços de IA promover treinamento em ética de IA proteger a privacidade individual e a segurança dos dados, e opor-se à coleta e utilização ilegais de informações pessoais.

Quadro 11 - Propostas da China para a governança global digital (conclusão)

Proposta	Principais Elementos
7. Bens públicos digitais	Novamente é reforçado o papel público do ambiente digital, e seu potencial para contribuir aos ODS. • O princípio da soberania nacional deve ser aplicado ao domínio digital e cibernético. Ou seja, os Estados têm jurisdição sobre ICTs, infraestruturas e dados dentro de seu território e o direito de estabelecer políticas públicas e leis dentro desse espaço que dialoguem com seus interesses e os interesses de suas organizações, empresas e cidadãos. • Aumentar a abertura para produtos digitais dialoga com o potencial que eles possuem de contribuir para o avanço dos Objetivos de Desenvolvimento Sustentável. • Respeitado esse princípio, assim como a segurança de dados, direitos legítimos e interesses dos cidadãos de outros Estados e seguindo o princípio do voluntarismo, os Estados podem discutir e construir gradualmente um consenso sobre os padrões, escopo, maneira de gestão e diretrizes para o uso de bens públicos digitais. • Os Estados devem garantir a digitalização de serviços públicos e fortalecer a cooperação em áreas como educação online, assim como na troca de dados para monitoramento e avaliação dos ODS.

Fonte: Elaborado pelo autor, com base em Ministério das Relações Exteriores da China (2023)

Dado esse contexto mais geral, vejamos como os sistemas ciber-físicos se encaixam dentro dele.

4.4.2 Como a China percebe os sistemas ciber-físicos?

> A sociedade humana já entrou em uma era digital sem precedentes. O rápido desenvolvimento de novas tecnologias, como computação em nuvem, Internet das Coisas, blockchain e inteligência artificial, impulsionou poderosamente o desenvolvimento econômico e social. O ciberespaço está profundamente integrado ao mundo real, e a extensão, profundidade e complexidade da dependência dos países no ciberespaço são sem precedentes. (CHINA, 2021, em *statement no OEWG)*[182]

[182] Em Inglês: “Human society has already entered an unprecedented digital era. The rapid development of new technologies such as cloud computing, the Internet of Things, blockchain, and

No caso Chinês, os documentos presentes no UNIDIR[183] relacionados à segurança cibernética não abordam diretamente o tema. Contudo, isso não significa uma ausência de preocupação chinesa no tocante à Internet das Coisas. Pelo contrário, o país tem uma série de documentos e políticas que dialogam com os sistemas ciber-físicos, entre aspectos econômicos e securitários. O quadro abaixo traz alguns deles, mas está longe de ser exaustiva. Um aprofundamento nesses documentos esbarra na barreira do idioma e também no fato de muitos links para documentos mais antigos do governo chinês se encontrarem, atualmente, fora do ar.

Quadro 12 - Percepção da China acerca de sistemas ciber-físicos (continua)

Documento	**Ano**	**Como aborda sistemas ciber-físicos/IoT?**
The Central Committee of the Communist Party of China and the State Council issued the "Overall Layout Plan for the Construction of “Digital China" (CHINA, 2023a)	2023	O documento menciona a Internet das Coisas dentro de um campo infraestrutural, de bases sólidas que a China precisa alcançar para se tornar a “Digital China” buscada. “O ‘Plano’ destaca a necessidade de estabelecer uma base sólida para a construção da China Digital. O primeiro passo é abrir a principal artéria da infraestrutura digital. Acelerar a construção colaborativa de redes 5G e redes ópticas gigabit, promover ainda mais o amplo desdobramento e aplicação do IPv6, promover o desenvolvimento abrangente da Internet das Coisas móvel e promover vigorosamente a aplicação em larga escala doBeidou”.[184] (s.p. Tradução GPT)

artificial intelligence has powerfully propelled the economic and social development. Cyberspace is deeply integrated with the real world, and the breadth, depth, and complexity of countries' dependence on cyberspace are unprecedented.”
Original em mandarim: 人类社**会**已经进入了前所未有的**数**字时代。云计算、物联网、**区**块链、人工智能等新技术快速发展，有力推动经济社**会**发展。**网**络空间与现实世界深度融合，各**国**对网络依赖的广度、深度和**复**杂程度前所未有，**网**络空间已成为你中有我、我中有**你**的命**运**共同体。**与**此同时，我们面临 越**来**越多的新风险和挑战

[183] National Cyberspace Security Strategy (2016); Global Initiative on Data Security (2020); China’s Military Strategy (2015); International Strategy of Cooperation on Cyberspace (2017); Cybersecurity Law (2017).

[184] Em inglês: “The "Plan" points out that it is necessary to lay a solid foundation for the construction of Digital China. The first is to open up the main artery of digital infrastructure. Accelerate the collaborative construction of 5G networks and gigabit optical networks, further promote the large-scale deployment and application of IPv6, promote the comprehensive development of the mobile Internet of Things, and vigorously promote the large-scale application of Beidou.”
Original em mandarim: 《规划》指出，要夯实数字中国建设基础。一是打通数字基础设施大动脉。加快5G**网**络与千兆光网协同建设，深入推进IPv6规模部署和应用，推进移动物联网全面发展，大力推进北 斗规模应用。

Quadro 12 - Percepção da China acerca de sistemas ciber-físicos (continuação)

Documento	Ano	Como aborda sistemas ciber-físicos/IoT?
China's Law-Based Cyberspace Governance in the New Era (CHINA, 2023b)	2023	Aqui a Internet das Coisas é usada para destacar o volume que a China representa no campo. O termo aparece em meio a uma narrativa de transformação em larga escala. "Uma garantia da transformação da escala para a força. A China está fortalecendo sua posição no ciberespaço por meio destes objetivos: infraestrutura de rede universalmente disponível, capacidade significativamente maior de inovação independente, desenvolvimento abrangente da economia digital, garantia de cibersegurança e capacidade equilibrada de ataques cibernéticos e defesa. Progressos significativos foram alcançados na China em direção a esses objetivos, como evidenciado pelo maior número de usuários da Internet do mundo, as redes de banda larga de fibra óptica e de telefonia móvel mais avançadas e maiores do mundo, e a liderança mundial em tecnologia, indústria e aplicações 5G. A Internet das Coisas (IoT) da China agora conecta mais terminais celulares do que usuários de telefones celulares".[185] (s.p, Tradução oficial, grifo do autor). O documento também traz destaque em esforços de proteção de dados para frentes relacionadas à IoT, como internet industrial e de veículos. "Na área de dados da internet, por meio de sistemas de monitoramento e gestão específica por categoria em todos os níveis, aumentou-se a capacidade de proteger e supervisionar a segurança dos dados, e fortaleceu-se a aplicação da lei sobre a segurança dos dados envolvendo a Internet Industrial, Internet dos Veículos e aplicações 5G*". (s.p., tradução oficial)*[186]
14th Five-Year Plan for National Informatization (DIGICHINA, 2022b)	2021	Focado especificamente em informatização, esse plano foi lançado ao final de 2021 e traz uma série de menções à Internet das Coisas. Partindo da tradução fornecida pelo Digital China, temos uma série de menções relacionadas a IoT. A primeira delas está na seção 3, de Objetivos de Desenvolvimento. O primeiro dos objetivos traz que o sistema de infraestrutura digital chinês deve ser mais completo. Dentro disso, novas tecnologias precisam ser popularizadas, como IPv6, o 5G, Internet Industrial, Internet de Veículos, entre outros. Haverá um esforço para que as tecnologias chinesas alcancem níveis mais avançados: "As capacidades da infraestrutura digital da China, incluindo 5G, Internet das Coisas, computação em nuvem e Internet Industrial, devem atingir níveis globalmente avançados". (p.12)[187]

[185] Em inglês: "A guarantee of the transformation from scale to strength. China is building up its strength in cyberspace through these goals: universally available network infrastructure, significantly greater capacity of independent innovation, comprehensive development of the digital economy, guarantee of cybersecurity, and balanced ability of cyber attacks and defense. Major progress has been made in China towards these goals, as evidenced by the world's largest number of netizens, the largest most advanced fiber-optic broadband and mobile telecommunication networks, and world-leading 5G technology, industry and applications. China's Internet of Things (IoT) now connects more cellular terminals than mobile phone users."

[186] Em inglês: "in the area of internet data, thro monitoring systems and category-specific management at all levels, it has increased the ability to protect and oversee data security, and strengthened law enforcement on data security involving the Industrial Internet, Internet of Vehicles, and 5G applications".

[187] Em inglês: "The capabilities of China's digital infrastructure, including 5G, Internet of Things, cloud computing, and Industrial Internet should reach globally advanced levels".

Quadro 12 - Percepção da China acerca de sistemas ciber-físicos (continuação)

Documento	Ano	Como aborda sistemas ciber-físicos/IoT?
		A menção seguinte aparece na seção “Major Tasks and Focus Projects”, na qual há um enfoque em promover infraestrutura para IoT nos próximos anos. Fala-se em “Promover a incorporação da IoT industrial no planejamento da construção da infraestrutura pública; acelerar a formulação de especificações de plataforma unificadas entre departamentos, fabricantes e indústrias. Coordenar a construção de uma nova rede privada de IoT metropolitana integrando IoT, interligação de dados e interligações inteligentes, acelerar o desenvolvimento colaborativo de 5G e IoT, e melhorar o compartilhamento de recursos e o nível de utilização abrangente das instalações sensoriais." (p.18)[188] As menções seguintes passam pelo desenvolvimento de patentes e direitos de propriedade relacionadas à Internet das Coisas e Internet Industrial; da integração da IoT com um ecossistema de chips, no qual a China pretende avançar suas pesquisas; mensuração de riscos, entre outros. Cabe destacar, por fim, a presença da Internet das Coisas relacionada ao Belt and Road. A China aponta como objetivo: "Promover a exploração cooperativa com países que estão construindo conjuntamente o 'Belt and Road' em novas áreas de infraestrutura aplicada. Realizar pesquisas conjuntas, planejamento, testes e demonstrações em áreas como centros de dados, plataformas de Internet das Coisas e plataformas de Internet industrial; avançar na cooperação integrada em padrões [...]" (p.43)[189]
The 14th Five-Year Plan (2021–2025) (the Plan) for National Economic and Social Development of the People’s Republic of China (PRC) (ADB, 2021)	2021	Aqui analisaremos o documento sobre o tema elaborado pelo Asian Development Bank (ADB, 2021). Em seu décimo quarto plano quinquenal - a China estabelece a Internet das Coisas entre os principais objetivos. Ela se relaciona à manutenção do PIB chinês, sendo apontada como um dos meios para isso. “O plano tem como objetivo manter a participação da indústria na GDP estável após uma década de declínio. Incentivos fiscais, acesso mais amplo ao crédito e uso mais eficiente do terreno industrial estão entre as ferramentas para apoiar o setor. A digitalização da economia continuará, com a participação da economia digital no PIB prevista para aumentar para 10% do PIB até 2025, ante 7,8% em 2020. A computação em nuvem, big data, internet (incluindo internet das coisas e internet industrial), blockchain, inteligência artificial e realidade virtual e aumentada serão apoiadas”. (CHINA, 2021a, p.3, grifo do autor)[190]

[188] Em inglês: "Promote the incorporation of industrial IoT into public infrastructure construction planning; accelerate the formulation of unified platform specifications across departments, manufacturers, and industries. Coordinate the construction of a new metropolitan IoT private network integrating the IoT, data linkage and smart linkages., accelerate the collaborative deployment of 5G and IoT, and improve the resource sharing and comprehensive utilization level of sensory facilities”.
[189] Em inglês: “Promote cooperative exploration with countries jointly building the “Belt and Road” in novel applied infrastructure areas. Jointly conduct research, planning arrangements, trials, and demonstrations in areas such as data centers, Internet of Things platforms, and industrial Internet platforms; advance integrated cooperation on standards[...]”.
[190] Em inglês. “The Plan aims to keep the share of manufacturing in GDP stable after a decade of decline. Fiscal incentives, wider access to credit, and more efficient industrial land use are among the

Quadro 12 - Percepção da China acerca de sistemas ciber-físicos (conclusão)

Documento	Ano	Como aborda sistemas ciber-físicos/IoT?
White Paper IoT (CAICT, 2020)	2020	É o mais recente White Paper lançado pela China sobre essa temática. Ao todo, foram 6 desde 2011. O documento apresenta um caráter bem técnico, ao discorrer sobre situação, desafios e padrões. Os White Papers como um todo carecem de análises mais aprofundadas em trabalhos futuros.

Fonte: Elaborada pelo autor com base em documentos chineses

Nos documentos, conseguimos perceber um forte caráter econômico dado para a temática de IoT na China. Como veremos abaixo, isso dialoga com a estratégia de desenvolvimento do país no tema, que já dura mais de uma década. Preocupações securitárias e infraestruturais, contudo, não deixam de ser abordadas e se encontrar presentes, sobretudo, em White Papers sobre o tema. Até então, a China já produziu 6 documentos específicos sobre Internet das Coisas, além de outros White Papers que abordam temas correlatos, como internet de veículos e Big Data.[191] Dito isso, vejamos um pouco mais sobre como o tema é abordado internamente no país.

4.4.3 Como o país vem abordando o tema internamente?

A implementação da Internet das Coisas na China possui um forte caráter estatal, na medida em que é percebida como estratégica para o desenvolvimento do Estado chinês, em seu esforço para se tornar um polo tecnológico, e colher os benefícios econômicos disso derivados. Os esforços chineses nessa linha começaram ainda em 2009. Conforme apontam Chen et. al (2018):

> Os líderes da China começaram a abraçar as implicações inovadoras da IoT em alto nível já em 2009, quando a IoT foi identificada como uma das cinco "indústrias emergentes estratégicas" (新兴战略产业) pelo então Premier Wen Jiabao. Hu Jintao, então presidente do Partido Comunista Chinês (PCC), deu seu aval ao esforço logo em seguida, em um discurso de 2010, e até 2012, esses endossos em alto nível havia sido traduzidos em uma abordagem ampla e estatal para o desenvolvimento da IoT, caracterizada pela emissão de diversos planos estatais em diferentes campos relacionados à IoT. O

tools to support the sector. The digitalization of the economy will continue with the share of the digital economy in GDP set to increase to 10% of GDP by 2025, from 7.8% in 2020. Cloud computing, big data, internet (including internet of things and industrial internet), block chain, artificial intelligence, and virtual and augmented reality will be supported".

[191]Os White Papers mais recentes podem ser encontrados em: http://www.caict.ac.cn/english/research/whitepapers/index_10.html. Acesso em: 01 jan. 2024.

> desenvolvimento da IoT na China progrediu a passos largos sob a tutela do governo e com substancial apoio financeiro e político do governo.[192]

De lá para cá, uma série de outras menções ao tema vem aparecendo em documentos chineses. O *Ministry of Higher Education and Science Denmark* (2019) faz um levantamento bem rico nesse sentido, em formato de linha do tempo. Os elementos marcantes desta linha podem ser observados no quadro abaixo.

Quadro 13 - Linha do tempo de menções à IoT na China (continua)

Acontecimento	**Ano**
IoT considerada como uma das cinco indústrias emergentes	2010
Primeiro White Paper sobre o tema produzido pela *China Academy of Telecommunication Research of the Ministry of Industry and Information Technology*	2011
Lançamento do 12th Five-Year-Development Plano for IoT	2012
Lançamento do Special Project Action Plan for IoT	2013
IoT é mencionada como um pilar da indústria em 90% nos planos de desenvolvimento das províncias e municípios chineses	2014
Presença de referências a IoT no Made in China 2025, ao falar de *smart manufacturing, smart home, smart cars.*	2015
IoT mencionada 20 vezes no National Informatization Plan for the Thirteen Five-Year plan.	2016

[192] Em inglês: “China’s leaders began to embrace the groundbreaking implications of the IoT at a high level as early as 2009, when the IoT was identified as one of five “strategic emerging industries” (新兴战略产业) by then-Premier Wen Jiabao. Hu Jintao, then-Chinese Communist Party (CCP) Chairman, lent his imprimatur to the effort shortly thereafter in a 2010 speech,4 and by 2012, these high-level endorsements had been translated into a wide-ranging, state-run approach to IoT development characterized by the issuance of a variety of state plans in different IoT-related fields. China’s IoT development has progressed by leaps and bounds under government tutelage and with substantial government monetary and policy support. “

Quadro 13 - Linha do tempo de menções à IoT na China (conclusão)

Acontecimento	**Ano**
Último White Paper lançado sobre o tema até a data da presente dissertação (dado do autor)	2020
Iot mencionada 9 vezes no National Informatization Plan for the Fourteen Five-Year plano (dado do autor)	2021

Fonte: Elaborada com base na linha do tempo presente no relatório China - IoT Nation, do *Ministry of Higher Education and Science Denmark* (2019, p.10)

Sendo percebida como estratégica para os planos de desenvolvimento chineses, a Internet das Coisas vem contando com forte apoio do Estado para se consolidar. De acordo com a GSMA (2015), em 2014 já havia um investimento na casa de $1,6 bilhão no setor:

> [...] O governo está promovendo a pesquisa e desenvolvimento, aplicações e serviços da IoT por meio do Fundo Especial de IoT. Bolsas são oferecidas para projetos autofinanciados, e subsídios de empréstimos apoiam empresas com financiamento bancário. Em 2014, o governo aumentou seu investimento anual em IoT para 10 bilhões de renminbi (aproximadamente 1,6 bilhão de dólares). (GSMA, 2015, p.8)[193]

Há de se mencionar também um esforço Chinês em criar padrões para IoT e consolidar esses padrões internacionalmente. O próprio GSMA menciona essa questão em 2015, ao apontar como “O governo central da China está liderando o desenvolvimento de padrões, apoiando o estabelecimento de uma associação de padrões da IoT com a esperança de que os padrões desenvolvidos na China prevaleçam internacionalmente” (GSMA, 2015, p.8).[194] Essa percepção é reforçada por Chen et al (2019):

> Os especialistas chineses em IoT estão ativamente envolvidos em esforços para influenciar os padrões internacionais de IoT e 5G que podem um dia "garantir" as vantagens chinesas na produção e custo, ao mesmo tempo que posicionam Pequim para dominar o setor de IoT como um todo. Pesquisadores militares e civis chineses estão estudando energeticamente as vulnerabilidades de segurança da IoT que um dia podem ser incorporadas

[193] Em inglês: “[...] the government’s iot Special fund is promoting iot research and development, applications and services. Grants are offered to self-funded projects, and loan subsidies support enterprises with bank-loan funding. in 2014, the government upped its annual investment in iot to rMB 10 billion ($1.6 billion)”.

[194] Em inglês: “China’s central government is leading the development of standards, supporting the establishment of an iot standards association with the hope that Chinese-developed standards will prevail internationally.”

> a trilhões de dispositivos IoT fabricados para cumprir os padrões internacionais preferidos da China. A legislação chinesa recente permite explicitamente que o regime assuma qualquer dado considerado necessário para proteger a segurança nacional, enquanto as empresas chinesas sujeitas a essas leis correm para adquirir o máximo de dados de IoT possível. Muitos desses esforços são guiados pelo ditame do Líder Supremo Chinês Xi Jinping de que "não pode haver segurança nacional sem segurança de rede." (CHEN ET AL. 2019, p.17)[195]

Essa corrida pela padronização tem um aspecto tanto político quanto securitário. Smid (2023) lembra como, ao adotar um padrão internacional que se baseie em seus padrões domésticos, a China estaria colocando uma pressão na comunidade internacional de se adequar aos seus padrões. Já em termos de segurança, o autor traz a percepção de que o criador da tecnologia conhece melhor do que ninguém as possíveis vulnerabilidades dessa própria tecnologia. Essa visão também é reforçada por Koniagina et. al (2023):

> O foco da China na segurança da IoT é definido por sua ênfase direta na segurança de rede como uma função de segurança nacional. O aparato coercivo do país supervisiona e direciona a coleta e divulgação de vulnerabilidades da IoT. Por sua vez, o governo regularmente divulga relatórios de vulnerabilidades de software por meio do Banco de Dados Nacional de Vulnerabilidades da China, dando ao setor privado a capacidade de identificar e corrigir imediatamente as fraquezas de suas arquiteturas de segurança. Os esforços contínuos da China para padronizar internamente a IoT fazem parte da estratégia nacional de renovação cumprida por meio do desenvolvimento econômico, segurança nacional e planejamento econômico centralizado (Kshetri 2017; Jiang 2019). (KONIAGINA et al. 2023, p. 261)[196]

Por fim, é importante ressaltar que, embora na maior parte de seus documentos e posicionamentos oficiais, a China destaque a Internet das Coisas a partir de seus potenciais econômicos e de desenvolvimento, quando observamos o White Paper de

---

[195] Em inglês: “Chinese IoT experts are actively engaged in efforts to influence international IoT and 5G standards that may one day “lock in” Chinese advantages in production and cost while positioning Beijing to dominate the IoT sector writ large. Chinese military and civilian researchers are energetically studying IoT security vulnerabilities that could one day be built in to trillions of IoT devices manufactured to comply with China’s preferred international standards. Recent Chinese legislation explicitly enables the regime to commandeer any data deemed necessary to protect national security, while Chinese companies subject to these laws rush to acquire as much IoT data as possible. Many of these efforts are guided by Chinese Paramount Leader (最高领导人) Xi Jinping’s dictum that “there can be no national security without network security.”

[196] Em inglês: “China’s emphasis on IoT security is defined by its direct focus on network security as a national security function. The country’s coercive apparatus oversees and directs the collection and release of IoT vulnerabilities. The government, in turn, regularly discloses software vulnerability reports via the Chinese National Vulnerability Database, giving the private sector the ability to immediately identify and fix their security architectures’ weaknesses (Chen et al. 2018). China’s ongoing efforts to internally standardize the IoT are part of the national revival strategy fulfilled through economic development, national security, and centralized economic planning”.

2020, são inúmeras as menções e preocupações em relação à segurança, que passam desde a dependência de produtos externos (como, por exemplo, microchips em meio a escassez dos mesmos globalmente) até preocupações mais diretas, como “fortalecer a construção de segurança da Internet das Coisas, garantindo as necessidades de segurança das aplicações em larga escala da Internet das Coisas” (CAICT, 2020).

Cabe lembrar também que, embora a China já contasse, em 2019, com 30% das conexões globais de IoT (3,63 bilhões de conexões), segundo o próprio White Paper, o país ainda enxergava o mundo vivendo uma “primeira fase” da Internet das Coisas, a qual denomina de “pré-explosão”. Essa fase teria início em 2016, e estaria sendo marcada pela estruturação da internet das coisas e das redes 5G. A partir disso, se seguirão duas fases, de “explosão” e “explosão total” na qual oferta e demanda primeiramente se equilibrarão e, posteriormente, a demanda se tornará o principal motor da IoT. Desse modo, as 8 bilhões de conexões previstas para 2025 ainda estariam longe de todo o potencial que a IoT possui. Ainda, a China percebe uma tendência, para os próximos anos, de a Internet Industrial das Coisas crescer e até mesmo superar os dispositivos voltados para o consumo. (CAICT, 2020) Observando dados como esses, é inegável a importância que o mercado de consumo chinês tem e terá no ramo da IoT.

4.5 AUSTRÁLIA

4.5.1 Como a Austrália percebe a governança do ciberespaço?

Para compreender o posicionamento da Austrália em relação à governança do ciberespaço, cabe lembrar, novamente, que ela é um dos Estados signatários da Declaração pelo Futuro da Internet. Logo, assim como no caso do Reino Unido, também podemos partir de uma adesão por parte da Austrália aos princípios ali defendidos. Cabe lembrar ainda que, desde 2021, Austrália, Reino Unido e Estados Unidos possuem uma aliança securitária tripartite, a AUKUS. A aliança, declaradamente, visa contrapor o que, nas palavras de Antony Blinken (Secretário de Estado dos Estados Unidos), configura “uso de coerção econômica por parte de Pequim contra a Austrália” (PADINGER, 2023).

Dado esse breve contexto, vejamos alguns elementos que a Austrália traz quando se fala em governança do ciberespaço. Para isso, vejamos as suas Estratégias de engajamento Cibernético Internacional, com versões em 2017 e 2021. Na versão de 2017, a Austrália traz um foco grande na questão do multi*stakeholderismo* como caminho para a governança da internet. O objetivo australiano é declaradamente de uma internet aberta, livre e segura, alcançada através de uma abordagem *multistakeholder.* Para atingir esse objetivo, a Austrália se compromete com três atividades: 1. Advogar por esse modelo de governança; 2. Se opor a esforços para trazer a internet para o controle governamental e 3. Aumentar a conscientização sobre questões de governança da internet na região do Indo-Pacífico.

Em relação ao ponto 1, a Austrália dá destaque à cooperação com atores não governamentais, se comprometendo a estabelecer anualmente um fórum de diálogo com a participação de atores não governamentais, incluindo consumidores, especialistas e o setor privado. Para o país, o setor privado também tem "desempenhado "um papel fundamental na condução da inovação que está no cerne do sucesso da Internet. Portanto, incluir a perspectiva do setor privado é fundamental para o crescimento e sustentabilidade a longo prazo do ecossistema digital." (AUSTRÁLIA, 2017, p.62)[197]

Já no ponto 2, a Austrália deixa clara sua oposição em trazer os mecanismos de controle da internet para o âmbito das Nações Unidas, onde os governos desempenham maior poder. Essa posição, como vimos, é defendida por China e Rússia, mas os países não são mencionados negativamente no documento, como no caso da estratégia dos Estados Unidos. Não há menção à Rússia e às menções à China são sob a ótica de diálogos diplomáticos.

Cabe destacar que essa percepção australiana dialoga diretamente com as novas tecnologias, incluindo a internet das coisas.

> A Austrália **se opõe a iniciativas que buscam colocar a governança e a gestão técnica da Internet sob o controle dos governos ou dentro do sistema das Nações Unidas (ONU), por exemplo, dentro da União Internacional de Telecomunicações da ONU**. Em vez disso, a Austrália advoga pela melhoria dos mecanismos existentes de governança multissetorial. Essa abordagem garantirá que a governança da Internet permaneça inclusiva, baseada em consenso, transparente e responsável. Isso será especialmente importante à medida que a Internet continue a evoluir

[197] Em inglês: "the private sector has also largely driven the innovation at the heart of the Internet's success. Therefore, including the perspective of the private sector is critical to the longer term growth and sustainability of the digital ecosystem".

> e a apoiar uma variedade de tecnologias emergentes. A governança da Internet das Coisas, regras para o uso de dados e privacidade e confiança online são todas questões que exigem uma abordagem colaborativa para a governança da Internet. (AUSTRÁLIA, 2017, p.62, grifo do autor)[198]

Por fim, no âmbito regional, a Austrália fala em coordenar suas posições com outros países da região, por meio de fóruns, workshops e eventos. Tal posicionamento é interessante, pois a região indo-pacífica é uma região de disputa de influência com a China, que possui um posicionamento diferente do australiano.

No documento de 2021, a Austrália mantém seu posicionamento de promover o modelo multistakeholder e, além de consciência, fala em aumentar as capacidades dos stakeholders na região indo pacífica. Em relação ao multistakeholderismo em si, o país entende que o modelo deve ser melhorado, mas não alterado. Embora entenda que os governos têm um papel de guia e "têm expertise em políticas públicas e estão posicionados de forma única para trazer uma ampla gama de considerações para discussões sobre o futuro da Internet". (AUSTRALIA, 2021a, p.82)[199], a Austrália vê um controle maior da governança pelos Estados como uma ameaça a um ciberespaço seguro.

> Nem todos os estados apoiam o modelo multissetorial, e muitos prefeririam limitar a capacidade dos stakeholders não governamentais de influenciar as decisões sobre o futuro da Internet. Isso permitiria a criação de uma Internet mais facilmente controlada pelos estados, restringindo a capacidade da Austrália de garantir que o ciberespaço seja seguro. [...] A Austrália se opõe a todas as tentativas de colocar a governança e a gestão técnica da Internet sob o controle dos governos ou dentro do sistema multilateral. (AUSTRALIA, 2021a, p.82)[200]

---

[198] Em inglês: "Australia **opposes moves to bring governance and technical management of the Internet under the control of governments or into the United Nations (UN) system, for example within the UN International Telecommunications Union**. Instead, Australia advocates for the improvement of existing mechanisms of multistakeholder governance. This approach will ensure that governance of the Internet remains inclusive, consensus-based, transparent and accountable. **This will be particularly important as the Internet continues to evolve and support a range of emerging technologies**. Governance of the Internet of Things, rules for the use of data, and privacy and trust online are all issues demanding a collaborative approach to Internet Governance".

[199] Em inglês: "have expertise in public policy and are uniquely placed to bring a broad range of considerations to discussions about the future of the Internet".

[200] Em inglês: "Not all states support the multistakeholder model, and many would prefer to limit the ability of non-government stakeholders to influence decisions on the future of the Internet. This would enable the creation of an Internet that is more easily controlled by states, restricting Australia's ability to ensure cyberspace is safe and secure. [...] Australia opposes all attempts to bring governance and technical management of the Internet under the control of governments or into the multilateral system".

Dado esse contexto, vejamos um pouco de como o país tem lidado com os sistemas ciber-físicos.

4.5.2 Como a Austrália percebe os sistemas ciber-físicos?

O quadro abaixo, seguindo os padrões anteriores, representa as menções ao tema nos principais documentos Australianos. Por si só, as análises presentes no quadro já resumem bem o posicionamento australiano, que foca no potencial dessas tecnologias para o futuro, percebe seus riscos, e advoga pelo estabelecimento de padrões de segurança a nível internacional.

Quadro 14 - Percepção da Austrália acerca de sistemas ciber-físicos (continua)

Documento	**Ano**	**Como aborda sistemas ciber-físicos/IoT?**
2023 - 2030 Australian Cyber Security Strategy (AUSTRALIA , 2023)	2023	A Internet das Coisas já aparece logo na introdução da estratégia. Após contextualizar sobre o volume e os prejuízos financeiros trazidos por ataques cibernéticos (um crime cibernético a cada 6 minutos e 3 bilhões de dólares em prejuízos a economia Australiana apenas com ataques *ransomware*), o documento aponta como o cenário tende a piorar com a internet das coisas, que abre um novo escopo de alvos cibernéticos. “A inteligência artificial e a aprendizagem de máquina trarão novos tipos de riscos. A Internet das Coisas levará bilhões de dispositivos adicionais sendo conectados à Internet, abrindo novos horizontes para ataques cibernéticos. E, nosso ambiente geopolítico é o mais desafiador que enfrentamos desde a Segunda Guerra Mundial.” (p.6)[201] A outra menção acontece dentro da seção de “Safe Technology” que, na estratégia de longo prazo, visa garantir a confiança dos australianos na segurança de seus produtos e serviços digitais. O problema apontado está em padrões de segurança que não são pensados desde o desenho do produto. A isso se soma um grande número de *“smart devices”* e, consequentemente, um risco sistêmico.

[201] Em inglês: “Artificial intelligence and machine learning will bring new kinds of risk. The Internet of Things will lead to billions of additional devices being connected to the Internet, opening new scope for cyberattack. And, our geopolitical environment is the most challenging we have faced since the Second World War”.

Quadro 14 - Percepção da Austrália acerca de sistemas ciber-físicos (continuação)

Documento	Ano	Como aborda sistemas ciber-físicos/IoT?
2023 - 2030 Australian Cyber Security Strategy (AUSTRALIA, 2023) Continuação	2023	Produtos e serviços sem segurança integrada podem apresentar vulnerabilidades que atores maliciosos podem explorar facilmente, potencialmente minando a confiança pública na tecnologia. Muitos produtos digitais não possuem padrões de segurança integrados por design, ou não são ativados por padrão. Como resultado, consumidores e empresas podem oferecer produtos e serviços menos seguros, com expertise insuficiente para gerenciar o risco. [...] Essas falhas de mercado são particularmente prevalentes no mercado global de 'Internet das Coisas' (IoT) ou dispositivos inteligentes, com a média de lares australianos prevista para ter 33 dispositivos conectados até 2025. À medida que o mercado de dispositivos inteligentes se expande para incluir produtos como veículos autônomos e dispositivos de energia distribuída, essas vulnerabilidades poderiam criar riscos sistêmicos para a sociedade e a economia - e potencialmente facilitar a interferência estrangeira cibernética." (p.31, grifo do autor).[202] Para lidar com esse desafio, a Austrália parte pelo caminho da adoção de padrões de segurança internacionais para dispositivos tecnológicos: em colaboração com a indústria, a Austrália se propõe a estabelecer padrões de segurança mandatórios para dispositivos de IoT. A possibilidade de estes padrões estarem alinhados a padrões internacionais também é levantada. Ainda, pensando nos consumidores, a Austrália fala do desenvolvimento de um esquema de rotulagem de produtos para *smart devices,* que se alinhe a iniciativas semelhantes de Estados Unidos, Singapura e Reino Unido. "O governo trabalhará com a indústria para incentivar a adoção de padrões internacionais para projetos seguros em tecnologias digitais, como dispositivos IoT. [...] O padrão poderia ser alinhado aos padrões internacionais para garantir consistência entre jurisdições e minimizar o ônus regulatório sobre empresas australianas, ao mesmo tempo em que atende aos nossos objetivos de segurança nacional. Para ajudar os consumidores a fazer escolhas informadas sobre a segurança dos dispositivos no mercado, o governo também desenvolverá um esquema de rotulagem voluntária para dispositivos inteligentes de consumo. Essas reformas alinharão a Austrália com os mercados internacionais, incluindo os Estados Unidos, Singapura e o Reino Unido." (p.32)[203]

[202] Em inglês: "Products and services without built-in security can present vulnerabilities that malicious actors can easily exploit, potentially undermining public trust in technology. Many digital products do not have security standards built in by design, or turned on by default. As a result, consumers and businesses can be offered less secure products and services, with insufficient expertise to manage the risk. [...] These market failures are particularly prevalent in the global 'Internet of Things' (IoT) or smart devices market, with the average Australian home set to have 33 connected devices by 2025. As the smart device market expands to include products like autonomous vehicles and distributed energy devices, these vulnerabilities could create systemic risks for society and the economy – and potentially facilitate cyber-enabled foreign interference."

[203] Em inglês: "The Government will work with industry to encourage the adoption of international standards for secure-by-design in digital technologies such as IoT devices. [...] The standard could be aligned to international standards to ensure consistency between jurisdictions and minimise the regulatory burden on Australian businesses, while meeting our national security objectives. To help consumers make informed choices about the security of devices on the market, the Government will also develop a voluntary labelling scheme for consumer-grade smart devices. These reforms will align Australia with international markets, including the United States, Singapore and the United Kingdom."

Quadro 14 - Percepção da Austrália acerca de sistemas ciber-físicos (continuação)

Documento	Ano	Como aborda sistemas ciber-físicos/IoT?
Australia's International Cyber and Critical Tech Engagement Strategy (AUSTRALIA, 2021a)	2021	O documento traz uma série de menções à Internet das Coisas. Inicialmente, a IoT já aparece definida como uma *"tecnologia crítica", com "significantly enhance, or pose risks to, Australia's national interests"* (p.10) ao lado de computação quântica, Inteligência Artificial e Biologia Sintética. Dentro do bloco de Segurança Cibernética, a Austrália menciona o desenvolvimento de um Code of Practice voluntário para IoT: "O Código de Prática Voluntário da Austrália: Protegendo a Internet das Coisas para Consumidores fornece orientações claras às empresas sobre os recursos de segurança cibernética que esperamos dos dispositivos conectados à Internet disponíveis na Austrália." *(p.50).*[204] Dentro da seção que fala sobre conectividade dentro da ASEAN, a Internet das Coisas também é citada dentro do escopo de tecnologias críticas que, em conjunto, tem um potencial de gerar até $625 bilhões ao ano para os países da ASEAN. (p.70). A mesma narrativa é adotada no âmbito da cooperação em parcerias para trocas de talentos e estudantes. "A Austrália reconhece o benefício das trocas de talentos direcionadas e dos fluxos de estudantes com nossos parceiros internacionais [...] países como Nova Zelândia, Estados Unidos, Reino Unido, Alemanha, Coreia do Sul, Singapura e Índia para aumentar a cooperação internacional em inovação tecnológica crítica, incluindo segurança cibernética, Internet das Coisas, blockchain, inteligência artificial e computação quântica." (p.76)[205] Há também um bloco específico para apresentar seu *Code of Practice,* já citado anteriormente, e colocado como um primeiro passo para aumentar a segurança de dispositivos de IoT no país. "Como um dos principais entregáveis da Estratégia de Segurança Cibernética da Austrália 2020, o Código de Prática é um conjunto voluntário de medidas que o governo recomenda que a indústria adote como padrão mínimo para dispositivos da Internet das Coisas (IoT). Composto por 13 princípios, o Código de Prática incentiva a segurança por design ao longo do ciclo de vida dos dispositivos IoT. Os princípios sinalizam aos fabricantes domésticos e internacionais a importância de proteger os consumidores e as características de segurança esperadas dos dispositivos IoT disponíveis na Austrália." (p.82)[206]

[204] Em inglês: "Australia's voluntary Code of Practice: Securing the Internet of Things for Consumers provides clear advice to businesses on the cyber security features we expect of Internet-connected devices available in Australia".
[205] Em inglês: "Australia recognises the benefit of targeted talent exchange and student pipelines with our international partners [...] countries like New Zealand, the United States, the United Kingdom, Germany, South Korea, Singapore and India to increase international cooperation on critical technology innovation, including cyber security, the Internet of Things, blockchain, AI and quantum computing"
[206] Em inglês: "As a key deliverable of Australia's Cyber Security Strategy 2020, the Code of Practice is a voluntary suite of measures the Government recommends industry adopt as the minimum standard for Internet of Things (IoT) devices. Comprised of 13 principles, the Code of Practice encourages security-by-design throughout the lifecycle of IoT devices. The principles signal to domestic and international manufacturers the importance of protecting consumers and the security features expected of IoT devices available in Australia".

Quadro 14 - Percepção da Austrália acerca de sistemas ciber-físicos (continuação)

Documento	Ano	Como aborda sistemas ciber-físicos/IoT?
Australia's International Cyber and Critical Tech Engagement Strategy (AUSTRALIA, 2021a) Continuação	2021	Por fim, ao falar de governança de dados, a Internet das Coisas é citada como um fator de aumento e consumo de dados, em um ecossistema em que dados vêm se tornando uma commodity. Isso pede por medidas de segurança e privacidade de dados. "As tecnologias críticas atuais e emergentes, como a Internet das Coisas e a aprendizagem de máquina, estão aumentando a produção e o consumo de dados, e dependem de conjuntos de dados em expansão para criar valor por meio de aplicativos como publicidade direcionada. Como tal, os dados se tornaram um ativo comercial e uma mercadoria para negociação. Isso torna mais importante do que nunca equilibrar as implicações de privacidade, segurança e econômicas da coleta, uso e transferência de dados." (p.88)[207]
Digital Economy Strategy 2030 (AUSTRALIA, 2021b.)	2021	A Internet das Coisas é apontada como um dos cinco campos nos quais a Austrália deve estar na vanguarda para que seja uma "*leading digital economy and society by 2030".* A Internet das Coisas aparece ao lado de inteligência artificial, análise de dados, blockchain e computação quântica. Na seção de tecnologias emergentes, a Austrália ressalta como essas tecnologias podem aumentar produtividade, criar empregos, resolver problemas e gerar crescimento de negócios. Percebe-se aqui um claro interesse econômico em dominar a área. "As tecnologias digitais e novos modelos de negócios impulsionarão a produtividade, criarão empregos, resolverão os problemas do mundo real de hoje e farão crescer os negócios e setores do futuro. Até 2030, esperamos ver avanços em tecnologias emergentes que possam transformar a economia australiana. Estas provavelmente incluirão inteligência artificial (IA), computação quântica, nanotecnologia, ciência cognitiva, captura e armazenamento de energia, mais dispositivos conectados por meio de uma maior penetração da Internet das Coisas (IoT) e o avanço adicional de tecnologias existentes com potencial não explorado. Compreender como essas tecnologias estão se desenvolvendo e as aplicações potenciais e os riscos que precisam ser gerenciados é essencial para fornecer as configurações políticas e regulatórias adequadas para apoiar a adoção em toda a economia. Ao compreender melhor as tecnologias de hoje e se preparar para as tecnologias do futuro, a Austrália está bem posicionada para abraçar novas oportunidades." *(p.57)*[208]

[207] Em inglês: "Current and emerging critical technologies, such as the Internet of Things and machine learning are increasing the production and consumption of data, and rely on growing datasets to create value through applications such as targeted advertising. As such, data has become a commercial asset and a commodity for trade. This makes it more important than ever to balance the privacy, security and economic implications of the collection, use and transfer of data."

[208] Em inglês: "Digital technologies and new business models will boost productivity, create jobs, solve the real-world problems of today and grow the businesses and sectors of tomorrow [...] By 2030 we would expect to see breakthroughs in emerging technologies that can transform the Australian economy. These are likely to include artificial intelligence (AI), quantum computing, nanotechnology, cognitive science, energy capture and storage, more connected devices through increased penetration of the Internet of Things (IoT), and the further advancement of existing technologies with undeveloped potential. [...] Understanding how these technologies are developing and the potential applications and risks that need to be managed, is essential to delivering the right policy and

Quadro 14 - Percepção da Austrália acerca de sistemas ciber-físicos (continuação)

Documento	Ano	Como aborda sistemas ciber-físicos/IoT?
Australia's Cyber Security Strategy (AUSTRALIA, 2020a)	2020	A estratégia de 2020 também é rica em menções à Internet das Coisas. A primeira delas é dentro da visão australiana presente na estratégia. A Austrália visualiza um ambiente online seguro para seus habitantes, seus negócios e serviços essenciais. Dentro disso, se propõe $1,67 bilhões em 10 anos em uma série de campos, dentre eles "orientações claras para empresas e consumidores sobre a segurança de dispositivos da Internet das Coisas." *(p.8).*[209]O tema é retomado na seção "Securing products and Services", na qual a Austrália ressalta o volume de dispositivos de IoT esperados para 2030 no mundo, variando entre 21 e 64 bilhões. A partir disso, a Austrália menciona que irá desenvolver o seu "*Code of Practice: Securing the Internet of Things for Consumers"* e que irá informar consumidores sobre o que levar em conta ao comprar aparelhos de Iot (p.33 - 34). O tema é retomado na seção "Securing products and Services", na qual a Austrália ressalta o volume de dispositivos de IoT esperados para 2030 no mundo, variando entre 21 e 64 bilhões. A partir disso, a Austrália menciona que irá desenvolver o seu "*Code of Practice: Securing the Internet of Things for Consumers"* e que irá informar consumidores sobre o que levar em conta ao comprar aparelhos de Iot (p.33 - 34). Um pouco mais a frente, o documento também traz um conjunto de perguntas que os consumidores devem se fazer antes de comprar um aparelho e no momento de configurá-lo, se comprometendo a trazer novas dicas em seu site (cyber.gov.au). (p.38) Por fim, dentro de uma tabela que resume o plano de ação para os próximos anos, para "criar um ambiente mais seguro para a Internet das Coisas", a Austrália se compromete a criar seu Code of Practice, esperando como benefícios que: "Os produtos da Internet das Coisas na Austrália terão uma cibersegurança aprimorada, reduzindo os custos na economia australiana atualmente suportados por vulnerabilidades de dispositivos [...] Os consumidores terão maior acesso a dispositivos seguros da Internet das Coisas, reduzindo sua exposição a atividades cibernéticas maliciosas." (p.44) [210]

regulatory settings to support uptake across the economy. [...] By better understanding the technologies of today and preparing for the technologies of the future, Australia is well placed to embrace new opportunities."

[209] Em inglês: "Clear guidance for businesses and consumers about securing Internet of Things devices".

[210] Em inglês: "Internet of Things products in Australia will have improved cybersecurity, reducing costs on Australia's economy currently borne by device vulnerabilities [...] Consumers will have greater access to secure Internet of Things devices, reducing their exposure to malicious cyber activity".

Quadro 14 - Percepção da Austrália acerca de sistemas ciber-físicos (conclusão)

Documento	Ano	Como aborda sistemas ciber-físicos/IoT?
Australia's International Cyber Engagement Strategy (AUSTRALIA, 2017)	2017	Já em 2017 a Austrália já trazia percepções sobre a relevância desse tema. O documento apresenta a iminência de dispositivos conectados à Internet das Coisas como um dos fatores determinantes para maiores desenvolvimentos securitários. "A crescente conectividade e a proliferação de dispositivos conectados à Internet (a Internet das Coisas) destacam a importância da segurança como um elemento fundamental no design e na entrega de produtos, sistemas e serviços de tecnologia da informação e comunicação (TIC)." (p.28)[211] A outra menção faz direta referência à governança da Internet das Coisas. A Austrália se opõe a uma governança centrada no Estado Nacional, advogando por uma governança colaborativa. "Isto será especialmente importante à medida que a Internet continua a evoluir e a apoiar uma variedade de tecnologias emergentes. A governança da Internet das Coisas, as regras para o uso de dados, e a privacidade e confiança online são todas questões que demandam uma abordagem colaborativa para a governança da Internet." (p.64)[212]

Fonte: Elaborado pelo autor, com base nos documentos da Austrália

Dentro dos documentos, há menções específicas a um código de boas práticas para as manufaturas presentes no país. Vejamos um pouco mais sobre isso.

4.5.3 Como o país vem abordando o tema internamente?

Inicialmente, a Austrália partiu para a estratégia de um código de conduta de caráter voluntário, lançado em 2020. O "*Code of Practice: Securing the Internet of Things for Consumers*" se embasou no Reino Unido e possui 13 princípios que direcionam as expectativas do governo australiano para com as manufaturas, para que garantam a segurança dos consumidores. Podemos pressupor que esse caráter voluntário advém da forte relação de confiança entre o governo australiano e os *stakeholders* privados, fortemente defendido em seus documentos. Nas palavras do governo australiano: "O Código de Prática é o primeiro passo em direção à melhoria da segurança de dispositivos inteligentes na Austrália. O Código de Prática [...]

[211] Em inglês: "Increasing connectivity, and the proliferation of devices connected to the Internet (the Internet of Things), highlights the importance of security as a fundamental driver in the design and delivery of information communication and technology (ICT) products, systems and services."
[212] Em inglês: "This will be particularly important as the Internet continues to evolve and support a range of emerging technologies. Governance of the Internet of Things, rules for the use of data, and privacy and trust online are all issues demanding a collaborative approach to Internet governance."

sinaliza as expectativas do governo para os fabricantes em relação à segurança dos produtos inteligentes." (HOME AFFAIRS, 2024)[213] A própria aplicação do código também traz esse elemento da confiança. Os *stakeholders* que se adequassem aos princípios deveriam manifestar com quais deles se adequaram, como, por exemplo: “Nossa organização cumpriu com os princípios 1, 2 e 3 do Código de Prática: Garantindo a Segurança da Internet das Coisas para Consumidores." (AUSTRALIA, 2020b, p.4)[214]

O código em si possui é curto e direto. Possui 10 páginas e ressalta seu caráter de primeiro passo e gerador de conscientização.

> O [Código] representa um primeiro passo na abordagem do Governo Australiano para melhorar a segurança dos dispositivos IoT na Austrália. Este Código de Prática é um conjunto voluntário de medidas recomendadas pelo Governo Australiano para a indústria, como padrão mínimo para dispositivos IoT. O Código de Prática também ajudará a aumentar a conscientização sobre salvaguardas de segurança associadas a dispositivos IoT, construirá uma maior confiança do consumidor na tecnologia IoT e permitirá que a Austrália aproveite os benefícios de uma maior adoção de IoT. (AUSTRÁLIA, 2020b)[215]

Os 13 princípios listados[216] focam principalmente em elementos de segurança dos dispositivos e dos dados que esses dispositivos movimentam. No documento, o próprio governo australiano também recomenda um foco maior aos três primeiros, com estabelecimentos de senhas fortes e únicas para os dispositivos (o que pode ser percebido como uma tentativa de evitar ataques estilo o Mirai Botnet); implementar uma política para descobrir vulnerabilidades dos produtos, com apoio da comunidade

---

[213] Em inglês:“The Code of Practice is a first step towards lifting the security of smart devices in Australia. The Code of Practice [...] signal Government expectations to manufacturers about the security of smart products”.

[214] Em inglês: “Our organisation has complied with principles 1, 2 and 3 of the Code of Practice: Securing the Internet of Things for Consumers”.

[215] Em inglês: “[The Code] represents a first step in the Australian Government’s approach to improve the security of IoT devices in Australia. This Code of Practice is a voluntary set of measures the Australian Government recommends for industry as the minimum standard for IoT devices. The Code of Practice will also help raise awareness of security safeguards associated with IoT devices, build greater consumer confidence in IoT technology and allow Australia to reap the benefits of greater IoT adoption.”

[216] 1. No duplicated default or weak passwords; 2. Implement a vulnerability disclosure policy; 3.. Keep software securely updated; 4. Securely store credentials ; 5. . Ensure that personal data is protected; 6. Minimise exposed attack surfaces; 7. Ensure communication security; 8.. Ensure software integrity; 9. Make systems resilient to outages; 10. Monitor system telemetry data; 11. Make it easy for consumers to delete personal data; 12. Make installation and maintenance of devices easy; 13. Validate input data.

cibernética, e manter os softwares atualizados. Na visão da Austrália, essas três medidas têm potencial para trazer os maiores benefícios de segurança no curto prazo.

Uma vez estabelecido o código, a Austrália passou a monitorá-lo. Na Estratégia de Segurança Cibernética de 2020 e em seu site oficial, o próprio país aponta que, em caso de o modelo voluntário não surtir o efeito esperado, outros tipos de medidas poderiam ser adotadas. Em 2021 foi conduzida uma consulta com as manufaturas do país, e se deparou com dificuldades de implementação, sobretudo em pequenos negócios, assim como um desejo por uma conexão maior com padrões internacionais.

> Grandes fabricantes os quais entrevistamos nos informaram que estavam cientes do Código de Prática, mas achavam difícil implementar orientações voluntárias baseadas em princípios. Essas empresas preferiam que o Governo apontasse para padrões alinhados internacionalmente. Embora as grandes marcas com as quais conversamos tivessem boas intenções de implementar uma forte cibersegurança, muitas empresas ainda não haviam implementado algumas recomendações de alta prioridade e baixo custo do Código de Prática, como políticas de divulgação de vulnerabilidades. (HOME AFFAIRS, 2024)[217]

Com base nisso, a Austrália passou a considerar o estabelecimento de padrões de segurança obrigatórios, e abriu consultas internas para essa avaliação. Dali também derivou a possibilidade de criação de um selo. Ambas as medidas estão sendo consideradas na estratégia 2023 - 2030.

Como a estratégia ainda é muito recente, cabe ficar de olho nos passos do país no tema nos próximos anos. As iniciativas discutidas têm sido vistas com bons olhos por organizações como a *Standards Australia*, que ajuda a definir os padrões de segurança do país. Nas palavras de seu CEO, “irá ajudar a aumentar a proteção para os consumidores, eliminar os jogadores ruins e melhorar nossa segurança geral.” (STANDARDS AUSTRALIA, 2023).[218]

De qualquer forma, é interessante perceber que mesmo dentro de um país que se opõe firmemente ao controle governamental no âmbito da governança da internet,

---

[217] Em inglês: “Major manufacturers we interviewed told us that they were aware of the Code of Practice but found it difficult to implement voluntary, principles-based guidance. These firms preferred the Government to point to internationally aligned standards. While major brands we spoke to had good intentions to implement strong cyber security, many firms had not yet implemented some high priority, low cost recommendations of the Code of Practice, such as vulnerability disclosure policies”.
[218] Em inglês: “will help lift protection for consumers, weed out the bad players and improve our security overall”.

a realidade prática vem demonstrando a necessidade de uma imposição obrigatória de padrões de segurança por parte do Estado na temática.

4.6 CONCLUSÃO: OS JOGOS DE PODER, INTERESSES E SEGURANÇA

Inicialmente, cabe aqui retomar a hipótese que embasou esse trabalho. Partia-se de uma premissa na qual os sistemas ciber-físicos seriam percebidos como fatores de potenciais vulnerabilidades de segurança. A percepção dessas vulnerabilidades seria um fator relevante para tornar os Estados mais presentes nos debates sobre governança da internet e dos sistemas ciber-físicos.

Ao longo da pesquisa e da escrita, percebeu-se que a premissa das vulnerabilidades dos sistemas ciber-físicos se confirma não só em dados e casos reais, como também nas narrativas dos próprios Estados Nacionais quando abordam o tema em seus documentos. Há preocupações reais sobre os produtos estarem indo para os mercados sem as devidas boas práticas de segurança. Isso porque boa parte dos *stakeholders* privados ou não conhecem, ou não dominam, ou optam por não seguir todos os padrões de segurança necessários para que esses sistemas estejam seguros não só em âmbito de consumo, mas também em âmbito de sociedade - pois, além de terem contato com o mundo físico, podendo ser usados para atingi-lo, podem ser meios para ataques e podem ser alvos de ataques por si só, devido às gigantescas quantidades de dados que movimentam.

Essas preocupações estão derivando em ações práticas por parte dos países que dialogam com a hipótese ao colocar os Estados como atores de liderança nesse processo de lidar com desafios de segurança. Embora para Estados como Rússia e China, que historicamente possuem uma tendência mais controladora sobre suas empresas, já fossem esperados movimentos nessa linha, é interessante observar como esses mesmos movimentos também estão sendo adotados pelos três Estados Ocidentais analisados. Até mesmo a Austrália que, ao falar de governança da internet em seus documentos, frisa mais do que qualquer um dos outros países a relevância do modelo *multistakeholder* e se opõe a qualquer tipo de controle governamental no âmbito da internet está se vendo obrigada a seguir por um caminho de normas de segurança obrigatórias internamente, ao perceber que o código de boas práticas de segurança para IoT, que possui caráter voluntário, não está surtindo os efeitos esperados em seus atores privados.

O Reino Unido também percebeu isso e tem prevista legislação obrigatória de segurança para os produtos de Internet das Coisas comercializados em seu território já em 2024. Os Estados Unidos, por sua vez, ainda estão com caráter voluntário para sua iniciativa de rotulagem de produtos, a partir de recomendações de segurança. Se forem seguir a tendência de Austrália e Reino Unido, isso deve mudar em breve. Em relação a isso, é interessante observar como o Reino Unido se coloca como uma liderança em modelo legislativo de segurança, que é passível até mesmo de ser exportado para a Austrália.

Cabe lembrar que há todo um cuidado de envolver os *stakeholders* no debate. Mas, a partir do momento em que há normas a serem seguidas e aqueles atores que não as seguirem apresentam algum grau de desvantagem competitiva ou mesmo de exclusão de mercado (no caso de normas obrigatórias) há um estabelecimento de um grau de hierarquia entre aqueles que estabelecem e aplicam a lei (Estado) e aqueles sob os quais a lei é aplicada (demais *stakeholders*).

Um quadro desse tipo é possível justamente num contexto de securitização dos debates sobre governança cibernética que vem acontecendo nos últimos anos, pós Snowden, e que vem opondo atores poderosos, como China e Rússia, a atores tão poderosos quanto, como Estados Unidos e, em menor grau, Reino Unido e Austrália.

As disputas entre eles passam tanto por questões envolvendo: a) a forma como o ciberespaço deve ser governando (num modelo mais multilateral, que se sustenta em direitos soberanos dos Estados sobre seu ciberespaço e em decisões tomadas com base em votos de Estados Nacionais ou mais *multistakeholder*, com decisões sendo tomadas em conjunto com igual); b) modelos de administração cibernética interna (mais ou menos controlados pelo Estado) e as narrativas que os envolvem; c) uma corrida por vantagens econômicas, que passa por elementos como a implementação de infraestruturas a exemplo do 5G em países estratégicos, pela corrida pela implementação de padrões nacionais a nível internacional para tecnologias como os sistemas ciber-físicos e pela construção de coalizões que possibilitem maior força e maiores probabilidades de sucesso nessas disputas.

Dialogando com isso, o Quadro 15 compila os principais pontos apresentados no capítulo, visando deixar mais claras as visões e posicionamentos dos países no tocante à governança do ciberespaço e dos sistemas ciber-físicos.

Quadro 15 - Compilação dos posicionamentos dos países analisados sobre governança e sobre sistemas ciber-físicos (continua)

Estado	Visão voltada para governança cibernética	Visão voltada para sistemas ciber-físicos
Estados Unidos	• Enxerga o ciberespaço como ambiente de conflito, tendo na China seu principal adversário. O país sente-se ameaçado pelo desenvolvimento tecnológico chinês; • Adota a narrativa de manter o ciberespaço num modelo *multistakeholder "open, free, global, interoperable, reliable and secure"* se opondo a modelos autoritários que vão contra isso. • Busca coalizões para preservar seus interesses no ciberespaço e fortalecer a capacidade de parceiros internacionais; • Visa isolar e gerar custos para os atores que caminham numa direção oposta.	• Vê o desenvolvimento da IoT como fator de risco para ataques cibernéticos; • Estabelecimento da política de US Cyber Trust Mark para orientar atores privados sobre boas práticas de segurança e se destacar no mercado em questões de padronização. • Quer ser referência global no tema.
Reino Unido	• Assinou a Declaração para o Futuro da Internet, junto aos Estados Unidos; • Se opõe aos modelos de China e Rússia; • Se propõe a liderar esforços para alcançar um ciberespaço aberto, livre e pacífico, visando fortalecer alianças para alcançar este fim e ter parceiros mais preparados para lidar com ameaças cibernéticas; • Prioriza apoiar países da Europa Oriental, África e Indo-Pacífico (tentando contrapor influência chinesa) além de continuar sua parceria com Oriente Médio e Américas; • Se propõe a estabelecer uma campanha de higiene cibernética internacional para aumentar custos de atividades maliciosas no ciberespaço; • Intencionam alcançar o top 3 de exportadores globais de soluções e expertises cibernéticas; • Junto a seus aliados, busca exercer influência nos padrões internacionais.	• Fala em ser protagonista em termos de desenvolvimento de padrões de IoT e demais tecnologias emergentes; • Estabelecem interesse em desenvolvimento de processos industriais de IoT; • Veem a IoT como fonte de expansão e crescimento econômico. • Estabeleceram uma série de documentos dentro do escopo do "Secure by Design". • Estabeleceram um Código de Conduta para orientar as empresas a adotarem práticas seguras na produção de produtos de IoT, priorizando a segurança dos usuários. • Estabeleceram normas de segurança obrigatórias que entram em vigor em 2024 para IoT, baseado no PSTI.

Quadro 15 - Compilação dos posicionamentos dos países analisados sobre governança e sobre sistemas ciber-físicos (continuação)

Estado	Visão voltada para governança cibernética	Visão voltada para sistemas ciber-físicos
Rússia	• Vê os sistemas de informação como ferramentas para desestabilizar regimes e gerar caos interno (não usam o termo cyber); • Diante disso, busca sua autonomia na regulamentação de seu espaço de informação. Prezam pela soberania cibernética e por conseguir alcançar uma infraestrutura cibernética independente; • Vê como ameaça o uso de ICTs para infringir a soberania e integridade territorial dos Estados; • Manifesta preocupação com monopólios tecnológicos e limites de acesso à tecnologia. Dessa preocupação deriva a busca por autonomia em sua produção tecnológica. • Tem a intenção de promover padrões nacionais russos no campo da segurança da informação e projetar esses padrões globalmente. • É contrária ao uso da internet para fins militares; • Defende que a ONU seja o principal fórum para debates e decisões de governança e que sejam estabelecidas legislações internacionais a partir dali.	• Demonstra preocupações com Internet das Coisas e Internet Industrial na sua estratégia 2017-2030, embora trate os dois termos como separados; • Tem poucas legislações específicas para IoT, porém o tema pode ser entendido como englobado dentro de outras legislações, especialmente as que tratam sobre segurança da informação. • Busca promover a definição de padrões internacionais através de esforços da Rosstandart; • Possui um comitê específico para o desenvolvimento de padrões de IoT (Technical Committee 194) • Estando lidando com limitações de investimento internas na área.

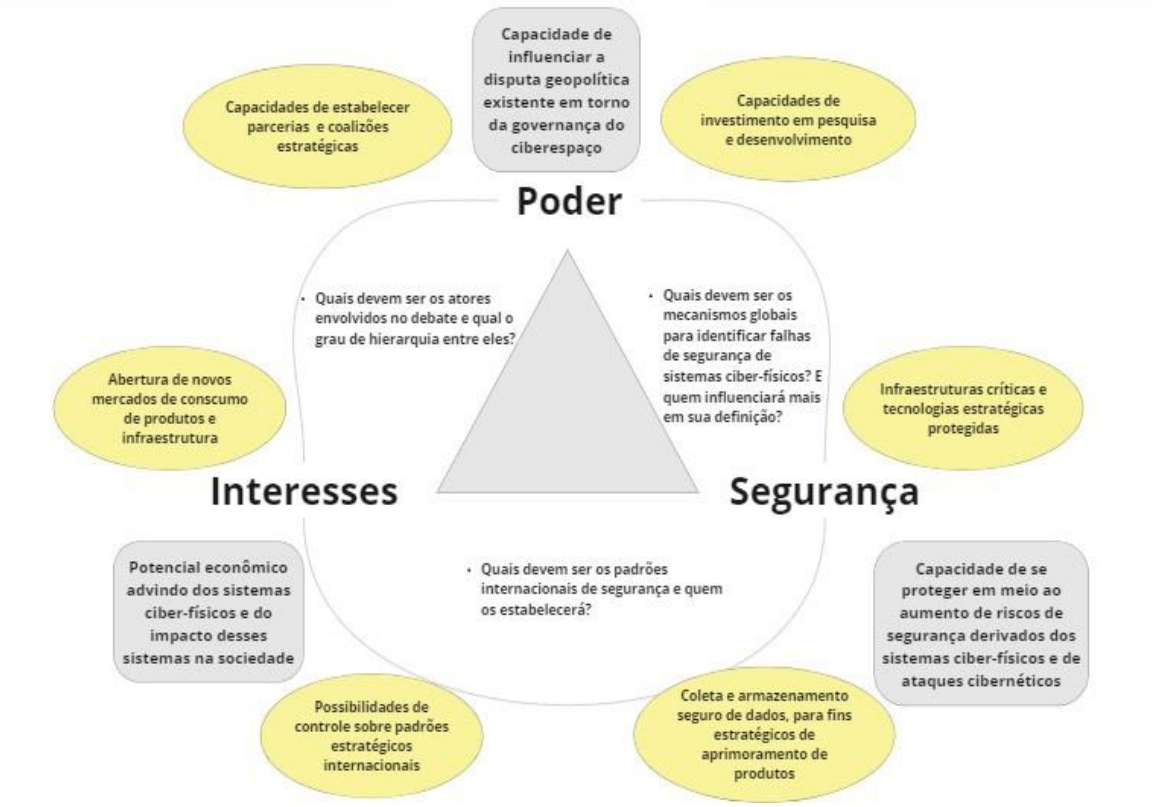
Quadro 15 - Compilação dos posicionamentos dos países analisados sobre governança e sobre sistemas ciber-físicos (conclusão)

Estado	Visão voltada para governança cibernética	Visão voltada para sistemas ciber-físicos
China	• Posicionamento favorável à governança multilateral, com a UN sendo o principal fórum e a ITU a principal reguladora; • Aproximação com a Rússia em relação às visões de governança; • Lançou a Global Data Security Initiative para definir princípios de segurança de dados globais. • Visa se colocar como parceiro confiável globalmente, através do fornecimento de novas tecnologias como o 5G; • Vê como inaceitáveis limitações à sua soberania cibernética; • Acreditam que as empresas devem se adequar à legislação dos países em que se estabelecem e não devem armazenar em território de um país dados coletados no exterior. • Defesa do desenvolvimento tecnológico e inovação como um Direito Humano; • Estabelecimento de parcerias dentro da Belt and Road Initiative; • Defende o direito dos Estados de moderar a internet sob sua soberania para garantir a ordem e a segurança nacional.	• Vê a IoT como essencial para seus planos de se tornar “Digital China”; • Está fazendo grandes esforços para proteção de dados relacionados à IoT; • Vem abordando a IoT como estratégica desde 2009, dialogando com o plano de desenvolvimento do país; • Já elaborou seis White Papers específicos para monitorar a situação da IoT no país, assim White Papers específicos para temas como Internet de Veículos; • Vem fazendo esforços para implementar padrões de IoT em âmbito global; • IoT é mencionada como pilar da indústria em 90% dos planos de desenvolvimento de províncias e municípios do país; • Internet Industrial com tendência de crescimento dentro do país.
Austrália	• Também é país signatário da Declaração pelo Futuro da Internet; • Foco grande em *multistakeholderismo* como caminho para a governança do ciberespaço, em oposição direta ao multilateralismo proposto por China e Rússia; • Visa aumentar a conscientização e capacidades em termos de governança da Internet na região do Indo-Pacífico.	• Estabeleceu um código de conduta voluntário para IoT, em 2020. • Também tem falado sobre iniciativas de rotulagem de produtos e dispositivos; • IoT está entre os 5 campos nos quais a Austrália se propõe focar para que se torne uma economia e sociedade de liderança digital até 2030. • Possui um grande desejo econômico em se desenvolver e dominar a área de IoT, pois a enxerga como uma tecnologia capaz de criar empregos, gerar crescimento econômico e aumentar a produtividade. • Está considerando a adoção de normas obrigatórias de segurança IoT.

Fonte: Elaborado pelo autor

A partir disso, conseguimos observar com mais clareza como o ecossistema dos sistemas ciber-físicos e da governança do ciberespaço se enquadra em um cenário de **jogos de poder, interesses e segurança**, que se complementam e acontecem simultaneamente. A figura abaixo busca sistematizar essa relação:

Figura 5 - Ilustração de jogos de poder, segurança e interesses



Fonte: Elaborado pelo autor

Quando pensamos em poder, cabe lembrar dos critérios que configuram uma superpotência cibernética estabelecidos por Segal (2016). O autor fala de 1. Poder econômico e tecnológico (relacionado à capacidade de desenvolver elementos centrais ao sistema); 2. Tamanho da economia (relacionado a número de usuários); 3. Relações Público-Privadas sólidas. 4. A capacidade de investimento do Estado em inteligência; 5. Uma narrativa atrativa.

Dentro das disputas de governança da internet e de sistemas ciber-físicos, esses elementos dialogam e se conectam em maior ou menor grau. A narrativa, por exemplo, vem sendo central nos documentos oficiais e posicionamentos internacionais dos países analisados.

Um exemplo claro é a disputa em torno da temática dos direitos humanos, que é abordada tanto em documentos do Ocidente quanto nos da China, mas com focos diferentes. Enquanto nos primeiros o foco é em liberdade de expressão online, na China o foco é no direito ao desenvolvimento como direito humano. Desse modo, da mesma maneira com que o Ocidente busca enfraquecer a China nos debates de governança por conta de suas restrições de conteúdo, a China busca enfraquecer o Ocidente por conta de suas ações unilaterais, como banimentos de empresas, apontadas como obstáculo para que prevaleça o direito ao desenvolvimento.

Sob essa ótica, a construção de coalizões pode ser percebida como uma tentativa de fortalecer uma narrativa comum para, a partir dela, ter mais sucesso em implementar sua visão para a governança. Um exemplo claro está na proposta do *Programme of Action* que, apesar da oposição da Rússia, contou com o apoio de 40 países, e tende a ser implementado após 2025. Venceu ali a coalizão mais forte, a narrativa mais forte. Foi exercido poder.

Olhando mais especificamente para o desenvolvimento de sistemas ciber-físicos, os elementos 1 e 3 que Segal aponta para poder também dialogam diretamente com “interesses” envolvidos no processo. Ao falar de interesses, é preciso ter em mente que o mercado de IoT tem grande potencial lucrativo e também grande potencial em melhorar a qualidade de serviços, tanto privados quanto públicos. Ou seja, avançar dentro desse mercado o quanto antes é estratégico tanto para atores públicos quanto para atores privados.

É preciso cuidado, contudo, quando se pensa em atores privados na liderança desse processo pois, como vimos, muitos deles, na pressa de lançar produtos, abrem mão de elementos securitários relevantes. Desse modo, parcerias público-privadas efetivas, na qual haja investimento Estatal e entes privados com capacidade técnica de se colocar à frente no mercado emergente por um lado, e padrões de segurança efetivos, incentivados e fiscalizados pelo Estado, de outro, se torna algo fundamental para gerar as capacidades de desenvolver os elementos centrais desse sistema (os produtos ciber-físicos) e nele prevalecer.

Dificuldades de investimento, por sua vez, se tornam barreiras nesse sistema. A Rússia possivelmente encontrando mais dificuldades em meio aos seus cenários de conflitos e eventuais sanções atreladas. Cabe lembrar que, ao falar de novas tecnologias, estamos falando de potenciais bilionários de mercado. Ou seja, alcançar

esses mercados de forma rápida e efetiva é estratégico para usufruir das vantagens que ele possibilita.

O outro elemento que compõe esse ecossistema é o da segurança, amplamente abordado ao longo deste trabalho. Ele passa tanto por garantir a proteção interna de sistemas ciber-físicos e, consequentemente, evitar danos físicos e econômicos derivados de ataques aos mesmos, quanto por, ao fazer isso, desenvolver padrões que garantam essa segurança e possam ser exportados e consolidados globalmente. Como pode-se perceber através da presença do termo em todos os países, hoje podemos entender que a principal disputa em torno dos sistemas ciber-físicos está na consolidação desses padrões. Estados que conseguirem se colocar nesse espaço rapidamente, tendem a colher os frutos políticos e econômicos tornando-se referências globais sobre o tema.

Como podemos ver através dos dados de receitas de IoT, na Tabela 1, hoje esses frutos estão sendo majoritariamente colhidos por Estados Unidos e China. Cabe observar como isso se modificará nos próximos anos.

Tabela 1 - Dados de receita de IoT por país

País	**Receita 2024**	**Usuários da Internet em 2022**	**População total 2022**
Estados Unidos[219]	US$ 199 bilhões	297.322.868 *dado de 2020	331.002.651 *dado de 2020
Reino Unido[220]	US$ 31,17 bilhões	65.045.228	68.468.662
China[221]	US$ 175,30 bilhões	1.010.740.000	1.448.314.408
Rússia[222]	US$ 19,67 bilhões	Sem dados disponíveis	Sem dados disponíveis
Austrália[223]	US$ 17,81 bilhões	23.391.152	25.990.169

Fonte: Elaborada pelo autor com base em dados do Statista (2024) e Internet World Stats (2022)[224]

[219] Dados de receita de IoT dos EUA. Disponível em: https://www.statista.com/outlook/tmo/internet-of-things/united-states Acesso em: 01 jan. 2024.

[220] Dados de receita de IoT do Reino Unido. Disponível em: https://www.statista.com/outlook/tmo/internet-of-things/united-kingdom

[221] Dados de receita de IoT da China. Disponível em: https://www.statista.com/outlook/tmo/internet-of-things/china Acesso em: 01 jan. 2024.

[222] Dados de receita de IoT da Russia. Disponível em: https://www.statista.com/outlook/tmo/internet-of-things/russia Acesso em: 01 jan. 2024.

[223] Dados de receita de IoT da Austrália. Disponível em: https://www.statista.com/outlook/tmo/internet-of-things/australia Acesso em: 01 jan. 2024

[224] Estatística do uso da Internet no mundo. Disponível em: https://www.internetworldstats.com/stats.htm Acesso em: 01 jan. 2024

5 CONSIDERAÇÕES FINAIS

> Com a combinação de enormes quantidades de dados e a crescente capacidade de monitorar indivíduos—na web, por meio de telefones móveis, através de câmeras de circuito fechado—parecemos estar deslizando para uma "sociedade de vigilância". A questão que temos que enfrentar é: por quem queremos ser vigiados: um governo, uma corporação, um hacker? Não há limites para a nossa tecnologia. (SEGAL, 2016, p 33)[225]

Assim como em outros momentos históricos da humanidade, estamos vivendo um momento de ruptura e reconstrução da forma como vivemos em sociedade. As novas tecnologias mudarão como nos relacionamos com o espaço e com a realidade ao nosso redor e, ao mesmo passo em que trazem benefícios inegáveis, em termos de qualidade de vida, também trazem riscos securitários para diversos aspectos sociais, desde os mais voltados a indivíduos até os mais voltados para Estados Nacionais.

Diante desse cenário, essa dissertação visou contribuir ao debate sobre uma dessas tecnologias - os sistemas ciber-físicos ou, mais popularmente, a Internet das Coisas. Esse tema tende a estar cada vez mais em voga nos próximos anos e pode ser olhado a partir de múltiplas lentes - como a econômica e a geopolítica - e de múltiplos atores - como Estados Nacionais, empresas multinacionais, e a própria sociedade civil, e se insere em um debate de governança que o precede em algumas décadas. A partir da perspective de diferentes Estados Nacionais, podemos perceber que o tema vem ganhando destaque ao longo do tempo e tende a continuar assim. Em alguns Estados, como o Reino Unido, legislações sobre os sistemas ciber-físicos já serão obrigatórias em 2024, ano de escrita dessa dissertação. Não será surpresa se Australia e Estados Unidos seguirem o mesmo caminho na próxima década, dada a proximidade dos posicionamentos adotados por esses países no campo da governança cibernética. Por sua vez, China e Rússia também percebem a relevância do tema e, com suas formas e desafios, também estão depositando energia e recursos nele.

O capítulo 4 desta dissertação buscou, justamente, trazer luz para as semelhanças e diferenças dos posicionamentos destes países, tidos como potências

[225]Em inglês: "With the combination of massive amounts of data and the growing ability to monitor individuals—on the web, via mobile phones, through closed circuit cameras—we appear to be sliding into a "surveillance society." The question we have to face is, by whom do we want to be surveilled: a government, a corporation, a hacker? There are no limits to our technology".

cibernéticas pelo *Cyber Power Index*, do Belfer Center, através de seus documentos oficiais voltados para a temática cibernética. Anteriormente a ele, o capítulo 3 se debruçou sobre o conceito dos sistemas ciber-físicos, apontando suas principais características e como eles trazem novos dilemas para o debate de governança. Cada vez mais se torna difícil encontrar um espaço que esteja desconectado do espaço cibernético. Como Laura DeNardis traz em seu livro, usado como uma das principais referências neste trabalho, vivemos a era da "*internet in everything"* e, nessa era, a privacidade tende a se tornar cada vez mais rara, em meio a coletas massivas de dados por aparelhos que, há algumas décadas, não se imaginava que poderiam fazer isso, como aspiradores e geladeiras. Da mesma forma, cresce a probabilidade de ataques em meios cibernéticos trazerem danos físicos, uma vez que aparelhos físicos e com capacidade motora, passam a estar conectados a uma rede global.

E todo esse quadro se monta em um cenário de governança que, como apontado pelo capítulo 2, vem sendo fruto de inúmeros debates ao longo das últimas décadas. Diante de um ambiente complexo, que, em essência, demanda uma série de protocolos e processos para funcionar, também há um elemento comercial e securitário essencial, que, ao longo dos últimos anos, vem aproximando um campo que nasceu com a promessa de "anarquia" de um cenário de maior controle por parte de Estados Nacionais.

É em meio a isso que se constitui um cenário de disputa de "poder, interesses e segurança", ilustrado na Figura 5, que sistematiza as principais descobertas obtidas a partir da análise dos documentos e da bibliografia utilizada. Poder, relacionado a controle e influência geopolítica e econômica sobre os rumos que a governança do ciberespaço e dos sistemas ciber-físicos devem ter; interesses relacionados à obtenção de vantagens políticas e econômicas dentro desse ambiente; e segurança relacionada a preservação de individuo, dados, infraestrutura e padrões nacionais, em meio à novas vulnerabilidades que surgem.

Apesar de contribuir ao debate, esta dissertação está longe de ter esgotado as discussões sobre o tema. Há uma série de caminhos de pesquisa a serem seguidos pelo autor ou por qualquer leitor desta dissertação que tenha interesse na área. Algumas sugestões de pesquisa possíveis são:

- Observar as perspectivas de governança e de sistemas ciber-físicos a partir de outros países e blocos. A União Europeia, apesar de não ter

sido trabalhada aqui pelo critério de escolha adotado, é uma das referências na temática. Pode-se observar a fundo seus documentos, comparando com as tabelas aqui apresentadas.

- Cabe olhar também para como os sistemas ciber-físicos vêm sendo abordados em grupos e fóruns regionais. Que tipos de coalizões estão sendo formadas no âmbito da governança e que impacto elas podem ter regionalmente?
- Outro caminho possível é o de fazer um esforço semelhante ao feito aqui para observar outras tecnologias emergentes que estão sendo citadas nos documentos e de igual potencial político econômico, como computação quântica, e inteligência artificial. No fim, essas tecnologias se complementam e dialogam entre si, sendo parte de um sistema complexo que carece ser trabalhado como um todo.
- Cabe também pesquisas de maior aprofundamento em aspectos mais técnicos do debate de sistemas ciber-físicos, mas voltados para o campo das Relações Internacionais. Há muito material dentro das ciências exatas, mas poucos trabalhos como o de DeNardis, que abordam o impacto desses elementos técnicos em um âmbito global e político de forma qualificada. Observar como as disputas políticas por padronizações e controles de mercado estão se dando em cada área (indústria, saúde, educação, veículos, etc.) pode trazer resultados ricos, tanto em termos quantitativos, como qualitativos;
- Há também espaço para dar atenção ao aspecto conceitual/terminológico do tema. Quais países usam “sistemas ciber-físicos”, quais usam “internet das coisas”, quais usam “smart”, e quais as diferenças nas definições de cada um deles;
- Cabe, por fim, um aprofundamento sobre as principais empresas e organismos multinacionais dentro do ramo dos sistemas ciber-físicos. Como elas estão contribuindo para os padrões? E qual seu real poder de influência frente aos Estados Nacionais? Dentro do portal da OEWG há *statements* interessantes nesse sentido, que podem servir de base para uma pesquisa mais aprofundada.

Olhar para o mundo ao nosso redor, para as *smart houses* de Porchat, e identificar novas perguntas é um exercício interessante para qualquer pessoa que consiga perceber esse momento histórico, sem se deixar ser engolida por ele.

REFERÊNCIAS

ADB. **The 14th Five-Year Plan of the People's Republic of China —Fostering High-Quality Development**. Disponível em: <https://www.adb.org/sites/default/files/publication/705886/14th-five-year-plan-high-quality-development-prc.pdf>. Acesso em 07 jan. 2024.

ANNA, Zharova; VLADIMIR, Elin. State regulation of the IoT in the Russian Federation: Fundamentals and challenges. **International Journal of Electrical and Computer Engineering**, v. 11, n. 5, p. 4542-4549, 2021.

ATLANTIC COUNCIL. **The 5×5—The Internet of Things and national security**. 2022. Disponível em: <https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-the-internet-of-things-and-national-security/>. Acesso em 20 jul. 2023.

AUSTRALIA. **Australia's International Cyber Engagement Strategy**. 2017. Disponível em: <https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf>. Acesso em 05 dez. 2023.

AUSTRALIA. **Australia's Cyber Security Strategy**. 2020a. Disponível em: <https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf>. Acesso em 05 de dez. 2023.

AUSTRALIA. **Code of Practice. Securing the Internet of Things for Consumers**. 2020b. Disponível em: <https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf>. Acesso em 05 dez. 2023.

AUSTRALIA. **Australia's international cyber and critical technology engagement across Government is guided by the International Cyber and Critical Technology Engagement Strategy**. 2021a. Disponível em: <https://www.internationalcybertech.gov.au/strategy>. Acesso em 05 dez. 2023.

AUSTRALIA. **Digital economy strategy 2030.** 2021b. Disponível em: <https://apo.org.au/node/312247>. Acesso em 05 dez. 2023.

AUSTRALIA. **2023–2030 Australian Cyber Security Strategy 2023.** Disponível em: <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf>. Acesso em 10 dez. 2023.

BARLOW, John Perry et al. **A Declaration of the Independence of Cyberspace.** 1996. Disponível em: <https://www.eff.org/cyberspace-independence>. Acesso em 10 jan. 2024.

BARTLES, Charles K. Getting Gerasimov Right. **Military Review**, v. 96, n. 1, p. 30-38, 2016.

BELF CENTER**. National Cyber Power Index 2022**. 2023. Disponível em:<https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf>. Acesso em 20 jul. 2023.

BLACKBERRY. **Global Threat Intelligence Report 2023.** 2023. Disponível em: <https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/bbcomv4/blackberry-com/en/solutions/threat-intelligence/2023/threat-intelligence-report-august/Blackberry-Global-Threat-Intelligence-Report-August-2023.pdf.> Acesso em 16 fev. 2024.

BRANDÃO, Hemerson. **IoT movimentará US$ 650 bilhões no mundo até 2026, mas Brasil tem gargalo.** Gizmodo.uol, 2022. Disponível em: <https://gizmodo.uol.com.br/iot-movimentara-us-650-bilhoes-no-mundo-ate-2026-mas-brasil-tem-gargalo/.> Acesso em 10 jan. 2024.

CAICT (China Academy for Information and Communications Technology). 2020. **White Paper on Internet of Things (2020)**. Disponível em: <http://www.caict.ac.cn/english/research/whitepapers/202012/t20201223_366678.html>. Acesso em 10 fev. 2024.

CANABARRO, Diego Rafael. **Governança global da Internet:** tecnologia, poder e desenvolvimento. 2014a.

CANABARRO, Diego Rafael. **Um panorama da governança global da internet a partir de 2014.** 2014b.

CANABARRO, Diego. **Governança Global da Internet: Aspectos Conceituais, Questões da Agenda Contemporânea e Prospectos para o Estudo do Tema.** INTERNET GOVERNANCE IN THE GLOBAL SOUTH, p. 74, 2018.

CARR, Madeline. Power plays in global internet governance. **Millennium,** v. 43, n. 2, p. 640-659, 2015.

CASO, Jeffrey; COLE, Zina; PATEL, Mark; ZHU, Wendy. **Cybersecurity for the IoT: How trust can unlock value.** McKinsey & Company, 7 abr. 2023. Disponível em: <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/cybersecurity-for-the-iot-how-trust-can-unlock-value#/>. Acesso em 10 fev. 2024.

CHEN, John et al. **China's Internet of Things.** Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission. October 2018.

CHINA. **National Cyberspace Security Strategy,** 2016. Disponível em: <https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/> Acesso em 20 jul. 2023.

CHINA. **Discurso da delegação chinesa na primeira reunião do Grupo de Trabalho Aberto das Nações Unidas sobre Segurança da Informação sobre a avaliação de ameaças no ciberespaço** (14 de dezembro de 2021, Sala 2)中国代表团在联合国信息安全开放式工作组首次会议关于网络空间威胁评估的发言 （2021 年 12 月14 日，2 号会议室). 2021.

CHINA. **The Central Committee of the Communist Party of China and the State Council issued the "Overall Layout Plan for the Construction of Digital China" (**

中共中央 国务**院印**发《**数字中国建**设**整体布局**规划**).** 2023a. Disponível em: <https://www.gov.cn/zhengce/2023-02/27/content_5743484.htm>. Acesso em 09 fev. 2024.

CHINA. **Full text: China's Law-Based Cyberspace Governance in the New Era**. 2023b. Disponível em: <http://www.scio.gov.cn/zfbps/zfbps_2279/202303/t20230320_709283.html#:~:text=Marked%20improvements%20have%20been%20made,and%20an%20effective%20supporting%20system.>. Acesso em 05 fev. 2024.

CISA. **Cybersecurity and Infrastructure Security Agency Strategic Plan 2023 - 2025**. 2022. Disponível em: <https://www.cisa.gov/sites/default/files/publications/StrategicPlan_20220912-V2_508c.pdf>. Acesso em 15 jan. 2024.

CISCO. **Midyear Cybersecurity Report**. 2017. Disponível em: <https://www.cisco.com/c/dam/m/en_in/products/security/pdfs/executive-summary-071417.pdf>. Acesso em 10 jan. 2024.

DENARDIS, Laura. Introduction**. Who Runs the Internet? The Global Multistakeholder Model of Internet Governance**. 2016.

DENARDIS, Laura. **The Internet in everything**. Yale University Press, 2020.

DENARDIS, Laura; RAYMOND, Mark. **Thinking clearly about multistakeholder internet governance.** In: GigaNet: Global Internet Governance Academic Network, Annual Symposium. 2013.

DENARDIS, Laura; RAYMOND, Mark. The internet of things as a global policy frontier. **UCDL Rev**., v. 51, p. 475, 2017.

DIGICHINA. Knowledge Base: **China's 'Global Data Security Initiative' 全球数据安全倡**议**.** Stanford University. 2022a. Disponível em: <https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/>. Acesso em jan. de 2024.

DIGICHINA. **Translation: 14th Five-Year Plan for National Informatization – Dec. 2021.** 2022b. Disponível em: <https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/>. Acesso em 07 fev. 2024.

ESTADOS UNIDOS. Departamento de Segurança Interna. **Strategic Principles for Securing the Internet of Things (IoT)**. 2016. Disponível em: <https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf.> Acesso em 01 jan. 2024.

ESTADOS UNIDOS. U.S. **Department of Homeland Security Cybersecurity Strategy**. 2018. Disponível em: <https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf>. Acesso em 10 jan. 2024.

ESTADOS UNIDOS. **Federal Cybersecurity Research and Development Strategic Plan.** 2019. Disponível em: <https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf>. Acesso em 10 jan. 2024.

ESTADOS UNIDOS. Congresso. **Internet of Things Cybersecurity Improvement Act of 2020.** Public Law 116–207, 116th Congress. 04 de dezembro de 2020. Disponível em: <https://www.congress.gov/bill/116th-congress/house-bill/1668/text.> Acesso em 01 jan. 2024.

ESTADOS UNIDOS. **Executive Order on Improving the Nation's Cybersecurity.** 12 maio 2021. Disponível em: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.> Acesso em 01 jan. 2024.

ESTADOS UNIDOS. **Declaration for the Future of the Internet**. 2022a. Disponível em: <https://www.state.gov/declaration-for-the-future-of-the-internet>. Acesso em 10 fev. 2024.

ESTADOS UNIDOS. **Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers.** 2023a. Disponível em: <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/.> Acesso em 01 jan. 2024.

ESTADOS UNIDOS. **National Cybersecurity Strategy.** 2023b. Disponível em: <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>. Acesso em 10 fev. 2024.

ESTADOS UNIDOS. **National Cybersecurity Strategy Implementation Plano**. 2023c. Disponível em: <https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf>. Acesso em 10 fev. 2024.

FEDERAÇÃO RUSSA, Decreto Presidencial. **Doctrine of Information Security of the Russian Federation** (Doutrina da Segurança da Informação da Federação Russa), nº 646, 5 de Dezembro de 2016. Disponível em: <https://www.mid.ru/en/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/2563163>. Acesso em 20 jul. 2023.

FEDERAÇÃO RUSSA. **Strategy for the Development of the Information Society in the Russian Federation 2017 - 2030.** 2017. Disponível em: <http://static.kremlin.ru/media/acts/files/0001201705100002.pdf>. Acesso em 01 fev. 2024.

FEDERAÇÃO RUSSA.. **Fundamentals of the state policy of the Russian Federation in the field of international information security (Основы государственной политики Российской Федерации в области международной информационной безопасности).** 2021. Disponível em: <http://www.scrf.gov.ru/security/information/document114/>. Acesso em 10 fev. 2024.

FEDERAÇÃO RUSSA, CHINA. J**oint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development.** 2022. Disponível em: <http://en.kremlin.ru/supplement/5770>. Acesso em 10 jan. 2024.

FEDERAÇÃO RUSSA. **Statement by the representative of the Russian Federation at the informal intersessional meeting of the Open-ended Working Group on Security of and in the Use of ICTs 2021-2025**. New York, 6 dez. 2022.

FEDERAÇÃO RUSSA. **Position of the Russian Federation on the "Programme of Action to advance responsible State behaviour in the use of information and communications technologies in the context of international security**. 2023.

FEDERAÇÃO RUSSA, BELARUS, SÍRIA, COREIA DO NORTE, NICARÁGUA. **Updated Concept of the Convention of the United Nations on Ensuring International Information Security.** 2023. Disponível em: <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention_on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf>. Acesso em 10 fev. 2024.

FIGUEIREDO, D.; RÊ, E. de; MENEZES, T. B. de. **A Rússia, o Ciberespaço e uma estratégia nacional.** Rede CTIDC. 2019. Disponível em: <https://redectidc.com.br/assets/files/rede-ctidc-a-russia-o-ciberespaco-e-uma-estrategia-nacional.pdf> Acesso em 01 jan. 2024.

FONSECA, Daniel Farias de; ROCHA, Marcio. The Cyber Issue and Realist Thinking. **R. Esc. Guerra Nav**, Rio de Janeiro, v.25, n.2, p. 517-543, 2019.

FORBES. **E-commerce global pode movimentar US$ 3,4 tri em 2025**. 2021. Disponível em: <https://forbes.com.br/forbes-tech/2021/01/e-commerce-global-pode-movimentar-us-34-tri-em-2025-retailtechs-americanas-brf-muito-mais/>. Acesso em 09 agost. 2023.

GSMA. **How China is Scaling the Internet of Things**. 2015. Disponível em: <https://www.gsma.com/newsroom/wp-content/uploads/16531-China-IoT-Report-LR.pdf>. Acesso em 05 dez. 2023.

HAGGART, Blayne; TUSIKOV, Natasha; SCHOLTE, Jan Aart (Ed.). **Power and authority in internet governance: return of the state?**. Routledge, 2021.

HOME AFFAIRS. 2024. **Voluntary Code of Conduct**. Disponível em: <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice>. Acesso em 01 jan. 2024.

HUREL, Louise Marie. **Cybersecurity and internet governance: Two competing fields?**. Available at SSRN 3036855, 2016.

HUREL, Louise Marie; LOBATO, Luisa Cruz. **Cyber-norms entrepreneurship? Understanding Microsoft's advocacy on cybersecurity**. Governing Cyberspace:

Behaviour, Power and Diplomacy, 2020.

INATINI et al. **Governance Principles for a Society Based on Cyber-Physical Systems. 2023.** Disponível em: <https://cislp.law.kyoto-u.ac.jp/cislp/files/Governance-Principles-for-a-Society-Based-on-Cyber-Physical-Systems_20230426.pdf>. Acesso em 20 jul. 2023.

ISO. **Cyber-physical systems**. 2023. Disponível em: <https://www.iso.org/foresight/cyber-physical-systems.html>. Acesso em 01 jan. 2024.

KONIAGINA, Mariia et al. Measures to Ensure Cybersecurity and Regulation of the Internet of Things in the Russian Federation: Effectiveness Assessment. **Journal of Economic Issues**, v. 57, n. 1, p. 257-274, 2023.

KUPTSOVA, Arina. **Правовое регулирование использования интернета вещей** (Legal Regulations on the use of Internet of Things). Образование и право, n. 7, p. 225-230, 2021. Disponível em: <https://cyberleninka.ru/article/n/pravovoe-regulirovanie-ispolzovaniya-interneta-veschey/viewer>. Acesso em 01 jan. 2024.

LIBICKI, Martin C. **Cyberdeterrence and cyberwar**. RAND corporation, 2009.

MALWAREBYTES. **What is Mirai Botnet.** Disponível em: <https://www.malwarebytes.com/what-was-the-mirai-botnet>. Acesso em 16 fev. 2024.

MCKENDRICK, Joe. **Malware Attacks Against IoT Devices Quadruple**. Disponível em: <https://www.rtinsights.com/malware-attacks-against-iot-devices-quadruple/.> Acesso em 16 fev. 2024.

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. A Trindade Conceitual Fundamental do Ciberespaço. **Contexto Internacional**, v. 42, p. 31-54, 2020.

MERICS. C**hina's Global Initiative on Data Security has a message for Europe.** 24 de setembro de 2020. Disponível em: <https://merics.org/en/comment/chinas-global-initiative-data-security-has-message-europe>. Acesso em 01 jan. 2024.

MINERVA, Roberto; BIRU, Abyi; ROTONDI, Domenico. Towards a definition of the Internet of Things (IoT). **IEEE Internet Initiative,** v. 1, n. 1, p. 1-86, 2015.

MINISTÉRIO DE RELAÇÕES EXTERIORES DA CHINA. **China's Positions on International Rules-making in Cyberspace**. 2021. Disponível em: <https://www.fmprc.gov.cn/eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html>. Acesso em 08 fev. 2024.

MINISTÉRIO DAS RELAÇÕES EXTERIORES DA CHINA. **China's Positions on Global Digital Governance.** 25 de maio de 2023. Disponível em: <https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202305/t20230525_11083607.html.> Acesso em 01 jan. 2024.

MINISTÉRIO DAS RELAÇÕES EXTERIORES DA CHINA. **Iniciativa Global de**

Segurança de Dados (全球数据安全倡议). 2024. Disponível em: <https://www.mfa.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/zclc_674645/qt_674659/202010/t20201029_7669146.shtml. 2024 (última atualização).> Acesso em 01 jan. 2024.

MINISTRY OF THE HIGHER EDUCATION AND SCIENCE DENMARK. C**hina IoT Nation - AI and Big Data**. 2019. Disponível em: <https://icdk.dk/-/media/websites/icdk/locations-reports/shanghai/2020_china_iot-nation_ai-and-big-data.ashx>. Acesso em 10 fev. 2024.

MUELLER, Milton. Is cybersecurity eating internet governance? Causes and consequences of alternative framings. **Digital Policy, Regulation and Governance**, v. 19, n. 6, p. 415-428, 2017.

MUELLER, Milton; BADIEI, Farzaneh. **Inventing Internet Governance:** The Historical Trajectory of the Phenomenon and the Field. Researching Internet Governance: Methods, Frameworks, Futures, p. 59-83, 2020.

NEW SOUTH WALES. **Internet of Things (IoT) Policy Guidance.** 2021. Disponível em: <https://www.digital.nsw.gov.au/sites/default/files/2022-09/iot-policy-guidance.pdf>. Acesso em 10 jan. 2024.

NIST. Framework for Cyber-Physical Systems**:** Volume 1, Overview, Version 1.0. **Cyber-Physical Systems Public Working Group,** Smart Grid and Cyber-Physical Systems Program Office, Engineering Laboratory. Junho 2017. Disponível em: <https://doi.org/10.6028/NIST.SP.1500-201.> Acesso em 01 jan. 2024.

NOCETTI, Julien. Contest and conquest: Russia and global internet governance. **International Affairs**, v. 91, n. 1, p. 111-130, 2015.

NYE JR, Joseph S. **Cyber power**. Harvard Univ Cambridge MA Belfer Center for Science and International Affairs, 2010.

NYE, Joseph S. Th**e regime complex for managing global cyber activities.** Global Commission on Internet Governance, 2014.

OTAN. **Allied Joint Doctrine for Cyberspace Operations**. 2020. Disponível em: <https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320>. Acesso em 24 ago. 2021.

PADINGER, Germán. **Understand what Aukus is, a security pact between Australia, the United Kingdom, and the USA.** CNN Brasil. March 15, 2023. Available at: <https://www.cnnbrasil.com.br/internacional/entenda-o-aukus-pacto-de-seguranca-entre-a-australia-reino-unido-e-eua/.> Acesso em 01 jan. 2024.

PANKOV, Vladimir. **Internet of Things awaiting 5G**. RPC+, 16 set. 2019. Disponível em: <https://plus.rbc.ru/news/5d6ef4f77a8aa969578cfc82.> Acesso em 10 jan. 2024.

PIJOVIĆ, Nikola. **The Cyberspace 'Great Game'. The Five Eyes, the Sino-Russian Bloc and the Growing Competition to Shape Global Cyberspace Norms**. In: 2021 13th International Conference on Cyber Conflict (CyCon). IEEE,

2021. p. 215-231.

PODER360. **Justiça sueca proíbe venda de equipamentos 5G da Huawei.** 2022. Disponível em: <https://www.poder360.com.br/tecnologia/justica-sueca-proibe-venda-de-equipamentos-5g-da-huawei/.> Acesso em 01 jan. 2024.

POSSA, Julia. **Huawei e ZTE, da China, estão banidas dos EUA pelo governo Biden.** Gizmodo, 2022. Disponível em: <https://gizmodo.uol.com.br/huawei-e-zte-da-china-estao-banidos-dos-eua-pelo-governo-biden/.> Acesso em 1 jan. 2024.

PWC. **Internet das Coisas na Rússia(IoT) в России)**. 2017. Disponível em: <https://media.rbcdn.ru/media/reports/IoT-inRussia-research_rus.pdf>. Acesso em 10 jan. 2024.

REINO UNIDO. **National Cyber Security Strategy 2016 - 2021**. 2016. Disponível em: <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>. Acesso em 10 jan. 2024.

REINO UNIDO. **Code of practice for Consumer IoT Security.** 2018. Disponível em: <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security>. Acesso em 10 jan. 2024.

REINO UNIDO. **National Cyber Strategy 2022**. 2022. Disponível em: <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022>. Acesso em 10 fev. 2024.

REINO UNIDO. **Collection Secure by Design. 2024**. Disponível em: <https://www.gov.uk/government/collections/secure-by-design>. Acesso em 05 dez. 2023.

RID, Thomas. Cyber war will not take place**. Journal of strategic studies**, v. 35, n. 1, p. 5-32, 2012.

RID, Thomas. **Rise of the machines:** A cybernetic history. WW Norton & Company, 2016.

RÚSSIA; CHINA. **Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development.** 4 de fevereiro de 2022. Disponível em: <http://en.kremlin.ru/supplement/5770>. Acesso em 20 fev. 2024.

SAMSUNG. **Samsung lança campanha com Fabio Porchat e João Vicente para mostrar os benefícios de uma vida conectada com SmartThings**. Samsung Newsroom Brasil, 2023. Disponível em: <https://news.samsung.com/br/samsung-lanca-campanha-com-fabio-porchat-e-joao-vicente-para-mostrar-os-beneficios-de-uma-vida-conectada-com-smartthings.> Acesso em 01 jan. 2024.

SECTOR, STANDARDIZATION; ITU, O. F. Series y**:** Global information infrastructure, internet protocol aspects and next-generation networks next generation networks–frameworks and functional architecture models**.** International Telecommunication Union, Geneva, Switzerland, **Recommendation ITU-T Y**, v. 2060, 2012.

SEGAL, Adam. **The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age**. Hachette UK, 2016.

SHAPIRO, Scott J. **The Strange Story of the Teens Behind the Mirai Botnet.** 2023. Disponível em: <https://spectrum.ieee.org/mirai-botnet>. Acesso em 16 fev. 2024.

SILVA, Victor Hugo. **Entenda riscos para a sua internet caso Fortaleza crie usina perto de cabos submarinos**. G1, 2023. Disponível em: <https://g1.globo.com/tecnologia/noticia/2023/10/03/entenda-riscos-para-a-sua-internet-caso-fortaleza-crie-usina-perto-de-cabos-submarinos.ghtml>. Acesso em 10 dez. 2023.

SMID, Henk H.F. **Internet of Things:** the China perspective**.** The Space Review, 17 abr. 2023. Disponível em: https://www.thespacereview.com/article/4566/1. Acesso em 15 fev. 2024.

STANDARDS AUSTRALIA. **Standards Australia and the Internet of Things Alliance Australia welcome 2023-2030 Cyber Security Strategy.** 2023. Disponível em: <https://www.standards.org.au/news/standards-australia-and-the-internet-of-things-alliance-australia-welcome-2023-2030-cyber-security-strategy>. Acesso em 5 jan. 2024.

STATISTA. **Internet of Things Market Forescast**. 2024. Disponível em: <https://www.statista.com/outlook/tmo/internet-of-things>. Acesso em 10 fev. 2024.

TADVISER. **Cyber-Physical Systems Committee of Rosstandart.** Technical Committee of Cyber-Physical Systems (TC 194)**.** 2024. Disponível em: <https://tadviser.com/index.php/Company:Technical_Committee_of_Cyber-Physical_Systems_(TC_194).> Acesso em 10 jan. 2024.

THADANI, Trisha; SIDDHIQUI, Faiz; LERMAN, Rachel; SHEFTE, Whitney; WALL, Julia; TRACKIM, Talia. **Tesla worker killed in fiery crash may be first 'Full Self-Driving' fatality**. The Washington Post, 13 fev. 2024. Disponível em: <https://www.washingtonpost.com/technology/interactive/2024/tesla-full-self-driving-fatal-crash/.> Acesso em 14 fev. 2024.

THE ECONOMIST. **The digital side of the Belt and Road Initiative is growing.** 2020. Disponível em: <https://www.economist.com/special-report/2020/02/06/the-digital-side-of-the-belt-and-road-initiative-is-growing.> Acesso em 05 jan. 2024.

UNGGE. **Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.** 2021. Disponível em: <https://eucyberdirect.eu/atlas/sources/ungge-2021-report>. Acesso em 20 jul. 2023.

UNOEWG. **Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.** 2021. Disponível em: <https://disarmament.unoda.org/open-ended-working-group/>. Acesso em 20 jul. 2023.

WHITE HOUSE. **National Maritime Cybersecurity Plan to the National Strategy for Maritime Security.** 2020. Disponível para download em: <https://cyberpolicyportal.org/states/united-states-of-america>. Acesso em 10 jan. 2024.

WHITE HOUSE. **Executive Order on Improving the Nation's Cybersecurity** 2021. Disponível em: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>. Acesso em 10 jan. 2024.

WHITE HOUSE. **Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers**. 2023. Disponível em: <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/>. Acesso em 10 fev. 2024.

WOLF, Marilyn; SERPANOS, Dimitrios Nikolaou. **Safe and secure cyber-physical systems and internet-of-things systems**. Cham: Springer, 2020.

WSIS. **Tunis Agenda for Information Society.** 2005. Disponível em: <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>. Acesso em 05 abr. 2023.