UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE RELAÇÕES INTERNACIONAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

Raquel Cristina Jorge de Oliveira

Segurança e defesa cibernética: um estudo do caso brasileiro à luz de países nórdicos e Estônia

Brasília
2021

Raquel Cristina Jorge de Oliveira

Segurança e defesa cibernética: um estudo do caso brasileiro à luz de países nórdicos e Estônia

Dissertação submetida ao Programa de Pós-Graduação em Relações Internacionais da Universidade de Brasília para a obtenção do título de Mestre em Relações Internacionais.
Orientador: Prof. Dr. Antonio Jorge Ramalho da Rocha

Brasília
2021

Raquel Cristina Jorge de Oliveira

Segurança e defesa cibernética: um estudo do caso brasileiro à luz de países nórdicos e Estônia

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. Antonio Jorge Ramalho da Rocha, Dr.
Instituto de Relações Internacionais, Universidade de Brasília

Prof. Jorge Henrique Cabral Fernandes, Dr.
Departamento de Ciência da Computação, Universidade de Brasília

Prof. Eiiti Sato, Dr.
Instituto de Relações Internacionais, Universidade de Brasília

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. Dr. Antonio Jorge Ramalho da Rocha
Orientador

Brasília, 2021.

Este trabalho é dedicado à minha família, tanto aos membros humanos quanto aos caninos.

AGRADECIMENTOS

Meu desconforto com demonstrações públicas de afeto e gratidão é notório motivo de piada entre familiares e amigos. Eis que são janelas que dão para alma e, portanto, prefiro mantê-las abertas apenas àqueles tão próximos que não apenas conhecem essa particularidade minha, mas também gracejam de maneira tenra sobre minhas bobagens. Nesta ocasião, abro exceção para agradecer a todos que contribuíram para que este trabalho fosse concluído. É apenas justo que o faça.

Em primeiro lugar, por óbvio, agradeço minha amada família, a quem dedico a dissertação. O apoio incondicional de todos foi indispensável em todas as etapas dos estudos. Agradeço particularmente a paciência em escutar minhas infinitas lamúrias. Os puxões de orelha de minha mãe merecem nota, assim como o carinho de meus cachorrinhos Nino, Julieta e Luke, companhias constantes nos estudos solitários a que fomos forçados em razão das circunstâncias sanitárias.

Em segundo lugar, agradeço meu generoso orientador, Professor Doutor Antonio Jorge Ramalho da Rocha, mais conhecido nos corredores do Instituto de Relações Internacionais como AJ. Homem de fala pausada e certeira, sempre pronto a ajudar e fornecer as necessárias correções. Não poderia ter escolhido mentor melhor.

Não poderia deixar de mencionar, em terceiro lugar, as equipes das Embaixadas da Suécia, da Dinamarca, da Finlândia e da Noruega, que se mostraram absolutamente solícitas. Agradeço, em particular, Sua Excelência Johanna Brismar Skoog, Embaixadora da Suécia no Brasil, e Coronel Robert Persson, Adido de Defesa da Suécia no Brasil.

Em quarto lugar, agradeço ainda os entrevistados do Ministério das Relações Exteriores, do Ministério da Defesa e do Gabinete de Segurança Institucional (GSI), que muito gentilmente se dispuseram a contribuir para essa pesquisa. Não os mencionarei nominalmente, mas quero deixar registrada minha gratidão, ainda que de maneira genérica. Em particular, agradeço o colega Eduardo Izycki, que viabilizou o contato com o GSI.

Por fim, agradeço aos colegas do grupo de Estudos Críticos de Segurança. As aulas foram fundamentais para sedimentar ou repensar os conceitos e argumentos empregados aqui. Meu único lamento é esse encontro não ter-se dado mais cedo na pesquisa.

A todos, meus agradecimentos.

"*Big Brother is Watching You*."

(George Orwell)

RESUMO

Neste trabalho, buscou-se aplicar métodos qualitativos para entender de que maneira a estratégia brasileira para segurança e defesa cibernética está estruturada. Partindo-se do princípio de que ameaças cibernéticas são fundamentalmente híbridas e transversais, optou-se por recorte que examina como se organizam países nórdicos e Estônia nesse campo. Identificou-se que a abordagem *whole of society* é pilar importante de suas respectivas estratégias, de maneira que não se vislumbra o enfrentamento eficiente desses novos desafios cibernéticos, principalmente da interferência híbrida, sem profunda e constante coordenação multinível entre diferentes setores do governo, da iniciativa privada e da sociedade civil. Conclui-se que, ao traçar diagnóstico parcial do que são ameaças cibernéticas e não implementar medidas efetivas de coordenação nem mesmo no âmbito governamental, o Brasil se coloca de maneira vulnerável frente a desafio que se estenderá pelas próximas décadas, sob risco, inclusive, de militarizar a tratativa da questão.

Palavras-chave: Segurança. Defesa. Ameaças cibernéticas.

ABSTRACT

In this work, we sought to employ qualitative methods in order to understand how the Brazilian strategy for cyber security and defense is structured. Assuming cyber threats are fundamentally hybrid and transversal, we chose an approach that examines how Nordic countries and Estonia are organized in this area. It was identified that the whole of society concept is an important pillar of their respective strategies, so much so it hardly seems efficient to face these new cyber challenges, mainly hybrid interference, without deep and constant multilevel coordination between different sectors of the government, private businesses and civil society. It is concluded that, by making a partial diagnosis of what cyber threats are and not implementing effective coordination measures, even at the governmental level, Brazil puts itself in a vulnerable position when it comes to a challenge that will stretch well into the next decades, even risking militarizing its handling of the issue.

Keywords: Security. Defense. Cyber threats.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABIN	Agência Brasileira de Inteligência
AGU	Advocacia-Geral da União
Bacen	Banco Central do Brasil
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CGI.br	Comitê Gestor da Internet no Brasil
ComDCiber	Comando de Defesa Cibernética do Exército
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
Cepesc	Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações
CGU	Controladoria-Geral da União
CPLP	Comunidade dos Países de Língua Portuguesa
Creden	Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo
CSIRT	Computer Emergency Response Team
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DPF	Departamento de Polícia Federal
DSIC	Departamento de Segurança da Informação
E-ciber	Estratégia Nacional de Segurança Cibernética
EMCFA	Estado-Maior Conjunto das Forças Armadas
FCKS	Joint Cyber Coordination Centre da Noruega
FI	Sweden's Financial Supervisory Authority
FMV	Swedish Defence Material Administration
GGE	Group of Governmental Experts
GLO	Operações de garantia da lei e da ordem
GPD/LD	General Political Department/Liaison Department
ICANN	Internet Corporation for Assigned Names and Numbers
ICTs	Information and Communication Technologies
IoT	Internet of Things
IVO	The Health and Social Care Inspectorate
MD	Ministério da Defesa
MJ	Ministério da Justiça
MRE	Ministério das Relações Exteriores

MSB Civil Contingencies Agency da Suécia

MUST/FRA Serviços de inteligência e segurança da Suécia

NB8 Nordic and Nordic-Baltic

NSA National Security Agency

PCC Partido Comunista da China

PLA Exército de Libertação Popular da China

StratCom Strategic Communications Centre of Excellence

OAS Organização dos Estados Americanos

OCDE Organização para a Cooperação e Desenvolvimento Econômico

ONU Organização das Nações Unidas

OSCE Organização para a Segurança e Cooperação na Europa

OTAN Organização do Tratado do Atlântico Norte

PD&I Pesquisa, Desenvolvimento e Inovação

P&D Pesquisa e Desenvolvimento

Prosul Fórum para o Progresso e Desenvolvimento da América do Sul

PTS Swedish Post and Telecom Authority

SAE Secretaria de Assuntos Estratégicos

SLV The Swedish Food Agency

SMDC Sistema Militar de Defesa Cibernética

STEM Swedish Energy Agency

TI Tecnologia da Informação

TS Swedish Transport Agency

UE União Europeia

SUMÁRIO

1 INTRODUÇÃO

Em novembro de 2019, o projeto de pesquisa que apresentei à banca era significativamente distinto desta dissertação. A arguição dos Professores Doutores Eiiti Sato e Jorge Fernandes foi um divisor de águas na pesquisa, particularmente pela exortação para que o escopo do trabalho fosse aumentado. Lembro-me, em especial, da orientação do Prof. Dr. Sato, para quem os frutos de uma pesquisa acadêmica podem, sim, ter aplicabilidade prática. Não que sempre assim deva ser; do contrário, programas de pós-graduação seriam francamente utilitários. Não, o que marcou o ponto levantado pelo caro professor é que a pesquisa não deve servir de artifício para o encastelamento da comunidade acadêmica, tão específica que pouco se possa derivar dela. Cumpre olhar pela janela e contemplar as questões do mundo lá fora. Essa é minha tentativa de colocar em prática as valiosas orientações recebidas naquela tarde.

Dificilmente poderia ser considerado revolucionário afirmar que o mundo está digitalizado. Dependemos do espaço cibernético para executar boa parte das tarefas que compõem nosso cotidiano. Lazer, trabalho, estudos, burocracias do dia a dia, *internet banking*, ligação de vídeo para amigos e familiares, *smartphones*, redes sociais e eletrodomésticos inteligentes: esses são apenas alguns exemplos do quão ubíqua é a conexão com a rede mundial de computadores na vida contemporânea. Ora, hoje em dia até mesmo as lâmpadas domésticas podem ser controladas pela internet.

Quanto mais conectado um país é, maior a superfície de ataque para atores maliciosos, como aventou Nye (2010) quando tratou do conceito de vulnerabilidade assimétrica. Não se trata apenas de *malware*, os famigerados vírus – que podem inclusive afetar equipamentos usados pelo governo e pelas forças armadas –, mas também de campanhas de desinformação potencializadas pelo uso de *big data* para personalizar as mensagens veiculadas (LUPION, 2019; BRADSHAW; BAILEY; HOWARD, 2020), entre outras possibilidades de incidentes danosos. Um DDoS, ou *Distributed Denial of Service*, por exemplo, poderia impedir o acesso a servidores do governo em momentos críticos. As possibilidades são vastas.

Segue que o estudo de segurança e defesa cibernética se mostra campo interessante e promissor de pesquisa, em franco florescimento. O desafio que ora se coloca se estenderá ainda nas décadas vindouras, de maneira que presenciamos apenas o início de uma era.

Partindo-se da constatação de que a questão cibernética é híbrida e transversal, não respeitando fronteiras entre países, áreas do conhecimento, segmentos populacionais e instituições governamentais, é esperado que afete considerações estratégicas de segurança e defesa. Seria impensável que não o fizesse.

Escolher países nórdicos e Estônia para estudo comparativo entre as estratégias de segurança e defesa cibernética adotadas por eles e aquela implementada pelo Brasil parece desconexa. Não é o caso. Cabe justificar, portanto, o recorte espacial adotado neste trabalho. A seleção feita baseou-se nas conclusões a que se chegou durante a leitura dos textos que embasam a pesquisa, em especial às constatações sobre a natureza dos conflitos cibernéticos, tal como elaborado por Valeriano e Maness (2014, 2015, 2018a, 2018b), Klimburg (2019) e Hanson *et al.* (2019), entre outros.

Se considerarmos que boa parte dos incidentes cibernéticos é constituída não por grandes ataques a infraestruturas críticas, mas por operações de baixa intensidade; que há considerável arcabouço teórico para pressupor que o presente e o futuro dos conflitos interestatais abrangerá segmentos cada vez mais amplos da sociedade; e que o ambiente cibernético tem servido marcadamente de veículo para a condução de operações híbridas, é adequado estudar países que lidam com ameaças dessa natureza há mais tempo, mormente advindas de atores em seu entorno estratégico.

Em vista das barreiras linguísticas, dado serem poucos os que divulgam documentos oficiais em língua inglesa, e do caráter impraticável de se recorrer à tradução automatizada, seria recomendável ater-se a países que dispusessem de estratégias, orientações e estudos oficiais disponíveis em língua inglesa. Face a essas considerações, chegou-se portanto à escalação de Suécia, Dinamarca, Noruega, Finlândia e Estônia. Optou-se por incluir Estados Unidos no time de exemplos em razão não apenas de sua relevância global e hemisférica, mas também de sua proeminência no âmbito cibernético: ainda que haja outros atores tão atuantes nesse campo, trata-se do país de maior capacidade cibernética ofensiva e defensiva no mundo.

Eis, portanto, a pergunta da pesquisa: de que maneira a estratégia brasileira de segurança e defesa cibernética se compara à de países nórdicos e Estônia? Adicionalmente, de maneira secundária, são importantes os seguintes questionamentos: Qual efetivamente é a natureza do desafio cibernético? Quais são os principais pontos das estratégias dos países nórdicos e da Estônia? Quais são as deficiências do modelo brasileiro? Quais possíveis sugestões se poderia colocar para o futuro? Empregaram-se métodos qualitativos de caráter

indutivo. Apoia-se no estudo bibliográfico, na análise documental e na condução de breves entrevistas com autoridades brasileiras atuantes no campo cibernético. A hipótese é que o Brasil carece de um sistema eficiente face à realidade das ameaças cibernéticas e às soluções encontradas pelos países analisados. O que se tentará demonstrar é que a opção brasileira por dar prioridade à segurança da informação e à proteção de infraestruturas críticas - em detrimento de abordagem baseada em visão ampla sobre o hibridismo dos desafios cibernéticos - coloca o país em posição vulnerável. Há, ainda, risco de militarização da segurança cibernética no Brasil.

A dissertação está dividida em três capítulos. No primeiro, construiu-se panorama sobre o assunto. Discutiram-se conceitos importantes, a natureza dos incidentes cibernéticos, suas implicações para conflitos interestatais em geral e o hibridismo do campo. No segundo, partiu-se para os exemplos práticos de países nórdicos e Estônia, com foco na análise de documentos oficiais relevantes. No terceiro e último capítulo, debruçou-se sobre o caso brasileiro, com interesse não apenas em estratégias, leis e regulamentos, mas também na particularidade das relações entre civis e militares, e o impacto que isso tem sobre as considerações cibernéticas no Brasil.

Ao fim do trabalho, espera-se ter contribuído para a discussão sobre o caso brasileiro e provido subsídios para se pensar a maneira como o país deve aplicar estratégias condizentes com o desafio e se organizar para enfrentar as próximas décadas de evolução do ciberespaço. O tema é interessante, multifacetado e dinâmico. Requererá, portanto, muita pesquisa ainda. Mal cobrimos a superfície do oceano cibernético e de suas consequências em diversos campos da vida humana, da Ciência Política, das Relações Internacionais – e isso é profundamente animador.

2 A QUESTÃO CIBERNÉTICA: PRESSUPOSTOS TEÓRICOS E CONTEXTUALIZAÇÃO

O design futurístico, a ambientação decadente e a temática distópica transformaram *Blade Runner* em um clássico do cinema noir. Ambientado na hipotética Los Angeles de 2019, o enredo acompanha o ex-policial Rick Deckard, interpretado por Harrison Ford, cujo trabalho como *blade runner* requeria a perseguição e consequente aposentadoria forçada dos chamados replicantes, robôs humanoides criados por intermédio de bioengenharia. Apesar de serem aparentemente indistinguíveis dos seres humanos, os replicantes lhes eram superiores em força, velocidade, agilidade, resiliência e inteligência. O fictício teste Voight-Kampf – possivelmente uma referência ao teste de Turing[1] – era a única maneira de identificá-los com razoável grau de precisão.

O marcado contraste entre luz e sombras da cinematografia *chiaroscuro* dá o tom de desconforto, incerteza e paranoia com que os efeitos da tecnologia sobre o meio ambiente e a sociedade são tratados. A tensão entre passado, presente e futuro é desenvolvida em um mundo no qual a tecnologia é concomitantemente avançada em alguns lugares e decadente noutros. Apesar de ter sido um fracasso espetacular de bilheteria, a jornada de Deckard em um futuro de memórias que podem ser implantadas, vida natural extinta e migração humana em massa para colônias extra-planetárias teve notável impacto cultural desde a estreia de *Blade Runner* em 1982. Influenciou, portanto, a subsequente produção de filmes, videogames, e animes pertencentes ao gênero de ficção científica.

Obras como a trilogia *Matrix*, a franquia *Ghost in the Shell* e o filme *Minority Report* beberam da fonte da obra-prima cinematográfica de Ridley Scott ao incorporar não apenas a estética *cyberpunk*, mas também o espírito de inquietação com um porvir profundamente tecnológico. A interseção entre ficção científica e *noir* inclui elementos estéticos e

[1] Introduzido pelo matemático e cientista da computação britânico Alan Turing em artigo de 1950, intitulado "*Computing Machinery and Intelligence*", o teste de Turing destina-se a provar a capacidade de uma máquina de comportar-se de maneira equivalente a um ser humano, ou, no mínimo, de forma indistinguível de um homem ou mulher de carne e osso. O teste não foi projetado para verificar a capacidade da máquina em avaliação de responder corretamente às perguntas, mas sim para averiguar quão próximas suas respostas são daquelas que seriam dadas por um ser humano padrão. Tal como conceitualizado por Turing em sua primeira versão, o teste consistiria em conversa de texto entre dois jogadores humanos e uma máquina projetada para fornecer respostas indistinguíveis daquelas de um ser humano. Separados fisicamente uns dos outros, estes seriam avaliados por um árbitro. Caso este não fosse capaz de identificar qual dos três participantes seria a máquina, diz-se que ela passou no teste. Para uma reflexão crítica sobre o teste de Turing e sua relevância histórica, ver Saygin, Cicekli e Akman (2000).

principalmente morais que, em última instância, informaram a construção de percepções coletivas sobre tecnologia e cibersegurança ao menos no Ocidente, onde esses produtos culturais foram consumidos de maneira irrestrita. Ao afirmar que conceitos são teleológicos, moldam percepções e discursos e têm até mesmo o condão de privar-nos da capacidade de discutir determinados assuntos de forma autônoma, Nissenbaum (2004) destaca em particular a construção em representações culturais da quase mitológica da figura do *hacker*, um terrorista da Era da Informação, de fabulosa capacidade técnica capaz de driblar sistemas de segurança sofisticados dispondo apenas de equipamentos básicos e conexão à rede mundial de computadores.

Para ela, a distorção da definição do que é um *hacker* dotou instituições que lidam com questões cibernéticas do poder de instrumentalizar modelos conceituais em busca de controle. Citando Bowker e Star (1999), Nissenbaum argumenta que a elaboração de conceitos pode ser arena de contestações político-sociais, de maneira que o enquadramento destes conceitos como puramente técnicos dificulta o tratamento de questões ontológicas que têm consequências normativas diretas. O cerne do argumento de Nissenbaum se coaduna com as observações nevrálgicas de Milliken (1999) a respeito da construção do discurso em Relações Internacionais. Milliken aponta que é significativo para a legitimidade de práticas internacionais que discursos fomentem no imaginário das audiências às quais se destinam expectativas sobre como as autoridades devem agir em prol e em nome da população em relação à segurança do Estado e ao provimento de assistência social, por exemplo. Complementa Milliken dizendo que

> *Throughout, discourses are understood to work to define and to enable, and also to silence and to exclude, for example, by limiting and restricting authorities and experts to some groups, but not others, endorsing a certain common sense, but making other modes of categorizing and judging meaningless, impracticable, inadequate or otherwise disqualified*. (MILLIKEN, 1999, p. 229)

Assim, ainda que baseada em representações incompatíveis com a realidade, a construção do discurso em torno do conceito do que seria um *hacker* teria, na visão de Nissenbaum, legado certa legitimidade àqueles envolvidos na prevenção de incidentes cibernéticos a influenciar, sob o verniz da autoridade técnica, a definição de conceitos que têm implicações políticas tangíveis.

Nessa linha, Hansen e Nissenbaum (2009) asseveram que cibersegurança, enquanto discurso em ascensão no campo da segurança internacional, é o produto do amálgama entre

um discurso técnico sobre segurança computacional e o conceito de securitização (Buzan; Waever; Wilde, 1997). As autoras dedicam particular atenção à construção do discurso técnico em cibersegurança ao afirmar que:

> *The privileged role allocated to computer and information scientists within cyber security discourse is in part a product of the logic of securitization itself: if cyber security is so crucial it should not be left to amateurs. Computer scientists and engineers are however not only experts, but technical ones and to constitute cyber security as their domain is to technify cyber security. Technifications are, as securitizations, speech acts that "do something" rather than merely describe, and they construct an issue as reliant upon technical, expert knowledge, but they also simultaneously presuppose a politically and normatively neutral agenda that technology serves*. (HANSEN; NISSENBAUM, 2009, p. 1167)

A questão que se levanta, portanto, é se, como se deduz dos argumentos de Nissenbaum (2004), Milliken (1999) e Hansen e Nissenbaum (2009), obras de ficção científica podem de fato favorecer a construção de um discurso *securitizador* que influencie a formulação de políticas públicas no âmbito cibernético. Shires (2019) aventa a possibilidade de que a cultura pop molde a percepção de espectadores em geral, e agentes políticos em particular, sobre cibersegurança e, indiretamente, influencie a formulação de normas destinadas ao tratamento do tema.

Como instrumento analítico, Shires cunhou o conceito de "*cyber noir"* para mapear a interação entre o discurso técnico em cibersegurança e o que ele chamou de discurso *noir* presente em obras da cultura pop como filmes, livros e séries de televisão. Ao entender discursos como capazes de definir e constranger a identidade de atores no âmbito da cibersegurança, Shires afirma que a sobreposição e tensão discursivas geram significados capazes de estruturar as condições sob as quais esses atores agem, ações estas que, no juízo do autor, perpetuam entendimentos que dificultam a distinção entre limites legais, morais e profissionais de atividades legítimas e maliciosas no ciberespaço. Para esses atores, diz Shires, as características mesmas do ciberespaço[2] constituiriam um obstáculo para a definição do que seriam ações legítimas e maliciosas.

Shires demonstra que até mesmo a terminologia usada por especialistas do ramo deriva de obras de ficção científica distópica, o que, de acordo com ele, é parte construção,

[2] Registre-se aqui o que Medeiros e Goldoni (2020) consideram a trindade conceitual fundamental do ciberespaço: "*deterritoriality, multiplicity of actors and uncertainty*", (MEDEIROS; GOLDONI, 2020, p. 31).

parte *branding*. A gramática visual e discursiva de obras pertencentes ao *cyber noir* informa a construção de definições e o enquadramento do tema, conclui o autor.

O entendimento de Young e Carpenter (2018) sobre a questão é ambivalente. Embora reconheçam que a presença de elementos da cultura pop em narrativas políticas, e vice-versa, os autores ponderam que essa constatação, por si só, não prova que a cultura pop tenha qualquer influência sobre o mundo político. Eles aventam inicialmente a possibilidade de que artefatos culturais circulem sem que produzam efeitos práticos sobre os comportamentos dos espectadores comuns e daqueles que participam da vida pública. Young e Carpenter entendem que o uso de elementos da ficção científica tenha efeitos majoritariamente discursivos e, mesmo assim, impacte predominantemente as parcelas da população que estejam razoavelmente familiarizadas com a gramática desse gênero cultural. Adicionalmente, o emprego de elementos da ficção científica em discursos políticos tem efeitos distintos de acordo com o alinhamento ideológico de cada um, concluem os autores.

Jones e Paris (2018) discordam em partes. Para os autores, o entendimento do impacto que obras de ficção têm sobre o cenário político deve ser estudado para que este cenário seja compreendido adequadamente. Eles defendem que uma abordagem baseada no gênero ao qual os artefatos culturais a serem analisados pertencem tem maior poder explicativo que análises baseadas unicamente no impacto de obras específicas, o que, informam eles, tem sido predominante e dificulta a extrapolação dos resultados dessas pesquisas para outros estudos. O estudo do impacto do gênero funcionaria em dois níveis: poderia esclarecer quais elementos específicos do gênero em questão estimulam os efeitos observados no estudo e complementa estudos já em curso que têm demonstrado a importância da narrativa, seja esta de ficção ou não-ficção, para os processos de cognição e persuasão do ser humano.

Ainda que os espectadores saibam que obras de ficção não retratam fatos, Jones e Paris explicam que há crescente evidência de que o processamento cognitivo de obras de ficção e não-ficção não seja fundamentalmente diferente. O que se sabe até o momento, adicionam, é que informações de ambas são incorporadas às estruturas de conhecimento do mundo real, às reações emotivas e, consequentemente, aos comportamentos subsequentes.

Jones e Paris se debruçaram sobre histórias de cunho totalitário e distópico em razão tanto de sua popularidade quanto de seu claro conteúdo político. Por intermédio da análise do

comportamento de *focus groups* e do uso de pesquisas de opinião[3], os autores pontuam que a motivação do espectador ao assistir a um filme ou ler um livro pertencente a esse gênero influencia a reação ao conteúdo.

> *While escapist ("hedonic") motivation may lead to one kind of emotional involvement driven by less in-depth cognitive processing—perhaps enhancing the likelihood of narrative persuasion—truth-seeking ("eudemonic") motivation may lead to another, fostering reflection on important issues (including political ones) and thus a greater potential for agenda-setting. Taken together, the results also suggest that narrative-specific and broader genre-wide agenda-setting effects may compete; for example, in Study 1, the Hunger Games treatment enhanced concern about "police brutality"—heavily featured in that narrative's specific storyline—but not "excessive government power," even though the former issue is logically related to the latter*. (JONES; PARIS, 2018, p. 977)

Em todos os indivíduos que participaram do estudo, complementam, a reação primordial não foi o declínio da confiança nas autoridades, da vontade de participar da vida política do país ou da expectativa de eficácia do governo. Na verdade, dizem Jones e Paris, a exposição à ficção totalitária e distópica levou os participantes mais atentos a desconfiarem da utilidade de participação política convencional e não-violenta.

A principal descoberta dos autores é que ficção totalitária e distópica pode aumentar a receptividade dos indivíduos a ações políticas radicais, tanto entre adultos quanto entre jovens. O efeito identificado, dizem, "*generally holds across multiple studies, multiple variables, and multiple examples of the genre. This finding is striking, and far from inevitable. Subjects might have reasonably (...) shown little inclination to incorporate lessons from the narrative into their general political attitudes*", (JONES; PARIS, p. 982).

Os participantes do estudo relataram a Jones e Paris que o clima de rebelião da ficção distópica os lembrou de que pessoas comuns podem questionar o *status quo* e se rebelar "contra o sistema". Os autores acreditam que isso seria compatível com experimentos recentes que sugerem a existência de um "*sleeper effect*", por meio do qual obras de ficção, por sua

[3] As hipóteses foram testadas em um grupo amostral de adultos em três estudos diferentes. No estudo 1, os assuntos foram atribuídos aleatoriamente a três grupos: um grupo de controle sem mídia ou um de dois grupos de tratamento distópico. Os estímulos distópicos foram apresentados a conteúdos narrativos típicos do gênero, pelo qual os autores esperavam distinguir entre os efeitos gerais do gênero e os efeitos devido às particularidades de uma determinada história. Para esse fim, eles construíram dois tratamentos diferentes. O primeiro incluiu seleções de *The Hunger Games*. Outro foi composto por seleções dos livros e filmes da série *Divergente*. Nos estudos 2 e 3, Jones e Paris (2018) procuraram investigar quais características do gênero distópico poderiam ser responsáveis pelos efeitos encontrados no estudo 1. Assim como no estudo 1, os autores utilizaram-se de pacotes de conteúdo midiático para a investigação.

característica de imersão e de suspensão dos mecanismos de contra-argumentação, podem ter efeitos persuasivos mais duradouros que aqueles produzidos por obras de não-ficção.

Portanto, ao contrário de Young e Carpenter (2018), Jones e Paris (2018) entendem que a ficção distópica pode expandir de maneira sutil a imaginação dos espectadores de maneira a incluir uma miríade de cenários não necessariamente presentes no jogo político usual. Embora enfatizem o fato de que o consumo de obras de ficção esteja longe de corresponder a radicalismo e a violência política na vida real, Jones e Paris asseveram que "*the stories we tell ourselves have profound implications for how we think about political ethics and political possibilities*", (JONES; PARIS, p. 983).

Em que pesem as divergências de pesquisadores a respeito do impacto tangível de narrativas de ficção sobre o cenário político, é razoável supor, face aos estudos disponíveis, que essas podem ter alguma influência sobre a maneira como se pensa sobre o mundo real e os revezes político-sociais. Como exposto por Nissenbaum (2004), a própria construção da figura mitológica do *hacker* teve efeitos sobre a formulação de estratégias de cibersegurança por meio do enquadramento contencioso da questão.

Na literatura, há tanto estudos defendendo a possibilidade de que cenários graves de ciberguerra possam vir a ocorrer, com possíveis efeitos cinéticos, mormente sobre a infraestrutura crítica dos países (KELLO, 2013; DEMCHAK e DOMBROWSKI, 2011; PAULWELS, 2019; HOFFMAN, 2007), quanto trabalhos que questionam essas conclusões e postulam que incidentes cibernéticos têm-se caracterizado predominantemente pela baixa intensidade (RID, 2012; CAVELTY, 2008; GUITTON, 2013; VALERIANO E MANESS, 2014, 2015, 2018a, 2018b). Há, portanto, vivas discussões sobre qual seria de fato a natureza dos incidentes cibernéticos.

2.1 A guerra cibernética vai acontecer?

2.1.1 Definições terminológicas

Antes de apresentar as discussões na literatura a respeito da possibilidade de que guerras cibernéticas sejam travadas, cumpre revisar brevemente a terminologia normalmente utilizada em textos que versam sobre esse tema. O glossário fornecido pela *Cyber Security Strategy* da Finlândia (FINLÂNDIA, 2013, p. 12-13) é completo, em que pese a concisão. Os

termos a serem empregados ao longo desta dissertação são assim definidos, de acordo com *Secretariat of the Security Committee* finlandês:

- Infraestrutura de informação – As estruturas e funções por trás de sistemas de informação que transmitem, transferem, recebem, armazenam eletronicamente ou de outra forma e processam informações (dados).
- Infraestrutura crítica de informação – Refere-se às estruturas e funções por trás dos sistemas de informação das funções vitais da sociedade que transmitem, transferem, recebem, armazenam, eletronicamente ou de outra forma, informações do processo (dados).
- Infraestrutura crítica – Refere-se às estruturas e funções que são indispensáveis para as funções vitais da sociedade. Elas compreendem instalações físicas e estruturas, bem como funções e serviços eletrônicos.
- Ciber ou *Cyber* – A palavra "ciber" é o prefixo de um termo ou o modificador de uma palavra composta, em vez de uma palavra autônoma. Sua inferência geralmente se refere ao processamento eletrônico de informações (dados), tecnologia da informação, comunicações eletrônicas (transferência de dados) ou sistemas de informação e computador. Apenas o termo completo da palavra composta pode ser considerado como possuindo significado. Acredita-se que a palavra cibernético se origine do verbo grego antigo κυβερεω (kybereo), ”orientar, guiar, controlar”.
- Risco cibernético – Significa a possibilidade de um acidente ou vulnerabilidade no domínio cibernético que, se se materializar ou estiver sendo utilizado, pode causar danos, prejudicar ou perturbar uma operação que depende do funcionamento do domínio cibernético.
- Domínio ou ambiente cibernético – Um domínio de processamento eletrônico de informações (dados) que compreende uma ou várias infraestruturas de tecnologia da informação.
- Segurança cibernética – O estado final desejado em que o domínio cibernético é confiável e no qual seu funcionamento é garantido.
- Ameaça cibernética – A possibilidade de ação ou incidente no domínio cibernético que, quando materializado, põe em risco alguma operação dependente do mundo cibernético.

- Sistema de informação – O sistema que compreende o pessoal, equipamento de processamento de informação, equipamento de transferência de dados e programas de software destinados a tornar alguma operação mais eficiente, mais fácil ou mesmo possível por meio de processamento de informações (dados).
- Proteção da privacidade – A proteção contra o ilegal ou a invasão prejudicial da privacidade pessoal. A proteção da privacidade inclui o direito à privacidade e outros direitos associados no processamento de dados pessoais. Dados pessoais significa qualquer informação sobre um indivíduo particular e qualquer informação sobre suas características pessoais ou circunstanciais, onde estas são identificáveis como relacionadas com ele / ela ou os membros da sua família ou agregado familiar.
- Segurança da informação – Medidas administrativas e técnicas que garantem a disponibilidade, a integridade e a confidencialidade das informações.

As definições são estáveis, de maneira que, ao utilizá-las em artigos, livros e relatórios, os autores se referem à mesma coisa. Apesar disso, há alguma celeuma a respeito da adequação de se usar termos como *cyberwar* e *cyber conflict*. A discussão sobre a adequação vocabular não pode ser separada daquela sobre a natureza empírica dos incidentes cibernéticos, de maneira que o assunto será retomado na próxima subseção.

2.1.2 Céticos ou alarmistas? As discussões sobre a intensidade dos incidentes cibernéticos

A respeito da natureza da guerra, Strachan (2006) argumenta que seus cinco elementos constitutivos seriam o uso ou ameaça do uso da força; a contenciosidade mútua, posto não ser a guerra uma atividade individual; o elevado grau de intensidade e considerável extensão das hostilidades; o caráter estatal, uma vez que os combatentes não lutam em causa própria, mas em nome de uma coletividade; e, finalmente, o objetivo último, definido normativamente em termos políticos, que, atingido, poderia ser considerado uma vitória.

Postos estes parâmetros, Strachan critica o uso do termo "novas guerras" para categorizar crimes violentos, pirataria e terrorismo, por exemplo. De acordo com o autor, essa abordagem provocaria uma crise existencial desnecessária para o pensamento teórico militar. Isso porque as novas guerras "*when engaged in by states, tend to be fought for political control of the people, for their hearts and minds, not for political control of the territory*

wherein they reside or of the resources which that territory contains", (STRACHAN, 2006, p. 23).

Convém esclarecer, no entanto, que Strachan não discorda da seriedade de questões como o aquecimento global, a luta por recursos naturais e a migração, para usar alguns exemplos fornecidos pelo próprio autor. Tampouco disputa Strachan a necessidade de se coordenar a ação conjunta para lidar com esses problemas por intermédio de mecanismos globais de governança. A questão, pontua o autor, é que temas do âmbito da segurança[4] não são guerras, e muitos deles serão resolvidos sem que seja necessário o envolvimento do aparelho militar. O risco de tratar assuntos da esfera de segurança como se necessariamente demandassem tratamento bélico, pontua Strachan, é que se militariza crises que não o deveriam ser, crises essas que poderiam ser adequadamente resolvidas recorrendo-se a expedientes que não deságuem em conflitos armados desnecessários. Não se deve confundir a necessidade de ajustar políticas públicas com supostas mutações na natureza da guerra, finaliza Strachan.

Os argumentos de Lind (1989) não são necessariamente incompatíveis com a admoestação de Strachan (2006); aquele, no entanto, traz reflexões interessantes sobre uma possível mudança no campo de batalha, a denominada quarta geração de guerras. O cerne do ponto de Lind é que cada mudança geracional na forma de se fazer guerra foi marcada pela dispersão do campo de batalha. Eis o porquê de o autor afirmar que a quarta geração de guerras provavelmente incluirá a totalidade da sociedade do país inimigo. Em conjunto com a relativa perda de importância de comandos centralizados, a ênfase na capacidade de manobra dos contingentes e o objetivo de levar o inimigo ao colapso interno sem necessariamente provocar sua destruição física, a quarta geração poderá ser dispersada, não-linear e indefinida. A diferença entre tempos de guerra e tempos de paz será indistinguível, assim como o poderá ser a separação entre civis e militares. Os ataques serão físicos, mas também socioculturais. Operações psicológicas deflagradas nos meios de comunicação podem se tornar comuns. Em suma, a quarta geração de guerras pode se basear em ideias, ao invés de o ser puramente em evoluções tecnológicas.

---

[4] O termo usado pelo autor no original em língua inglesa é "security", não "safety", outra palavra cuja tradução para a língua portuguesa poderia ser "segurança". A verdade é que, caso queiramos ser rigorosos, não há palavras diferentes em português para as acepções de "security" e "safety", de maneira que "segurança" deve ser empregada, ainda que se corra o risco de incorrer em certa confusão conceitual.

As observações de Hoffman (2007) seguem lógica argumentativa parecida com a de Lind (1989). Hoffman discorre longamente sobre o conceito de guerras híbridas[5], que "*instead of separate challengers with fundamentally different approaches (conventional, irregular or terrorist), we can expect to face competitors who will employ all forms of war and tactics, perhaps simultaneously*", (HOFFMAN, 2007, p. 7). O autor frisa que a questão não é exatamente o declínio de conflitos interestatais ou de modos convencionais de se fazer guerra, mas a fusão de diferentes modalidades de guerra – regular ou não, nos termos usados por ele.

Em relação à ideia de quarta geração de guerras, Hoffman conserva certo ceticismo. Seu argumento é que mesmo conflitos da antiguidade continham elementos da quarta geração. Há exemplos mais recentes, segundo o autor, que teriam ocorrido durante a segunda geração e que contêm elementos da quarta: o conflito civil nas Filipinas, ocorrido na virada do século XX, e as campanhas do Coronel T. E. Lawrence. Na opinião do autor, ao invés de sermos testemunha da emergência de uma forma completamente nova de guerrear, é possível que o fenômeno seja o amálgama de métodos já existentes. Ainda que seja reticente em relação a vaticinar a emergência de uma nova geração de conflitos armados, Hoffman acredita que a discussão é profícua por encorajar forças armadas e academia a reexaminar crenças e estudar atentamente as guerras irregulares.

Nessa toada, Hoffman recorre à literatura chinesa, em especial às ideias do Coronel Qiao Liang e de Wang Xiangsui[6], que propõem um conceito de guerra além dos tradicionais meios militares. A ideia é que o avanço tecnológico tem forçado a sobreposição dos domínios da política, da economia, da cultura, das forças armadas, da religião e da diplomacia. Esses fatores, prossegue, "*are rendering more and more obsolete the idea of confining warfare to the military domain and of using the number of casualties as a means of the intensity of a war*", (HOFFMAN, 2007, p. 23). Como complemento à análise, o autor apresenta três

---

[5] Bressan e Sulg (2020) tecem considerações complementares sobre uma "*grey zone*". É a *grey zone*, acreditam, a tática adequada para um mundo hiperconectado. Na *grey zone*, é possível derrotar outro país sem que se envie um soldado sequer. Por intermédio de exercício de construção de um cenário de paz e guerra na vizinhança imediata do continente Europeu em 2030, argumentam as autoras que "*a positive future of peace and the necessary management of the grey zone absent effective global governance require a better and more honest understanding of violence and domination in both war and peacetime*", (BRESSAN; SULG, 2020, p. 1). O ponto para elas é que, ausentes campos de batalha tradicionais, deve-se abandonar a noção de que a paz universal era uma realidade fora destes. O que substituiria, então, os campos de batalha? Ambiguidade e nuance entre paz e guerra. É para este meio termo que Bressan e Sulg julgam que o futuro se encaminhará. Estarão bem posicionados nesse cenário os atores que reconhecem essa ambiguidade e a usam para seu proveito, em contraposição àqueles que sequer percebem as mudanças que estão em curso. Nas palavras das autoras, o oposto de paz não é guerra, como em uma dicotomia, mas violência e opressão ao longo de um contínuo de intensidade.

[6] LIANG, Qiao; XIANGSUI, Wang. **Unrestricted Warfare**. [S.I.]: PLA, 1999.

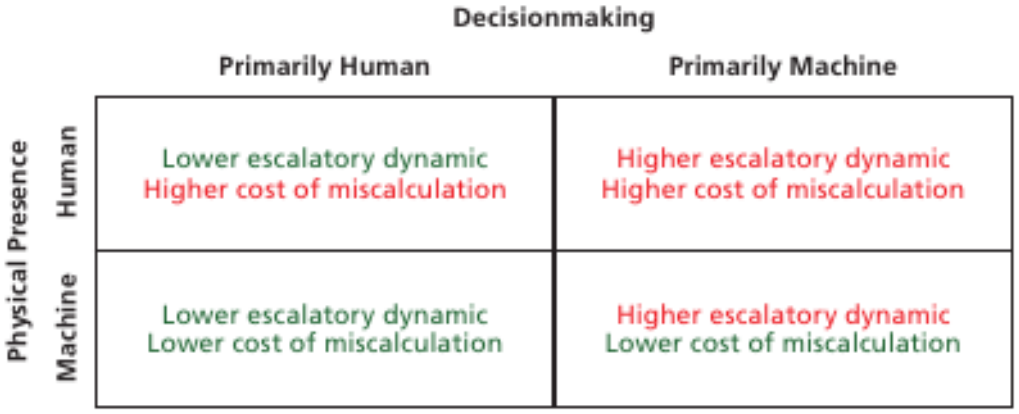
conceitos propostos por Liang e Xiangsui para se pensar a guerra que transborda os limites tradicionalmente considerados:

> *Omni-directionality – requires that commanders observe a potential battlefield without mental preconditions or blind spots. The designing of plans, employment measures, and combinations must make use of all war resources which can be mobilized. The commander is enjoined to make no distinction between what is or is not the battlefield. All the traditional domains, (ground, seas, air, and outer space) as well as politics, economics, culture, and moral factors are to be considered battlefields.*
>
> *Synchrony – enjoins on commanders to link the disaggregated nature of multiple battlefields in different domains with consideration of the temporal dimension. In other words, "conducting actions in different spaces in the same period of time" to achieve desired effects. Instead of phases, with the accumulated results of multiple battles, strategic results can now be attained rapidly by simultaneous action or at designated times.*
>
> *Asymmetry – here the authors recognized that asymmetry manifests itself to some extent in every aspect of warfare. However, asymmetry has been sought in operational terms within traditional military dimensions. In war beyond limits, the spectrum for overlooking the normal rules is much wider*. (HOFFMAN, 2007, p. 25)

Estes elementos seriam úteis para compreender taticamente, portanto, os conflitos polimorfos que Hoffman denomina guerras híbridas. O autor explica que a definição, a juízo dele, é a soma do que preconizam os defensores da quarta geração de guerras – a natureza ambígua dos conflitos contemporâneos e a perda do monopólio da violência por parte do Estado; de Liang e Xiangsui – os conceitos de omni-direcionalidade, sincronia e assimetria; de John Arquilla e T. X. Hammes – o poder das redes; dos teóricos das guerras compostas – a mistura de capacidades convencionais e não-convencionais; e de acadêmicos australianos – a dispersão do teatro de operações e o oportunismo dos adversários do futuro.

O uso de Inteligência Artificial no campo de batalha[7] é um assunto que também tem recebido atenção nas discussões acadêmicas sobre a interseção entre conflitos armados e evoluções tecnológicas cibernéticas. Wong *et al.* (2020) teoriza que a sistemas que se utilizem de Inteligência Artificial podem não só afetar a capacidade de dissuasão, mas também provocar a escalada acidental de crises de maneira acelerada, fomentando instabilidade. É possível que haja consequências para a estabilidade estratégica. Essas observações são compartilhadas por Davis (2019), Johnson (2019a; 2019b) e Taddeo e Floridi (2018).

Figura 1 – Configurações homem-máquina e dinâmica potencial de escalada de conflitos



Fonte: Wong *et al.* (2020)

Ao diminuir os custos e riscos do uso de força letal, sistemas autônomos poderiam facilitar o uso da força e tornar conflitos armados mais frequentes, conjecturam os autores. Eles argumentam que a presença de seres humanos no processo de tomada de decisão de sistemas autônomos diminui a velocidade de escalada de situações com potencial bélico. Por outro lado, corre-se também o risco de humanos interpretarem a situação de maneira equivocada. O risco seria maior quanto menos vidas humanas fossem colocadas em perigo, o

[7] Galliott e Wyatt (2020) avaliaram em estudo com militares de baixa patente da *Australian Defense Force Academy* que "*a significant majority would be unwilling to deploy alongside fully autonomous LAWS. (...) allowing a robot to use lethal force retains a discursive weight that influences a significant minority to claim that they would be uncomfortable deploying alongside robots that have comparable operational independence to systems that are already in use by the ADF*", (GALLIOTT; WYATT, 2020, p. 32). A percepção dos participantes sobre a segurança, precisão e confiabilidade dos sistemas autônomos era o fator mais importante na disposição deles a empregar esses recursos em cenário de conflagração armada. Horowitz e Scharre (2021) concordam. Eles acrescentam que "f*or militaries, balancing between the risks of going too slow versus going too fast with AI adoption is complicated by the fact that AI, and deep learning in particular, is a relatively immature technology with significant vulnerabilities and reliability concerns.* (...) *When trained with inadequate data sets or employed outside the narrow context of their design, AI systems are often unreliable and brittle. AI systems can often seem deceptively capable, performing well (sometimes better than humans) in some laboratory settings, then failing dramatically under changing environmental conditions in the real world*", (HOROWITZ; SCHARRE, 2021, p. 7).

que diminuiria, a princípio, o custo da decisão tomada e incentivaria estratégias ousadas. Wong *et al.* acredita ainda que a dinâmica de escalada de conflitos pode mudar consideravelmente quando adversários de quadrantes distintos se enfrentam (Figura 1).

Tradicionalmente, a dissuasão requereria que humanos compreendessem humanos adversários. Com o uso de sistemas autônomos, os autores resumem a dinâmica de compreensão mútua da seguinte maneira: humanos devem entender suas próprias máquinas e as máquinas dos adversários; máquinas devem entender seus humanos e também os humanos e as máquinas adversários. Multiplicam-se as chances de que ocorram erros de interpretação, cálculo e percepção.

Em relação à aplicação para a sociedade como um todo de tecnologias que façam uso de inteligência artificial, Chiusi *et al.* (2020) vaticinam que, na Europa, ao menos, já se lida com avançado grau de automatização das atividades sociais em geral: na educação secundária, no sistema de saúde e no judiciário[8], por exemplo. O emprego de sistemas automatizados, no entanto, é nebuloso, de maneira que não se sabe exatamente como esses sistemas funcionam[9] e quais são seus efeitos sobre os seres humanos que gerenciam. Trata-se, portanto, de déficit democrático[10], dado que não houve e não há debate significativo sobre o assunto na Europa, segundo os editores. Mesmo o propósito desses sistemas não costuma ser explicado à população, tampouco o são os benefícios que eles deveriam trazer à sociedade. A situação é viabilizada pelo que eles chamam de *techno-solutionist trap*, a ideia de que problemas sociais são "*bugs*" que podem ser consertados com o uso de tecnologias que passariam, então, a ser adotadas de maneira acrítica.

> *When touted as "solutions", ADM systems immediately veer into the territory described in Arthur C. Clarke's Third Law: magic. And it is difficult, if not impossible, to regulate magic, and even more so to provide transparency and*

[8] O exemplo fornecido neste caso é o da Itália, onde se testa algo chamado de "*predictive jurisprudence*". Esta consistiria no uso da automação para orientar magistrados na identificação de tendências interpretativas com base em julgados anteriores sobre o tema que estiverem se debruçando na ocasião. No campo da "*predictive policing*", tecnologias de reconhecimento facial têm-se tornado ubíquas no continente europeu: escolas, estádios esportivos e aeroportos são alguns dos locais que a empregam. Tanto aplicativos quanto monitoramento por vídeo são utilizados com esse fim.

[9] Franke (2021) tece considerações complementares no que diz respeito à capacidade da inteligência artificial perpetuar preconceitos preexistentes e à importância da qualidade dos dados fornecidos a sistemas de inteligência artificial. Knight (2019) já havia feito ressalva similar na *MIT Technology Review*.

[10] Pinto (2020) defende a democratização de tecnologias de ponta, de maneira que estas sirvam à sociedade efetivamente. O argumento da autora é que "*the impact on civil and political rights and on social, economic and cultural rights should be considered before the deployment of a technology by the state and evaluated afterwards. Accountability lines must be drawn, so that the interventions are carefully designed*", (PINTO, 2020, p. 21).

> *explanations around it.* (…) *most critiques of such systems are framed as an all-out rejection of "innovation", portraying digital rights advocates as "neo-luddites".* (…) *what we need to see now is actual policies changing – in order to allor greater scrutiny of these systems.* (…) *Only through an informed, inclusive, and evidence-based democratic debate can we find the right balance between the benefits that ADM systems can – and do – provide in terms of speed, efficiency, fairness, better prevention, and access to public services, and the challenges they pose to the rights of us all*. (CHIUSI *et al.*, 2020, p. 10)

O esforço do relatório de aclarar esses pontos resulta em sugestões de políticas públicas a serem implementadas, como registros de livre consulta dos sistemas automatizados usados pelo poder público; criação de *framework* de responsabilização; desenvolvimento de métodos de auditoria dos algoritmos desses sistemas; apoio a organizações da sociedade civil para atuarem como *watchdogs* de sistemas automatizados; e banimento de reconhecimento facial que possa ser usado para vigilância em massa, entre outras medidas.

* * *

Embora apenas tangenciem a questão da Inteligência Artificial, Valeriano e Maness (2018b) trabalham a mudança da natureza dos conflitos estritamente no âmbito cibernético. Com base em estudos empíricos, os autores não creem em um padrão de alta intensidade dos ciberconflitos, nem que haja grande probabilidade de ocasionarem reações cinéticas. Em verdade, dizem, é difícil sequer encontrar estudos comparativos sobre o assunto, pois a tendência na área é focar em episódios que provavelmente são pontos fora da curva, como o caso Stuxnet, de 2010; o vazamento da Sony, ocorrido em 2014; e o ataque DDoS da Rússia sobre a Estônia, em 2007.

Eles também demonstram ceticismo em relação à revolução tecnológica no campo militar, que implicaria mudanças acentuadas no modo como operações de combate são conduzidas. Opõem-se, portanto, a Kello (2013) e aproximam-se de Lindsay (2013) e Gartzke e Lindsay (2015) ao concordarem com estes no que diz respeito aos constrangimentos impostos aos atores internacionais para amplo emprego de armas cibernéticas em sua total capacidade.

A análise qualitativa preliminar de Valeriano e Maness (2014) aponta que, conquanto haja evidência de que ocorra uma miríade de disputas cibernéticas entre Estados pós-soviéticos, estas raramente evoluem para ameaças sérias à segurança nacional. Em consonância com Rid (2012), os autores pontuam que conflitos cibernéticos parecem emular

primordialmente a dinâmica da espionagem ou do conflito econômico ao invés do rito da guerra, visto que não houve ainda mortes atribuídas a ataques no ciberespaço. Os autores definem conflito cibernético, então, como "*use of computational technologies in cyberspace for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities short of war and away from the battlefield*", (VALERIANO; MANESS, 2014, p. 2). Em suas próprias palavras, é uma tática agressiva de política externa. Citando Kahn (1960), eles propugnam uma teoria da autocontenção no ciberespaço:

> *Direct deterrence between two parties often fails. When states try to enhance their security position through threats, alliances, and military buildups, they often fail to provoke the reaction intended – concessions. In fact, they often provoke further conflict and extreme threats (Vasquez, 1993; Hensel & Diehl, 1994). Comprehensive restraint relates to deterrence from spectacular attacks such as nuclear weapons or devastating internet operations focused on power systems and health services. States are restrained from such action through fears of retaliation and escalation of the conflict beyond control. (...) Extending this concept to cyber relations would suggest that restraint does not work at the low level of disputes such as distributed denial of service method (DDoS) incidents or simple vandalism, since there is little to restrain a state from acting at this level. More comprehensive measures, on the other hand, are off the table. It is unlikely that a state would be willing to attack and destroy a power network, social services facility, or government organization such as the Department of Defense due to the fear of retaliation. The dispute then makes little sense since the costs of engagement are potentially devastating and unlimited*. (VALERIANO; MANESS, 2014, p. 4)

Outro ponto importante levantado pelos autores diz respeito ao caráter eminentemente regional dos incidentes cibernéticos. Em discordância de suposições sobre a eclosão de conflitos entre atores localizados em pontos distantes do globo, Valeriano e Maness (2014) acreditam que a autocontenção no campo cibernético significa que os países que de fato empreendem operações cibernéticas provavelmente são rivais locais, em função principalmente da relevância imediata dos desentendimentos mútuos. Isso não significa, contudo, que países extraneos a determinada região não possam conduzir operações cibernéticas locais:

> *Further, states with aims of exerting influence in a particular region may also turn to cyber tactics. Low level cyber operations constitute a relatively unimportant matter to other states. Small aggressions indicate states expanding their standing and power through these interactions. It is a form of control; states hoping to rise within a regional power hierarchy are likely to leverage any form of capability. States striving for regional strength in relation to their neighboring rivals, such as China, Israel, and India, are the likely cyber conflict culprits. Regional dynamics*

> *lead us to hypothesize that states will use cyber capabilities on neighbors rather than global rivals with few exceptions.* (VALERIANO; MANESS, 2014, p. 5)

Em análise quantitativa sobre a frequência de conflitos entre Estados rivais de 2001 a 2011, os autores chegam à conclusão de que poucos são os que de fato empreendem batalhas cibernéticas, mesmo aqueles que estão envolvidos em disputas militares públicas.

Figura 2 - Países mais ativos em incidentes cibernéticos

Table VI. Top ten states by number of rival cyber dyads

State	*Number of cyber dyads*	*Total cyber incidents*	*Total cyber disputes*
China	6	40	29
United States	5	35	12
India	3	18	5
Japan	3	15	13
North Korea	3	15	5
Russia	3	11	5
South Korea	2	18	8
Iran	2	18	4
Israel	2	12	4
Pakistan	1	13	3

Fonte: Valeriano e Maness (2014)

Explicam os autores que, enquanto países de média projeção internacional podem ser ativos em incidentes cibernéticos locais, o teatro de operações das grandes potências é global. A dupla mais ativa é composta por Estados Unidos e China, como visto na Figura 1. Eles apontam que a principal tática utilizada por ambos é a apreensão de material sensível, uma espécie de espionagem. Os dados apresentados por Valeriano e Maness (2014) reforçam a conclusão dos autores sobre a prevalência da autocontenção nas interações cibernéticas:

> *States will not risk war with their cyber capabilities because there are clear consequences to any use of these technologies. States are not reckless, but terrorists and other cyber activists might not be so restrained. The interesting result of the process is that while cyber terrorists will likely proliferate, their ability to do damage will be limited due to the massive resources and conventional intelligence methods needed to make an operation like Stuxnet successful. Stuxnet and Flame could be the harbingers of the future, but in reality it was a collusion of discrete events that worked out for the attacker (Lindsay, 2013). With a will to attack, there must also come a way to attack. With such a high burden on luck and ability, it will be rare to see such important disputes continue in the future* (…) *Cyber conflict is in our future, but these events will only be as devastating as the target allows them to*

> *be as long as the attacker is restrained by logic, norms, and fear of retaliation.* (VALERIANO; MANESS, 2014, p. 5)

Os autores levantam a hipótese de que o recurso às hostilidades em ambientes virtuais seja subutilizado naquele momento, mas suas observações não foram alteradas em escritos mais recentes. Valeriano e Maness (2018b; 2018a) não acreditam que os avanços tecnológicos tornarão possível a países de pequeno porte multiplicar sua capacidade ofensiva. Conquanto esse possa ser o caso de Estônia e Coreia do Norte, dizem, não o é para os demais. Valeriano e Maness (2015), em concordância com Lindsay (2013), asseveram que são as grandes potências as maiores beneficiárias das tecnologias cibernética. O motivo é simples: armas cibernéticas não são simples de se usar ou baratas de se desenvolver. Isso significa que é necessário dispor de robustos recursos humanos especializados e generosa rubrica orçamentária para desenvolver capacidades equivalentes às das grandes potências cibernéticas – Estados Unidos, Israel, Rússia e China.

Wigell (2019) tece considerações complementares, mas, ao invés de se referir a conflagrações cibernéticas, fala de interferência híbrida. Tratar-se-ia de uma espécie de operação de baixa intensidade que não necessariamente desembocaria em consequências cinéticas. Para Wigell, esta seria a maior ameaça à estabilidade das democracias ocidentais[11], e não a possibilidade de que uma guerra híbrida ocorra:

> *While much of the debate on hybridity has revolved around 'little green men' and other grey zone military tactics, the more pressing challenges from a Western perspective are the more subtle, non-military activities deployed by authoritarian regimes to penetrate democratic society. Hybrid interference is a concept developed to capture non-military practices for the mostly covert manipulation of other states' strategic interests.1 As such, it should be distinguished from hybrid warfare, which is essentially a military approach to conducting 'indirect war' under special circumstance*s. (WIGELL, 2019, p. 4)

Não parece absurdo supor, então, que o ponto da questão cibernética não é uma hipotética guerra disputada no ciberespaço, mas a corrosão do tecido social por meio de ataques híbridos.

---

[11] O termo "democracias ocidentais" é utilizado pelo autor ao longo do artigo. Este será mantido quando for feita menção a seu trabalho por questão de fidelidade ao que ali foi expresso. No entanto, em nossa opinião, há certo grau de etnocentrismo na expressão. Ainda que Wigell se refira à tradição política ocidental, o reiterado uso do termo em contraposição a agressores híbridos parece tecer generalizações indevidas a respeito dos sistemas políticos de Estados orientais – que, diga-se, também podem ser alvo de interferência híbrida. Insistimos que essa colocação não invalida de maneira alguma as valiosas reflexões do autor. Trata-se apenas de ressalva terminológica.

O método identificado pelo autor é a instrumentalização dos valores e infraestrutura democrático-liberais como disfarce para a natureza disruptiva dessa influência híbrida. Atores autoritários usam uma série de meios não-militares e secretos para semear discórdia entre países democráticos e abalar a coesão interna desses Estados, explica Wigell. Bressan e Sulg (2020) referem-se a conceito semelhante ao refletir sobre a chamada *grey zone*, ou zona cinzenta. A ideia é que alguns atores entendem como gerenciar a ambiguidade entre guerra e paz e explorá-la. Para as autoras, o idealismo ocidental que foca na dicotomia entre guerra e paz leva à incapacidade de sequer enxergar a existência dessa zona cinzenta. Trata-se de um conceito mais amplo que o de interferência híbrida, portanto. Citando Schadlow (2014), as autoras asseveram que o espaço entre guerra e paz não é constituído por um descampado, mas sim por um cenário repleto de competições políticas, econômicas e securitárias que requerem a constante atenção de governos.

> *(...) while 'open societies saw themselves as the uncontested winners and expected that the remaining autocracies, with the help of western pro-democracy actors, would be relegated to the dustbin of history', they have failed to effectively counter authoritarian influencing and propaganda (...) Their war against the grey zone resulted in authoritarian tendencies that undermine the very principles of its own liberal democratic model instead of defending values of openness and human rights – while remaining ineffective against an expanding grey zone. (...) But it does not lead to large-scale wars and rising counts of war casualties. The suffering happens in the grey zone of creeping authoritarianism and it stays under the radar of newspaper headlines. Thus, the scenario is meant to show that there is no black and white dichotomy between a positive, peaceful post-war era with a dominant role of the United States and its allies, which has helped avoid another world war and interstate wars in Western Europe, and a negative, multipolar world of chaos, violence and trouble. Instead, the key to understanding what is happening and how to find an alternative is to acknowledge the grey in both eras – because the opposite of peace is not war, but violence and oppression – not as a dichotomy, but on a continuum.* (BRESSAN; SULG, 2020, p. 11)

Assim, concluem as autoras, o que se chama de *grey zone warfare* é uma tática adequada para um mundo hiperconectado. Relações simbióticas interestatais no campo do comércio, por exemplo, existem há séculos, ponderam; mas com a crescente dependência da Internet e de tecnologias como o 5G, até mesmo espaços privados da vida dos indivíduos podem ser instrumentalizados em disputas de zona cinzenta, tornando possível a subjugação de um dado país sem que haja necessidade de utilizar-se de destacamentos militares. O futuro não terá campos de batalha, acreditam, pois todo e qualquer lugar será um campo de batalha em potencial. Além disso, "*information warfare turns communication into spaces where no single truth exists, but individuals feel like they have to pick what is true. (...) This renders the*

democratic negotiation of a common political project in a society almost impossible", (BRESSAN; SULG, 2020, p. 12). Indivíduos poderão escolher entre várias "verdades", continuam, ou uma combinação subjetiva e intertextual de "verdades" históricas, jurídicas, sociais, culturais e políticas. Para as autoras, a zona cinzenta permite que se explore o deslocamento do objeto referente de segurança, o qual moveu-se da sociedade em direção ao indivíduo. Isso facilita a exacerbação da fragmentação e da polarização da sociedade por meio da provocação de conflitos dentro de unidades familiares, o que pode escalonar até sociedades, Estados, regiões e alianças. Deve-se prestar atenção ao cenário de zona cinzenta, dizem, pois essa representa um espaço não-regulado no qual o novo normal é testado e, posteriormente, legitimado, tornando difusos entendimentos, discursos e práticas.

Eis o porquê da insistência de Wigell sobre a revisão de estratégias de dissuasão. O conceito por ele sugerido, dissuasão democrática, se apóia na ideia de que os valores democrático-liberais – como liberdade de expressão, pluralismo, liberdade jornalística, livre-mercado – não precisam necessariamente ser vulnerabilidades de segurança. Estes podem ser usados como instrumentos na construção da dissuasão democrática proposta por Wigell, de maneira que perpetradores de agressões híbridas interpretem como crível a capacidade de resposta a esses ataques. Assim, acredita o autor, a resiliência e robustez das democracias ocidentais seriam incrementadas.

O desafio, portanto, seria conciliar a resistência à interferência híbrida sem que se comprometam os valores democráticos que essa resistência procura defender. O incremento do controle estatal sobre a sociedade civil não constitui estratégia viável; tampouco o é a emulação do recurso à desinformação, à interferência em assuntos eleitorais de outros países e à instrumentalização da corrupção, o que também corroeria os valores democráticos. O ponto é que "*beyond the rigidness of state-based solutions, Western democracy harnesses market and society-based approaches to dealing with risks and threats. These can readily be used to strenghten deterrence against hybrid interference*", (WIGELL, 2019, p. 4).

Ainda que na teoria e na prática da dissuasão o recurso ao poderia bélico seja frequente, a militarização das respostas à interferência híbrida é contraproducente, de acordo com o autor. Para ele, mesmo que as discussões sobre hibridismo foquem em táticas militares de natureza dúbia, como os *"little green men*" usados pela Rússia no conflito com a Ucrânia iniciado em 2014*,* os desafios urgentes são as iniciativas sutis, não-militares empregadas por regimes autocráticos para penetrar o tecido social de países democráticos. São práticas

estratégicas que empregam uma miríade de técnicas de controle reflexivo cujo propósito é semear dissensões e manipular percepções e comportamentos. A natureza sorrateira dessas técnicas permite que se evite o confronto direto com o país-alvo, enfraqueça sua coesão interna e permita a negação plausível de qualquer envolvimento do agressor com os ataques híbridos.

A interferência híbrida é uma abordagem que pode ser customizada com diferentes técnicas a depender das vulnerabilidades específicas do país-alvo. Wigell categoriza os instrumentos de manipulação e incentivo a dissensões em três grandes grupos: diplomacia clandestina, geoeconomia e desinformação.

A diplomacia clandestina envolveria o fomento ao que Wigell chama de "*counter-elites*" e a agitadores locais. Pode envolver também o apoio a partidos radicais ou secessionistas, lobistas, figuras influentes e movimentos de protesto. Assim, enfraquece-se o apoio ao governo central e polariza-se o ambiente político. Dissensões étnicas ou religiosas, inclinações antigoverno ou anti-establishment podem ser instrumentalizados para desgastar a confiança no governo e em sua legitimidade. Como exemplo de diplomacia clandestina, o autor menciona o apoio dos EUA aos Contra na Nicarágua, o apoio do Irã ao Hezbollah no Líbano e o fomento do AKP turco a dissensões na diáspora turca em particular e na muçulmana em geral com o fim de rejeitar valores ocidentais e insuflar tensões étnicas.

A questão, diz Wigell, é que apesar de a diplomacia clandestina estar normalmente associada à atuação de serviços de inteligência, ela também pode abarcar organizações criminosas como aliadas no provimento de capacidades adicionais e de negação plausível de envolvimento com as atividades dessas organizações. Ele faz referência ao crescente corpo de evidências da colaboração entre organizações criminosas na Europa e os serviços de inteligência russos e entre o Partido Comunista Chinês e organizações criminosas em Taiwan. Para o autor, violência artificialmente insuflada por milícias e gangues pode ser instrumentalizada para provocar tensões étnicas e políticas. Wigell acrescenta que essa simbiose entre crime e inteligência é particularmente nebulosa no ciberespaço, no qual ainda se tem a participação de ciberativistas em atividades que turvam ainda mais a diplomacia clandestina.

A geoeconomia, por sua vez, refere-se ao uso de instrumentos econômicos para viabilizar a interferência estratégica nos países-alvo. Wigell inclui na categoria o uso de sanções econômicas, mas não na forma como se entende normalmente na Organização das

Nações Unidas, no entanto. Consoante a sutileza dos métodos empregados no conceito de interferência híbrida, as sanções seguiriam, por exemplo, o método russo:

> *A prominent example is Russia's use of its energy resources as a means of driving political wedges within EU-member states, as well as between them at the European level. The Kremlin has also been channelling money to populist and anti-EU parties and movements to accelerate centrifugal forces within the Union. Capturing strategic sectors of the economy, such as critical infrastructure, finance and media, by which the Kremlin can attempt to destabilize the target country and manipulate local economic conditions, generate unfair profits for some local stakeholders while punishing others, and in that way achieve greater political influence, has formed part of this toolbox.* (WIGELL, 2019, p. 5)

A construção de relacionamentos com atores-chave do setor industrial e da vida política pode ser frutífera se é enquadrada em contexto de oportunidades de negócio. Cria-se, assim, uma rede de contatos locais em posições de poder que podem advogar em prol dos interesses do país perpetrador da interferência. É o método empregado pela China, de acordo com Wigell, em particular no seu entorno imediato. Denominado Qiaowu, foi utilizado com particular esmero na Austrália e na Nova Zelândia, aliados dos Estados Unidos na região indo-pacífica.

Assim, continua o autor, o uso da corrupção e do *lobby* reforçam o papel da geoeconomia dentro do conceito de interferência híbrida. Redes de corrupção atravessam fronteiras e fomentam a formação de quintas-colunas que atuam como intermediárias na interferência em processos econômicos e políticos dos países-alvo. A geoeconomia e a diplomacia clandestina se complementam e formam um ciclo de corrupção por intermédio do qual o tecido institucional do país-alvo erode paulatinamente. O terreno torna-se fértil para forças radicais oportunistas, aprofundando portanto a polarização política.

Por fim, a desinformação diz respeito à distribuição de informações falsas ou parcialmente incorretas no ecossistema de comunicação de dado país. A tecnologia é aliada também neste âmbito, pois "*the hyper-connected nature of cyberspace works as a force multiplier – it allows external powers to plant, disseminate and lend credibility to disinformation*", (WIGELL, 2019, p. 6).

As campanhas de desinformação são pensadas para criar um clima de desconfiança e insatisfação. A distorção dos fatos é crucial para que esse objetivo seja atingido. Inundar sites noticiosos e redes sociais com "versões alternativas" dos acontecimentos acaba por atrapalhar a capacidade da população de separar fato de ficção. A consequência, de acordo com Wigell,

são danos à confiança que a população deposita não apenas em veículos tradicionais de mídia, mas em fontes profissionais de informação em geral. Os próprios algoritmos nos quais as redes sociais se baseiam desempenhariam papel importante nesse jogo ao amplificar o "*echo chamber effect*" que o autor destaca. Bradshaw e Howard (2019), Bradshaw, Bailey e Howard (2020)[12], Hanson et al. (2019), Lupion (2019) produziram reflexões detidas sobre o problema da desinformação, inclusive com dados quantitativos e metodológicos sobre as campanhas por eles monitoradas, cujo caráter, dizem, é eminentemente estatal – ainda que se use terceiros para fins de *plausible deniability*.

Um exemplo dado pelo autor é a estratégia russa em países em que haja ansiedade exacerbada a respeito do influxo de refugiados. Divulga-se massivamente casos reais e falsos de crimes cometidos por refugiados, ao mesmo tempo em que se retrata os governos de países ocidentais como se fossem relutantes ou incapazes de lidar com a questão. Com a opinião pública já dividida sobre o assunto, campanhas de desinformação nesses moldes intensificaram a polarização.

O interessante é que as narrativas promovidas por campanhas de desinformação não precisam necessariamente ter efeitos sobre a totalidade da população do país-alvo, mas apenas sobre porção desta que constitua contingente suficiente para aprofundar clivagens políticas. Wigell defende que criar incertezas sobre verdades objetivas abre espaço para que movimentos políticos radicais ganhem espaço para divulgação de suas ideias até então marginalizadas[13].

---

[12] Bradshaw, Bailey e Howard (2020) ratificam e complementam os achados de Bradshaw e Howard (2019) sobre o que denominam *industrialized disinformation*, fenômeno que "*remains a critical threat to democracy*", (BRADSHAW; BAILEY; HOWARD, 2020, p. i). Em relação à atividade de tropas cibernéticas, verificou-se em 2020 que 81 países utilizam-se das redes sociais para espalhar *computational propaganda*, um aumento em relação a 2019, quando se identificou 70 países que empregavam essas ferramentas. Sobre a postura das *big tech* no que diz respeito à instrumentalização de suas plataformas por essas tropas cibernéticas, Bradshaw, Bailey e Howard (2020) notam a disposição dessas empresas em agir para remover contas inautênticas entre janeiro de 2019 a novembro de 2020, embora notem que tropas cibernéticas ainda gastaram US$10 milhões em anúncios políticos veiculados em redes sociais. Finalmente, sobre o fornecimento de serviços de campanhas de manipulação por agências privadas, os autores afirmam terem mapeado em 2020 empresas que atuam em 48 países. Desde 2018, foram identificadas mais de 65 empresas oferecendo serviços dessa natureza, e cerca de US$60 milhões foram gastos em contratos com tais agências desde 2009. A conclusão é que "*industrialized disinformation has become more professionalized and produced on a large scale by major governments, political parties, and public relations firms*. (…) *These techniques will also continue to evolve as new technologies — including Artificial Intelligence, Virtual Reality, or the Internet of Things — are poised to fundamentally reshape society and politics.* (…) *Social media platforms can be an important part of democratic institutions, which can be strengthened by high-quality information. A strong democracy requires access to this information*", (BRADSHAW; BAILEY; HOWARD, 2020, p. 21).

[13] Sobre desinformação, cumpre mencionar os argumentos de Sultan (2019). Em referência ao método russo – e de países que o copiam, como Irã e China, de acordo com sua opinião –, o autor afirma que a velocidade de resposta às narrativas falsas é fundamental. "*If we are to be successful in countering the false narratives and*

O autor reforça seu argumento de que a autocontenção do Estado, o pluralismo, a liberdade jornalística e o livre mercado, pilares das democracias ocidentais, proveem brechas para ações hostis que se manifestem por intermédio da combinação personalizável de diplomacia clandestina, geoeconomia e desinformação. O uso desses instrumentos é impulsionado pelos valores liberais que buscam erodir. Enquanto prática estratégica, a interferência híbrida aproveita-se da abertura característica de regimes democráticos – em particular dos veículos de mídia independentes que, portanto, enfrentem poucos constrangimentos derivados da regulação estatal – como vetores de campanhas de desinformação. Wigell complementa o raciocínio ao dizer que o desafio posto pela interferência híbrida põe em xeque a autocontenção do Estado, pois esta colocaria em risco a estabilidade das democracias ocidentais.

É nesse momento que Wigell desenvolve melhor o conceito de dissuasão democrática. Ele o compara com o que tradicionalmente se entende por dissuasão em relação a quatro pontos principais: agência, base de poder, métodos, resposta e objetivo de segurança.

Figura 3 – Dissuasão Tradicional e Dissuasão Democrática.

	Traditional Deterrence	Democratic Deterrence
AGENCY	State-based	Whole-of-society
POWER BASE	Hard	Soft
MEANS	Military	Non-military
RESPONSE	Symmetrical	Asymmetrical
SECURITY AIM	Absolute	Restricted

Table 1. Contrasting traditional deterrence with democratic deterrence

Fonte: Wigell (2019)

O ponto principal do quadro acima, para o autor, é a diferença entre os tipos de resposta que são dadas na dissuasão tradicional e na dissuasão democrática. Ele pontua que a

propaganda, we need to be developing social media countermeasures and Standard Operations Procedures (SOPs) to parallel the deployment of personnel and ground communication systems", (SULTAN, 2019, p. 46).

interferência híbrida necessariamente leva a resposta para fora do campo no qual a ação ocorre. Isso significa dizer que a assimetria é característica inescapável da dissuasão democrática, pois responder à interferência híbrida fazendo uso dos mesmos métodos que essa emprega, como interferência em eleições, operações corruptas e campanhas de desinformação, por exemplo, aprofundam a deterioração dos valores democrático-liberais e da legitimidade normativa das democracias ocidentais. Acrescente-se a isso a natural dificuldade de atribuição em casos de interferência híbrida em razão tanto do uso de terceiros quanto de inteligência artificial para execução dos planos.

Por isso, continua Wigell, a dissuasão democrática acomoda a constatação de que não é possível impedir todas as agressões perpetradas dentro de uma estratégia de interferência híbrida. Para compreender isto, é útil pensar na dissuasão democrática como mais próxima da prevenção a crimes que da dissuasão nuclear, diz o autor. Nem todos os crimes podem ser impedidos e nem todos constituem grave ameaça à segurança nacional. Isto posto, o objetivo passa a ser aplacar a frequência e a efetividade da interferência externa.

Face aos argumentos desenvolvidos ao longo do artigo, é curioso que Wigell afirme que a dissuasão militar pode contribuir para o arrefecimento da interferência híbrida ao fomentar dúvidas sobre a intensidade da resposta cinética a uma provocação. Ele considera que métodos tradicionais de dissuasão devem não apenas ser mantidos, mas também intensificados.

Outro fator importante, de acordo com Wigell, é tornar robusta a resiliência do Estado e da sociedade por intermédio do tratamento de suas vulnerabilidades. Ele menciona nominalmente a abrangente estratégia de segurança da Finlândia, cujo mote é a cooperação consistente entre autoridades, indústria e sociedade civil com o fim de assegurar as funções vitais do Estado e da sociedade; da Suécia, denominado modelo de “defesa total”; e da Noruega, modelo de “apoio e cooperação”.

A efetividade dessas estratégias face à interferência híbrida, aponta o autor, reside na centralidade atribuída à cooperação entre diferentes setores da sociedade. Para ele, atores da sociedade civil são fundamentais no monitoramento da interferência híbrida, com destaque para o papel de vigilância do jornalismo investigativo de meios de comunicação independentes e autônomos. Por isso, diz Wigell, as democracias ocidentais devem incentivar grupos da sociedade civil em geral e da mídia em específico que se dedicam ao monitoramento e detecção de iniciativas de interferência híbrida.

Eles têm o potencial de investigar de maneira contínua e minuciosa laços diplomáticos, planos de desinformação e redes geoeconômicas entre agressores híbridos e grupos domésticos nos campos dos negócios e da política, por exemplo. Atores domésticos, completa o autor, frequentemente compreendem melhor as dinâmicas locais e são mais ágeis na avaliação destas. Sistemas de alerta rápido, programas de alfabetização midiática e treinamento de profissionais de mídia no reconhecimento de campanhas de desinformação são exemplos de medidas específicas que podem ser implementadas. Conclui Wigell que o apoio à sociedade civil e o incentivo à mídia independente e autônoma fortalecem a resiliência cognitiva da sociedade.

A regulação de redes sociais como o Facebook e o Twitter é citada por Wigell como medida importante de contenção de operações de influência híbrida[14]. O porquê da defesa dessa via de ação é direto: transparência nas plataformas de redes sociais, extensível a anúncios políticos, pode ser instrumental no combate a campanhas de desinformação ao expor os mecanismos por intermédio dos quais elas são implementadas. Além disso, a transparência pode auxiliar a exposição e interrupção de alianças entre agressores híbridos e grupos domésticos, de maneira que o sigilo com o qual suas pautas são promovidas seja impossibilitado.

A transparência proposta pelo autor não se restringe às redes sociais. Esta deve ser incentivada também no mercado financeiro, pois contrainteligência econômica pode ser reforçada por parcerias público-privadas com *hedge funds* e outros operadores financeiros. Wigell defende que ONGs, partidos políticos, veículos de mídia, institutos de pesquisa e *think tanks* devem sim ser obrigados a apresentar publicamente suas fontes de financiamento[15].

Wigell também acredita que as democracias ocidentais devem tirar proveito de suas estruturas políticas de inclusão. A construção da resiliência depende do conhecimento da população a respeito de ameaças híbridas e de seu envolvimento no combate a elas. Assim,

---

[14] Não seria razoável mencionar a regulação das redes sociais, vedete das discussões sobre combate a *fake news*, sem acenar ao debate sobre seu lugar em regimes democráticos de direito. Não é questão pacífica, em absoluto. A sugestão de Wigell faz sentido dentro dos argumentos que ele desenvolve ao longo do artigo sobre interferência híbrida, mas é preciso sopesar a utilidade da medida no plano teórico com seus possíveis efeitos colaterais práticos. A esse respeito, os seguintes textos levantam pontos interessantes Rochefort (2020), Tusikov e Haggart (2019), Brannon (2019), Suzor (2018), Flew (2015), Jørgensen e Zuleta (2020), Samples (2019), Anderson e Rainie (2020), Turner (2018), Helberger (2019), Gorwa (2019), Lindner e Aichholzer (2019), Campos, Maranhão e Abrusio (2020).

[15] Thorsten Benner não chega a ser a voz que clama no deserto a respeito desse assunto, mas o financiamento de regimes autocráticos a instituições ocidentais, nomeadamente universidades e *think tanks*, é assunto constante em suas redes sociais. Benner (2015; 2017; 2018; 2019a; 2019b) traz boas reflexões a respeito.

um entendimento abrangente sobre segurança é necessário, pois a resistência aos ataques de atores hostis ao pluralismo democrático requer que se foque no aprimoramento da coesão social. O autor recorre ao emprego do conceito holístico de *societal security*, ou segurança social em nossa tradução, para defender que se entenda a política inclusiva e o bem-estar social como soluções no campo da segurança para clivagens sociais. Não é possível, acredita Wigell, falar em dissuasão democrática a interferência híbrida sem mencionar políticas públicas que aprimorem a educação, a coesão social e o bem-estar da sociedade como um todo, inclusive de minorias étnicas e diásporas. Oportuno lembrar que estes podem ser usados como vetores de esforços de interferência híbrida.

A atualização da legislação eleitoral também é um ponto importante levantado pelo autor, para quem boa parte dos países ocidentais não leva em consideração em seus códigos eleitorais a possibilidade de que atores hostis estrangeiros tentem influenciar pleitos fazendo uso de táticas como financiamento de partidos políticos e associações. Novamente, a parceria entre iniciativa privada, governo e sociedade civil pode ser apoiada na busca de alternativas para o monitoramento eficiente de tentativas de interferência eleitoral.

Os perpetradores devem julgar críveis os limites que, ultrapassados, levarão os países-alvo de interferência híbrida a agir. Para Wigell, além de possíveis sanções e contramedidas a serem empregadas, a democracia em si é instrumento de *soft power* que pode desafiar os agressores em seu próprio território:

> *Pushing the truth against internal propaganda and cover-ups in authoritarian regimes will serve as a challenge to them. Going harder on Western values, for instance, by visibly strengthening programmes of democracy and human rights promotion would communicate resolve and threaten to shift the battleground to the authoritarian states' home turf. In this vein, cultivating Western democracies' own influence networks and proxies, using civil society as a middleman, and other means of soft power such as cultural institutions, citizen diplomacy and connectivities, provide the means for democratic compellence. Supporting political dissent, not only in target autocracies, but also among their diasporas residing in Western democracies can be an effective way to break through authoritarian controls.* (WIGELL, 2019, p. 13)

Ironicamente, a proposta parece deveras semelhante à definição de diplomacia clandestina do próprio autor. Wigell antecipou essa observação e ofereceu uma defesa do *soft power* da democracia. Para ele, "*whereas hybrid interference is covert, and therefore illegitimate, democracy and human rights promotion is overt and transparent, and therefore a form of legitimate public diplomacy, albeit with a sharp edge designed for compellence purposes*", (WIGELL, 2019, p. 14). O autor declara em seguida que, ao contrário da

interferência híbrida, a dissuasão democrática obedece às prescrições do Direito Internacional. Logo após, adverte as democracias ocidentais de que o investimento na dissuasão democrática pode levar ao endurecimento da repressão interna nos países que recorrem à interferência híbrida, mas, em última instância, a exposição de seu autoritarismo impulsionará a busca por legitimidade normativa, o que tende a favorecer as democracias ocidentais e reforçar seu *soft power*.

Forçoso observar que Wigell parece recorrer ao *wishful thinking* nesse ponto. O autor não oferece evidências de que essa é a sequência lógica de acontecimentos uma vez que as democracias ocidentais invistam no *soft power* democrático. Acreditar que o endurecimento da repressão interna tornará óbvio o autoritarismo de dado país e, portanto, dará fôlego à oposição democrática no plano doméstico equivale a acreditar que o arco da história corre necessariamente para o que no Ocidente se considera progresso. Trata-se de profissão de fé.

O argumento de que a dissuasão democrática é permitida pelo Direito Internacional e a interferência híbrida não parece relativamente frágil. À parte discussões sobre o porquê da legitimidade de um em detrimento do outro, a estratégia aventada por Wigell mostra-se coerente com a linha argumentativa por ele defendida: o caminho para lidar com ameaças híbridas cujo fim seja a erosão dos valores democrático-liberais não é sucumbir à tentação de responder aos ataques utilizando-se dos mesmos instrumentos dos agressores, mas sim aprofundando os mesmos valores que estão sob ataque. Para o autor, estes constituem trunfo. A resposta concertada de outras democracias fortalece o potencial dissuasório dessa estratégia:

> *By signalling preparedness to harden sanctions in a coordinated manner, Western democracies would strengthen deterrence. Such compellence is naturally most effective when not having to carry out the threat in the end, and thus hinges on credibility. Threatening forceful and concerted cyber retaliation, while also undertaking some retaliatory measures, should form part of the strategy*. (WIGELL, 2019, p. 14)

2.2 *The Darkening Web*: a ameaça de mudança da natureza do ambiente cibernético

Klimburg (2018) argumenta que os objetivos dos Estados no ciberespaço, em consonância com os avanços tecnológicos de um mundo interconectado, são fonte de riscos não desprezíveis para o bem-estar humano. É um ponto parecido com o levantado por Wigell (2019). Klimburg, no entanto, preocupa-se principalmente com a própria natureza do

ambiente cibernético. Para ele, os riscos supracitados referem-se não apenas à capacidade de empreender destruição de larga escala em conflitos interestatais, mas, principalmente, ao dano possivelmente catastrófico a sociedades democráticas liberais por meio da instrumentalização de informações em geral como armas em campanhas hostis entre países rivais. O grande problema que se enfrenta, segundo o autor, é a possibilidade de que, em um futuro não tão distante, a Internet se torne artefato de dominação. Klimburg não despreza os desafios técnicos do ciberespaço – crimes cibernéticos, inteligência, assuntos militares, governança e gerenciamento de crises de segurança nacional são alguns dos assuntos citados por ele –, mas critica o que chama de "armadilha conceitual ocidental", que levaria analistas a supor que os desafios de cibersegurança sejam predominantemente técnicos e não humanos.

Com efeito, o autor reconhece que o desenvolvimento tecnológico do ciberespaço deteriorou a capacidade de governos o regularem e legislarem a seu respeito. A velocidade dessas transformações tem implicações sérias para a segurança nacional, fomentando o que Klimburg chama de "*bottom-up driven policy process*": o componente técnico domina a formulação de políticas públicas, sobrepondo-se ao *framework* jurídico e político.

O conceito de superfície de ataque também é importante para a compreensão do problema. Quanto mais amplo e complexo os sistemas de informação, maior a dificuldade de defendê-los. Trata-se do que Nye (2010) chamou de vulnerabilidade assimétrica: atores de maior porte dependem de sistemas complexos que podem ser atacados com maior facilidade.

Klimburg alerta, inclusive, que o comportamento *online* já é manipulado por interesses escusos, o que incentiva o florescimento de uma indústria dedicada à descoberta de maneiras de extrair perfis psicológicos e de personalidade de usuários utilizando-se das informações fornecidas por *big data*. O objetivo seria compilar formas cada vez mais eficientes de manobrar esses usuários para fins comerciais e políticos. Isso é viável também porque comportamentos *online* e *offline* são cada vez mais indistinguíveis e simbióticos.

Em democracias liberais, diz Klimburg, esse instrumental é majoritariamente empregado no campo do marketing digital. No entanto, alerta, não é o caso em países como China e Rússia, os dois grandes exemplos por ele analisados. Ambos têm doutrinas de informação consolidadas que baseiam não apenas ações de vigilância interna, mas também operações de influência e guerras de informação direcionadas à população de outros países. Para Klimburg, democracias liberais tendem a focar em narrativas de ataques puramente técnicos no ciberespaço, enquanto autocracias como China e Rússia temem, sobretudo, os ataques psicológicos de narrativas de guerras de informação.

Há duas formas de enxergar o poder estatal no ciberespaço, diz Klimburg: vendo-o como novo instrumento dos tradicionais conflito interestatal e espionagem; ou definindo-o como um franco fomentador de guerras de informação com toques de propaganda e controle discursivo.

> *For nearly two decades, Russia, together with like-minded states such as China and Iran, has repeatedly brought forward international resolutions attempting to support what is today called "national cyber-sovereignty". The Cyber-sovereignty faction consistently tries to emphasize that information in all its forms is a weapon, most often employed by "terrorists" but really extending to any information (read: internet content) that is uncomfortable to the ruling elite. Essentially, it is shorthand for enabling wide-reaching Internet censorship and other types of activity to ensure the regime stability of these authoritarian states*. (KLIMBURG, 2018, p. 16)

O objetivo, diz, é reenquadrar a informação como arma a ser regulada. Com certo exagero vocabular, Klimburg chama isso de um *armageddon* que deve ser evitado por democracias liberais. Isso requereria a rejeição em larga escala do comportamento hostil no ciberespaço direcionado não apenas à infraestrutura crítica e à economia de países-alvo, mas também à mídia e às fontes de informação política. Propaganda, *fake news* e guerras de informação têm por alvo a erosão da confiança.

Sobre ataques famosos, como o SYNful Knock[16], Klimburg explica que eles perpassam as camadas do ciberespaço: social, de dados, lógica e física. Alguns apenas são factíveis para atores sofisticados; outros podem ser perpetrados por aqueles que comparativamente dispõem de menos habilidade, mas têm acesso a softwares usados em testes de segurança. É preciso ser cuidadoso para não confundir *hacking* técnico com operações no ciberespaço em geral, alerta o autor. Ao incorrer nesse erro, pressupõe-se que a quebra da confidencialidade, da integridade e da disponibilidade de dados é o único objetivo de um agressor cibernético. Para Klimburg (2008), o que frequentemente escapa aos civis é que forças militares e agências de inteligência não necessariamente querem apenas apreender ou manipular dados. Podem ter como alvo também influenciar informações e alterar opiniões e percepções. Dessa maneira, *hacking* pode ser apenas uma ferramenta para atingir outros objetivos.

[16] Trata-se de ataque direcionado a roteadores da fabricante Cisco. O SYNful Knock afetou aproximadamente 20 países. Adicionalmente, o implante podia ser ativado remotamente. Isso foi possível não por causa de *backdoors*, mas porque os roteadores saem de fábrica com senhas padrão. Para análise técnica sobre o ataque, ver Hau, Lee e Homan (2015).

O autor considera importante salientar que, em sua maioria, os ataques cibernéticos não são confirmados em público. São mantidos em segredo por empresas e governos, tanto por receio de consequências político-econômicas quanto de danos reputacionais e desdobramentos jurídicos. Klimburg sustenta que, na maior parte dos casos, o alvo não sabe que sofreu um ataque cibernético. Além disso, agências de inteligência podem ter conhecimento sobre esses ataques, mas não estão livres para informá-lo.

A respeito da abordagem *multistakeholder* para questões cibernéticas, Klimburg prefere a definição da Agenda de Tunis[17], de 2005, que incluiria Estados, o setor privado, a sociedade civil, as organizações intergovernamentais, as organizações internacionais, a comunidade técnica e a comunidade acadêmica. Para o autor, a vantagem dessa definição é ser precisa.

O assunto no qual ele se detém longamente, no entanto, não é a arquitetura da governança da Internet, à qual, de acordo com ele, os países ocidentais tendem a se aproximar por intermédio de ministérios da economia ou infraestrutura. Não, para Klimburg, o nó górdio está no campo da cibersegurança internacional, "*the realm of pure diplomacy, with issues of war and peace firmly on the table. And unlike in Internet governance, government interest is certainly welcome*", (KLIMBURG, 2008, p. 118). Ele acrescenta que há necessidade real e urgente de lidar com a crescente possibilidade – e as consequências que adviriam da concretização desse cenário – de que Estados entrem em conflito no ciberespaço e por intermédio dele. Nesse diapasão, o autor afirma que os objetivos comuns de evitar a escalada acidental das hostilidades, bem como a perda de controle sobre estas, foram estabelecidos em maio de 2015 na quarta *Global Conference on Cyberspace*, ocorrida na Haia, Holanda.

A avaliação do autor é que países que advogam a soberania cibernética, dentre os quais merecem destaque Rússia e China, têm vantagem significativa na valsa política pelo controle do ciberespaço por estarem continuamente em postura ofensiva. Klimburg observa que, por desafiarem a ortodoxia estabelecida, esses países mantêm a inciativa e o *momentum* político em comparação àqueles que tentam conservar o arranjo da Internet como domínio livre da ingerência governamental. Assim, no *front* de batalha estão não apenas a definição de abordagem *multistakeholder*, mas também a maneira como a informação é tratada enquanto

[17] A Agenda de Tunis para a sociedade da informação foi uma declaração consensual adotada em 18 de novembro de 2005 no contexto do *World Summit on the Information Society* em Túnis, na Tunísia. Esta defendia a criação de um fórum de governança da Internet e uma estrutura nova, enxuta de *multistakeholder* de governança para a Internet (WSIS EXECUTIVE SECRETARIAT, 2005).

sujeito de segurança nacional. Em última instância, diz o autor, o objetivo de soberanistas cibernéticos é a reconceitualização da ordem global tal como definida pelo Ocidente.

Klimburg argumenta que a Rússia tem liderado desde 1998 tentativas de levar a Organização das Nações Unidas a adotar postura mais assertiva no que diz respeito a questões de cibersegurança. Essas tentativas incluiriam esforços para encorajar o abandono dos termos cibersegurança e ciberespaço, vocábulos eivados de imprecisão, na opinião russa. Em seu lugar, a Rússia advogaria o emprego da expressão *information security*, que poderia ser traduzida como segurança da informação. O problema, explica o autor, é que o entendimento russo sobre o que seria segurança da informação nada tem a ver com o que países ocidentais imaginam quando se deparam com a expressão.

> *The Russian and Chinese definition of information security reflects those nations' attempts to legitimize state control over all aspects of information, in particular toward hostile content. While Russia has not managed to get the term accepted in the UN (the accepted compromise is ICT security, which is actually even further away from cybersecurity), it does not stop Russia from submitting the same UN resolution, again and again, in a persistent attempt to advance the term "information security".* (KLIMBURG, 2019, p. 119)

Assim, de acordo com o autor, tanto para a Rússia quanto para sua predecessora, a União Soviética, a Organização das Nações Unidas (ONU) é fonte de fascínio ambivalente: por um lado, representa a ordem mundial tal como definida pelo Ocidente, ancorada sobre o respeito ao Estado de Direito, a salvaguarda dos direitos humanos e a limitação da soberania das nações na prática; por outro lado, continua Klimburg, a ONU representaria para a Rússia a oportunidade de jogar contra o Ocidente em seu próprio tabuleiro, por assim dizer, "*by leading the majority of the 192 nations in the UN General Assembly (UNGA) who are not Western and not rich into a showdown (...). Russia has long seen its ultimate global role as the natural leader of the antiliberal world order (...)*", (KLIMBURG, 2019, p. 119).

Em relação ao ativismo multilateral do eixo autocrático, o autor discorre em particular sobre o *Group of Governmental Experts* (GGE) criado no âmbito da Organização das Nações Unidas para discutir segurança da informação e medidas de cooperação internacional nessa seara. A criação desse GGE foi proposta pela Rússia em 2001 e a primeira reunião se deu em 2004 sem que houvesse consenso entre os participantes sobre definições terminológicas.

O destaque da segunda reunião em 2010 teria sido, para Klimburg, o reconhecimento da importância do desenvolvimento de normas que delineiem a responsabilidade dos Estados por atos cometidos no ciberespaço. Já em 2013, na terceira reunião do GGE, enfatizou-se a posição de que normas e medidas de construção de confiança deveriam ser desenvolvidas também em organizações regionais de segurança. Ainda na terceira reunião, obteve-se consenso sobre a aplicabilidade do Direito Internacional a todos os aspectos dos conflitos cibernéticos, o que, observa o autor, incluiria implicitamente o Direito Internacional Humanitário e a Carta da ONU. Klimburg acrescenta que China e Rússia, no entanto, renegaram essas conclusões posteriormente. Em 2015, a quarta reunião foi marcada por desdobramentos dessa retração, com China e Rússia preocupadas com a possibilidade de que os Estados Unidos invocasse o artigo 51 da Carta da ONU em resposta a ciberespionagem.

Apesar dessa celeuma, os Estados Unidos capitanearam a aprovação, por consenso, de três normas que regulassem o comportamento dos Estados no ciberespaço: que estes não deveriam interferir na capacidade de centros de estudos, resposta e tratamento de incidentes de segurança (CERTs, na sigla em inglês) de agir face a incidentes, ou mesmo usar tais centros para conduzir ataques; que Estados deveriam apoiar-se mutuamente na investigação de incidentes; e, finalmente, que Estados se comprometeriam a não atacar a infraestrutura crítica uns dos outros. Propôs-se, ainda, uma quarta norma, que versava sobre espionagem com fins econômicos. Esta, no entanto, não foi adotada. A avaliação de Klimburg é que a quarta reunião constituiu uma vitória para o bloco de países que apoiavam a conservação da internet livre, em oposição àqueles que adotavam posturas ciber-soberanistas[18].

Embora reconheça que o GGE não era o único grupo na ONU que discutia cibersegurança internacional, Klimburg defende que era o mais importante. É neste foro que os países ciber-soberanistas buscam colocar suas pautas em discussão e, conquanto não tenham obtido êxito no GGE supramencionado, Klimburg adverte que a legitimação internacional de suas posições segue como objetivo, em particular dos chamados “três males” discutidos no âmbito da Organização para Cooperação de Xangai: o terrorismo, o separatismo

[18] Desde então, outras iniciativas foram criadas na Organização das Nações Unidas para discussão do tema. A mais recente foi estabelecida pela Assembleia Geral em 2018 por intermédio da resolução 73/266 para estudo da questão da segurança no uso de ICTs. O processo divide-se em duas vertentes: um *Open-ended Working Group* e um *Group of Governmental Experts* (GGE). O período de trabalho será de 2019 a 2021, quando o GGE deverá apresentar à Assembleia Geral um relatório final sobre o encorajamento de comportamentos responsáveis dos Estados no ciberespaço no contexto da segurança internacional. O GGE será composto por 25 países e fará consultas informais tanto aos membros da ONU quanto a organizações regionais, como a União Africana, a União Europeia e a Organização dos Estados Americanos. O Presidente do Grupo é o Embaixador Guilherme de Aguiar Patriota. Para mais informações a respeito, ver Organização das Nações Unidas (2020).

e o extremismo[19]. Definir a informação como arma serve a esse propósito, de acordo com o autor.

Para China e Rússia, continua Klimburg, a aplicação do Direito Internacional Humanitário a questões cibernéticas é um ponto particularmente sensível. O autor atribui essa reticência à maneira como o binômio compreende a constituição do poder cibernético, que seria caracterizado não pela capacidade de atacar infraestrutura crítica, mas sim de influenciar e manipular o discurso político no campo civil. A implicação óbvia é que ambos essencialmente consideram a dimensão cibernética um meio de controle e influência de populações, e não necessariamente uma expansão do leque convencional de ferramentas de guerra e espionagem.

Propagandas midiáticas que empreguem mentiras, a instrumentalização de blogueiros falsos e de exércitos de *trolls*, campanhas de assassinato de reputações, *fake news*, ataques direcionados a jornalistas e pesquisadores de destaque e até mesmo tentativas de subverter o processo democrático são métodos amplamente condenados no Ocidente, na opinião de Klimburg, embora tenham sido frequentemente empregados durante a Guerra Fria. Desde então, pontua o autor, tem-se conservado consenso democrático de que essas medidas devem ser consideradas apenas em casos extremos e certamente não devem ser o padrão. Ocorre que a popularização da *Internet of Things* (IoT) potencializou consideravelmente a capacidade de se conduzir operações dessa espécie.

Eis a questão: a ideia de que não há ligação clara entre ciberataques técnicos e psicológicos é predominante no Ocidente, mas abertamente rejeitada por oficiais e especialistas chineses e russos em artigos e em contextos diplomáticos, observa o autor.

> *Opening the Pandora's box of information warfare is something that Western governments have largely avoided (...). Russia's return to full-fledged propaganda war in recent years has prompted some Western governments to reopen discussions on elements that are essentially part of information warfare. The situation is further imperiled by the reality that though the United States in particular put thoughts of all-out information warfare to rest in 1999 (and instead backed information operations, or IO, and expanded signals intelligence gathering), some aspects of information warfare have proven harder to kill and continue to lurk in the shadows of standard operating procedures and concepts of operations.* (KLIMBURG, 2019, p. 129)

[19] Sobre esse assunto, ver Aris (2009).

O que se pode concluir das informações dadas, assevera o autor, é que a ameaça de narrativas de guerra de informação, com a legitimação internacional da posição autocrática de que toda informação é uma arma, é um dos grandes desafios que sociedades democráticas enfrentam hoje. A consequência é transformar a livre expressão e os direitos humanos básicos em campo de batalha. Ainda que as consequências cinéticas de conflitos cibernéticos possam ser assaz graves, na avaliação de Klimburg a deflagração de uma guerra de informação apresenta perspectiva insidiosa por ameaçar a fundação das liberdades democráticas.

Ao comparar as perspectivas dos Estados Unidos e da Rússia sobre poder cibernético, o autor observa que há no país norte-americano tensão entre missões ofensivas e defensivas no ciberespaço, de um lado, e aspectos lógicos – isto é, códigos de programação – e psicológicos do conflito cibernético – no que Klimburg se refere a entre *information ops* e guerras de informação. Em referência às elucubrações de Marshall McLuhan, o autor pontua que essa tensão destaca a diferença entre a percepção da dimensão cibernética ou como apenas outra ferramenta de guerra ou como algo que traz à baila guerrilhas de informação que enfraquecem a divisão entre participação militar e civil.

A pergunta que se levanta sobre o porquê de China e Rússia terem visões tão particulares sobre poder cibernético é respondida por Klimburg em exposição a propósito da doutrina de ambos países sobre ciberespaço e informação. No que diz respeito à Rússia, as raízes foram lançadas ainda na União Soviética, especificamente na década de 1950. Nessa época, explica, o imaginário sobre uma dimensão cibernética estava intrinsecamente relacionado a noções de controle estatal sobre informações e indivíduos. Assim, pensadores estratégicos das searas militar e de inteligência refletem sobre conflitos no campo da informação há aproximadamente 60 anos.

Essa reflexão aprofundada é marcadamente diferente da abordagem ocidental a sistemas em rede. Curiosamente, o interesse russo em *kibernetika* foi pesadamente influenciado pelo trabalho do matemático americano Norbert Wiener, um relativo desconhecido em seu próprio país, conta Klimburg.

Já em 1961, no 22º Congresso do Partido Comunista, o manifesto do encontro asseverava que a cibernética, entendida como uma ramificação das teorias de matemática e redes que possibilitava organização ótima e mecanismos de controle tanto para máquinas quanto para humanos, era crucial para se atingir o verdadeiro Comunismo. A forte ênfase doutrinária no poder da informação era segmentada em duas dimensões distintas: controle da cadeia de produção e do movimento de tropas; e capacidade de empreender guerra de

informação contra um oponente. Ambas dimensões tinham por objetivo a derrota do inimigo – no primeiro caso com a aplicação de força física sobre o alvo e no segundo com a manipulação do processo de tomada de decisão em todos os níveis da cadeia de comando. Klimburg explica que, para os americanos, a guerra psicológica é uma ferramenta tática e operacional. Para os soviéticos, algo que poderia influenciar o próprio teatro de operações, assim como a vida política em geral. Os soviéticos acreditavam que uma guerra poderia ser lutada – e ganha – sem que o outro lado sequer soubesse que ela havia sido declarada.

Esse conceito estratégico de operações psicológicas, ou PSYOPS, é a base do conceito de controle reflexivo, prossegue o autor. Esse seria o processo por meio do qual um inimigo transmite ao outro as razões ou a base para sua tomada de decisões. O controle reflexivo implica o domínio completo sobre o processo de tomada de decisões do adversário. O objetivo é fornecer informações ao alvo para predispô-lo a fazer as escolhas desejadas pelo iniciador do ataque.

Em 2000, a visão russa sobre a importância da informação foi explanada na *Information Security Doctrine*, publicada naquele ano. No documento, definem-se dois tipos de ataques de base informacional: técnico e psicológico. Ataques técnicos incluem *hacking*, guerra eletrônica e outras atividades que, observa Klimburg, os ocidentais classificariam como operação cibernética. O autor relata que, ao definir ataques psicológicos, o documento fala repetidas vezes em propaganda estrangeira, que poderia ser espalhada por meio de agentes russos, como ameaça à integridade espiritual da Rússia. Outras ameaças incluiriam a expansão descontrolada do setor de mídia estrangeira no espaço nacional de informação, assim como as atividades de jornalistas, ONGs, missionários e instituições religiosas. A mídia é entendida como um bem estratégico em favor das políticas russas. Assim, poder-se-ia explicar às audiências estrangeiras a perspectiva do país e seus objetivos na arena internacional. A questão da desinformação é mencionada com frequência ao longo da Doutrina. É razoável supor, portanto, que a principal preocupação russa é a falta de controle sobre as informações que circulam dentro de suas fronteiras. Klimburg esclarece que o que a Rússia entende por informação seria visto nos países ocidentais como o funcionamento usual da mídia, da sociedade civil e da democracia. Segue que, para a Rússia, a informação tem quatro dimensões: guerra eletrônica, inteligência, guerra de *hacking* e guerra psicológica. Citando a teoria de guerra ambígua, ou *covert war*, do general russo Valery Gerasimov, o autor observa que:

> *In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template. The experience of military conflicts – including those connected with the só called colored revolutions in north Africa and the Middle East – confirm that a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war*. (GERASIMOV *apud* KLIMBURG, 2019, p. 221)

Logo, ao contrário do conceito clausewitziano de guerra como estado temporário e anormal, prossegue Klimburg, o marxismo-leninismo a define como permanente, um estado contínuo entre nações hostis, não um ponto atípico de suas interações. Ainda que a União Soviética aceitasse a definição legal internacional de guerra, e tenha incorporado essa definição em seu sistema legal, diz o autor, no marxismo-leninismo todos os recursos do Estado eram considerados parte indissociável de uma luta permanente.

Sobre a relação da China com o ciberespaço, o autor faz um corte temporal por ocasião da ascensão de Xi Jinping ao poder como presidente, ocorrida em 2013, como marco da adoção de uma postura assertiva em relação ao poder cibernético do país. A mudança, prossegue, relaciona-se com a máxima de Deng Xiaoping, segundo a qual a estabilidade social estaria acima de todos os outros objetivos. O Livro Branco das Forças Armadas, de 2015, informa o autor, já deixava claro que, para a China, cibersegurança era tão importante quanto segurança naval, nuclear ou espacial, com grandes chances de se tornar a força motriz de todos os conflitos vindouros.

O crucial para o Partido Comunista da China (PCC), portanto, é o controle das atividades de seus cidadãos online. A tarefa, admita-se, é dantesca. Desde 2008, explica Klimburg, a China tem a maior presença de usuários da internet, com crescimento de cerca de 22 milhões de internautas em 2000 para algo em torno de 720 milhões em 2016, aumento que se deve largamente às redes sociais. No entanto, boa parte desses usuários interage exclusivamente com conteúdo e produtos chineses. O aplicativo Weibo, uma espécie de Twitter, é popular entre os internautas chineses. Isso leva o autor a afirmar que existiriam duas "internets": a colcha de retalhos global que gira em torno dos conteúdos produzidos nos Estados Unidos e a hiper-localizada internet chinesa.

Isso não invalida o fato de que a China depende de hardware e software desenvolvidos fora do país. Ademais, aponta Klimburg, o PCC ainda não conseguiu impedir que seus cidadãos interajam com conteúdos produzidos além de suas fronteiras físicas,

tampouco censurar a produção destes conteúdos. Ainda que hiper-localizada, a internet chinesa não é impermeável, conclui.

É certo que a preferência da população chinesa por redes sociais locais tem implicações para as tentativas do PCC de monitoramento do comportamento de seus cidadãos. Klimburg menciona um sistema de pontuação para fins de atribuição de crédito social que teria previsão de ser implementado a partir de 2020. De acordo com o governo, o objetivo seria encorajar a "cultura da sinceridade". A estimativa do autor é de que o sistema, que se valeria inclusive de reconhecimento facial para fins de monitoramento de atividades, esteja operacional até o fim de 2020[20]. Para Klimburg, "*the world will have a model of what the Internet can become when it is fully chained as a tool of population control, and the panopticon of the darkened web, with all its haunting aspects of total social control, will have arrived, at least in embryonic form*", (KLIMBURG, 2019, p. 259).

Ao retomar o tema da importância das redes sociais no contexto chinês, o autor assevera que o fato de elas serem vistas como um ativo para o regime do Partido Comunista da China é um desenvolvimento perigoso. As redes sociais fornecem *feedback* rápido sobre preocupações locais, de modo que funcionam como plataforma de amplo espectro para as iniciativas governamentais. As redes sociais também ajudam o PCC a monitorar críticas e descontentamentos que possam dar origem a protestos. Para Klimburg, trata-se de um exemplo do que seria uma "*responsive authocracy*", ou autocracia responsiva, sensível em certa medida aos anseios da população para atingir máxima influência com intervenções discretas, aparentemente mínimas, mas na verdade amplas. Em conjunto com o sistema de atribuição de pontuação para fins de crédito social, o potencial de vigilância não encontra precedentes, observa Klimburg.

> *As it is already today, its extensive reach and connection with intelligence capabilities make it a much more powerful tool than any Western-style focus group or poll. Essentially, it is well on its way to becoming the perfect propaganda monitoring and planning tool, and if and when it is paired with a "social-credit scoring tool", it will become a nightmarishly effective form of government control.* (KLIMBURG, 2019, p. 274)

[20] Ao que consta, o sistema está em estágio avançado de operacionalidade. Em artigo para o *The Diplomat*, Yan (2020) esclarece que a lista de comportamentos indesejados que levariam à perda de pontos no sistema não foi tornada pública. Ele aponta, no entanto, sinais de que a exportação de partes do sistema de atribuição de crédito social para países vizinhos já estaria em curso. Para considerações detidas sobre o sistema chinês, ver Langer (2020), Shahin e Zheng (2020), Dai (2020) e Lee (2019).

Com efeito, continua, há indícios de que a China tem buscado reforçar sua política de empreender guerras de informação por meio de operações de influência. A chamada Doutrina das Três Guerras, que, de acordo com Klimburg, é frequentemente mencionada em documentos oficiais chineses que versem sobre conflitos cibernéticos, explora níveis abstratos de conflito interestatal: *lawfare*, ou o uso do Direito Internacional para promoção de objetivos estratégicos; guerra midiática, que corresponderia à tentativa de conquistar a opinião pública internacional; e guerra psicológica, cujo principal objetivo é a construção de um sistema de punições e recompensas que perpasse diferentes níveis de poder e coaja oponentes. Desde a proclamação da Doutrina em 2003, continua Klimburg, o Exército de Libertação Popular (PLA, na sigla em língua inglesa) operacionalizou a estratégia e a incorporou ao *General Political Department/Liaison Department* (GPD/LD), divisão que trabalha em colaboração com os braços de inteligência chineses, por exemplo, na identificação de elites políticas, empresariais e militares no exterior relevantes para os interesses chineses. Ao fim e ao cabo, essa pesquisa produz mapas cognitivos que informam a condução de operações de influência com foco em conversão, exploração e subversão.

Citando as três faces do poder sobre as quais Nye (2012) dissertou, Klimburg pontua que Estados podem projetar poder liderando processos de mudança, controlando pautas ou estabelecendo preferências. O primeiro ponto estaria mais relacionado à coerção, segundo Klimburg, e à percepção tradicional de que o poder é a capacidade de fazer os outros obedecerem a nossa vontade. O segundo ponto está mais próximo à cooptação que à coerção. Diz respeito à determinação de quais assuntos serão discutidos, bem como à condução de discussões internacionais a um ponto que favoreça o país detentor de maior influência. O terceiro e último ponto estaria relacionado à capacidade de moldar as crenças e perspectivas de um grupo sem qualquer pressão ou direcionamento aparente. Pode ser chamado de *soft power*, no qual se exerce uma atração de caráter positivo, mas Klimburg observa que a terceira face do poder pode se manifestar também por intermédio da manipulação e da distorção. A visão de que o poder cibernético seria apenas mais uma ferramenta para conflitos armados subscreveria à primeira face do poder, enquanto a instrumentalização da dimensão cibernética para fins de guerra de informação ou *information ops* é compatível com a terceira.

Ciberataques podem ter tanto efeitos sobre bases de dados quanto sobre o estado mental da população vitimada. Isso significa dizer que operações ofensivas podem ser bem-sucedidas politicamente mesmo que não consigam produzir efeitos práticos em termos de infraestrutura, por exemplo. É a lógica, explica o autor, dos ataques espalhafatosos que Irã

e Coreia do Norte ocasionalmente empreendem. Apesar de pouco danosos, formam, em última instância, a percepção de que esses atores têm maior potencial ofensivo no plano cibernético do que de fato têm, atribuindo-lhes, portanto, maior status. É por isso que Klimburg acredita ser reducionista definir o poder cibernético como questão pura e simplesmente de *hard power*.

> *I believe cyber to be the epitome of a soft-power problem: one that depends on highly intangible issues such as legitimacy, cooperation, and trust – not only among governments, but also between governments and the crucial non-state actors that build and maintain the Internet. Parsing cyber power requires seeing beyond the traditional hallmarks of brute force encapsulated in national security structures and understanding that there are many ways for nations to play crucial roles in this domain. (...) But lateral thinking is needed if a true assessment of an actor's cyber power is to be attempted. The toolbox of those dealing with arms control issues is relatively straightforward, but it may also be somewhat limiting. For as the old saying goes, if all you have is a hammer, then every problem looks like a nail.* (KLIMBURG, 2019, p. 313)

Em termos de governança, o desafio mais agudo é a coordenação de diferentes atores, instituições e grupos em trabalhos conjuntos sobre o ciberespaço. Isso requer uma abordagem de cooperação incomum para governos, observa Klimburg. Para que essa simbiose funcione, é necessário manter um equilíbrio de poder entre, basicamente, três *stakeholders*: governo, setor privado e sociedade civil, que se desdobram cada um em uma miríade de subgrupos. A convivência cooperativa entre eles é fundamental.

2.3 Conclusão parcial

Nesse capítulo, a questão cibernética foi apresentada como eminentemente híbrida, que tem desafiado a distinção entre conflito e paz. Isso significa que atravessa diversos domínios do conhecimento, de maneira que abordagens parciais restam insuficientes. A ubiquidade da *internet* na vida contemporânea trouxe à baila a questão da dependência que se tem atualmente de dispositivos eletrônicos de comunicação para a execução de uma miríade de tarefas, das mais corriqueiras às mais estratégicas – pense-se, por exemplo, nas atividades das Forças Armadas. Assim, o *cyber* aumentou a possível superfície de ataque para atores maliciosos que se aproveitam dessas fragilidades para não apenas empreender ataques a infraestrutura crítica, mas também à própria resiliência cognitiva e democrática de dada população. Nesse diapasão, comentou-se estudos que apontam serem ataques apocalípticos a

infraestruturas críticas possíveis, mas raros e improváveis. *Stuxnet* não é o padrão, mas a exceção. O grosso dos ataques cibernéticos são de baixa intensidade. Eis o porquê de se ter escolhido a análise do texto de Klimburg (2019) para fechar o capítulo: defende-se que o grande desafio trazido pela questão cibernética não é uma hipotética guerra disputada no ciberespaço, mas a corrosão do tecido social por meio de ataques híbridos.

3 EXEMPLOS PRÁTICOS DE ESTRATÉGIAS DE SEGURANÇA E DEFESA CIBERNÉTICA

A escolha de países que sirvam de exemplo para o estudo comparativo entre as estratégias de segurança e defesa cibernética por eles adotadas e a propugnada pelo Brasil parecerá aleatória em um primeiro momento. Neste estudo, o caminho percorrido para se optar pela seleção que ora se apresenta baseou-se em conclusões a que se chegou durante a revisão da literatura, particularmente no que diz respeito à natureza empírica dos conflitos cibernéticos e aos países mais atuantes no campo ofensivo de incidentes dessa natureza.

A leitura das reflexões propostas por Valeriano e Maness (2014, 2015, 2018a, 2018b), Paulwels (2019), Klimburg (2019), Bradshaw e Howard (2019), Lupion (2019) e Hanson *et al.* (2019), aponta com consistência seis países como ativos no ambiente cibernético. Estes são Estados Unidos, China, Rússia, Israel, Irã e Coreia do Norte. Faz-se primordial observar que os três primeiros são os mais citados pelos autores mencionados.

Partindo-se do princípio de que o grosso dos incidentes cibernéticos é constituído não por grandes ataques a infraestruturas críticas, mas por operações de baixa intensidade; que há razoável base teórica para supor que o presente e o futuro dos conflitos interestatais abrangerá segmentos cada vez mais amplos da sociedade; e que o ambiente cibernético tem servido marcadamente de veículo para a condução de operações híbridas, as considerações doutrinárias colocadas por Klimburg (2019) a respeito da Rússia fazem desse ator objeto interessante de estudo.

Nessa toada, faria sentido olhar para os países de interesse desse ator para estudar as formas como se organizam internamente no que diz respeito à segurança e à defesa cibernética. Esbarra-se, no entanto, em barreiras linguísticas, dado que são poucos os que divulgam documentos oficiais em língua inglesa. Seria impraticável recorrer à tradução automática para a leitura dos textos que estivessem nos idiomas oficiais dos países objetos de estudo. Adicionalmente, correr-se-ia o risco de que filigranas do idioma se perdessem no emprego desse método de tradução, à parte os naturais erros que ocorrem na tradução feita por máquinas, os quais não poderiam ser identificados sem o conhecimento consistente do idioma de origem. Assim, seria recomendável ater-se a países que dispusessem de estratégias, orientações e estudos oficiais disponíveis em língua inglesa.

Outro ponto de preocupação na seleção de exemplos para este capítulo é a disponibilidade de volume satisfatório de informações públicas sobre o assunto a se estudar.

Este dependeria, claro, da abertura dos países escolhidos com informações a nível estratégico de uma área sensível. Novamente, não são todos os alvos, por assim dizer, da Rússia que disponibilizam liberalmente essas informações.

Em face dessas considerações, chegou-se portanto à escalação de Suécia, Dinamarca, Noruega, Finlândia e Estônia. Optou-se por incluir Estados Unidos no time de exemplos em razão não apenas de sua relevância global e hemisférica, mas também de sua proeminência no âmbito cibernético: ainda que haja outros atores tão atuantes nesse campo, trata-se do país de maior capacidade cibernética ofensiva e defensiva no mundo (CRANDALL; THAYER, 2018). Não convém ignorá-lo.

O interesse russo na região nórdica não é mera conjectura. McGwin (2019) chamou a atenção para a aproximação dos laços de cooperação entre Suécia, Dinamarca, Noruega e Finlândia, formalizados já desde 2009 com a criação da aliança militar Nordefco. O autor aponta que, recentemente, preocupações com a hostilidade russa têm levado o quarteto a intensificar a troca de informações de inteligência, por exemplo. Acesso rápido ao espaço aéreo dos parceiros já é permitido, com possibilidade de expansão para águas territoriais. O objetivo no curto prazo seria aproximar as operações das forças armadas desses países, com destaque para o desejo de Suécia e Finlândia de aproximar-se da OTAN (Organização do Tratado do Atlântico Norte) – o que, realce-se, provocou avisos severos da Rússia. Receios de ataques cinéticos não são consideráveis, de acordo com McGwin, mas o grupo mantém-se alerta quanto a incidentes hostis nos domínios físico e cibernético.

Fiskvik (2016) já levantara pontos semelhantes. Para o autor, a agressão militar russa na Ucrânia e a anexação da Crimeia desafiam a situação geopolítica do pós-Guerra Fria na Europa. Esses acontecimentos teriam sido uma espécie de *reality check* para o quarteto supracitado, pois apesar do senso de identidade nórdica comum, suas políticas de segurança e defesa não eram integradas. Fiskvik acredita, talvez em tom um pouco diferente de McGwin, que o foco não é incrementar uma comunidade nórdica de segurança, mas aproximar-se da OTAN. Frisando que uma relação cordial com a Rússia no longo prazo é objetivo do quarteto nórdico, Fiskvik acrescenta, no entanto, que a assertividade russa é preocupação constante para o grupo, particularmente para a Finlândia, que tem extensa fronteira compartilhada com a Rússia – a Noruega, grande exportador de hidrocarbonetos e, portanto, competidor da Rússia nos mercados de energia globais, também divide fronteira com os russos, embora a extensão seja consideravelmente menor que a finlandesa. Os finlandeses preocupam-se com a capacidade de suas forças armadas de defender o país frente a hostilidades russas; os suecos,

por sua vez, temem atividade militar russa no Mar Báltico, em particular na ilha de Gotland; para os dinamarqueses, o Báltico também causa preocupação; já para a Noruega, a questão é a proteção do *High North*, que abrangeria não apenas a porção norte do país, mas também a região ártica como um todo. Embora acredite não haver base para afirmar que as atividades russas recentes tenham incentivado a aproximação entre os países nórdicos, Fiskvik (2016) observa que estas fomentaram a visão comum nórdica de que a segurança regional deteriorou-se. Em tempo, Suécia e Finlândia são membros da União Europeia. A Noruega é membro apenas da OTAN e Dinamarca, por sua vez, é membro de ambas organizações internacionais.

Pynnöniemi (2013) atesta que os desafios de segurança da região nórdica consistem basicamente em uma combinação da questão ainda em aberto da entrada na OTAN; do advento de um autoritarismo brando na Rússia e do problema da proteção à infraestrutura crítica na região nórdico-báltica. Para a autora, é possível contextualizar a presença russa na região nórdica aplicando-se três enquadramentos analíticos.

O primeiro seria que a região nórdica pode ser entendida como singular, como espaço para a exploração de novas formas de interação entre a Europa e a Rússia. O argumento é que os fóruns regionais de cooperação, como o *Artic Council*, de 1996, e o *Nordic Dimension*, lançado em 1998, forneceram contexto para a transmissão, exploração e adaptação das normas e valores europeus. O espaço de interação é enquadrado em termos de novas ameaças de segurança e explicado por meio de compreensão abrangente do paradigma de segurança, pontua Pynnöniemi. Nesse contexto, prossegue a autora, tem-se uma divisão clara entre o atual estado das coisas e o período da Guerra Fria. Isso concretizaria o debate sobre os conceitos de não-alinhamento e neutralidade. No entanto, ressalva, questões de segurança não costumam ser tratadas em contextos de cooperação interregional, à qual se reservam temas como proteção ambiental, reforma de sistemas de segurança social e desenvolvimento de infraestrutura.

O segundo enquadramento analítico diz respeito à possibilidade de enxergar a região nórdico-báltica como uma espécie de portal para a Rússia, um ponto de conexão que pode aproximá-la do Ocidente. A abordagem, explica Pynnöniemi, baseia-se em lógica de crescente interdependência – na avaliação da autora, vista como uma situação positiva tanto para nórdicos quanto para russos –, homogeneização e competição por mercados. Em nível regional, o foco tem sido facilitação de comércio e políticas baseadas em projetos. A Rússia

tem-se mantido consistente em sua política de preferência por cooperação inter-regional baseada em projetos e investimentos, conquanto relute em abraçar o conceito de *flow economy*, na avaliação da autora.

O terceiro e último enquadramento analítico é o que se chama de recuperação da importância geopolítica da região nórdico-báltica, com ênfase na renovação dos interesses das grandes potências no Ártico, na construção do gasoduto russo cruzando o Mar Báltico e no incremento da capacidade naval russa na região. Para Pynnöniemi, pode-se entender esses fatores como sinais de uma reorientação geopolítica no "norte europeu", termo frequentemente usado na literatura acadêmica russa em lugar de "região nórdica", explica. O motivo para essa valsa semântica é simples: "região nórdica" carrega peso histórico-político subjetivo, enquanto "norte europeu" é conceitualmente difuso, termo maleável que pode ser usado para legitimar diferentes configurações histórico-espaciais da região, assevera a autora. A expressão criaria duas associações: uma que ligaria Suécia, Dinamarca, Noruega e Finlândia à identificação russa como uma nação também do norte, e outra que amenizaria a subjetividade do status de país nórdico. Pynnöniemi observa que os termos "*wider north*" (ou "norte expandido", em língua portuguesa), em referência à região ártica expandida, e "*greater northern region*" (ou "grande região norte"), que conectaria o Báltico e o Barents.

Complementando essas considerações, Pynnöniemi (2019) acrescenta que duas observações principais podem ser feitas a partir da visão estratégica russa: primeiramente, que esta corresponde a uma visão da política mundial consoante a *realpolitik*, na qual os Estados entram em competições de soma zero por poder e recursos. Em segundo lugar, que a nova ordem mundial emergiria por causa do conflito entre sistemas diferentes de valores e de desenvolvimento. Para a autora, haveria semelhança entre esse diagnóstico russo e a situação durante a Guerra Fria. Ademais, prossegue, a Estratégia Nacional de Segurança da Rússia orienta-se em direção à estabilidade estratégica com outras grandes potências. A manutenção da paridade estratégica em dissuasão nuclear e convencional é o meio usado para se atingir esse objetivo. No entanto, em razão da disparidade entre as capacidades ofensivas russas e as de seus adversários geopolíticos, reavivou-se o conceito de abordagem assimétrica, prevalente durante a Guerra Fria. Este refere-se não apenas a assuntos militares, mas também a dependência econômica e sanções, além de iniciativas diplomáticas, políticas e informacionais que previnam a eclosão de um conflito que ameace a soberania e estabilidade doméstica da Rússia.

Um dos métodos empregados na abordagem assimétrica são as operações de influência. Em referência a estudo de 2017 da *Foreign Policy* sobre a resiliência finlandesa a iniciativas dessa natureza, Pinnöniemi (2019) destaca o robusto sistema público de educação da Finlândia, a longa experiência em lidar com investidas russas e uma estratégia governamental abrangente que permite ao país resistir a propagandas coordenadas e a campanhas de desinformação. Ainda que a Finlândia não seja o principal alvo da propaganda russa na Europa, pelo menos 20 campanhas de desinformação foram identificadas pelas autoridades finlandesas em 2018, aponta a autora. Padrões semelhantes foram observados na Suécia.

Para Pinnöniemi (2019), o caso da interferência russa nas eleições presidenciais dos Estados Unidos em 2016 reacendeu o debate entre países nórdicos sobre operações de influência. Na Suécia, por exemplo, a *Civil Contingencies Agency* (MSB) é responsável pelo monitoramento de campanhas de informação estrangeiras. Na Finlândia, a tarefa é distribuída entre diferentes autoridades governamentais. Desde 2017, prossegue, a Finlândia abriga a Hybrid CoE, agência ligada à União Europeia cujo objetivo é coordenar o combate a ameaças híbridas. Para a autora, esse é um indício de que se percebe aumento do nível de ameaça à União Europeia como um todo e a países específicos do grupo. Assim, diz, a questão não é se a Rússia tenta influenciar os países nórdicos por intermédio de diferentes técnicas, mas sim quão eficiente ou intensa essa influência é.

A autora explica que boa parte das pesquisas divulgadas recentemente sobre o tema focam nas tentativas russas de influenciar outros países por meio da mídia tradicional e das redes sociais. De meados da década de 2000 em diante, a Rússia criou serviços de *broadcasting* direcionados ao público ocidental em idiomas ocidentais e de acordo com padrões ocidentais. Os principais exemplos são os conglomerados RT e Sputnik, além de grupos operantes nas redes sociais. Isso permite à Rússia divulgar sua mensagem ao público ocidental de maneira direta, em abordagem consagrada pelos padrões jornalísticos ocidentais. Em tese, essa formatação tornaria dificultoso o processo de detecção de narrativas falsas.

No entanto, aponta Pinnöniemi, as tentativas russas de promover seus *talking points* sobre o conflito na Ucrânia não lograram êxito. Pesquisa conduzida pelo *Riga Stratcom Center* em 2017 citada pela autora teria mostrado que a minoria dos entrevistados na Finlândia conheciam os veículos RT e Sputnik. A maioria dos entrevistados não conheciam ou não assistiam os canais. No entanto, havia clara ideia de que as notícias fornecidas pela

mídia estatal russa não eram confiáveis. Adicionalmente, pontua a autora, os principais meios de comunicação na Finlândia e na Suécia conservaram-se críticos às meta-narrativas sobre os eventos prévios à eclosão do conflito ucraniano, além dos respectivos governos terem apoiado a implementação de sanções pela União Europeia. Nesse sentido, a propaganda e a desinformação russas não teriam surtido efeito[21].

Conclui Pynnöniemi (2019) informando que embora as chamadas Medidas Ativas russas, ou *Active Measures* – técnicas encobertas ou públicas para influenciar eventos e comportamentos de outros países – tenham caráter razoavelmente padronizado, a máxima leninista de se trabalhar com o meio material ainda é importante. Isso significa que o contexto formado por relações históricas com a Rússia, rede criminosa local, ambiente midiático, entre outros, molda a forma como os russos empregam seu arsenal de técnicas de influência.

Lanozka (2016), traça um diagnóstico das vulnerabilidades dos países que estiveram sob domínio soviético a táticas de guerra híbrida, em particular dos Estados do Báltico, dentre os quais a Estônia. Para o autor, são quatro os atributos que facilitam a subversão de origem russa, atrasam a escalada do conflito, dificultam intervenção estrangeira e tornam possível a guerra híbrida. Aqui vale ressaltar que Lanozka entende guerras híbridas mais como estratégias que novas formas de se fazer guerra.

Os quatro atributos mencionados por ele são a heterogeneidade étnica; a presença de traumas históricos latentes; a inexpressividade da sociedade civil local e a complexidade

[21] Ao comentar o fracasso da incursão dos conglomerados RT e Sputnik na Finlândia e na Suécia, Nimmo (2017) faz referência a outras tentativas russas de influenciar decisões políticas nesses países. Sobre a questão da proximidade sueca com a OTAN, diz o repórter que "*in June 2015 Russia's ambassador to Sweden, Viktor Tatarintsev, told the Dagens Nyheter newspaper in an interview that Russia would take "military countermeasures" if Sweden were to join NATO. His comment followed a sharp rise in Swedish support for NATO accession, triggered by Russia's illegal annexation of Crimea in March 2014: support had been only 17% in 2012, but jumped to 31% in 2014. Tatarintsev's threat did not initially have the intended consequences: according to a poll published in September 2015, 41% of Swedes said that they favoured accession, while 39% opposed it. The long-term effect may have been more substantial: by July 2016, support for joining NATO had slipped to 33% of respondents. Moreover, when the Swedish parliament ratified a Host Nation Support agreement with NATO in May 2016, both far-right and far-left MPs argued that a rapprochement with NATO could "increase the tension in our neighbourhood" and lead to Sweden being targeted by "others", comments seen as referring primarily to Russia and its threats. Nonetheless, the agreement was approved by an overwhelming majority of 291-21, and popular support for NATO in July 2016 remained double the 2012 figure. In Finland, meanwhile, scepticism towards Russia has grown sharply since the 2014 Crimean annexation. A poll released in December 2016 showed that 50% of Finns considered Russia a threat, compared with a figure of just 28% in 2010*"", (NIMMO, 2017). Ele atribui a resiliência sueca e finlandesa à consciência das populações sobre os perigos da desinformação e da propaganda. Além disso, há elevados níveis de confiança nos veículos jornalísticos do *mainstream*, os quais são enfáticos no tratamento de campanhas de informação de origem russa, segundo Nimmo. Isso não significa, contudo, que a pressão de operações de desinformação nesses dois países tenha arrefecido. As táticas, diz o repórter, parecem ter mudado para o uso de atores políticos nas margens do debate sueco e finlandês como "procuradores" das investidas de Moscou.

regional. A Rússia teria subsídios mais adequados para compreender esse amálgama de características.

A heterogeneidade étnica é relevante pois, embora não signifique conflito automático, provê ao Kremlin oportunidade de incitar discórdias. Um exemplo é o financiamento de grupos secessionistas em países que têm objetivos de política externa que Moscou entenda prejudiciais a seus objetivos. Outra tática empregada com frequência pela Rússia é posicionar-se como protetora dos direitos políticos de russos étnicos, ainda que tal apoio não tenha sido solicitado. Nesse caso, o perigo, diz Lanozka, é que o governo local veja a minoria russa como uma espécie de quinta coluna. A repressão e vigilância decorrentes serviriam de pretexto para ações enérgicas do Kremlin.

No que diz respeito a traumas históricos, "*a historical experience of domination can create an acute sensitivity to external threats*", (LANOZKA, 2016, p. 183). Adicionalmente, observa o autor, eventos traumáticos na região fomentaram o surgimento de nacionalismos ao longo do século XX. O estoque de ressentimentos e símbolos que o Kremlin poderia usar para dividir e sobrepujar sociedades em seu alvo é vasto, pontua o autor. Daí resulta a inexpressividade da sociedade civil na região, o que preveniu a formação de robustas redes sociais, na avaliação de Lanozka.

> *The weakness of civil society in the region has several implications for local political order. First, norms conducive to liberal democracy and civic values, including those that promote community participation and intergroup cooperation, remain underdeveloped. Second, given that, as Francis Fukuyama has written, 'civil society serves to balance the state and to protect individuals from the state's power', authoritarianism remains a persistent feature of the post-Soviet space. (…) In robust liberal democracies such as the Baltic countries, civil society is stronger than anywhere else in the former Soviet space. Nevertheless, in both Estonia and Latvia there are large numbers of stateless people who are not yet integrated into either local political institutions or the domestic economy*. (LANOZKA, 2016, p. 185)

O problema é que a sociedade civil é importante para, no contexto de guerras híbridas, amenizar a exploração de clivagens sociais. Para o autor, uma sociedade civil ativa serve como agente imunizador contra tentativas de desestabilização política. Em conjunto com traumas históricos e heterogeneidade étnica, a complexidade regional exacerba-se. A vantagem tática que a compreensão dessa combinação de fatores lega à Rússia permite ao país caracterizar os erros de cálculo do Ocidente como apoio a determinado grupo em detrimento de outros. Toca-se assim em um ponto sensível que leva países que teriam capacidade de

resistir a táticas de desinformação russas a acatar a narrativa do Kremlin sobre os acontecimentos, explica Lanozka. Isso permite a Moscou usar os desenvolvimentos políticos locais para promover seus próprios interesses, o que não significa que as táticas de guerra híbrida logrem êxito em qualquer país sobre o qual sejam utilizadas.

Com efeito, o autor aponta quatro condições principais para que a guerra híbrida seja empregada. Em primeiro lugar, o país beligerante tem comparativamente maior poder de fogo na região que os demais, mas esse poderio não necessariamente se mantém em escala global, o que significaria que o beligerante "*can threaten to unleash greater violence than its target can marshal in order to deter a particular military response from that target. Not having global escalation dominance means that the belligerent wishes to contain the conflict locally and deter external intervention*", (LADOZKA, 2016, p 189). Em segundo lugar, o beligerante pode desejar estender sua esfera de influência e desafiar o *status quo* por intermédio do exercício de influência sobre o regime político do país-alvo. Em terceiro lugar, a vulnerabilidade que a ausência de uma sociedade civil robusta traz permite ao beligerante manipular ansiedades e animosidades locais com o fim de enfraquecer o alvo internamente. Em último lugar, há grupos étnicos ou linguísticos no país-alvo que têm algum nível de ligação com o beligerante, o que lhe confere certo verniz de legitimidade no enquadramento de suas ações hostis, além de prover vantagens na coleta de informações sobre pontos de pressão locais.

Em suas considerações finais, o autor adverte que soluções predominantemente militares não são eficientes em cenário de guerra híbrida, uma vez que

> (…) *too much emphasis on deterring aggression at higher levels of violence might undercut deterrence at lower levels of violence. Such is the stability–instability paradox that Glenn Snyder describes. Under conditions of mutual assured destruction between two nuclear-armed adversaries, direct and major war becomes very unlikely, since both sides seek to avoid annihilation. Consequently, both sides might perversely find it safe to engage in conflicts that do not involve nuclear weapons. Therefore, bolstering alliance capabilities at higher levels of violence could make hybrid warfare even more attractive. After all, hybrid warfare exploits the vulnerability of targets at yet lower levels of violence, whereby the belligerent can plausibly deny that it is even engaging in aggression. The belligerent could thus deter its target from undertaking escalatory measures. It also denies adversaries a clear, compelling rationale for military intervention by obfuscating the nature of local crises fomented from without*. (LANOZKA, 2016, p. 191)

O ponto crucial, afirma, é que a dimensão política importa quando se trata de cenários ideais para o emprego de táticas de guerra híbrida. No que diz respeito ao Báltico e

às ex-repúblicas soviéticas, conclui o autor, estar sob o guarda-chuva da OTAN não é suficiente para deter ataques híbridos em si, mas é útil na provisão de um arcabouço institucional que incremente contrainteligência e *law enforcement capabilities* conjuntas.

Schmidt-Felzmann (2017) analisa detidamente métodos empregados por campanhas de desinformação russas na região nórdica. Na avaliação da autora, o alvo das operações é o indivíduo, em primeiro lugar, posto ser esse o responsável pela tomada de decisões, por gerenciar diferentes instituições do Estado, preparar análises para formuladores de políticas públicas, escrever reportagens sobre os desafios enfrentados por autoridades do governo, etc. Por isso, argumenta, o nível individual de tomada de decisões pode facilitar ou obstruir o exercício de influência por parte do Kremlin sobre deliberações políticas do país-alvo.

Schmidt-Felzmann destaca cinco métodos principais usados sistematicamente pela Rússia em países nórdicos para exercer pressão psicológica sobre seus alvos. O primeiro é a seleção de indivíduos (e de instituições para as quais trabalhem) e a destruição pública de suas reputações com acusações relacionadas a sua suposta incompetência, além de outros pontos sensíveis. O segundo método é a promoção de acusações de russofobia para constranger críticos na região e evitar que deem declarações públicas críticas às ações do Kremlin. O terceiro diz respeito à seleção de indivíduos que são ameaçados publicamente com consequências severas caso não corrijam comportamentos e declarações acusatórios em relação à liderança russa e aos objetivos por ela estabelecidos. O quarto método identificado por Schmidt-Felzmann é a comparação de críticos a outros parceiros russos de cooperação, contrastando seus comportamentos segundo o binômio amigável *versus* hostil, com recompensas dadas ao ator amigável e retaliações distribuídas ao hostil. O quinto e último método é o aprofundamento da destruição da reputação de indivíduos selecionados, com a manipulação e a fabricação de declarações públicas, e a propagação de falsas representações sobre eles. O objetivo segue intimidá-los e abafar críticas.

A autora comprova o emprego de todos esses métodos, com maior ou menor grau de êxito. Ela destaca com particular atenção o fracasso da incursão dos portais RT e Sputnik na região. Consideráveis preocupações foram expressas na Dinamarca, na Noruega, na Suécia e na Finlândia por ocasião de seu lançamento do Sputnik em abril de 2015. O conteúdo não versava sobre assuntos locais, rememora Schmidt-Felzmann, mas era francamente favorável à Rússia e crítico à União Europeia, à OTAN, aos Estados Unidos e ao Ocidente no geral.

Em razão dos recursos volumosos já investidos pela Rússia nas atividades do RT na região, cresceu o receio de impactos negativos sobre as sociedades nórdicas que o influxo de notícias falsas e manipuladas pudesse ter. Surpreendentemente, conta a autora, já em março de 2016 o Sputnik saiu do ar nos quatro países nórdicos. Indícios de que a operação não ia tão bem quanto planejado já podiam ser observados, por exemplo, nas críticas à qualidade dos textos noticiosos divulgados pelo portal. Aventa-se também a possibilidade de que o recorte editorial do Sputnik, com promoção de teorias da conspiração, tenha prejudicado as chances de êxito da operação nórdica da empresa midiática. Além disso, destaca-se, caso se meça o alcance do portal pelo número de interações em suas redes sociais, não se tem cenário animador. Schmidt-Felzmann observa, contudo, que não se tem uma resposta comprovada para o fim abrupto das atividades do Sputnik.

Segue que o resultado do aumento de operações de informação russas direcionadas aos países nórdicos foi o desenvolvimento de ferramentas e contramedidas para a defesa dos cidadãos de cada país nórdico, explica Schmidt-Felzmann. A principal área de preocupação é a defesa de espaços de informação livres e abertos, com ênfase nos veículos de mídia, contra a desinformação de origem russa. Faz-se ressalva à participação norueguesa, notando que

> (...) an analysis conducted in 2015 about the targets and effects of Russian propaganda concluded that Norway has not been a prioritized target of Russian disinformation activities (...) Norway is not currently engaged in either of the two multinational Centres of Excellence that have been set up under the EU and NATO umbrella to deal with the problems associated with propaganda, disinformation and influence operations. (SCHMITD-FELZMANN, 2017, p. 56).

Isso não impede, continua a autora, que a Noruega tenha, junto com Suécia, Dinamarca, Finlândia e Islândia, além de Lituânia, Letônia e Estônia, se comprometido com o fórum de cooperação *Nordic and Nordic-Baltic* (NB8) contra desafios de informação apresentados pela Rússia. A Dinamarca, por sua vez, junto com outros Estados da União Europeia, defendeu a criação de uma equipe de "*mythbusters*" no *European External Action Service* (EEAS). Esta seria uma força-tarefa dedicada a lidar com a desinformação do Kremlin e que responderia direto ao Alto Representante da União Europeia para Política Externa e de Segurança[22]. A *East StratCom Task Force* foi então criada em setembro de 2015 e a Dinamarca forneceu apoio logístico e financeiro. A Suécia aderiu à força-tarefa em 2016, mas a Finlândia preferiu dedicar-se ao StratCom CoE da OTAN na Letônia.

[22] O posto é cumulativo com o de Vice-Presidente da Comissão Europeia.

O treinamento de especialistas para identificar operações de informação e para combater desinformação em circulação na internet foi implementado na Finlândia, destaca a autora. Em 2016, a *National Defence Training Association* da Finlândia começou a oferecer cursos sobre como identificar campanhas de desinformação e como conduzir estratégias de comunicação em tempos de crise. Uma unidade exclusivamente dedicada à informação e às comunicações foi colocada como responsável pela coordenação de informações entre os ministérios finlandeses para assegurar que informações falsas fossem imediatamente desmentidas, tanto em meios de comunicação online quanto offline. Enviou-se também um especialista ao StratCom CoE em Riga, Letônia. A partir de 2015, informa Schmidt-Felzmann, autoridades suecas também passaram a participar nos seminários e conferências promovidos pelo órgão da OTAN.

Especificamente na Suécia, prossegue, a *Civil Contingencies Agency* (MSB) foi instruída pelo governo a desenvolver uma estratégia de defesa psicológica como parte do conceito de defesa total reintroduzido a partir de 2015. A unidade da MSB que coordena o trabalho contra operações de influência desenvolve sua capacidade de monitorar e responder a operações de informação russas com uma equipe de linguistas e em estreita cooperação com as forças armadas suecas, os serviços de inteligência e segurança (MUST e FRA) e a polícia (Säpo).

A MSB também treina representantes de autoridades regionais e locais para detectar, identificar e responder a operações de informação. É dessa unidade, explica Schmidt-Felzmann, que provêm os especialistas que foram enviados à Força-Tarefa em Bruxelas e ao Centro em Riga. Adicionalmente, diz a autora, o governo sueco consulta com frequência representantes de veículos de comunicação para desenvolver medidas de defesa mais eficientes, inclusive contra ataques cibernéticos.

Schmidt-Felzmann critica, no entanto, a falta de entendimento dos países nórdicos sobre como lidar com a pressão psicológica sofrida por indivíduos e grupos profissionais atacados no contexto de campanhas de intimidação do Kremlin, em especial como os governos dos países nórdicos podem proteger de maneira efetiva não apenas esses indivíduos e grupos, mas também o papel que eles exercem nas instituições e processos democráticos.

Sobre as estratégias de Noruega, Suécia, Finlândia e Dinamarca, Kunz (2018) vê diferentes percepções sobre a Rússia e seu relacionamento com cada um desses países, o que resulta em estratégias distintas. Para a Suécia, a Rússia foi o maior desafio geopolítico por

séculos, explica a autora. Confrontaram-se em guerras e dividiram extensa fronteira até a independência da Finlândia em 1917. Durante a Primeira e Segunda Guerras Mundiais, a Suécia optou pela neutralidade; na Guerra Fria, pelo não-alinhamento. Agora, diz Kunz, a segurança é assunto predominante em debates estratégicos no país, em particular sobre a situação da região do Mar Báltico. Em geral, a Rússia é criticada com firmeza, avalia.

A Finlândia, por sua vez, pertenceu tanto ao império sueco quanto ao império russo. Os primeiros anos pós-1917 foram marcados por conflitos entre os "vermelhos", favoráveis à união com a União das Repúblicas Socialistas Soviéticas (URSS) e os "brancos", partidários da independência. Após investida soviética e a Guerra de Inverno em 1939, seguidas por uma Guerra de Continuação em 1941 e a consequente perda territorial, a Finlândia também optou pela neutralidade durante a Guerra Fria, em linha com a Doutrina Paasikivi-Kekkonen[23], lembra Kunz. Em 1995, com a acessão à União Europeia, a Finlândia formalizou sua aderência ao Ocidente.

Para Kunz, ao contrário de seus vizinhos – e a autora destaca a Suécia –, a Finlândia conservou preocupação com a robustez de suas Forças Armadas. A Rússia é vista como um vizinho com o qual se deve dialogar, independente de desejos pessoais. Assim, conclui a autora, "*Finland's Russia policy is therefore marked by its pragmatism, favouring as much cooperation as possible while at the same time remaining alert and uncompromising over the foundations of the European security order*", (KUNZ, 2018, p. 7).

A avaliação da autora é que, desde a independência, em 1905, a Noruega se preocupa sobretudo com a situação do Atlântico Norte. Kunz argumenta que o país tenta equilibrar sua aposta na Aliança Atlântica e em Washington com a manutenção de relações normais com a Rússia, um equilíbrio delicado.

> *The two countries resolved a longstanding dispute over their border in the Barents Sea in 2010, but other issues continue to cast a pall over their relationship, not least the conflict in Ukraine and its consequences. The presence of American forces on Norwegian soil since 2017 has become a source of tension. Russia also believes that Norway could be "more cooperative" in the High North.* (KUNZ, 2018, p. 7)

A Dinamarca, na opinião da autora, parece ser o menos preocupado com a Rússia entre os países nórdicos. No entanto, as investidas russas no Báltico e ameaças de caráter cibernético e informacional têm chamado a atenção de Copenhague para o Báltico, assevera.

[23] Trata-se de doutrina de política externa estabelecida pelo presidente finlandês Juho Kusti Paasikivi e conservada por Urho Kekkonen, seu sucessor. O objetivo da orientação de neutralidade era conservar a soberania e o caráter democrático do país. Para análise sobre a doutrina, ver Singleton (1982).

Para todos os países nórdicos, a opinião de Kunz é que a economia vem em segundo lugar, após a segurança. Com exceção da Finlândia, esclarece, o comércio com a Rússia não é significativo para países do norte europeu[24].

Tampouco é assunto premente para os países nórdicos a questão energética, vaticina a autora. Como evidência, ela aponta o fato de que a Noruega é um dos maiores exportadores de petróleo e gás do mundo[25], autossuficiente em hidrocarbonetos e competidor da Rússia em mercados mundiais. A Dinamarca também seria, na avaliação da autora, relevante exportador dessas commodities, enquanto a Suécia supriria parte de suas necessidades energéticas por meio da importação de gás da Dinamarca e de outros vendedores do mercado mundial. Da Rússia, diz Kunz, importa apenas petróleo e, em teoria, poderia mudar de fornecedor. Situação diferente vive a Finlândia, que importa todo o gás que consome diretamente da Rússia. No longo prazo, a autora não crê que esse seja um problema, pois tem-se tomado medidas de redução de vulnerabilidade energética por meio do investimento em fontes renováveis de energia, com destaque dado pela autora ao projeto *Baltic Connector*, que ligará as redes de gás da Finlândia e da Estônia[26].

No que diz respeito à Rùssia, o que tem preocupado os países nórdicos nos últimos anos, na opinião de Kunz, são o aumento do orçamento de defesa, a mudança de postura no Extremo Norte e em Kaliningrado, os exercícios militares com a Bielorrússia – a autora faz referência em especial aos exercícios Zapad, ocorridos em 2017 –, incidentes aéreos e

---

[24] Diz Kunz: "(…) *trade volumes were already low and they fell further after 2014, mainly because of Russia's economic counter-sanctions. These economic ties matter most for Finland. While Russia was Finland's number one trading partner in 2013, it fell to number five in 2015 after Finnish exports declined by 35% and imports by 37%. only 6% of Finnish exports went to Russia in 2016, compared to 59% to the rest of the EU. As for Sweden, Russia accounted for only 1.4% of Swedish trade volumes in 2017, down from 2% in 2012: Russia therefore ranks as Sweden's 15th largest trading partner. The volume of trade declined between 2014 and 2016 because of sanctions, with Swedish exports to Russia falling 33% and Russian exports to Sweden down 44%.. In 2011, 2% of Danish exports went to Russia, which was then the 13th largest market for Danish companies. Sanctions led to a 40% decrease in exports. Meanwhile, the Russian market absorbed 2% of Norwegian exports in 2015. between 2014 and 2015, Norwegian exports to Russia declined by a third*", (KUNZ, 2018, p. 8). Tratam-se, portanto, de informações relativamente desatualizadas. Em consulta ao site *Statistics Finland*, vê-se que, em 2019, a Rússia foi o segundo maior parceiro do país em importações, e o quinto em exportações. O site *Statistics Sweden* mostra que a Rússia foi em 2020 o décimo quinto parceiro em exportações, e o décimo oitavo em importações. Em consulta ao site *UN Comtrade* para o ano de 2019, vê-se que a Rússia não figura nem entre os 15 maiores parceiros em exportações e importações. Chega-se à mesma conclusão para a Dinamarca em 2019, em consulta ao mesmo site.

[25] A autora diz ser a Noruega o 5º maior exportador de petróleo e gás do mundo. Mesmo em 2018, ano no qual o texto de Kunz foi publicado, o país não se encontrava em posição tão alta na lista de comercializadores dessas commodities. De acordo com o *The World Factbook* da *Central Intelligence Agency* (CIA), a Noruega foi o décimo quarto maior exportador de petróleo em 2014. Kunz comete certo exagero retórico nesse ponto. Com efeito, a Noruega é um relevante exportador, mas não se encontra no cume.

[26] As construções encerraram-se em 2019 e, em 2020, começou a operação comercial do empreendimento.

marítimos e a veemência dos protestos russos contra a acessão de Suécia e Finlândia à OTAN. Nas palavras de Kunz, "*They now perceive containing the Russian threat to be a priority when it comes to external security*", (KUNZ, 2018, p. 10).

As zonas de pressão estariam em duas regiões: a do Mar Báltico – estratégica para Finlândia, Suécia e, em menor grau, Dinamarca, diz Kunz –, e a do Ártico/Atlântico Norte. No Báltico, antes da anexação da Crimeia, a Rússia invadiu deliberadamente o espaço aéreo sueco em 2013. Consoante a autora, não se teria receio de uma invasão convencional, mas de um *revival* do caso Ucraniano, no qual forças irregulares, os famigerados "*little green men*", entrariam em um país báltico, o que acionaria o artigo 5 do Tratado de Washington[27]. Aventa-se também a possibilidade de ataque a territórios estratégicos como as finlandesas Ilhas de Aland ou a sueca Ilha de Gotland. A região do Ártico/Atlântico Norte, continua a autora,

> (…) *plays a crucial role in Russian military strategy, first and foremost for nuclear deterrence. Moscow also bases its military strategy on the idea of a "bastion" which seeks to control the waters and airspace around it to prevent an adversary from entering them in order to transfer troops or provide supplies. A2AD is therefore once more at the heart of the scenarios being considered. If Moscow for example managed to block the "GIUK" (Greenland, Iceland, Great Britain) gap, Norway would find itself behind enemy lines and the United States would be unable to come to its aid. Nevertheless, the region is not a priority for NATO* (…). (KUNZ, 2018, p. 11)

Isso colocaria a Noruega em posição diferente à de seus vizinhos. Oslo conclama a OTAN a incrementar suas capacidades marítimas, assim como as de seus membros. A Dinamarca, por exemplo, explica a autora, teme a exacerbação das tensões com a Rússia. Para Copenhague, conquanto a situação possa mudar no futuro, não há papel operacional imediato para a OTAN no Ártico. No que diz respeito ao Atlântico, no entanto, criou-se em 8 de novembro de 2017 um Comando abrangendo essa região[28]. Em todo caso, para Kunz, a

---

[27] Este é o artigo que trata da defesa coletiva da OTAN. De acordo com a própria organização, é o cerne da fundação da OTAN e do espírito de solidariedade dentro da Aliança. O texto do artigo diz: "*The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security*", (ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE, 1949).

[28] Trata-se do primeiro comando da OTAN dedicado à região desde 2003. Foi declarado operacional em 2020 (ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE, 2020).

deterioração do ambiente estratégico tem tido efeito direto sobre as políticas de defesa nacional, inclusive no incentivo à formação de parcerias de cooperação intra e extrarregionais[29].

As estratégias de Noruega e Dinamarca se apoiam sobre a OTAN e consistem essencialmente em defender parte do território até a chegada de reforços aliados. A Noruega tem insistido na defesa coletiva baseada no artigo 5 do Tratado de Washington desde a década de 1990. A autora avalia que a abordagem sueca é parecida, conquanto não seja membro da Aliança. A reorientação para a defesa territorial sueca teve início em 2015, diz Kunz, e baseia-se no chamado "*threshold effect*", segundo o qual deve-se focar em tornar um ataque à Suécia demasiadamente custoso, o que, claro, depende da habilidade de autodefesa do país, com ou sem ajuda externa. Como, no entender finlandês, a ameaça russa jamais foi dissipada, manteve-se estrutura funcional de forças armadas, com contingentes da ativa e da reserva suficientes para que fosse possível ao país defender seu território sem a ajuda de aliados. Kunz aponta que os demais países nórdicos têm retomado investimentos no desenvolvimento de capacidades de defesa, após anos de baixa alocação de recursos para essa rubrica[30].

Com a retomada da conscrição militar na Suécia em 2010, que contou com relativo apoio da população, diz a autora, o serviço militar é, agora, obrigatório nos quatro países nórdicos. Isso traz à baila a atualização do conceito de defesa total, ou *total defence*, parte importante das estratégias nórdicas de defesa durante a Guerra Fria[31].

> *The model of "total defence" covers all the activities designed to prepare society for war and has been exported far beyond the North. The idea is that all resources, including civilian ones, should be mobilised to defend the nation, whether that be*

---

[29] Diz Kunz: "*After the United States, Great Britain is the most important partner for the Nordic countries. The Danish army, for instance, is sometimes described as a 'branch' of the British army, given how closely the two countries have cooperated operationally since the war in Iraq and the deployment of Danish troops to Afghanistan.* (…) *Interest in political and military cooperation with Germany is also growing. Due to its weight on the international stage but also because of its Russia policy, Berlin is often viewed as a stabilising force. The Swedish Defence Minister has repeatedly stated that he would like to intensify cooperation with Germany.* (…) *As for France, it is regarded in Copenhagen as a country with a similar strategic culture to Denmark's, while Oslo is watching the changes to NATO's maritime strategy with interest, and the role that France could play in it. Since the annexation of Crimea, cooperation agreements have also been signed between the Nordic countries and Poland, and the Netherlands and the Baltic states. In terms of bilateral cooperation between the Nordic countries, the cooperation between Sweden and Finland has become the most extensive.* (…) *Such cooperation is seen in Helsinki and Stockholm as a political priority and could apply in time of war. It therefore marks a major shift, as it may potentially call into question the principle of military non-alignment*", (KUNZ, 2018, p. 24-26).

[30] Ver Ringsmose (2013).

[31] Vale comentar que, para Braw (2021), o sistema de *total defense* dos países nórdicos foi desmobilizado nos estertores da Guerra Fria. Para a autora, o único que ainda o teria operante seria a Finlândia.

> *energy supplies and the medical sector or "psychological defence" and the population's willingness to defend the country. Another crucial element of total defence is cyber security and the security of communications and electronic infrastructure*. (KUNZ, 2018, p. 16)

Na avaliação da autora, as ameaças cibernéticas são um dos assuntos que mais preocupa os formuladores de políticas públicas nórdicos. Nesse diapasão, ela destaca a participação desses países em três instituições dedicadas ao combate a incidentes dessa natureza: o *Centre of Excellence for Countering Hybrid Threats* (Hybrid CoE), em Helsinki; o *Strategic Communications Centre of Excellence* (StratCom) em Riga e o *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE) em Tallinn.

Sobre o conceito de defesa total, Wither (2020) e Saxi, Sundelius e Swaney (2020) trazem reflexões válidas. Em relação às repercussões para os países bálticos, Saxi, Sundelius e Swaney entendem que o esforço dos países nórdicos – para eles, Noruega, Suécia e Finlândia, apenas – em incrementar a resiliência da sociedade por intermédio da dupla conceitual defesa total e segurança abrangente provavelmente não alterará o cálculo estratégico russo no curto prazo. Os autores argumentam, no entanto, que no longo prazo a aplicação combinada dessa dupla conceitual e do Artigo 3 do Tratado do Atlântico Norte[32] podem reforçar a resistência e a dissuasão no que diz respeito a medidas hostis de guerra híbrida, além de servir como complemento ao que chamam de *regional denial-based deterrence strategy*.

Os nórdicos, argumentam Saxi, Sundelius e Swaney (2020), estão em posição privilegiada para coordenar-se com os países bálticos e outros parceiros em direção a uma cooperação multilateral mais robusta em tecnologias de defesa, compartilhamento de informações e melhores práticas de implementação de defesa total. Os autores acreditam, inclusive, que os nórdicos poderiam exportar resiliência para a região ao participar de projetos de infraestrutura e energia que União Europeia tiver com os países bálticos, ampliando esforços de conexão de infraestruturas entre aliados e parceiros, diminuindo assim a dependência de atores hostis. Os países bálticos, por sua vez, deveriam adotar enfaticamente uma estratégia *whole-of-society*, recomendam, pois

> *Russia works to achieve its strategic objectives through the use of "hostile measures"—a broad range of tools applied simultaneously and without a clear causal logic. This approach is characterized by the exploitation of economic, ethnic,*

[32] Diz o Artigo 3 do Tratado Constitutivo da OTAN: "*In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack*", (ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE, 1949).

> *linguistic, regional, religious, social, and other divisions in target nations, often as preparation for higher-level violence or hybrid warfare. Russian leaders hope that the effect of these measures will create opportunities to exploit. This approach has been disorienting, perplexing, or puzzling to the U.S., allied, and partner strategy and policy communities as it stands in sharp contrast to their more familiar formal system of preplanning to achieve objectives through a specific strategy or particular tactics. Deterring and defending against Russian aggression in the BSR, prior to open hostilities, or "left of bang", is a political problem that requires a broader adaptive approach. In light of the threat environment, the governments of Norway, Sweden, and Finland rely on unique strategies of total defense and comprehensive security, with an emphasis not just on territorial security, but on crisis response, societal resilience, and regional security. Due to their broad conception of security, Nordic total defense strategies are well suited to enhancing resilience to hostile measures, countering hybrid challenges, delaying or disrupting short warning aggression, and for some, supporting regional allied efforts*. (SAXI; SUNDELIUS; SWANEY, 2020, p. 3)

A defesa total moderna, defendem, é uma abordagem *whole-of-society* para a segurança nacional que envolve a ação coordenada das forças armadas, de paramilitares, da polícia, dos ramos civis do governo, do setor privado e da população em geral, o que seria uma versão encorpada de medidas convencionais de defesa e dissuasão. A defesa total seria particularmente adequada para fazer frente a operações de informação, prover defesa psicológica para a população, reforçar a segurança interna, construir resiliência de serviços e infraestrutura crítica, complementar a defesa militar, apoiar parceiros e aliados e responder a desastres naturais e outros tipos de crise não causadas por ação humana. Por um lado, explicam os autores, a defesa total é uma abordagem não convencional e assimétrica cujo alvo é influenciar o cálculo de custos e benefícios do adversário. Por outro, é uma estratégia que abarca a sociedade como um todo e a prepara para enfrentar crises de toda sorte.

Wither (2020) reforça o envolvimento da sociedade civil como distintivo na estratégia de defesa total. Para o autor, o conceito está ancorado em bases físicas e psicológicas robustas. A soma de resiliência de infraestruturas e resiliência da sociedade constitui a resiliência nacional, a pedra fundamental da defesa total. Se entendida como a capacidade da sociedade de resistir e se recuperar com rapidez e facilidade de choques e estresses por meio de uma combinação de fatores civis, econômicos, comerciais e militares, a resiliência complementa a defesa territorial, que seria a dimensão puramente militar da defesa total, diz Wither.

O conceito de defesa total seria particularmente benéfico em situações nas quais não há limite claro para o início das hostilidades, tornando-a útil face a ameaças híbridas. Adicionalmente, trata-se de uma ideia predominantemente não-militar, "*seeking to solidify the*

status quo with capabilities that are themselves defensive", (SAXI; SUNDELIUS; SWANEY, 2020, p. 4).

Os desafios, como se poderia supor, dizem respeito à mentalidade corporativista de diferentes carreiras, bem como à diferença entre os treinamentos por elas implementados. Civil e militar, setor público e privado, todos têm seus jargões, formas de organização, preferências por determinados tipos de soluções, métodos de compartilhamento de informações, o que pode atravancar a comunicação e o trabalho conjuntos.

3.1 SUÉCIA

A *A national cybersecurity strategy* (SUÉCIA, 2017a) não é aberta com argumentos de todo incomuns. Com efeito, afirma-se logo nas primeiras linhas que a transformação digital é um fenômeno global que tem impactos sobre todos os setores da sociedade[33]. Ainda que haja oportunidades associadas a ela, continua o documento, os riscos e ameaças que vêm a reboque – cuja dificuldade de detecção é diretamente proporcional à velocidade com que inovações são feitas – devem ser gerenciados estrategicamente, posto terem o condão de impactar não apenas a segurança da Suécia, mas também sua estabilidade econômica.

Estabelece-se na Estratégia que questões de segurança cibernética dizem respeito à sociedade como um todo, *the whole of society*. Enfatiza-se que não é possível resolver desafios de segurança isoladamente. Isso se mostra particularmente importante no caso de questões cibernéticas, em que diferentes *stakeholders* trabalham de maneiras distintas em diferentes contextos. A colaboração é, portanto, fundamental, assevera o documento, principalmente entre os setores público e privado. Isso é repetido *diversas* vezes ao longo da Estratégia. Por óbvio, inovações tecnológicas são capitaneadas pela iniciativa privada, que também é proprietária e gerente de boa parte dessa infraestrutura.

Decorre dessa constatação o fato de que desafios cibernéticos são compartilhados com outros países, de maneira que as soluções estratégicas devem ser desenvolvidas por meio da colaboração internacional e da ênfase em medidas preventivas. Cita-se a União Europeia

[33] Relatório da Comissão Europeia (2019b, p. 4) indica ser de 75% o índice de suecos que usam a *internet* para enviar documentos ao governo, número surpreendentemente maior que o da Estônia, por motivos que serão explicitados na subseção dedicada a este país.

(UE) e demais fóruns multilaterais como palco preferencial para tal coordenação, com destaque para as iniciativas regulatórias da UE nesse campo[34].

O objetivo é estruturar iniciativas *risk based* de segurança cibernética que apoiem a transformação digital contínua da Suécia sem perder de vista a segurança e os interesses nacionais – são citados nominalmente direitos humanos, liberdades civis, competitividade econômica e funcionamento da sociedade. Em relação ao primeiro e ao último item, a Estratégia complementa-os com proteção à vida e à saúde da população, bem como a capacidade de defesa de valores fundamentais, tais como democracia e Estado de Direito. A ambição sueca, de acordo com o documento, é posicionar-se como líder mundial no aproveitamento das oportunidades trazidas pela transformação digital.

Para fins de esclarecimento semântico na leitura da Estratégia, o documento informa de saída que se compreende segurança cibernética como medidas de segurança que preservem a confidencialidade, a autenticidade e a disponibilidade de informação. Confidencialidade significa que pessoas não autorizadas não conseguem acessar determinada informação. Autenticidade é a integridade da informação, que não é modificada, manipulada ou destruída por pessoas não autorizadas. Disponibilidade, por fim, diz respeito ao pronto acesso de pessoas autorizadas à informação solicitada. Prescrições sobre segurança da informação são encontradas em alguns instrumentos regulatórios, como o *Protective Security Act* (SUÉCIA, 2019b), que versa sobre atividades sensíveis de segurança na Suécia e as medidas protetivas cabíveis.

O documento diz expressamente que a abertura de uma sociedade democrática depende da habilidade de se manter níveis satisfatórios de confidencialidade, autenticidade e disponibilidade no trato da informação, o que implica a proteção da própria informação e dos sistemas usados para a armazenar e transferir. Eis a importância da segurança cibernética para a Suécia: salvaguardar não apenas sistemas de informação em sentido estrito, mas também a democracia como um todo. O exercício de direitos e liberdades depende do acesso a informações confiáveis, sem as quais a tomada de decisões embasadas resta comprometida. A Estratégia põe em xeque até a qualidade e efetividade de todos os tipos de contatos e atividades empreendidos na convivência social caso esse ponto não seja observado. O caso

[34] Recentemente, a União Europeia (2020) divulgou nova estratégia de segurança cibernética. Fora isso, ocorreram nos últimos meses propostas de diretivas sobre medidas de segurança cibernética, início das atividades do *Stakeholder Cybersecurity Certification Group* e comunicação da Comissão Europeia sobre medidas de implementação do 5G (UNIÃO EUROPEIA, 2021).

das informações de cunho sensível é salientado, em particular a possibilidade de que estas sejam perdidas, roubadas, manipuladas e divulgadas àqueles não autorizados a consumi-las. Diz-se informações relacionadas à privacidade dos indivíduos, mas também as atinentes a

> (…) *law enforcement, technological products, business relations, total defence or circumstances concerning other states. Today, the systems for handling information are mainly based on digital information and communications technology. This applies not least to the systems that Sweden depends on to govern and lead the country during extensive strains that might result from crisis or war. Such systems must be secured. Furthermore, many societal activities are based on functioning digital information and control systems that continuously handle large quantities of sensitive information in order to control, e.g. electricity distribution, water supply, transportation, transport infrastructure or hospital equipment. Industrial activities such as engineering and processing are also dependent on functioning digital information and control systems today. Incidents and attacks with regard to Swedish trade and industry can have far-reaching consequences, both for individual companies and entire value chains, thus threatening Swedish jobs.* (SUÉCIA, 2017a, p. 5).

O documento entende que a internet é uma infraestrutura global. Se a infraestrutura crítica sueca está intrinsecamente ligada à internet, a vulnerabilidade resultante pode ter consequências difíceis de antecipar e gerenciar. Ainda que as ameaças possam advir não apenas de ataques planejados, mas também de eventos adversos que comprometam a integridade de cabos submarinos e satélites, por exemplo, a Estratégia sueca identifica a ação de países e atores a eles ligados – ou atores que disponham de capacidade ofensiva equivalente – como a mais séria ameaça à segurança cibernética sueca.

A justificativa é que estes dispõem de recursos suficientes para o emprego de métodos avançados de ataque. Assim, ataques cibernéticos e intrusão em sistemas de TI, conforme disposto no documento, podem constituir ameaça separada ou fazer parte de um conjunto de instrumentos militares e políticos de poder. Os alvos podem ser tanto a infraestrutura crítica em tempos de paz – o que, em alguns casos, poderia ser considerado ataque armado, de acordo com o documento – ou os valores fundamentais suecos, atacados por intermédio de campanhas de desinformação e influência. A expectativa é que ataques cibernéticos direcionados aos meios de comunicação, à grande mídia, tornem-se mais frequentes.

> *Disinformation can be used to intentionally disseminate untrue or misleading details in order to influence people's attitudes, standpoints and actions in a certain direction. An influence campaign is centrally controlled, while also offering the use of a broad spectrum of methods, both open and covert, a subset of which might be data intrusion and other cyberattacks. It can also include political, diplomatic, economic and military instruments of power. The dissemination of incorrect or misleading information risks undermining confidence in our public institutions and challenges the security of society. Source criticism and access to a diversity of*

> *independent media and news agencies strengthen awareness and counteract the effects of disinformation and influence campaigns*. (SUÉCIA, 2017a, p. 6 – 7)

Diante desse cenário, a Estratégia reforça que a responsabilidade pela proteção do país recai sobre toda a sociedade e que os esforços devem ser contínuos se o objetivo é manter níveis satisfatórios de segurança cibernética. O reforço da segurança técnica deve levar em consideração que, em boa parte dos casos, é o erro humano que abre portas exploradas em ataques cibernéticos. Eis o porquê de se sugerir que é importante "*raise the awareness and ability of all users of IT systems and to create conditions for developing a security culture throughout society*", (SUÉCIA, 2017a, p. 7). A Estratégia entende que as prioridades devem ser assegurar aos esforços de segurança cibernética uma abordagem sistemática e abrangente; incrementar a segurança de redes, produtos e sistemas; incrementar a capacidade de prevenção, detecção e gerenciamento de ataques cibernéticos e incidentes de TI em geral; aumentar a possibilidade de prevenção e combate a crimes cibernéticos; aumentar o conhecimento sobre o tema e fomentar a construção de expertise e robustecer a cooperação internacional.

No que diz respeito à primeira prioridade, assegurar aos esforços de segurança cibernética uma abordagem sistemática e abrangente, o documento designa as autoridades governamentais centrais, as autoridades municipais, as autoridades estaduais – o termo usado é "counties" – e a iniciativa privada como responsáveis por sua própria segurança cibernética e pela condução de esforços contínuos de incremento da segurança do país como um todo.
A ideia é que todos os *stakeholders* tenham a visão abrangente de segurança cibernética como uma área complexa e multidisciplinar que inclui tecnologia, administração, economia e direito. Por isso a Estratégia insiste que a segurança cibernética deve ser parte integral das atividades de todos os níveis e setores da sociedade. As medidas de segurança devem criar um ambiente sólido de gerenciamento de informação para tempos de paz e de crise.

Nesse diapasão, determina-se ainda a elaboração de um modelo nacional no qual iniciativas de segurança cibernética possam se basear. Assim se uniformizará a condução de esforços de segurança cibernética, ao invés de cada *stakeholder* adotar métodos distintos para lidar com o assunto, baseados em quadros regulatórios diferentes e avaliações díspares de ameaças e riscos. Ainda que o gerenciamento de informações seja de responsabilidade de cada órgão ou organização, o governo central entende que há valor na coordenação de esforços de segurança cibernética, de maneira que atores possam avaliar de maneira uniforme

ameaças, riscos e medidas a serem implementadas. Dessa maneira, informações similares teriam níveis equivalentes de proteção em todos os lugares e o modelo constituiria uma plataforma comum para os esforços sistemáticos de segurança cibernética que tornasse possível a coordenação de regulamentações, métodos, ferramentas e treinamentos de forma célere. Isso facilitaria o monitoramento do governo central e criaria boa capacidade operacional caso haja ataques graves. Já há exemplos na própria Suécia:

> *The Cooperation Group for Information Security (SAMFI) plays an important role through its work for secure information assets in society. SAMFI consists of a number of central government authorities that have particular tasks in the area of cyber security: the Swedish Civil Contingencies Agency (MSB), the Swedish Defence Materiel Administration, the National Defence Radio Establishment (FRA), the Swedish Armed Forces, the Swedish Police Authority, the Swedish Post and Telecom Authority (PTS) and the Swedish Security Service. MSB has administrative responsibility for the group. The collaborative forum, the National Cooperative Council against Serious IT Threats (NSIT), analyses and assesses threats and vulnerabilities regarding serious or qualified cyberattacks against our most security-sensitive national interests. NSIT consists of the Swedish Security Service, FRA and the Swedish Armed Forces through its Military Intelligence and Security Service (MUST). (...)Public-private collaboration is a voluntary, agreed cooperation between public and private stakeholders. The cyber security area has several examples of platforms for public-private collaboration. One of these is MSB's establishment of a number of forums for information sharing (FIDI) in different sectors and areas: FIDI Telecom, Swedish CERT forum, FIDI Finance, FIDI Health and Social Care, FIDI Operations and FIDI Supervisory Control And Data Acquisition (SCADA). The area of electronic communications also has the National Telecommunications Coordination Group (NTSG). NTSG is a voluntary cooperation forum aimed at supporting the restoration of the national infrastructure for electronic communications during extraordinary events in society*. (SUÉCIA, 2017a, p. 10)

Em relação à segunda prioridade, incrementar a segurança de redes, produtos e sistemas, a Estratégia salienta, além da efetividade e segurança dos meios de comunicação eletrônica, a disponibilidade desta independente das condições de funcionamento além das fronteiras do país. Ou seja, trata-se de busca por autosuficiência, na medida em que isto seja possível em termos de infraestrutura integrada internacionalmente. A criptografia, assim como soluções de TI, devem ser aplicadas para atender às necessidades de comunicação de toda a sociedade. Um argumento levantado pela Estratégia é que os desenvolvimentos no campo de políticas públicas de segurança resultaram na retomada de planejamento sob a égide da defesa total. Assim, aos agentes de ordem pública, segurança, saúde e defesa deve ser assegurada a possibilidade de comunicarem-se mutuamente com segurança, tanto em condições normais quanto em crises – fala-se em guerra no documento. Nesse diapasão, o ponto nevrálgico para os suecos é que políticas públicas e quadros regulatórios devem ser

atualizados com maior frequência em tempos de desenvolvimentos tecnológicos e mudanças internacionais acelerados, inclusive a legislação penal sueca (SUÉCIA, 2017a, p. 19), com destaque para a cooperação jurídica internacional (SUÉCIA, 2017a, p. 21), já no âmbito da terceira prioridade. Os documentos oficiais que complementam esses pontos são *A Completely Connected Sweden by 2025 – a Broadband Strategy* (SUÉCIA, 2016a) e *For sustainable digital transformation in Sweden – a Digital Strategy* (SUÉCIA, 2017b). Novamente, como ocorre em diversos pontos ao longo da Estratégia, bate-se na tecla da colaboração *whole of society* como fundamental no campo cibernético, pois "(...) *in-depth and systematic collaboration both with the sector's stakeholders and between authorities in the area of cyber security and supervision constitutes a good basis for increasing expert support to the cyber security efforts of authorities that have sectoral responsibility*", (SUÉCIA, 2017a, p. 14).

A promoção do expertise e o aumento do conhecimento sobre o tema, a quarta prioridade, passa pelo conhecimento da sociedade como um todo sobre as vulnerabilidades no ciberespaço. A MSB – agência sueca de contingências civis, subordinada ao Ministério da Justiça – mapeia e examina os esforços de segurança cibernética da sociedade em parceria com *stakeholders* pertinentes. Há também, no entanto, dimensão acadêmica: o documento propõe o incentivo à condução de pesquisa e desenvolvimento (P&D) e educação universitária de alto nível nos campos de segurança cibernética, TI e telecomunicações. Ou seja, trata-se de investimento em capital humano:

> *Efforts to safeguard society's cyber security need to be conducted in a long-term and effective manner, and serve the interests of fundamental societal values, such as the protection of personal privacy. This presupposes that these efforts are based on a knowledge base that is both deep and broad with regard to needs, risks, vulnerabilities, threats and opportunities. The need for skilled personnel in the area of cyber security is also great. A lack of cutting-edge expertise affects both the private and public sectors. It should thus be in the interest of all relevant stakeholders to find long-term solutions to satisfy the increasing needs for skilled labour. The area of cyber security brings to the fore many complex research questions that often require a multidisciplinary approach. Research in fields such as data encryption is of an advanced technical nature, while research focusing on the individual relates to subjects such as organisational and behavioural science. The development of self-driving cars and intelligent cities raises, for example, sociotechnical, legal and ethical issues that relate directly to cyber security.* (SUÉCIA, 2017a, p. 22-23)

Novamente, o que se coloca é a que questão cibernética atravessa fronteiras – físicas, profissionais e, nesse caso, educacionais. Cooperação, coordenação e interdisciplinaridade são

ideias repetidas ao longo da Estratégia. Há, inclusive, lei sueca disciplinando a questão. A *Government Bill Collaborating for Knowledge* (SUÉCIA, 2016b) versa sobre investimentos de pesquisa focados em áreas como o chamado *Research Centre for Future Digital Transformation Technology*. Foram criados também grupos de trabalho e programas de parceria inovadora para robustecer a produção intelectual e profissional sobre o tema.

Em relação à cooperação internacional, o que se coloca é que "*international cooperation on cyber security is to be enhanced, as part of the objective of a global, accessible, open and robust internet characterised by freedom and respect for human rights*", (SUÉCIA, 2017a, p. 24). Isto é, não se trata necessariamente de parceria eminentemente técnica a respeito da questão cibernética, mas de parceria em torno da manutenção de valores democráticos, de defesa da liberdade de fluxos econômicos – inovação, competitividade e desenvolvimento social – e, finalmente, de combate a ataques cibernéticos. Destaca-se a importância dos Direitos Humanos, que não se restringem ao mundo *offline*. Com efeito, argumenta-se no documento que uma abordagem centrada em direitos deve ser o ponto de partida de debates sobre a transformação digital. Ora, privacidade e segurança cibernéticas são indispensáveis para o exercício de direitos e liberdades, e para o aproveitamento das possibilidades legadas pelas ICTs, pontua-se. Assim, o acesso à internet aberta, segura e livre é de suma importância para a luta global pela preservação e expansão dos Direitos Humanos, da democracia, do Estado de Direito e do desenvolvimento – aqui entendido em sentido amplo, relacionado à educação, às finanças, à agricultura, à saúde, ao meio ambiente e à igualdade de gênero.

É o domínio, por óbvio, das Relações Internacionais e da Política de Segurança. Para a Estratégia, a questão cibernética foi assunto delimitado e técnico para tema de fundamental importância para a paz, segurança e desenvolvimento globais. As ações de Estados nessa seara têm tido repercussão cada vez mais intensa em RI e Segurança. O documento entende que o principal ponto de tensão interestatal no trato da temática é a visão sobre o papel dos Estados e de seu direito a monitorar, controlar e limitar fluxos de informação e infraestrutura.

> *The Government's goal for the development of the internet is a global, accessible, open and robust internet characterised by freedom and respect for human rights. The credible and effective promotion of the freedom aspect requires a developed international cooperation to manage the security challenges. External developments, including those in Sweden's surrounding region, underline this need. Adequate security measures will continue to be needed with reference to national security or for combating cybercrime. At the same time, there is a risk that the desire to control information flows will gain the upper hand in the actions of many states.*

> *Tendencies towards the fragmentation and restriction of the internet go against Sweden's fundamental values and long-term economic and security-policy interests. The Government maintains that such a development must be addressed by means of developed international cooperation. There are also fundamental tensions between states in their view of the roles and responsibilities of non-state actors. The Government wants to counteract a state-led administration of the internet and stresses the central roles and responsibilities of non-state actors for a free and secure internet, where the private sector and civil society can assert their legitimate interests. It is clear that both vulnerabilities and security measures concern and involve the private sector and civil society as a whole. Cooperation and dialogue with non-state actors thus need to continue being developed at the international level*. (SUÉCIA, 2017a, p. 25)

O documento vê dificuldades na ONU, por exemplo, em razão da interpretação das normas de Direito Internacional relativas ao ciberespaço. No entanto, há certo otimismo em relação a discussões sobre o estabelecimento de padrões internacionais voluntários e medidas de construção de confiança para o incentivo ao comportamento responsável dos Estados nesse âmbito, com a possibilidade de uso de regras e acordos internacionais para responsabilização de violadores. A Suécia, reforça a Estratégia, deve ter papel ativo nesses debates para prevenir conflitos e apoiar o consenso internacional sobre padrões de comportamento aceitável no campo cibernético.

Outros dois documentos de interesse são a *National approach to Artificial Intelligence* (SUÉCIA, 2018a) e o *Comprehensive cyber security action plan 2019-2022* (SUÉCIA, 2019). Os dois primeiros derivam da Estratégia; já o segundo é uma prestação de contas da Ministra das Relações Exteriores da Suécia, Ann Linde, frente ao Parlamento do país. Vale levantar alguns pontos sobre todos.

A *National approach* já adianta a importância que o país dá à Inteligência Artificial, e o objetivo é fornecer as condições necessárias para que essa seja usada para benefício de toda a sociedade sueca. Vê-se a tecnologia com potencial fundamentalmente positivo, com destaque para a possibilidade de impulsionar o crescimento econômico do país e prover soluções para desafios socioambientais, entre outros usos mencionados no documento. Os pontos negativos levantados dizem respeito à possível manipulação de dados, parca transparência, perda de confiança, danos financeiros e possíveis consequências deletérias para o funcionamento do regime democrático. Não se trava discussões aprofundadas a respeito do lado negativo da Inteligência Artificial, no entanto; a mensagem principal do documento é que a Inteligência Artificial pode contribuir para o desenho de um setor público mais eficiente, de maneira que a Suécia deve aproveitar seus benefícios, modular os riscos e

posicionar-se como líder no campo, com notável vantagem competitiva no que diz respeito a essa tecnologia, e ambiente de negócios propício à proliferação de empresários e pesquisadores especializados. Ventila-se o conceito de Inteligência Artificial sustentável, que corresponde a uma tecnologia ética, segura, confiável e transparente. Em consonância com a *A national cybersecurity strategy* (SUÉCIA, 2017a), fala-se em abordagem *whole of society* também para a Inteligência Artificial. A visão sueca parece ser essencialmente economicista, e os usos militares da tecnologia sequer são mencionados. O desenvolvimento mais recente foi o anúncio do governo sobre o projeto de expandir a cooperação em Inteligência Artificial com países do eixo nórdico-báltico, sob liderança da Suécia (SUÉCIA, 2018b), assim como a cooperação dos países nórdicos no que diz respeito ao 5G (SUÉCIA, 2018c). Até o momento, houve apenas uma declaração de intenções.

O *Comprehensive cyber security action plan 2019-2022* tem caráter mais técnico. Trata-se de documento produzido por sete órgãos do governo sueco, liderados pela *Swedish Civil Contingencies Agency* (MSB). Integram o plano, ainda, a *National Defence Radio Establishment* (FRA); a *Swedish Defence Material Administration* (FMV); as *Swedish Armed Forces*; a *Swedish Post and Telecom Authority* (PTS); a *Swedish Police Authority* e o *Swedish Security Service*. As medidas devem ser postas em prática individualmente por cada órgão, de maneira conjunta ou em colaboração com demais atores relevantes. Essa colaboração, aliás, foi empreendida até na elaboração do Plano, posto que *stakeholders* da sociedade como um todo foram consultados por intermédio de *workshops* e reuniões. São 79 iniciativas derivadas do mandato imposto pela Estratégia, divididas em três eixos: assegurar a abordagem sistemática e abrangente de esforços de segurança cibernética; incrementar a segurança de redes, produtos e sistemas; e fortalecer a capacidade de prevenção, detecção e gerenciamento de incidentes de TI e de ataques cibernéticos. Para cada iniciativa, designa-se expressamente quais órgãos serão responsáveis por executá-la, assim como se coloca a data limite para que a iniciativa seja completada. Muitas das iniciativas envolvem as Forças Armadas diretamente – são aproximadamente 34 de 79.

A Suécia já implementou por completo a *NIS Directive* (UNIÃO EUROPEIA, 2016), legislação da Comissão Europeia sobre Segurança da Informação e das Redes, derivada da *EU Cybersecurity strategy* (UNIÃO EUROPEIA, 2013), com aplicação sobre toda a União Europeia, cujo foco é o desenvolvimento de capacidades nacionais, colaboração além das fronteiras nacionais – há, inclusive, um *NIS cooperation group*, fórum de troca de informações entre membros da UE sobre a implementação da normativa – e supervisão

nacional de setores críticos. O ponto focal da *NIS Directive* é a *Swedish Civil Contingencies Agency* (MSB). A *Swedish Post and Telecom Authority* é a agência responsável por gerenciar provedores de serviços digitais, enquanto as autoridades competentes para operadores de serviços essenciais são a *Swedish Energy Agency* (STEM), a *Swedish Transport Agency* (TS), a *Sweden's Financial Supervisory Authority* (FI), o *The Health and Social Care Inspectorate* (IVO), a *The Swedish Food Agency* (SLV) e a *The Swedish Post and Telecom Authority* (PTS). A equipe nacional responsável por respostas a incidentes de segurança computacional – *National CSIRT* – é a CERT.SE, ligada à MSB.

3.2 FINLÂNDIA

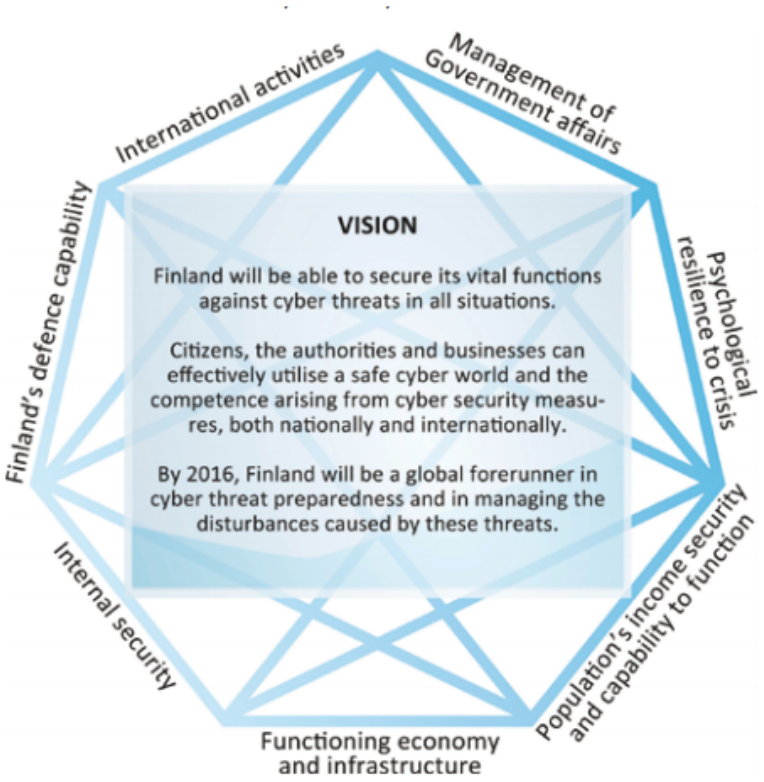
A *Finland's Cybersecurity Strategy* (FINLÂNDIA, 2013) vê o domínio cibernético como essencialmente internacionalizado. O crescimento da intensidade informacional da sociedade, o aumento da propriedade estrangeira de meios de comunicação, a integração entre informação e ICTs, o uso de *open networks* e a dependência da eletricidade são citados como causas das mudanças das necessidades de segurança das funções vitais da sociedade em condições normais e de emergência. Interessante ressaltar o que a Finlândia entende por funções vitais da sociedade. Estas incluem o gerenciamento de assuntos governamentais, relações internacionais, capacidades de Defesa finlandesas, segurança interna, funcionamento adequado da economia e da infraestrutura do país, a segurança econômica da população e a *resiliência psicológica a crises*.

Assim como a Estratégia da Suécia, a da Finlândia acredita no potencial positivo do domínio cibernético e das novas tecnologias, com prováveis impactos positivos para a economia finlandesa, pois "*National cyber security is interconnected with the success of Finnish companies*", (FINLÂNDIA, 2013, p. 1). O termo chave utilizado no documento é *comprehensive security*, ou segurança abrangente, o que se aplicaria não apenas ao escopo temático da segurança cibernética, mas também ao leque de atores envolvidos em sua sustentação. Não se usa os termos *whole of society*, mas a ideia está presente ao longo da Estratégia finlandesa. Um comentário interessante feito nas primeiras páginas da Estratégia é que segurança cibernética não deve ser um conceito jurídico que leve à concessão de novas competências a autoridades ou órgãos do governo. Nesse sentido, a ideia é que todos ajam dentro de suas atribuições.

O mais alto nível de gerenciamento de segurança cibernética cabe ao governo, de acordo com o documento. Determina-se que cada ministério e braço administrativo é responsável por segurança cibernética e resposta a crises dentro de suas atribuições. A Estratégia também pontua que a natureza das ameaças cibernéticas reforça a importância não apenas da cooperação, mas também da coordenação flexível e eficiente.

Para a Finlândia, seu histórico de forte tradição em cooperação público-privada e intersetorial a colocam em posição privilegiada na vanguarda da segurança cibernética. Também contribuiriam para essa avaliação a extensão territorial do país, sua cultura colaborativa e seu capital humano especializado.

Figura 4 – Visão finlandesa sobre segurança cibernética



Fonte: Finlândia (2013)

São sete os princípios que governam a abordagem finlandesa para segurança cibernética. Estes estão assentados sobre a primazia do governo sobre assuntos cibernéticos; a importância da flexibilidade; o destaque da cooperação internacional; a necessidade de se investir em pesquisa, desenvolvimento e educação; e, finalmente, a conveniência de se fomentar as atividades da iniciativa privada no campo cibernético.

> 1. In line with the Government decree on the tasks assigned to ministries, matters which relate to cyber security as a rule fall within the remit of the Government. Each ministry is in its sector responsible for preparing cyber security related matters and appropriate arrangement of administrative matters. 2. As cyber security is an essential part of the comprehensive security of society the approach for its implementation follows the principles and procedures established in the Security Strategy for Society. 3. Cyber security relies on the information security arrangements of the whole society. Cyber security depends on appropriate and sufficient ICT and telecommunication network security solutions established by every actor operating in the cyber world. Various collaborative arrangements and exercises advance and support their implementation. 4. The approach for the implementation of cyber security is based on efficient and wide-ranging information-collection, an analysis and gathering system as well as common and shared situation awareness, national and international cooperation in preparedness. This requires the establishment of a Cyber Security Centre as well as the development of 24/7 information security arrangements for the entire society. 5. Cyber security arrangements follow the division of duties between the authorities, businesses and organisations, in accordance with statutes and agreed cooperation. Rapid adaptability as well as the ability to seize new opportunities and react to unexpected situations demand strategic agility awareness and compliance from the actors as they keep developing and managing the measures which are aimed at achieving cyber security. 6. Cyber security is being constructed to meet its functional and technical requirements. In addition to national action, inputs are being made into international cooperation as well as participation in international R&D and exercises. The implementation of cyber security R&D and education at different levels does not only strengthen national expertise, it also bolsters Finland as an information society. 7. Cyber security development will heavily invest in cyber research and development as well as in education, employment and product development so that Finland can become one of the leading countries in cyber security. 8. In order to ensure cyber security development, Finland will see to it that appropriate legislation and incentives exist to support the business activities and their development in this field. Basic know-how in the field is gained through business activity. (FINLÂNDIA, 2013, p. 5)

Além dos princípios, há ainda dez parâmetros a serem implementados. O primeiro preconiza a criação de um modelo de colaboração eficiente entre as autoridades e demais atores com o fito de fomentar avanços em segurança e defesa cibernéticas. O segundo parâmetro recomenda esforços no sentido de conscientizar atores vitais para a garantia do que os finlandeses entendem ser as funções vitais da sociedade sobre a abrangência das questões de segurança cibernética – aqui se faz referência às infraestruturas críticas. O terceiro parâmetro prevê a manutenção e melhora da capacidade de negócios e organizações-chave na detecção e no combate a ameaças cibernéticas com potencial disruptivo para o ambiente de negócios. O quarto parâmetro preocupa-se com a garantia de que a polícia tenha como prevenir, expor e investigar crimes cibernéticos. O quinto parâmetro delega às Forças Armadas Finlandesas a tarefa de desenvolver capacidade de defesa cibernética. O sexto parâmetro mira o fortalecimento da segurança cibernética nacional por intermédio da

participação nas atividades de organizações internacionais e de fóruns multilaterais relevantes para o tema – trata-se, portanto, de tarefa para o Ministério das Relações Exteriores da Finlândia; menciona-se nominalmente a União Europeia, a Organização para a Segurança e Cooperação na Europa (OSCE), a Organização do Tratado do Atlântico Norte (OTAN) e a Organização para a Cooperação e Desenvolvimento Econômico (OCDE)[35].

O sétimo parâmetro urge, na linha do segundo parâmetro, o desenvolvimento do *cyber expertise* de toda a sociedade. O oitavo parâmetro observa a necessidade de se apoiar a implementação de medidas de segurança cibernética com iniciativas legislativas. O nono parâmetro recomenda o engajamento da iniciativa privada com tarefas de segurança cibernética concretas e o décimo parâmetro indica que a implementação da Estratégia será monitorada e coordenada por um Comitê de Segurança – que, à época em que a Estratégia foi lançada, não havia sido criado ainda.

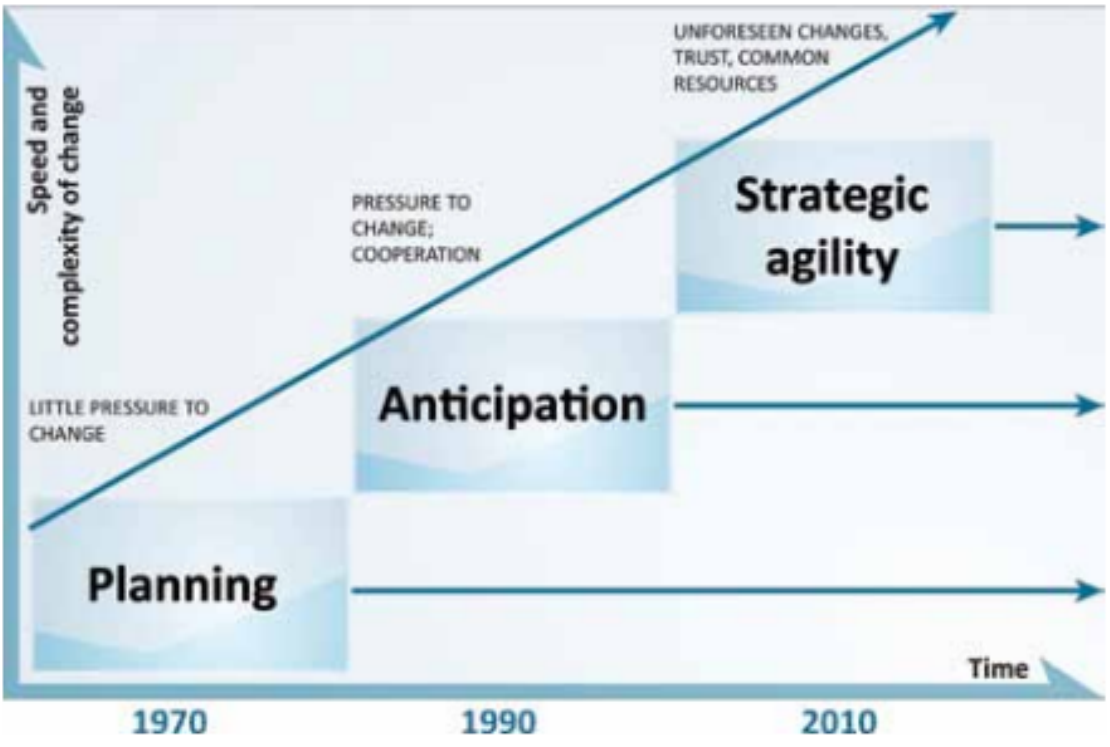
A Estratégia é acompanhada por um dossiê de apoio que discorre longamente sobre assuntos de importância vital para a segurança cibernética. O objetivo da inclusão desse anexo é fornecer informações precisas sobre o espaço cibernético. Há algumas informações interessantes nas páginas do dossiê.

Uma delas é a defesa da chamada agilidade estratégica. A ideia é que o gerenciamento da segurança cibernética propugna sensibilidade estratégica, comprometimento coletivo e fluidez de recursos. O que isso significa? De acordo com o documento, a sensibilidade estratégica diz respeito à capacidade de avaliar e reagir com celeridade a situações críticas. O comprometimento coletivo, direcionado basicamente à liderança do país, requer consciência integrada da situação, gestão coordenada e em rede e otimização de benefícios coletivos. Por fim, o uso flexível de recursos demanda a capacidade de implementar contramedidas e alocar recursos financeiros com rapidez. Em resumo, diz o dossiê, para que se lide adequadamente com os desafios cibernéticos deve-se combater a rigidez de estruturas governamentais encasteladas. Conclui-se que é necessário criar nova abordagem coordenada e em rede para as estruturas do governo.

---

[35] Trata-se, grosso modo, de lista parecida com a da Estratégia sueca: "*Today, cyber security issues are treated from different perspectives in a large number of international organisations and formats, e.g. the UN, EU, OSCE, Council of Europe, OECD, NATO, the Nordic-Baltic cooperation, and in several specialised international organisations and processes (e.g. ICANN, IETF, ITU and IGF), which treat questions of the operation, control and administration of the internet. In addition to this, there are initiatives and processes of significance to the international discussion on rules and standards, such as the "London Process", Freedom Online Coalition (FOC) and the Swedish initiative Stockholm Internet Forum (SIF)*", (SUÉCIA, 2017, p. 25).

Figura 5 – Agilidade Estratégica



Fonte: Finlândia (2013)

Em 2017, a Finlândia publicou documento complementar à Estratégia de 2013. O *Implementation Programme for Finland's Cybersecurity Strategy for 2017 – 2020* (FINLÂNDIA, 2017a). Trata-se da segunda versão de documento dessa natureza: em 2014, o S*ecurity Committee* já tornara público versão anterior do programa de implementação, na qual 74 medidas foram prescritas a ministérios do governo finlandês e também a outros atores[36]. A nova foi elaborada com base também nas avaliações de setores administrativos do governo, da iniciativa privada, da academia e das ONGs, as quais foram levadas em consideração pelo *Security Committee* na escrita da segunda versão do programa.

[36] Dentre os resultados obtidos por essa primeira versão do programa de implementação, a Finlândia destaca cinco: "*The Government Security Network (TUVE) project and the development of sector-independent ICT tasks; The National Cyber Security Centre established at the Finnish Communications Regulatory Authority (FICORA) and the development of associated CERT activities; The Development Project for the Central Government 24/7 Information Security Operations (SecICT) and the related improvement of monitoring and warning; The Development Project for Jyväskylä Security Technology (JYVSECTEC); and Cyber security courses organised by the National Defence Training Association of Finland*", (FINLÂNDIA, 2017a, p. 5). A avaliação é, portanto, de que este foi um exercício profícuo.

Um dos pontos levantados pela Finlândia (2017a, p. 5) de se desenvolver modelos de gerenciamento estratégico para a segurança cibernética – algo, aliás, já aventado na Estratégia de 2013. São interessantes as perguntas que se coloca no início do Programa, e que subsidiam as páginas subsequentes:

> *What kind of management and steering structures, models and legislation should be created to achieve the Cyber Security Vision? What kind of models for compiling and disseminating joint situational awareness among the public administration, the business community and NGOs should be established and developed?* (…) *What kind of far-reaching administrative and technological actions are needed to retain confidence in the cyber domain in normal conditions, during disruptions in normal conditions and emergency conditions?* (…) *What kind of curricula for developing expertise should be available to citizens, the business community and the public administration? Who will provide the curricula and generate scientific information?* (FINLÂNDIA, 2017a, p. 8)

O que se faz é desenhar uma matriz que comporta tanto os parâmetros delineados na Estratégia de 2013 quanto às ações que devem ser tomadas para que eles sejam cumpridos, de maneira que se tenha uma visão planejada de como os objetivos devem ser atingidos. Por exemplo, para a definição de quem comporá o grupo de liderança estratégica, algo conectado aos parâmetros 1, 4, 5, 6 e 9, define-se que a responsabilidade cabe essencialmente a três atores, com certa possibilidade de extensão desse rol para incluir outros cujo envolvimento se faça necessário: *Secretariat of the Security Committee*, *Prime Minister's Office*, *Ministry of Finance*. No todo, além dos três supramencionados, os seguintes atores são convocados nominalmente a tomarem parte no esforço de condução dos trabalhos: *Ministry of Finance*, *Ministry of Transport and Communications*, *Government ICT Centre (Valtori)*, *Ministry of Foreign Affairs*[37], *Ministry of Defence*, *Ministry of the Interior*, *the Police*, *Ministry of Justice*, unidades de serviços e fornecedores da iniciativa privada que prestem serviços à administração pública, *Ministry of Social Affairs and Health*, *Population Register Center*, *Ministry of Agriculture and Forestry*, *National Land Survey of Finland*, *Finnish Patent and Registration Office*, *National Emergency Supply Agency*, *State Treasury*, *Finnish Government Shared Services Centre for Finance and HR*, *Tax Administration*, *JAMK University of Applied Sciences*, *National Defence Training Association of Finland*, *Finnish Association for the*

[37] Salta aos olhos uma inovação do Ministério das Relações Exteriores finlandês: a figura do *Ambassador of Hybrid Affairs*. A ideia é que o responsável pelo cargo contribua para a construção do expertise do Ministério sobre o assunto, e ajude a destacar a Finlândia enquanto líder global em questões relacionadas a ameaças híbridas. O primeiro diplomata a ocupar o posto foi o Embaixador Mikko Kinnunen. A Finlândia entende que o hibridismo da questão significa que ela resvala em política externa, segurança, comércio e comunicação estratégica, entre outros domínios. O objetivo seria influenciar a coesão interna de um país e, por conseguinte, erodir sua segurança no sentido amplo do termo. (FINLÂNDIA, 2018).

Welfare of Older People, *Confederation of Finnish Industries*, *Ministry of Education and Culture* e *Finnish National Agency for Education*[38]. Note-se que as atribuições não são exaustivas, tampouco excludentes.

Figura 6 – Segurança Abrangente

Fonte: Finlândia (2017b)

Finalmente, o *The Security Strategy for Society* (FINLÂNDIA, 2017b) é, dos três documentos finlandeses citados, o mais extenso e aprofundado. É uma espécie de atualização pontual da Estratégia de 2013[39] e compilado do *expertise* acumulado pelo país. Discorre-se longamente sobre o conceito de segurança abrangente, entendido como o modelo finlandês de preparação da sociedade para intercorrências, baseado fundamentalmente na cooperação entre autoridades governamentais, iniciativa privada, organizações da sociedade civil e cidadãos em geral. O ponto é que:

> *The practical implementation of comprehensive security takes place on the basis of cross-administrative strategies, strategies for individual administrative branches, implementation programmes and other documents. These include the Internal Security Strategy, the Finnish Cyber Security Strategy and their implementation programmes*. (FINLÂNDIA, 2017b, p. 7)

[38] Não consta dessa listagem não exaustiva o *National Cyber Security Centre* e a *Finnish Transport and Communications Agency* (Traficom). Note-se, no entanto, que ambos são o ponto focal para a implementação da *NIS Directive* da União Europeia na Finlândia.

[39] Registre-se que a Estratégia de 2013 não é o documento mais antigo do governo finlandês sobre a chamada segurança abrangente da sociedade. A primeira estratégia administrativamente transversal remonta a 2003 e focava a proteção das funções vitais da sociedade, assim como o fazia a de 2006. Importante notar que o foco não eram as questões cibernéticas, mas uma avaliação multifatorial de situações com potencial de afligir a coesão da sociedade finlandesa.

Antes de passar à Noruega, cumpre destacar brevemente artigo de Bjola e Papadakis (2020) sobre a abordagem finlandesa para a construção de resiliência digital. Na visão dos autores, os pilares da estratégia do país para tornar a sociedade mais resistente à desinformação, por exemplo, são um sistema público de educação que investe em alfabetização digital e midiática que permita aos indivíduos identificar vieses narrativos; liberdade de imprensa e integridade jornalística; relacionamento positivo da população com veículos de comunicação tradicionais; ambiente midiático não-polarizado; transparência política; e comunicação estratégica proativa no sentido de evitar a radicalização de grupos marginalizados. Em resumo, trata-se de investir na salubridade da esfera pública e na prevenção da radicalização do que os autores chamam de *counterpublics*[40].

3.3 NORUEGA

A Noruega já está em sua quarta estratégia de segurança cibernética. A última versão, *National Cyber Security Strategy for Norway* (NORUEGA, 2019a), foi publicada 16 anos depois da primeira, apresentada em 2003, e tem por distinto das demais o reforço da importância de cooperação entre a administração pública e a iniciativa privada; entre civis e militares; e entre países. A Estratégia é acompanhada da *List of Measures* (NORUEGA, 2019b), extenso documento complementar que detalha lista de medidas a serem tomadas para a implementação das diretrizes delineadas na Estratégia. As revisões subsequentes ocorreram em 2007 e 2012 (NORUEGA, 2012). Em 2015 foi tornado público relatório sobre vulnerabilidades digitais da sociedade norueguesa, de autoria do *Committee on Digital Vulnerabilities in Society* (NORUEGA, 2015). Além disso, em 2017, o Parlamento da Noruega trouxe à tona o primeiro *white paper* dedicado exclusivamente à segurança cibernética, o *Cyber Security – a joint responsibility* (NORUEGA, 2017a).

Ainda que reforce em diversas ocasiões ao longo do documento a importância da colaboração e da parceria entre atores relevantes nos âmbitos nacional e internacional, a Estratégia faz distinção protocolar entre segurança cibernética civil[41] e segurança cibernética militar. A primeira está sob comando do *Ministry of Justice and Public Security*, enquanto a

[40] Reportagem especial de Mackintosh (2019) para a CNN fornece exemplos práticos de como esses pontos que seriam levantados por Bjola e Papadakis (2020) estavam sendo colocados em prática.

[41] Complementarmente, há legislação na Noruega que prevê que as comunicações entre governo e população sejam feitas de maneira digital por *default*, a não ser que o cidadão requisite de outra maneira (COMISSÃO EUROPEIA, 2019e, p. 11).

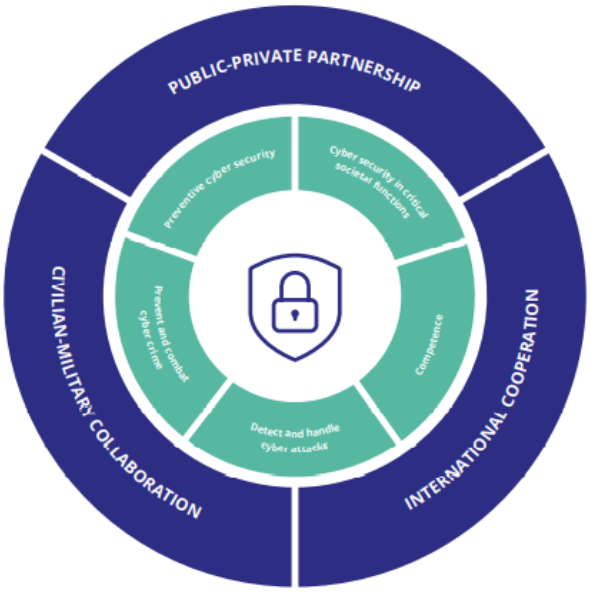
segunda é responsabilidade do *Ministry of Defence*. São nominalmente citados, também, o *Ministry of Local Government and Modernisation*; o *Ministry of Foreign Affairs*; a *Norwegian National Security Authority*; o *National Police Directorate*; o *Norwegian Police Security Service*; o *Norwegian Intelligence Service;* a *Agency for Public Management and eGovernment*; a *Norwegian Data Protection Authority;* a *Norwegian Communications Authority*; o *Norwegian Directorate for Civil Protection* e o *Norwegian Centre for Information Security*[42].

Os cinco objetivos estratégicos delineados no documento são a digitalização segura das empresas norueguesas; o apoio às funções críticas da sociedade por intermédio de infraestrutura digital confiável; aprimoramento das competências em segurança cibernética em consonância com as necessidades da sociedade; fomento à capacidade norueguesa de detectar e gerenciar ataques cibernéticos; e fortalecimento da capacidade da polícia de prevenir e combater crimes cibernéticos.

O *Joint Cyber Coordination Centre* (*Felles cyberkoordineringssenter* – FCKS) é um *hub* colaborativo entre diferentes autoridades do governo norueguês. O foco é a detecção e o gerenciamento de ataques cibernéticos, além da avaliação de riscos e da confecção de análises estratégicas. Participam dele a *National Security Authority*, o *Norwegian Intelligence Service*, o *Norwegian Police Security Service* e o *National Criminal Investigation Service*.

[42] Note-se que, por não ser membro da União Europeia, a Noruega não implementou, por óbvio, as *NIS Directive*.

Figura 7 - Visão norueguesa sobre segurança cibernética



Fonte: Noruega (2019)

O que distingue a Noruega das outras estratégias de segurança cibernética, no entanto, é o fato de que dedica um documento separado à dimensão internacional do assunto. Trata-se da *International Cyber Strategy for Norway* (NORUEGA, 2017b), um documento sucinto cujo principal objetivo estratégico é colocar a Noruega em posição de influenciar desenvolvimentos sobre o espaço cibernético na arena internacional – o conceito-chave colocado é previsibilidade das condições de desenvolvimento e uso do ciberespaço. Para a Noruega, é importante que se conserve a abertura, a segurança, a robustez e a liberdade da internet, e a cooperação internacional é nevrálgica para a consecução desse objetivo. O documento explica que, em 2016, o Ministério das Relações Exteriores da Noruega chegou a estabelecer um grupo de coordenação cibernética internacional que deveria sincronizar as posições do país sobre políticas públicas para o espaço cibernético com aquelas discutidas em fóruns internacionais. O documento é encerrado com uma declaração sobre a prevalência dos direitos humanos também no ciberespaço, o que se traduziria em termos estratégicos no apoio àqueles que defendem a liberdade de expressão *online*; na promoção do entendimento sobre a importância da segurança cibernética; na parceria com outros países, com a iniciativa privada e com atores não-governamentais para assegurar o acesso livre e seguro à internet; e,

finalmente, na construção de consensos sobre a proteção do direito à privacidade no espaço cibernético.

3.4 DINAMARCA

A *Danish Cyber and Information Security Strategy 2018-2021* (DINAMARCA, 2018) é o resultado da colaboração entre 13 ministérios, coordenados pela *Agency for Digitisation*, órgão ligado do Ministry of Finance. Participaram o *Ministry of Defence*; o *Ministry of Justice*; o *Ministry of Industry, Business, and Financial Affairs*; o *Ministry of Health*; o *Ministry of Transport, Building, and Housing*; o *Ministry of Energy, Utilities, and Climate*; o *Ministry of Environment and Food*; o *Ministry of Taxation*; o *Ministry of Higher Education and Science*; o *Ministry of Foreign Affairs*; o *Ministry of Education*; e o *Ministry of Economic Affairs and the Interior*.

É a segunda estratégia de segurança cibernética do país. A primeira foi a *National Strategy for Cyber and Information Security 2015-2016* (DINAMARCA, 2015), que lançou as bases por meio de iniciativas como a criação via *Centre for Cyber Security*[43], a autoridade nacional de segurança de TI, de uma *threat assessment unit* e um centro consultivo para segurança de ICTs, entre outras. Outros documentos que compõem o ecossistema dinamarquês de estratégias digitais, por assim dizer, são *A Stronger and More Secure Digital Denmark* (DINAMARCA, 2016), que está em processo de atualização, e *National Strategy for Artificial Intelligence* (DINAMARCA, 2019).

No total, são 25 iniciativas prescritas na Estratégia.

> Everyday Safety: 1.1 Creating a national cyber situation centre; 1.2 Minimum requirements for authorities' work on cyber and information security; 1.3 Regulatory initiatives in the cyber area; 1.4 Monitoring of critical ICT systems in central government; 1.5 Common digital portal for reporting; 1.6 National centre for processing of cases concerning ICT crime; 1.7 Enhanced collaboration on prevention of ICT-related attacks and enforcement in response to such attacks; 1.8 Higher security for identity documents; 1.9 Improved prioritisation of national ICT infrastructure; 1.10 Secure communication in central government.
>
> Better Competencies: 2.1 Digital judgment and digital competencies acquired via the educational system; 2.2 Information portal; 2.3 Research into new technology; 2.4 Corporate partnership to increase ICT security in the Danish business community; 2.5 Collaboration on competence development and the fostering of a security culture

[43] Esse é o ponto de contato para questões relativas à implementação da *NIS Directive*. É também o CSIRT dinamarquês.

> in central government; 2.6 Improved awareness drives aimed at citizens and businesses.
>
> Joint Efforts: 3.1 Sub-strategies at sectoral level and decentralised cyber security units; 3.2 Cross-sectoral eforts to support cyber and information security in critical sectors; 3.3 Management of suppliers of outsourced ICT services; 3.4 Strengthened national coordination; 3.5 Increased level of involvement in international collaboration; 3.6 Evaluation of the current state of cyber and information security; 3.7 Overview of information worthy of protection; 3.8 Information security architecture; 3.9 National and international eforts to safeguard data ethics and protection of personal data. (DINAMARCA, 2018, p. 17)

Assim como nas Estratégias de Suécia, Finlândia e Noruega, ainda que com outros termos, reforça-se ao longo do documento o que a Dinamarca chama de responsabilidade compartilhada. A ideia é que cidadãos, iniciativa privada e governo familiarizem-se com os riscos cibernéticos e os gerenciem de maneira conjunta. Assim, "*the central government is responsible for safeguarding national security. Businesses and authorities are responsible for safeguarding security at their own organisations.* (...) *all citizens will have to understand how their actions can afect their own digital security and that of others*", (DINAMARCA, 2018, p. 13). Isso está alinhado às três áreas prioritárias no documento, preparo tecnológico; conscientização sobre segurança cibernética e da informação entre cidadãos, iniciativa privada e governo; e melhora da cooperação e da coordenação entre as autoridades governamentais responsáveis – inclusive no nível regional e municipal.

Há, ainda, os princípios do sistema de gerenciamento de crises dinamarquês, que constam do anexo da Estratégia. São eles o princípio da responsabilidade setorial, no qual a autoridade responsável pelo cotidiano do departamento também deve lidar com crises naquele setor; o princípio da similaridade, segundo o qual os procedimentos e responsabilidades cotidianas devem, na medida do possível ser aplicados ao sistema de gerenciamento de crise; o princípio da subsidiariedade, cujo mote é que a resposta a emergências deve ser gerenciada o mais próximo da área afetada quanto possível; o princípio da cooperação, autoexplicativo; e o princípio da precaução, que preconiza ser preferível superestimar o nível de preparação para uma situação sobre a qual não se tem informações precisas.

Interessante citar os parâmetros publicados em 2018 para todas as iniciativas legislativas que versem sobre digitalização. São elas:

> *Simple and distinct rules: Legislation should be simple and distinct, thus contributing to a more uniform and digital administration; Digital communication: Legislation should underpin digital communication with citizens and corporations; Enable automated digital case processing: Legislation should underpin fully or*

> *partly automated digital case processing while still taking into account the legal rights for citizens and companies; Consistency across Authorities - uniform concepts and re-use of data: Data and definitions of concepts are re-used across authorities; Safe and secure data management: Data security should be prioritised: Using public IT-infrastructure: Public IT-solutions and standards should be applied; Legislation should prevent fraud and errors: Legislation must be designed to support the use of IT for purposes of control.* (COMISSÃO EUROPEIA, 2019c, p. 8)

Foi divulgada em fevereiro de 2021 pelo Ministério das Relações Exteriores dinamarquês, ainda, a *Strategy for Denmark's Tech Diplomacy* (DINAMARCA, 2021). Em consonância com os outros documentos mencionados nessa subseção, a importância dos direitos humanos, dos valores democráticos e da integridade da sociedade dinamarquesa são reforçados. De interesse é a declaração de que o objetivo da Estratégia é trabalhar em direção a um futuro tecnológico mais justo, democrático e seguro, pois "*new technologies also provide authoritarian regimes with new opportunities for digital surveillance, behaviour control, oppression and censorship*", (DINAMARCA, 2021, p. 4). Demonstra-se preocupação com a concentração de poder na mão de grandes conglomerados de tecnologia, as chamadas *Big Tech*, e se vê esses mesmos conglomerados como peões das disputas geopolíticas entre Estados Unidos e China. As prioridades estratégicas da diplomacia tecnológica da Dinamarca são, portanto, responsabilidade, no sentido de que a indústria da tecnologia deve cumprir sua responsabilidade social; democracia, posto que a governança digital global deve ser assentada sobre valores democráticos e respeito aos direitos humanos; e segurança, pois a tecnologia sustenta a segurança[44] da Dinamarca.

O mais interessante da Estratégia é a dissertação sobre a figura do *Tech Ambassador*. Como o próprio nome sugere, trata-se de diplomata dedicado às questões tecnológicas. As bases geográficas de ação são Copenhague, Vale do Silício e Pequim, os dois últimos notáveis *hubs* de inovação. Os eixos de ação do *Tech Ambassador* são seis: representar o governo dinamarquês na relação com a indústria tecnológica global com o fim de promover *accountability* e diálogo crítico; coletar informações sobre inovações tecnológicas, de maneira a manter o tema no topo da agenda de prioridades dinamarquesas; construir coalizões com *stakeholders*, como organizações multilaterais, sociedade civil, iniciativa privada e outros países; contribuir para a construção de *expertise* no debate público dinamarquês sobre o tema; auxiliar o desenvolvimento de políticas públicas cabíveis por intermédio da coleta de

[44] Forçoso ressaltar que a tradução para ambos termos usados em língua inglesa, *safety* e *security*, é segurança. Não há tanta nuance na tradução, motivo pelo qual se faz esta observação.

informações e perspectivas de outros países; e promotor da Dinamarca como país pioneiro na digitalização da sociedade, promovendo as exportações de tecnologia e atraindo investimentos. É uma ideia produtiva.

3.5 ESTÔNIA

Dos países que são citados neste capítulo, a Estônia é, provavelmente, o mais avançado na digitalização do governo e da sociedade. Desde 2005, por exemplo, o país digitalizou por completo um dos rituais mais importantes de um regime democrático, as eleições (E-ESTONIA, 2021). O sistema estoniano, o i-Voting[45], permite que os eleitores depositem seus votos de qualquer computador que tenha acesso à internet. Isso pode ser feito de qualquer lugar do mundo, em eleições locais ou nacionais. Aproximadamente um terço dos votos de cada ciclo eleitoral da Estônia são depositados via i-Voting (ESTÔNIA, 2021). Resta coerente com relatório da Comissão Europeia (2019a) que aponta índices absolutamente díspares entre percentuais da população da Estônia e da União Europeia em geral que usam a internet para enviar documentos para o governo: 70% da população estoniana contra 30% da europeia como um todo[46].

A *Cyber Strategy* (ESTÔNIA, 2019) é a terceira do país. A primeira foi a *Cyber Security Strategy* (ESTÔNIA, 2008)[47], ainda sob a coordenação do equivalente ao *Ministry of Defence*, e a segunda, a *Cyber Security Strategy* (ESTÔNIA, 2014), já sob o *Ministry of Economic Affairs and Communications*. Os esforços do país no sentido da digitalização, no entanto, antecedem em muito a divulgação desses documentos (ESTÔNIA, 2019, p. 18).

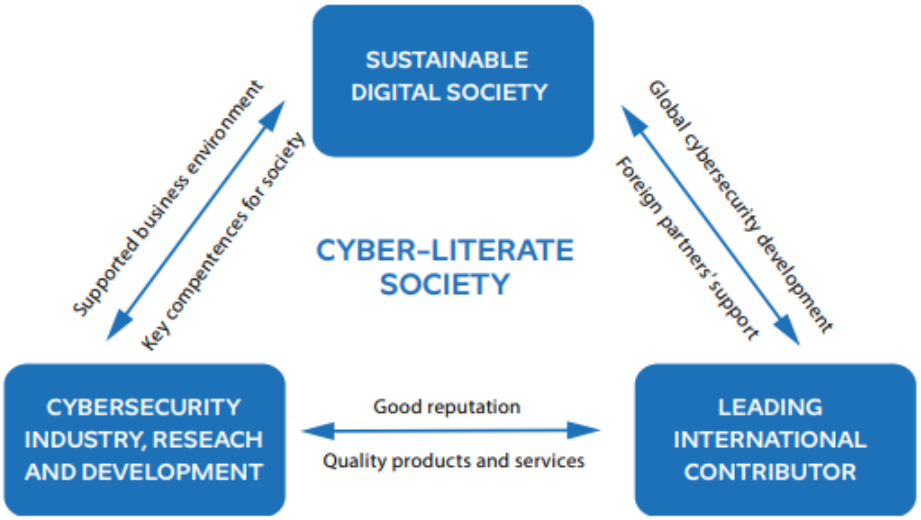
---

[45] Registre-se que o sistema i-Voting não foi criado pelo governo estoniano, tampouco é por ele gerenciado. O modelo adotado pelo país para o fornecimento de serviços públicos em meios digitais, do próprio sistema de voto digital, passando pela autenticação e a criptografia de comunicações, assenta-se sobre parceria público-privada. No caso do i-Voting, a empresa responsável por sua criação e manejo é a Cybernetica AS, com sede em Tallinn. É interessante notar, ainda, que, por meio do e-Estonia Briefing Center, a Estônia oferece, em parceria com as empresas que prestam serviços ao governo do país, diversas modalidades de consultoria para representantes de governos, formuladores de políticas públicas em geral, executivos, jornalistas e investidores que se interessarem pelo modelo de digitalização estoniano. O e-Estonia Briefing Center é uma espécie de agência híbrida que envolve o governo e a iniciativa privada.

[46] Note-se que não foi adotada legislação específica sobre a digitalização do governo até o momento. Tratam-se de esforços independentes de obrigação legal. Há leis específicas sobre segurança cibernética, proteção de dados pessoais e segurança de sistemas de informação, por exemplo (COMISSÃO EUROPEIA, 2019a, p. 11).

[47] Importante notar que a publicação se deu no ano seguinte ao famigerado ataque cibernético sofrido pelo país. O estopim para o episódio foi a mudança de local de um memorial que comemorava a libertação da Estônia do jugo nazista, libertação essa trazida a cabo pelo exército soviético. Para estudo sobre o caso, ver Herzog (2011).

Figura 8 - Objetivos da *Cyber Security Strategy*



Fonte: Estônia (2019)

No que diz respeito a estruturas governamentais, o planejamento está a cargo do *Ministry of Economic Affairs and Communications*, em cooperação com o *State Information System Authority*[48], a *Technical Surveillance Authority*, o *Estonian Internet Foundation*, o *State Infocommunication Foundation*, a *Enterprise Estonia* e a *Startup Estonia* em assuntos de segurança das redes e dos sistemas de informação. A coordenação estratégica é atribuição do *Government of the Republic security committee's cybersecurity council*. Têm atribuições nessa seara também o *Ministry of Education and Research*, o *Ministry of Justice*, o *Ministry of Defence*, o *Police and Border Guard Board*, o *Internal Security Service*, o *Ministry of the Interior*, o *Ministry of Foreign Affairs*[49], o *Ministry of Finance* e o *The Government Office*[50].

Na Estratégia de 2019, coloca-se que o documento tem caráter horizontal. Isso significa, continua-se, que estão envolvidos a administração pública – tanto civis quanto militares –, provedores de serviços essenciais, iniciativa privada em setores estratégicos e a comunidade acadêmica. A Estratégia coloca que, para uma sociedade digital ser bem-sucedida, a garantia da segurança cibernética e o desenvolvimento de uma sociedade de

[48] Além de ser o CSIRT do país, é também o ponto de contato para a implementação da *NIS Directive*.
[49] Importante lembrar que a Estônia abriga o *NATO Cooperative Cyber Defence Centre of Excellence* (CCD COE).
[50] A lista não é exaustiva, e há ainda outras agências e órgãos envolvidos.

informação devem compor um todo estratégico. Assim, "(…) *the maintenance and development of a sustainable digital environment also requires cross-sectoral focused cooperation. This can only be ensured by means of a strong and coherent sectoral strategy*", (ESTÔNIA, 2019, p. 8). O documento coloca a segurança cibernética como fundamental para que a Estônia possa usufruir do potencial transformador que o espaço cibernético oferece ao crescimento socioeconômico do país. Diz-se, ainda, que a proteção e promoção dos direitos e liberdades fundamentais deve ser estendida ao ambiente virtual, e que a transparência do governo e a confiança da população são imprescindíveis a uma sociedade digital. Em consonância, portanto, com as estratégias analisadas até o momento.

São quatro os objetivos colocados, e a cada um correspondem medidas que devem ser cumpridas até 2022. O primeiro é construir uma sociedade digital sustentável, assentada sobre a resiliência tecnológica; a prevenção e resolução de incidentes cibernéticos; e o fomento ao desenvolvimento de um modelo abrangente de governança e de uma comunidade coesa de segurança cibernética. O segundo objetivo é fortalecer a indústria e dos centros de pesquisa e desenvolvimento ligados à segurança cibernética por meio de investimentos. O terceiro objetivo estratégico é posicionar a Estônia como um dos principais e mais confiáveis atores da arena internacional no que diz respeito à segurança cibernética, fim que deve ser atingido com cooperação internacional[51] em questões do espaço cibernético e promoção de "*sustainable cybersecurity capacity building*" ao redor do mundo.

O quarto e último objetivo estratégico é incentivar a alfabetização digital da Estônia, com foco não apenas na conscientização da sociedade sobre segurança cibernética, mas também no desenvolvimento de mão de obra capacitada para atender às demandas dos setores público e privado. Sobre esse último ponto, aliás, a Estratégia reconhece não haver margem de manobra em razão do pequeno contingente populacional de que o país dispõe. A solução proposta é intensificar mecanismos de cooperação e comunicação com vistas à redução da fragmentação de *expertise*. Fala-se também em auditoria dos recursos de cibersegurança do Estado, para que se desenvolva estrutura organizacional compatível, pois "f*or Estonia, cybersecurity does not mean protecting technological solutions; it means protecting digital society and the way of life as a whole*", (ESTÔNIA, 2019, p. 18).

---

[51] A título de informação, registre-se que norma regulamentando a cooperação internacional no campo da troca de informações sobre serviços de saúde, por exemplo, foi promulgada em novembro de 2018. Começou a funcionar também por intermédio do endereço eletrônico digilugu.ee uma espécie de unificação dos sistemas nacionais de agendamento de consultas médicas, exames complementares, e demais compromissos do campo da saúde (COMISSÃO EUROPEIA, 2019a, p. 6).

3.6 Estados Unidos

Os Estados Unidos têm a *National Cybersecurity Strategy* (ESTADOS UNIDOS DA AMÉRICA, 2018a), editada pela Casa Branca; a *Cyber Strategy* (ESTADOS UNIDOS DA AMÉRICA, 2018b), editada pelo Department of Defense; e a *Cybersecurity Strategy* (ESTADOS UNIDOS DA AMÉRICA, 2018c), editada pelo Department of Homeland Security. Os três documentos são complementares e inéditos, isto é, não há versões anteriores. Forçoso reconhecer que há a *International Strategy for Cyberspace* (CASA BRANCA, 2011), documento de quatro páginas no qual se prevê, inclusive, a possibilidade de que os Estados Unidos respondam de maneira cinética a ataques no ciberespaço. De interesse há, ainda, o relatório da *Cyberspace Solarium Commission*[52] (ESTADOS UNIDOS DA AMÉRICA, 2020), co-presidida pelo Senador Angus King (sem filiação partidária, do Maine) e pelo Representante Mike Gallagher (Republicano, do Wisconsin).

A implementação da Estratégia editada pela Casa Branca está a cargo do *National Security Council Staff*. Os pilares estão divididos em prioridades, por sua vez divididas em eixos temáticos. São quatro pilares: proteger o povo americano, o território nacional e o *American Way of Life*; promover a prosperidade dos Estados Unidos; preservar a paz por intermédio da força; e promover a influência americana.

Para o primeiro pilar, em relação à segurança das redes federais de informação, as prioridades são centralizar o gerenciamento e o controle da segurança cibernética civil; sincronizar o gerenciamento de risco e as atividades de tecnologia da informação; melhorar a cadeia de transmissão de gerenciamento de risco; fortalecer a segurança cibernética para prestadores de serviço do governo federal; e incorporar práticas inovadoras aos protocolos do governo. Sobre a segurança de infraestruturas críticas, as prioridades são estabelecer papéis e responsabilidades; priorizar ações de acordo com os riscos nacionais identificados; estabelecer fornecedores de ICTs como facilitadores de segurança cibernética; proteger a democracia do país[53]; viabilizar investimentos em segurança cibernética e em pesquisa e desenvolvimento; e melhorar a segurança cibernética dos setores marítimo, espacial e de

[52] O nome é inspirado no *Project Solarium* do governo general cinco estrelas Dwight David Eisenhower, presidente dos Estados Unidos da América de 1953 a 1961. *Solarium* foi um exercício de desenho de estratégia e política externa a ser executado a nível nacional. Para análise crítica sobre o assunto, ver artigo de Feaver e Inboden (2018) na revista *Foreign Policy*.

[53] Aqui fala-se especificamente da proteção à infraestrutura das eleições.

transportes. Para combater o crime cibernético e melhorar o monitoramento de incidentes, vislumbra-se a modernização de legislação relacionada à vigilância eletrônica e a crimes computacionais; a redução de ameaças de organizações criminosas transnacionais que operem no espaço cibernético; a apreensão de criminosos localizados no exterior; e o fortalecimento da cooperação jurídica com aliados.

No que diz respeito ao segundo pilar, promover a prosperidade dos Estados Unidos, a promoção de uma economia digital vibrante e resiliente deve ser atingida por meio do incentivo a um *marketplace* adaptável e seguro; da concessão de prioridade à inovação; do investimento em infraestrutura; da promoção do livre fluxo de dados através de fronteiras; da manutenção dos Estados Unidos como líder em tecnologias emergentes; e da promoção do ciclo completo de segurança cibernética[54]. A proteção à inovação americana será efetivada por intermédio de revisão dos mecanismos de investimento e operação estrangeiros nos Estados Unidos; manutenção de um sistema de proteção à propriedade intelectual forte e equilibrado; e proteção da confidencialidade e da integridade das ideias americanas. Para o desenvolvimento de recursos humanos qualificados em segurança cibernética, a Estratégia prescreve a construção de um programa de desenvolvimento de mão de obra; fornecimento de oportunidades educacionais para os trabalhadores americanos; expansão da força de trabalho de segurança cibernética no governo federal; e reconhecimento e promoção de indivíduos talentosos.

O terceiro pilar, preservação da paz por intermédio da força, tem dois eixos temáticos: fortalecimento da estabilidade cibernética com incentivo a edição de normas que definam comportamentos estatais responsáveis e dissuasão de comportamentos inaceitáveis no espaço cibernético. No primeiro eixo temático, a ação prevista é eminentemente diplomática: encorajar a adesão universal a normas cibernéticas. Já no segundo eixo temático, prevê-se a coleta de informações objetivas e colaborativas da chamada *Intelligence Community*; a formação de uma iniciativa de dissuasão cibernética; além do combate e da exposição de *information operations*.

Em relação ao quarto e último pilar, promover a influência americana, os eixos temáticos são promover uma internet aberta, confiável e segura e incentivar a formação de capacidades cibernéticas na comunidade internacional. As medidas prescritas para o primeiro

[54] Como se explica na própria estratégia, "*The United States Government will promote full-lifecycle cybersecurity, pressing for strong, default security settings, adaptable, upgradeable products, and other best practices built in at the time of product delivery. We will identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace* (…)", (ESTADOS UNIDOS DA AMÉRICA, 2018a, p. 15).

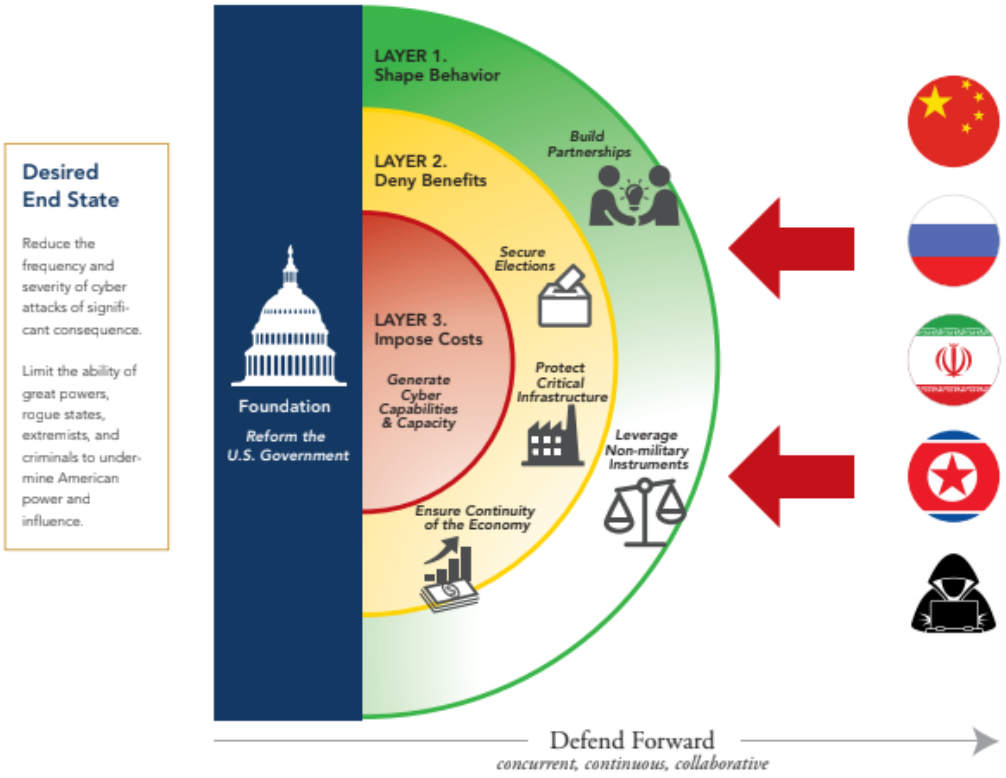
e para o segundo eixos temáticos são também fundamentalmente diplomáticas: proteger e promover a liberdade na internet; formar uma coalizão composta por países, representantes da iniciativa privada, acadêmicos e representantes da sociedade civil; promover um modelo de governança da internet *multi-stakeholder*; promover infraestrutura de comunicações e conexão à internet que sejam confiáveis; promover os produtos americanos em mercados internacionais; e incentivar a complementaridade das capacidades cibernéticas dos aliados dos Estados Unidos.

O que o documento do *Department of Defense* traz de diferente é o detalhamento da visão da Defesa sobre a questão. Fala-se com todas as letras, por exemplo, que

> *We are engaged in a long-term strategic competition with China and Russia. These States have expanded that competition to include persistent campaigns in and through cyberspace that pose long term strategic risk to the Nation as well as to our allies and partners. China is eroding U.S. military overmatch and the Nation's economic vitality by persistently exfiltrating sensitive information from U.S. public and private sector institutions. Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes. Other actors, such as North Korea and Iran, have similarly employed malicious cyber activities to harm U.S. citizens and threaten U.S. interests. Globally, the scope and pace of malicious cyber activity continue to rise. The United States' growing dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent and unacceptable risk to the Nation*. (ESTADOS UNIDOS DA AMÉRICA, 2018b, p. 1)

O foco, continua o texto, são os países que podem ameaçar a prosperidade e a segurança dos Estados Unidos, particularmente China e Rússia. Os objetivos são, em resumo, assegurar a capacidade das Forças Armadas de conduzir operações em um ciberespaço hostil, reforçar a cooperação das Forças Armadas por meio de exercícios conjuntos, defender a infraestrutura crítica dos Estados Unidos, proteger os sistemas de informação do *Department of Defense* e expandir a cooperação não apenas com outros órgãos do governo americano, mas também com a iniciativa privada e com países aliados. Já o que o documento do *Department of Homeland Security* (DHS) traz de novo é a listagem de medidas que diversos órgãos do governo tomaram para implementar suas diretrizes. Coloca-se, por exemplo, que, em 2017, o DHS editou uma diretiva operacional vinculante que ordenava a tomada de medidas para garantir a segurança de mensagens eletrônicas em particular e acesso à internet em geral em todos os órgãos do governo federal.

Figura 9 – Defesa Cibernética em Camadas



Fonte: Estados Unidos da América (2020)

O documento mais interessante, no entanto, é o relatório da *Cyberspace Solarium Commission* (ESTADOS UNIDOS DA AMÉRICA, 2020), que é acompanhado, inclusive, de propostas legislativas. Trata-se de um diagnóstico da estrutura de segurança cibernética dos Estados Unidos. O documento já coloca logo em suas primeiras linhas que os Estados Unidos está em risco de sofrer não apenas um ataque cibernético catastrófico, mas também de ser alvo de milhares de intrusões diárias que afetem transações financeiras e o sistema eleitoral do país, por exemplo. Isso sem falar nos bilhões de dólares que o país perdeu em roubo de propriedade intelectual empreendido por ciberespionagem, patrocinada por países antagonistas. O relatório conclui que a dissuasão é possível; depende de uma economia resiliente; requer reforma da estrutura do governo e participação ativa do setor privado no fortalecimento de seus protocolos de segurança cibernética; e prioriza a segurança das eleições americanas. A consequente proposta de dissuasão em camadas apoia-se sobre três pernas: modelar comportamento, ou promover atitudes responsáveis no espaço cibernético; negar vantagens, ou reforçar em parceria com o setor privado a segurança de redes críticas e do ecossistema cibernético americano; e impor custos, ou construir capacidade de retaliar no

ciberespaço contra agressores. É o que o relatório chama de *deterrence by denial* e *defend forward*.

Entre as prescrições legislativas do relatório, algumas chamam a atenção. Em relação à reforma da estrutura do governo, vislumbra-se a criação de comitês permanentes sobre segurança cibernética em ambas casas do Congresso[55]; a nomeação de um diretor nacional para questões cibernéticas, a ser sabatinado pelo Senado; e o recrutamento de servidores federais dedicados às questões cibernéticas. Pretende-se, ainda, criar no âmbito do *Department of State* um *Cyber Bureau* e nomear um *Assistant Secretary* dedicado às questões cibernéticas – fala-se muito ao longo do relatório sobre ameaças externas. Outras propostas são a reestruturação da *Election Assistance Commission*, o estabelecimento de um *National Risk Management Cycle*, criar *Critical Technology Security Centers*, empreender campanhas para a conscientização da população sobre segurança cibernética, incrementar a colaboração entre o setor privado e a comunidade de inteligência, aprovar lei que obrigue a notificação ao governo sobre incidentes cibernéticos e o estabelecimento de mecanismos extras de financiamento do *U.S. Cyber Command*.

3.6 Conclusão parcial

Neste capítulo, viu-se como os países nórdicos – Suécia, Finlândia, Noruega e Dinamarca –, a Estônia e os Estados Unidos organizam seus ecossistemas de segurança cibernética nos âmbitos estratégico e tático. Com exceção dos Estados Unidos, que adotou uma abordagem *top-down* na elaboração de sua Estratégia, os demais trilharam caminho mais horizontalizado na confecção de suas respectivas estratégias, envolvendo representantes de diversos grupos de interesse. Todos reconhecem ser de suma importância engajar não apenas os ramos do governo diretamente associados a questões tradicionais de segurança e defesa, mas a sociedade como um todo. Entende-se por sociedade como um todo governo – a nível federal, regional e local –, sociedade civil e iniciativa privada, e todos os seus subgrupos. Em particular, as estratégias dos países nórdicos e da Estônia destacam reiteradas vezes a importância da cooperação doméstica e internacional, com Dinamarca e Finlândia adotando,

[55] Registre-se que já há algumas estruturas dedicadas às questões cibernéticas no governo dos Estados Unidos. São elas a *Cybersecurity and Infrastructure Agency* (CISA), ligada ao *Department of Homeland Security* (DHS); o *Cyber Threat Intelligence Integration Center* (CTIIC), ligado ao gabinete do *Director of National Intelligence* (DNI); e, claro, no âmbito das Forças Armadas, o *U.S. Cyber Command*.

inclusive, a inovadora figura do *Tech Ambassador*, no caso dinamarquês, e do *Ambassador of Hybrid Affairs*, no caso finlandês. Deve-se notar que a doutrina da Defesa Total informa muito da abordagem nórdica sobre o assunto, de maneira que se deve ter em consideração o caráter eminentemente cultural da maneira como assuntos de segurança e defesa são tratados por esses países. Ao fim e ao cabo, tem-se que todos os países estudados veem a questão cibernética como um campo híbrido que requer, para ser adequadamente tratado, níveis elevados de coordenação e cooperação com amplíssimo espectro de atores.

4 O CASO BRASILEIRO: PRESSUPOSTOS PÁTRIOS

Antes de entrar no assunto deste capítulo e analisar a estratégia brasileira de segurança cibernética, cumpre tecer – talvez de maneira tardia nesse trabalho – breves comentários sobre as delimitações conceituais de segurança e defesa. Ainda que sejam distintos, defende-se que, no que diz respeito às questões cibernéticas, não faz sentido traçar fronteiras tão rígidas entre ambos, motivo pelo qual se usa os termos em conjunto. A transversalidade do ciberespaço e o hibridismo das ameaças dele derivadas tendem a esmaecer limites. Coloque-se pois entendimentos oportunos sobre essas definições para partirmos de pontos claros. As ideias de Medeiros Filho (2010) a respeito são cabais quando da consideração sobre o caso brasileiro. Para o autor,

> Do ponto de vista da teoria da integração, *defesa* corresponderia aos objetivos daquilo que Karl Deutsch chamou de *Comunidade de Segurança Amalgamada*, enquanto *segurança* corresponderia ao modelo de *Comunidade de Segurança Pluralística*. Enquanto a primeira sugere unidades políticas em competição, a segunda sugere cooperação entre unidades que compõem determinada comunidade de interesses. Enquanto o ideal da defesa é o poder, o ideal da segurança é a ordem. (MEDEIROS FILHO, 2010, p. 46)

Assim, para o Medeiros Filho, defesa sugeriria medidas direcionadas à tratativa de conflitos entre unidades políticas soberanas "realizadas à 'sombra da guerra', em um sistema internacional anárquico (…). As ameaças de defesa são de natureza geralmente externa, estatal e militar", (MEDEIROS FILHO, 2010, p. 45). Já o conceito de segurança estaria relacionado a vulnerabilidades sociais e fragilidades de políticas públicas, "o que sugere a adoção de soluções cooperativas para o seu tratamento", (MEDEIROS FILHO, 2010, p. 45). O centro do conceito de defesa seria poder, e o do conceito de segurança seria ordem.

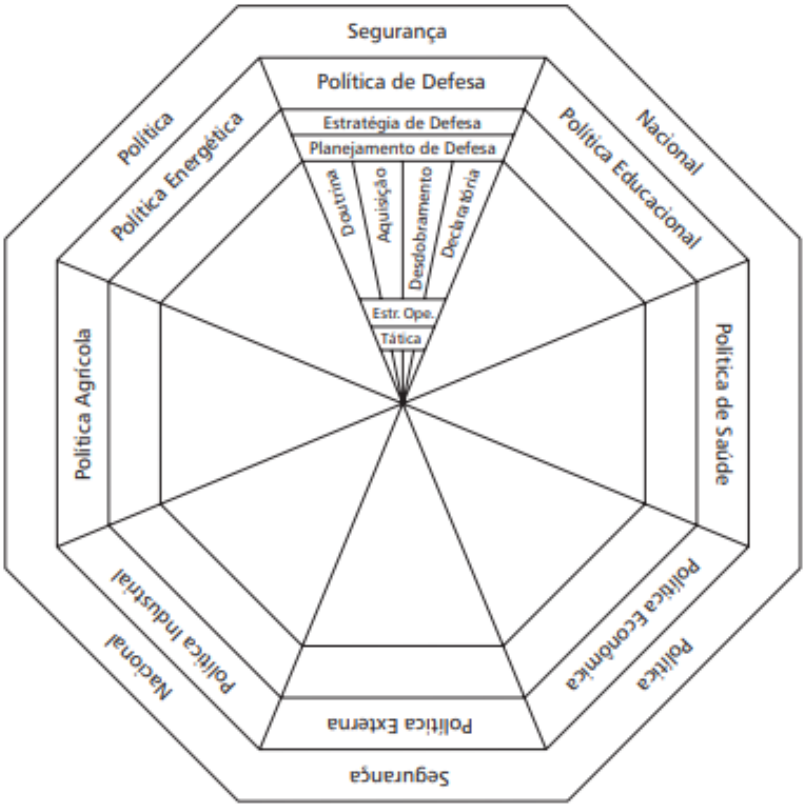
Figura 10 – Esquema de setores de segurança adaptado do modelo de Buzan

Fonte: Medeiros Filho (2010).

De maneira complementar, Rudzit e Nogami (2010, p. 6) discorrem sobre as correntes tradicional e nova no que diz respeito a perspectivas quanto a assuntos que devem ser considerados de segurança nacional. Ambas entendem ameaça como algo externo ao Estado – o que não necessariamente se aplicaria a países em desenvolvimento, conforme citação de Mohammed Ayoob (1992) feita pelos autores. Há, no entanto, divergências sobre o que poderia ser considerado ameaça. A corrente tradicional entende que o conflito militar é o elemento-chave para a compreensão do conceito, com alguma defesa também da centralidade do Estado na análise de segurança. A corrente nova, por sua vez, é, de acordo com os autores, reação ao "imenso 'afunilamento' que o campo de estudos estratégicos sofreu pela obsessão militar e nuclear da Guerra Fria. Este sentimento foi estimulado pelo aparecimento das agendas econômica e ecológica no cenário internacional durante as décadas de 1970 e 1980", (RUDZIT; NOGAMI, 2010, p. 6). Teria havido uma reação que advogava o estreitamento do leque temático dos estudos estratégicos sob argumento de que a ampliação progressiva deste enfraqueceria a coerência intelectual do campo.

Para os autores, então, a grande questão seria como se dão os arranjos de políticas do Estado a fim de estabelecer sua segurança. Adaptando modelo de Stephanie Neuman (1984), os autores desenharam a seguinte figura:

Figura 11 – Modelo Teia-de-Aranha



Fonte: Rudzit e Nogami (2010)

Portanto, para os autores, a política de defesa seria a "articulação entre os objetivos colocados pelo mais alto órgão político e os meios militares", (RUDZIT; NOGAMI, 2010, p. 13). A política de segurança nacional articularia os interesses nacionais em sentido amplo, bem como o método para a coordenação entre objetivos e meios de proteção dos interesses. Assim, "quanto mais alto o nível político, maior participação civil e menor o militar, chegando a inverter quando chega no nível tático", (RUDZIT; NOGAMI, 2010, p. 21).

Isto posto, outra tarefa preliminar a ser cumprida antes de entrar no assunto propriamente dito é delinear a organização da arquitetura de segurança cibernética no Brasil. Vale adiantar que esta se preocupa principalmente com segurança da informação e proteção a infraestruturas críticas, e não se ocupa de ameaças híbridas - uma negligência, portanto. Para esse fim, o trabalho de Diniz, Muggah e Glenny (2014) é providencial. Os autores argumentam que, embora o crime organizado seja uma das maiores ameaças ao espaço cibernético brasileiro, os recursos estão direcionados às soluções militares, mais adequadas a casos excepcionalíssimos de conflito armado. Não se enfatizaria tanto capacidades policiais,

como as da Polícia Federal, para identificar crimes cibernéticos em geral e responder a eles. Pouco se discute os atores responsáveis pelas ameaças cibernéticas, *modus operandi* e motivações. Não se distingue os diferentes tipos de ameaças cibernéticas. A ausência, continuam Diniz, Muggah e Glenny, de posição governamental unificada sobre o assunto – o texto, registre-se, é de 2014 e, portanto, anterior à edição da Estratégia Nacional de Segurança Cibernética – e de dados confiáveis a respeito de crimes cibernéticos fez com que a abordagem brasileira sobre o assunto fosse desequilibrada.

> *At a minimum, policy makers require a better understanding of the strategies, tactics and resources of hackers and cyber-crime groups, the ways in which traditional crime is migrating online and the implications of new surveillance technologies. The government should also encourage a broad debate with a clear communications strategy about the requirements of cyber-security and what forms this might take. More critical reflection on the form and content of measured and efficient strategies to engage cyber threats is also needed. Improved coordination between state police forces to better anticipate and respond to cyber-crime is essential. If Brazil is to build a robust and effective cyber-security strategy, an informed debate must begin immediately*. (DINIZ; MUGGAH; GLENNY, 2014, p. 1)

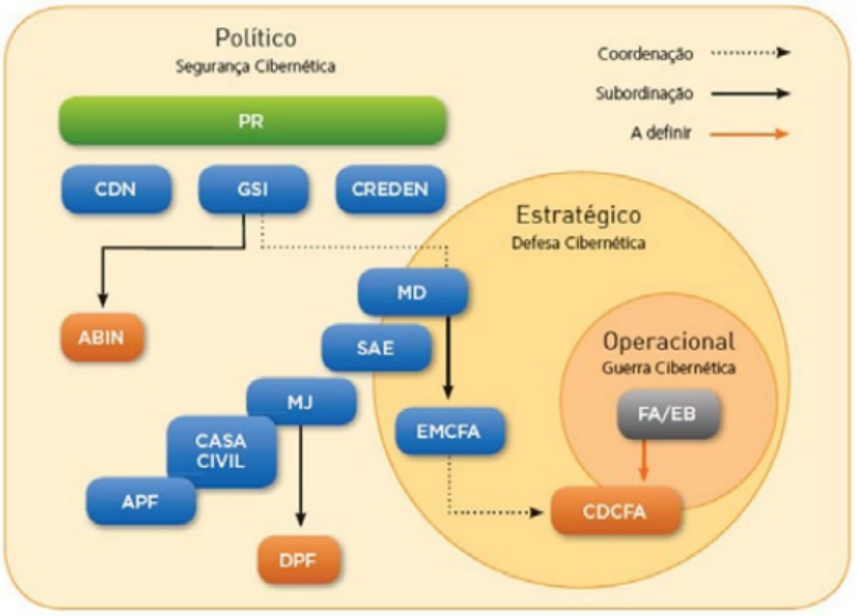
Apesar desses pontos nebulosos, prosseguem, o governo brasileiro montou uma infraestrutura de segurança e defesa cibernéticas relativamente densa. Esta concentra-se apenas em alguns pontos das ameaças cibernéticas, em particular aquelas provenientes de atores estrangeiros. Eis o porquê dos autores atribuírem ao Comando de Defesa Cibernética do Exército (CDCiber) centralidade na postura do país no que diz respeito ao assunto. Há um descompasso entre a evolução das ameaças e o aparato brasileiro de segurança cibernética, voltado para a resposta a guerras cibernéticas e o combate ao terrorismo. Assim, dizem, é possível concluir que o governo brasileiro tem adotado abordagem securitizada para ameaças cibernéticas, em detrimento de desafios que afetem diretamente os cidadãos, como é o caso de crimes cometidos em ambientes digitais[56]. "*This not only has consequences for public policy and spending; the oversized military response also risks compromising citizens' fundamental rights owing to, among other things, pervasive surveillance and censorship*", (DINIZ; MUGGAH; GLENNY, 2014, p. 4).

[56] Diniz, Muggah e Glenny (2014, p. 9) acreditam existirem três categorias principais de crimes cibernéticos no Brasil: crime cibernético convencional, crime cibernético complexo e novas ameaças. A primeira categoria se referiria crimes de conteúdo ou de caráter econômico sob alçada das forças de segurança, como a acesso ilegal a dados sigilosos, divulgação de pornografia infantil, fraude bancária e roubo de identidade, entre outros. A segunda categoria diz respeito a crimes de espionagem comercial e ativismo *hacker* sob alçada da tríade inteligência, forças armadas e forças de segurança, como terrorismo cibernético, guerra cibernética e ataques à infraestrutura crítica. Por fim, a terceira categoria relaciona-se a violência interpessoal organizada ainda não monitorada por ator específico, como lavagem de dinheiro, evasão fiscal e uso de tecnologias de comunicação específicas para cometimento de delitos, entre outros.

Essa abordagem securitizada se coadunaria com um esforço de redefinição do papel das forças armadas brasileiras – assunto que será tratado em subseção posterior. Por um lado, dizem os autores, as forças armadas têm fortalecido o controle das fronteiras e o combate ao tráfico de drogas; por outro, têm expandido seu alcance e influência sobre o campo cibernético. Para eles, "*Brazil's government is making use not only of the country's nascent cyber-security architecture, but also of its cyber-governance expertise more broadly, to project soft power in bilateral relations and multilateral forums*", (DINIZ; MUGGAH; GLENNY, 2014, p. 4).

Múltiplos órgãos públicos estão envolvidos no gerenciamento da segurança cibernética no Brasil. O esquema elaborado pelos autores é instrumental na identificação do leque de atores relacionados ao campo.

Figura 12 - A arquitetura brasileira de segurança cibernética[57]



Fonte: Diniz, Muggah e Glenny (2014)

[57] A legenda das siglas empregadas na Figura 10 é a seguinte. **PR**: Presidência da República; **CDN**: Conselho de Defesa Nacional; **GSI**: Gabinete de Segurança Institucional; **CREDEN**: Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo; **ABIN**: Agência Brasileira de Inteligência; **MD**: Ministério da Defesa; **SAE**: Secretaria de Assuntos Estratégicos; **MJ**: Ministério da Justiça; **APF**: Administração Pública Federal; **DPF**: Departamento de Polícia Federal; **EMCFA**: Estado-Maior Conjunto das Forças Armadas; **CDCFA**: Comando de Defesa Cibernética das Forças Armadas; **FA/EB**: Forças Armadas/Exército Brasileiro.

Como se vê, é um esquema hierárquico. O Gabinete de Segurança Institucional (GSI) tem precedência sobre boa parte dos órgãos civis apresentados. Subordinam-se ao GSI o Departamento de Segurança da Informação (DSIC), responsável por garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das comunicações e informações da administração pública federal em coordenação com o Ministério da Casa Civil. Também estão subordinados ao GSI a Secretaria de Assuntos Estratégicos (SAE) e a Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo (Creden). Para os autores, DSIC, SAE e Creden são importantes nos debates no país sobre segurança cibernética[58].

Também merecem destaque o Departamento de Polícia Federal (DPF), que, sob supervisão do Ministério da Justiça (MJ), tem unidades dedicadas à segurança cibernética; a Agência Brasileira de Inteligência (Abin), que tem competências para proteção das instituições públicas, atividade conduzida por intermédio do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (Cepesc); e o Ministério da Defesa (MD), que supervisiona as forças armadas e, de particular interesse para o tema, o Estado-Maior Conjunto das Forças Armadas (EMCFA).

Para Diniz, Muggah e Glenny, o esquema demonstra que o governo brasileiro tem preparado as forças armadas para liderar a proteção do Brasil no campo cibernético, conquanto o uso deste espaço seja majoritariamente civil. Não se trata de uma escolha neutra, para os autores, pois, apontam, na América Latina – que, recorde-se, viu regimes autoritários diversos ao longo do século XX –, apenas Colômbia incentivou níveis parecidos de envolvimento das forças armadas na questão cibernética. O porquê, continuam, é multifacetado.

> *For one, the armed forces are making a serious bid to expand their role as a key actor in shaping the direction of Brazilian affairs. While Brazil's democratic system continues to mature, the military is also being restructured and is seeking a new role in Brazil's domestic and foreign future.* (...) *This growing influence of the armed forces in civilian affairs has yet to be subjected to much domestic scrutiny.* (...) *At least part of the reason why there has yet to be much debate on the role of the Brazilian armed forces in cyber-security is that much of their activities are shrouded in secrecy. There is no public record or information detailing when the army first*

[58] Em novembro de 2020 e, portanto, posteriormente à publicação do artigo de Diniz, Muggah e Glenny, o Sistema Militar de Defesa Cibernética (SMDC) entrou em vigor. Seu órgão central é o Comando de Defesa Cibernética (ComDCiber). É integrado por oficiais das três forças e é responsável por ações que visem a proteção do país contra ataques cibernéticos. Há previsão, ainda, de que se engaje em cooperação interagências, particularmente no que diz respeito à proteção de infraestruturas críticas. Para mais informações, ver Brasil (2020d).

> *started developing its operational capacities in cyberspace. It was not until 2008 that the cyber field was officially incorporated into military doctrine. That year, cyber was designated one of the three main pillars for a renovated military, along with aerospace and nuclear power. Since then, the Ministry of Defense has invested significant resources in the area.* (...) *The Ministry of Defense named the Army as the lead in developing cyber defense capabilities (the Navy is responsible for nuclear, while the Air Force has aerospace under its purview)*. (DINIZ; MUGGAH; GLENNY, 2014, p. 24)

Para os autores, é problemático que às forças armadas tenha sido dado o controle de aparato com prerrogativas de supervisão inclusive de assuntos civis, o Comando de Defesa Cibernética (CDCiber), que se coordena com o Ministério da Defesa e que, por sua vez, segue diretrizes do GSI nesse campo. A estratégia inclui atividades cibernéticas de inteligência; ciência e tecnologia; capacidades operacionais; doutrina e recursos humanos. Estão à disposição do CDCiber um simulador de guerra cibernética e um laboratório de análise de códigos maliciosos.

Os autores identificam quatro riscos principais acarretados por essa abordagem. Em primeiro lugar, a arquitetura cibernética brasileira delega competências claras a seus principais atores em um domínio que é difuso. Aqui os autores referem-se especificamente à ainda difícil questão da atribuição, o que poderia levar o Exército, por exemplo, a se envolver em situações nas quais não teria atribuições legais e operacionais claras. Esse ponto explicitaria, ademais, a importância da cooperação entre os órgãos envolvidos na arquitetura brasileira.

Em segundo lugar, o discurso dos órgãos supracitados é enviesado, dizem Diniz, Muggah e Glenny. "*Many military actors refer to "ungoverned spaces" and the "Wild West" when describing cyberspace. These terms are typically accompanied by assertions of the need to conquer and control this space*", (DINIZ; MUGGAH; GLENNY, 2014, p. 26). Isso, como se viu em capítulos anteriores, é problemático pela caracterização equivocada do caráter real dos incidentes cibernéticos, bem como de seus possíveis efeitos. Para os autores, dada a história recente do país com o autoritarismo, esse discurso é inquietante precisamente pela real chance de que, em breve, militares tenham acesso a dados privados de civis. Isso coloca em xeque questões de privacidade e de controle democrático das forças armadas.

Em terceiro lugar, para os autores, essas iniciativas brasileiras têm sido implementadas antes do desenho claro e unificado de uma estratégia – relembramos aqui a data em que o texto foi publicado. E em quarto e último lugar, recursos escassos são desviados de prioridades e gastos de maneira inadequada, pois, dizem, "*Although the primary*

threats to Brazil's cyberspace are arguably related to economic crime and should result in corresponding increases in resources allocated to police entities, the armed forces are receiving the bulk of support", (DINIZ; MUGGAH; GLENNY, 2014, p. 26).

E a dimensão diplomática nesse cenário? Para o trio de autores, as movimentações brasileiras têm sido promissoras. Eles citam a realização da conferência NetMundial em São Paulo, em 2014, em parceria com a Alemanha e a *Internet Corporation for Assigned Names and Numbers* (ICANN), assim como a proposta brasileira no evento de criação de um Marco Civil global para a internet, cuja governança *multistakeholder* deveria ser aprofundada. Destaque também é dado à atuação regional do país por intermédio da Organização dos Estados Americanos (OAS), em particular os esforços de coordenação do combate a crimes cibernéticos e a adoção por parte do Brasil das diretrizes da OAS contidas no *Comprehensive Inter-American Strategy to Combat Threats to Cyber-Security*, documento adotado pela Assembleia Geral da organização em 2004. No âmbito da União de Nações Sul-Americanas (Unasul), o Brasil fomentou esforços de coordenação entre ministros de Defesa, da Justiça e do Interior. Ainda não está claro se essa verve se manterá no Fórum para o Progresso e Desenvolvimento da América do Sul (Prosul).

É necessário atualizar as informações trazidas por Diniz, Muggah e Glenny sobre a atuação diplomática brasileira na seara cibernética. Com efeito, ainda que o Brasil tenha tido um período de relevante atividade diplomática na esteira das revelações de 2013 sobre a espionagem empreendida pela *National Security Agency* (NSA) dos Estados Unidos[59], algumas delas, aliás, em parceria com a Alemanha, não parece que esse ímpeto se manteve ao longo do tempo. Sim, é verdade que o tópico levantado à época era a privacidade em meios digitais. Mas, após 2014, foram poucas as iniciativas com temática relacionada a esse âmbito (BRASIL, 2015, 2017), de maneira que as ações de 2013 e 2014 (BRASIL, 2013a, 2013b, 2014), inclusive as mencionadas pelos autores, eram reações às revelações sobre os métodos da NSA, e não necessariamente os primeiros passos de uma estratégia coerente de política externa sobre tema de crescente relevância[6061]. Declarações de encontros multilaterais, como a

[59] Para resumo sobre o caso, ver Reuters (2013).

[60] Em abril de 2021, o Ministro Conselheiro Eugenio Vargas Garcia foi indicado pelo governo brasileiro como um dos especialistas a participar das negociações intergovernamentais no âmbito da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (Unesco) sobre a ética da inteligência artificial. Informações sobre a iniciativa podem ser encontradas em Unesco (2021). Ressalte-se, portanto, que se tem dado atenção à questão da inteligência artificial, tanto no Ministério das Relações Exteriores quanto em outros órgãos do governo brasileiro.

[61] Em abril de 2021, quando este trabalho estava em processo de finalização, o Brasil lançou a Estratégia Brasileira de Inteligência Artificial. Como mencionado na nota acima, o governo tem investido energia no tema. A Estratégia é um documento extenso e interessante cujo ponto central é o conceito de eixos: três

Declaração de Osaka dos Líderes do G20, por exemplo, de 2019, ou a Declaração de Xiamen, de 2017, mencionam pontualmente a construção de sociedades digitais, mas segurança cibernética não é considerada nesses documentos.

Em termos de instrumentos vinculantes, não há muitos exemplos de acordos ou memorandos que versem sobre segurança ou mesmo cooperação cibernética. Dos 11.935 atos firmados pelo Brasil desde 1822 (BRASIL, 2021b), cerca de 13 têm alguma relação com o tema, a maioria de maneira incidental no âmbito de assistência jurídica mútua – sobre crimes cibernéticos, portanto – ou de cooperação em telecomunicações, ciência e economia digital. O único instrumento que trata especificamente de segurança cibernética foi firmado com o Suriname em novembro de 2020, e tem por objetivo estabelecer diretrizes para execução de projeto de criação de centro de resposta a incidentes cibernéticos naquele país.

Em consultas ao Gabinete de Segurança Institucional (GSI), ao Ministério da Justiça e Segurança Pública, ao Ministério das Relações Exteriores, ao Ministério da Defesa, ao Comando do Exército e ao Comando da Marinha, com base na Lei nº 12.527 (BRASIL, 2011), a Lei de Acesso à Informação, perguntou-se se existiam grupos de trabalho interministeriais, ou agrupamentos equivalentes, sobre segurança ou defesa cibernética nos quais cada órgãos estivesse envolvido. Caso existissem, questionou-se também a frequência de encontro, o nível hierárquico dos participantes e o escopo de trabalho do grupo.

O GSI, por exemplo, participa apenas do Comitê Gestor de Segurança da Informação, instituído em 26 de dezembro de 2018. Este reúne-se em caráter ordinário semestralmente, podendo ser convocado a qualquer momento pelo coordenador, o próprio GSI. O escopo do trabalho é assessorar o Gabinete em atividades relacionadas à segurança da informação. Além do GSI, da Controladoria-Geral da União (CGU), da Secretaria-Geral da Presidência da República, da Secretaria de Governo da Presidência da República, da Advocacia-Geral da União (AGU) e do Banco Central (Bacen), estão envolvidos os Ministérios da Casa Civil; da Justiça e da Segurança Pública; da Defesa; das Relações Exteriores; da Economia; da Infraestrutura, da Agricultura, Pecuária e Abastecimento; da

---

horizontais, que atravessam os seis verticais. Os eixos horizontais são legislação, regulação e uso ético; governança de inteligência artificial; aspectos internacionais. Os verticais, por sua vez, são educação; força de trabalho e capacitação; pesquisa, desenvolvimento, investimento e empreendedorismo; aplicação nos setores produtivos; aplicação no poder público; e segurança pública. Trata-se de plano bem estruturado que já conta com iniciativas de aplicação no âmbito do Ministério da Ciência, Tecnologia e Inovações e da Embrapii. Há ainda previsão de que o Ministério, em parceria com a Fapesp e o Comitê Gestor da Internet no Brasil, crie oito centros de pesquisa aplicada em inteligência artificial. Há, ainda, o programa IA² MCTI, que tem por fim fomentar projetos de pesquisa e desenvolvimento focados em soluções de inteligência artificial.

Educação; da Cidadania; da Saúde; de Minas e Energia; da Ciência, Tecnologia, Inovações e Comunicações; do Meio Ambiente; do Turismo; do Desenvolvimento Regional; e da Mulher, Família e Direitos Humanos. Representam seus respectivos órgãos nesse Comitê ocupantes de cargo em comissão.

Não há grupos interministeriais sobre defesa cibernética. Além do Comitê Gestor, o Ministério da Defesa participa também do Comitê Gestor da Internet no Brasil (CGI.br). Há, no entanto, um Grupo de Trabalho Interforças (GTI) para o setor cibernético, cujos encontros acontecem no Comando de Defesa Cibernética (ComDCiber). A lista de participantes não é divulgada por questões de segurança, de maneira que não se sabe o nível hierárquico dos participantes. De acordo com o Comando da Marinha, participam oficiais de diversas patentes.

4.1 As políticas, as Estratégias, as leis e os regulamentos

Na Constituição Federal da República Federativa do Brasil de 1988 (BRASIL, 1988), tem-se alguns dispositivos de interesse para a temática. Neles, colocam-se basicamente princípios norteadores. Destaque-se os artigos 1º, 4º, 21 (incisos I a VI; XVIII; XXVIII), e 136 que, em resumo, versam sobre princípios norteadores da República, das Relações Internacionais do país, e das condições para declaração de estado de defesa e de sítio.

Outro instrumento relevante é o documento unificado do Plano Nacional de Defesa e da Estratégia Nacional de Defesa (BRASIL, 2012), onde se diz que

> 2.1.1. Coordenada pelo Ministério da Defesa, a PND articula-se com as demais políticas nacionais, com o propósito de integrar os esforços do Estado brasileiro para consolidar o seu Poder Nacional, compreendido como a capacidade que tem a Nação para alcançar e manter os objetivos nacionais, o qual se manifesta em cinco expressões: a política, a econômica, a psicossocial, a militar e a científico-tecnológica. (BRASIL, 2012, p. 11)

A visão que é expressa de Segurança – compreendida como condição – e Defesa – conjunto de medidas do Estado, sobretudo de caráter militar –, portanto, baseia-se na defesa da tríade território, soberania e interesses nacionais. Menciona-se também a garantia ao cidadão do exercício de prerrogativas e de deveres sacramentados na Constituição Federal de 1988 (BRASIL, 1988). O desenvolvimento brasileiro, entendido em sentido amplo, também é apontado como fundamental, pois "contribui para o aproveitamento e a manutenção das

potencialidades nacionais e para o aprimoramento de todos os recursos de que dispõe o Estado brasileiro", (BRASIL, 2012, p. 11).

Assim, o Plano e a Estratégia se propõem a, sob batuta do Ministério da Defesa, serem implementados de maneira integrada com as iniciativas de outros braços do Estado, tendo em mente as prescrições constitucionais que orientam a condução das relações do Brasil no campo internacional – destaque é dado à predileção brasileira por "um mundo cuja governança se baseie em valores, instituições e normas internacionais", (BRASIL, 2012, p. 13). Vale ressaltar que prioridade é concedida ao que se chama de entorno estratégico brasileiro, conceito que abarca a América do Sul, o Atlântico Sul, a Antártica e a costa ocidental da África, com menção especial à Comunidade dos Países de Língua Portuguesa (CPLP).

A segurança e a defesa cibernéticas são mencionadas expressamente, ainda que de maneira breve. Diz-se que são "essenciais para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações de interesse nacional", (BRASIL, 2012, p. 16). O ataque a sistemas de comunicações também é mencionado na página seguinte, com especial preocupação em relação ao possível bloqueio de informações de interesse nacional, o que poderia "paralisar atividades vitais para o funcionamento das instituições do País", (BRASIL, 2012, p. 18). Outra preocupação expressa é a desigualdade tecnológica entre países. A avaliação do Plano e da Estratégia é que "as tecnologias disruptivas acentuarão as assimetrias na área da Defesa, influenciando o equilíbrio de poder regional e mundial e subvertendo tradicionais conceitos e lógicas de geopolítica", (BRASIL, 2012, p. 20). Eis o porquê de o investimento em inovação ser crucial, argumenta-se no documento. Cumpre notar que o maior envolvimento da sociedade brasileira no campo da defesa nacional é um dos objetivos delineados, pois "trata-se de aumentar a percepção de toda a sociedade brasileira sobre a importância dos assuntos relacionados à defesa do País, incrementando-se a participação dos cidadãos nas discussões afetas ao tema e culminando com a geração de uma sólida cultura de Defesa", (BRASIL, 2012, p. 25). É um ponto levantado novamente algumas páginas à frente, quando se volta a falar em interação – é este o termo empregado – com a sociedade brasileira e articulação com a Administração Pública Federal.

Logo adiante, na parte do documento dedicada à Estratégia Nacional de Defesa propriamente dita, ao se discorrer sobre o quão vital é que o país disponha de formas de vigiar, controlar e defender, menciona-se, além do território, das águas jurisdicionais

brasileiras e do espaço aéreo, a necessidade de conservar seguras as linhas de comunicação marítimas e as de navegação aérea, em particular no Atlântico Sul. Nesse sentido,

> Os setores governamental e industrial e o meio acadêmico, voltados para a ciência, tecnologia e inovação - CT&I, devem ser priorizados e integrados de modo a contribuir para assegurar que o atendimento às necessidades de produtos de defesa seja apoiado em tecnologias críticas sob domínio nacional. (BRASIL, 2012, p. 35)

De maneira complementar, a mobilização e o desenvolvimento tecnológico de defesa e a gestão da informação são consideradas parte da Capacidade Nacional de Defesa, em conjunto com a proteção, a pronta-resposta, a dissuasão, a coordenação e controle, a logística e a mobilidade estratégica e mobilização.

Adicionalmente, o incremento do número de especialistas civis em defesa é objetivo delineado no documento. Preconiza-se o aumento do

> (…) envolvimento da sociedade brasileira nos assuntos dessa área, por meio de aulas, palestras, seminários, cursos e atividades correlatas, além de trabalhos de forma conjunta em projetos de desenvolvimento e de interesse do setor de defesa, como também na criação de uma carreira de especialistas nessa área. (BRASIL, 2012, p. 43)

Além disso, o setor cibernético é considerado, junto com o nuclear e o espacial, estratégico para a defesa nacional, que "transcendem à divisão entre desenvolvimento e defesa e entre o civil e o militar. Importa, nesse contexto, a capacitação do País como um todo, bem como conferir ao Poder Nacional condições de adaptar-se às circunstâncias (...)", (BRASIL, 2012, p. 59), ideia também mencionada no Livro Branco de Defesa Nacional (BRASIL, 2020b). A Estratégia coloca, no campo da defesa, o setor nuclear sob responsabilidade da Marinha; o cibernético do Exército e o Espacial da Força Aérea. O desenvolvimento dos setores estratégicos de defesa, aliás, é uma das estratégias de defesa para o "Fortalecimento do Poder Nacional".

No setor cibernético, continua o documento, o foco são as infraestruturas críticas. Entende-se que se deve aprimorar, no âmbito do Estado brasileiro, a segurança da informação e das comunicações e também a segurança cibernética. Pesquisa, defesa e inovação também são mencionadas como áreas que devem ser incentivadas, "com foco nas tecnologias que permitam o planejamento e a execução das atividades Cibernéticas no âmbito do Setor de Defesa e que contribuam com a Segurança Cibernética no âmbito nacional, envolvendo a comunidade acadêmica doméstica e internacional", (BRASIL, 2012, p. 61). Fala-se em

fortalecimento da colaboração entre as forças armadas de outros países, o que se chama de setor de defesa brasileiro, a comunidade acadêmica nacional, a iniciativa privada, o setor público e a base industrial de defesa.

Por sua vez, a Estratégia Nacional de Segurança Cibernética (BRASIL, 2020a), também conhecida como E-ciber, está preocupada em grande medida com a segurança da informação. Derivada da Política Nacional de Segurança da Informação (BRASIL, 2018), a E-ciber entende que as ameaças cibernéticas surgem na mesma proporção e intensidade com que o espaço cibernético é utilizado, o que colocaria em risco a administração pública e a sociedade, pois

> (…) proteger o espaço cibernético requer visão atenta e liderança para gerenciar mudanças contínuas, políticas, tecnológicas, educacionais, legais e internacionais. Nesse sentido, o Governo, a indústria, a academia e a sociedade em geral devem incentivar a inovação tecnológica e a adoção de tecnologias de ponta, e manter constante atenção à segurança nacional, à economia e à livre expressão. (BRASIL, 2020a, p. 2)

Admite-se na E-ciber que as iniciativas gerenciais sobre segurança cibernética são fragmentadas e pontuais; que não há alinhamento normativo, estratégico e operacional; e que há "diferentes níveis de maturidade da sociedade em segurança cibernética, o que resulta em percepções variadas sobre a real importância do tema", (BRASIL, 2020a, p. 2).

O documento está organizado em dois eixos, a saber: eixos de proteção e segurança e eixos transformadores. Cada um desses subdivide-se em itens. Estão atrelados ao primeiro eixo os seguintes pontos: governança da segurança cibernética nacional; universo conectado e seguro: proteção e mitigação de ameaças cibernéticas; e proteção estratégica. Ao segundo eixo, conectam-se seguintes os pontos: dimensão normativa; dimensão internacional e parcerias estratégicas; pesquisa, desenvolvimento e inovação; e educação.

Com o fito de que o Brasil se torne país de excelência em segurança cibernética, tem-se os objetivos de tornar o Brasil mais próspero e confiável no ambiente digital; aumentar a resiliência brasileira às ameaças cibernéticas[62]; e fortalecer a atuação brasileira em segurança cibernética no cenário internacional.

Estabeleceram-se, ainda, dez ações estratégicas para que esses objetivos sejam alcançados. São elas fortalecer as ações de governança cibernética; estabelecer um modelo

[62] Amado (2021) informou, em matéria para a revista Época, que a ocorrência de ameaças cibernéticas no país quintuplicou durante a pandemia.

centralização de governança no âmbito nacional; promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade; elevar o nível de proteção do Governo; elevar o nível de proteção das infraestruturas críticas nacionais; aprimorar o arcabouço legal sobre segurança cibernética; incentivar a concepção de soluções inovadoras em segurança cibernética; ampliar a cooperação internacional do Brasil em segurança cibernética; ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade – fala-se, entre outras medidas, em criar grupos de trabalho e fóruns sobre segurança cibernética e incentivar iniciativas de Pesquisa, Desenvolvimento e Inovação (PD&I) em segurança cibernética; e elevar o nível de maturidade da sociedade em segurança cibernética. Cada uma dessas ações se desdobra em outras medidas.

É enfatizada no documento a importância de que o Brasil disponha de "indústria de segurança cibernética inovadora, apoiada por pesquisas e por produções científicas de alto nível, capaz de reter talentos que possam contribuir com a indústria nacional e realimentar o ciclo de produção do conhecimento. Verifica-se uma dissonância entre os projetos conduzidos pelas universidades públicas e privadas e as necessidades em soluções de segurança cibernética por parte do setor produtivo", (BRASIL, 2020a, p. 22). Nesse ponto é que se menciona o papel estratégico do Ministério da Educação na implementação de programas que incentivem o desenvolvimento de capacidades em segurança cibernética não apenas nas universidades, mas também na educação básica. O conceito de *digital literacy*, ou alfabetização digital, é destacado. Para a E-ciber, a segurança cibernética passa necessariamente por três conceitos: capacitação de profissionais que atuem em áreas relacionadas; formação dos segmentos da sociedade que ainda estejam em período escolar; e conscientização da sociedade como um todo, pois a "efetividade do desenvolvimento de uma cultura de segurança cibernética por intermédio da conscientização, formação e capacitação depende de uma gestão de conhecimento bem estruturada, a fim de dar continuidade a todos os processos envolvidos, formar profissionais no estado-da-arte e em função da dinâmica do surgimento e da obsolescência das competências de segurança cibernética", (BRASIL, 2020a, p. 28).

Além disso, também se enfatiza a "necessidade urgente de cooperação entre os países para mitigar ameaças", (BRASIL, 2020a, p. 24). Em específico, entende-se ser de competência do GSI, em articulação com o Ministério das Relações Exteriores (MRE) a negociação de atos internacionais relacionados ao tratamento da informação classificada. Em relação às outras ações de caráter internacional, não se designa um órgão específico.

Demonstra-se na E-ciber preocupação em criar instrumentos normativos específicos para a realidade brasileira. Menciona-se a Política de Governança Digital (BRASIL, 2016), a Estratégia Brasileira para a Transformação Digital (BRASIL, 2018) e a Governança no Compartilhamento de Dados (BRASIL, 2019) como indicativos da digitalização do governo federal.

Embora não seja mencionado pela E-ciber, o Marco Civil da Internet (BRASIL, 2014) também deve ser considerado uma evolução legal importante, particularmente no que diz respeito ao artigo 3º – que estabelece os princípios que regem a disciplina do uso da internet no país, em particular a proteção da privacidade e dos dados pessoais, além da preservação e garantia da neutralidade de rede – e ao artigo 7º – que considera o acesso à internet fundamental para o exercício da cidadania. É importante também a Lei Geral de Proteção de Dados (BRASIL, 2018), por disciplinar o tratamento de dados pessoais em meios digitais ou não.

É de interesse notar que a E-ciber torna clara a preferência do governo federal por um modelo centralizado de gestão em segurança cibernética. Justifica-se a preferência com base no relatório da Comissão Parlamentar de Inquérito da Espionagem, ocorrida em 2014, segundo o qual "a distribuição e o trato dos assuntos relacionados à segurança cibernética no País, não tem colaborado para que o Governo possua uma visão geral do assunto, o que dificulta a execução de ações mais eficazes nesse campo", (BRASIL, 2020a, p. 13). Eis o motivo de se justificar a criação de um sistema único que agregue atores estatais e não estatais envolvidos com segurança cibernética, com o fim de se alinhar estratégica, doutrinária e operacionalmente. Entende-se que é responsabilidade do governo federal a discussão de opções para o robustecimento institucional da segurança cibernética brasileira, com destaque para o Gabinete de Segurança Institucional (GSI), pois

> (…) não se vislumbra a necessidade da criação de novos e dispendiosos organismos governamentais, sendo suficiente redimensionar a atual estrutura do Gabinete de Segurança Institucional da Presidência da República, de forma a lhe possibilitar a atuação em âmbito nacional. Portanto, urge a necessidade de uma lei que regule as ações de segurança cibernética, que especifique atribuições, que aponte mecanismos de diálogo com a sociedade e que torne possível, ao Gabinete de Segurança Institucional da Presidência da República, com a participação de representantes de todos os entes nacionais, exercer o papel de macro coordenador estratégico, ao proporcionar alinhamento às ações de segurança cibernética e ao contribuir para a evolução de todo o País nesse campo, de forma convergente e estruturada. Conclui-se, ainda, ser necessário e urgente que o Governo federal priorize a aplicação de recursos na área da segurança cibernética. (BRASIL, 2020a, p. 14).

4.1.1 O que dizem as autoridades sobre o assunto?

Com o objetivo de entender o que autoridades atuantes em Defesa, Relações Exteriores e Segurança pensavam sobre os desafios cibernéticos enfrentados pelo Brasil, elaborou-se questionário na ferramenta *Google Forms* com 11 perguntas a serem feitas àqueles diretamente responsáveis por departamentos dedicados ao trato de questões cibernéticas. Tratou-se, portanto, de número reduzido de entrevistados: quatro ao todo. Assim, o fim deste exercício não foi elaborar um mapa das opiniões das autoridades do governo brasileiro em geral, mas saber o que pensam os que ocupavam cargos de liderança nessa seara.

O questionário foi enviado por e-mail para as autoridades selecionadas em 2020. As respostas foram depositadas diretamente no formulário. Foi oferecido anonimato a todos, com o objetivo de que se sentissem à vontade para responder às perguntas. A expectativa era coletar suas impressões sobre os desafios cibernéticos enfrentados pelo país e, assim, entender o direcionamento que Ministério das Relações Exteriores (MRE), Ministério da Defesa (MD) e Gabinete de Segurança Institucional (GSI)[63] davam ao tema. Trocando em miúdos, trata-se de um termômetro.

De maneira geral, o que se viu nas respostas foi relativa satisfação com a estratégia brasileira de segurança e defesa cibernética, tanto em termos de preparação para se lidar com ameaças quanto de prioridade dado ao assunto. Houve algum reconhecimento da necessidade de se envolver a iniciativa privada e a sociedade civil no assunto. Em resumo, ainda que se reconheça que alguns ajustes devem ser feitos, a avaliação geral é de que o Brasil está no caminho certo.

Foram usadas tanto perguntas de resposta aberta quanto de classificação numérica em intervalo de 0 a 5[64]. Em ordem crescente, os enunciados e as respostas mais interessantes foram os seguintes:

- Como o (a) senhor (a) vê a questão cibernética em sua área de atuação? Quais os principais desafios colocados?

[63] Ressalte-se que foi tentado contato com a autoridade correspondente na Agência Brasileira de Inteligência (Abin), mas não houve interesse em participar da pesquisa.
[64] Será colocada em anexo a este trabalho captura de tela do questionário e das respostas em sua totalidade.

- *Em minha área de atuação, os principais desafios são dar efetividade ao previsto nos diversos normativos de Segurança Cibernética (face à sua transversalidade), mantê-los atualizados (face à dinamicidade do setor) e antecipar-se à elaboração de normativos que contemplem a rápida evolução tecnológica*.
- *Existe dificuldade na aquisição de inovações tecnológicas e há grande dependência dos EUA, em todo o Mundo Ocidental.*

- Em uma escala de 0 a 5, em que 0 significa "nenhuma prioridade" e 5 significa "prioridade máxima", qual a importância dos desafios de defesa cibernética para o Brasil?
  - Três entrevistados selecionaram a opção 5 e um a opção 4.
- Em uma escala de 0 a 5, em que 0 significa "não preparado" e 5 significa "adequadamente preparado", o Brasil tem o instrumental para lidar de maneira adequada com ameaças de caráter cibernético do ponto de vista legal e técnico?
  - Metade dos entrevistados escolheu a opção 3 e a outra metade a opção 4.
- Para o (a) senhor (a), quais seriam os principais entraves institucionais brasileiros no trato da questão cibernética?
  - *A falta de uma adequada gestão do conhecimento de segurança e defesa cibernética em nível nacional. Isso iria requerer uma plataforma integradora para informar onde estão os talentos; um mapeamento da demanda e oferta de competências na área, de oportunidades de trabalho e de capacitação disponíveis; benchmarking e indicadores de desempenho de pessoas, de cursos, de empregadores; dentre outros, tudo em uma mesma ontologia.*
  - *Não vejo entraves institucionais. Há diversos ministérios e órgãos governamentais com competência na matéria, e que se coordenam no marco de reuniões interministeriais e na elaboração de instrumentos normativos.*
- Em sua opinião, quais setores do governo têm ou deveriam ter primazia sobre o trato de ameaças de caráter cibernético?
  - *A principal característica da cibernética é sua transversalidade. Portanto, o governo como um todo deve tratar do assunto. O GSI-PR como um assunto de segurança nacional, o Ministério das Relações Exteriores nas questões internacionais, o da Educação na capacitação, o da Ciência, Tecnologia,*

Inovações e Comunicações na inovação tecnológica, o da Economia na alocação de recursos, apenas para citar alguns exemplos.

- *Visualizo em linhas gerais três órgãos no âmbito do governo. O GSI, por intermédio do CTIR Gov, já possui um papel de coordenação nas atividades referentes a prevenção, tratamento e resposta a incidentes cibernéticos (ressalta-se que cada órgão da APF é encarregado de prover sua própria segurança e realizar tratamento de incidentes consoante os normativos exarados pelo GSI). A Polícia Federal, por intermédio do seu Serviço de Repressão a Crimes Cibernéticos (SRCC) é o órgão central para crimes cibernéticos. No contexto da Defesa Cibernética, o Comando de Defesa Cibernética (ComDCiber) é o órgão central do MD.*

- Em uma escala de 0 a 5, em que 0 significa "insuficiente" e 5 significa "ideal", o (a) senhor (a) vê como suficiente o arcabouço legal atinente à questão cibernética?
  - Três entrevistados selecionaram a opção 4, e um a 2.
- Como o (a) senhor (a) avalia o desenho preliminar da Estratégia Nacional de Segurança Cibernética?
  - *Eficiente, mas teórico. Para pôr em prática as ações ideais, é necessário investimento.*
  - *A E-Ciber já sinalizou o direcionamento da Seg Ciber no Brasil ao descrever as ações estratégicas a serem adotadas. Tais ações espelham os anseios nacionais (pois foi fruto de diversas reuniões entre órgãos governamentais, do setor privado e da academia, além de ter sido posta à consulta pública) e, no cenário internacional, encontram-se alinhadas com estratégias de diversos outros países. Apesar de sua recente publicação, há uma percepção que já reverberou positivamente em diversos setores da sociedade brasileira e da comunidade internacional.*
- Em sua opinião, qual a posição do Brasil nas discussões sobre defesa cibernética no plano internacional?
  - *Em defesa da regulamentação internacional por meio de um instrumento vinculante.*
  - *Posso responder as questões de Segurança Cibernética. Sobre esse questionamento de Defesa Cibernética, seria mais apropriado verificar com alguém do setor. Mas minha percepção é que avançamos a largos passos nas*

diversas áreas e nos programas que contemplam a Defesa Cibernética. Prova disso é o desempenho das equipes brasileiras nas "cyber olimpíadas" e eventos congêneres, a maturidade do Exercício Guardião Cibernético (envolvendo ComDCiber, GSI e órgãos públicos e privados) e a projeção que o Brasil tem no cenário internacional nessa área.

- Em uma escala de 0 a 5, em que 0 significa "nenhuma relevância" e 5 significa "relevância máxima", o (a) senhor (a) acredita que a inciativa privada deve desempenhar algum papel no âmbito cibernético?
  - Três entrevistados escolheram a opção 5, e um a opção 4.
- Ainda em relação à participação da iniciativa privada no âmbito cibernético, caso avalie que este deva desempenhar algum papel no âmbito cibernético, o (a) senhor (a) destacaria algum setor específico?
  - *A iniciativa privada é um dos principais atores (ao lado do governo e da academia) e pode prover cursos, soluções de segurança, eventos, desenvolver startups em prol da inovação, dentre outros.*
  - *Inovação, capacitação e proteção de infraestruturas.*
- Em uma escala de 0 a 5, em que 0 significa "nenhuma relevância" e 5 significa "relevância máxima", o (a) senhor (a) acredita que a sociedade civil deve desempenhar algum papel no âmbito cibernético?
  - Todos os entrevistados escolheram a opção 5.

Ao fim do questionário, foi dado ainda espaço para que o (a) entrevistado (a) colocasse considerações adicionais que julgasse pertinentes, oportunidade na qual apenas dois entrevistados apresentaram breves comentários. Alguns pontos das respostas acima merecem destaque. Na primeira pergunta, é interessante notar dois pontos das respostas selecionadas: dificuldade de aquisição de tecnologias e de implementação e atualização das prescrições normativas de segurança cibernética – essencialmente, pelo amplo escopo da questão e pela velocidade com que desenvolvimentos acontecem. É coerente, portanto, com a elevada classificação dada à prioridade que os desafios de defesa cibernética têm para o Brasil, tema da segunda pergunta, e com a classificação moderada dada na terceira pergunta à preparação técnica e legal do país para fazer frente a esses desafios.

Na quarta pergunta, salta aos olhos a disparidade entre as respostas selecionadas. Se, de um lado, uma delas demonstra satisfação com os arranjos institucionais brasileiros para questões cibernéticas, de outro é revelada alguma preocupação com a insuficiência da "gestão do conhecimento de segurança e defesa cibernética em nível nacional", especificamente na gestão de recursos humanos na área. Já nas respostas à quinta pergunta, há apoio a abordagem *whole of government*, mas também a crença de que os principais órgãos envolvidos deveriam ser o GSI, a Polícia Federal e o Ministério da Defesa.

Na questão seis, três entrevistados julgaram o arcabouço legal brasileiro para questões cibernéticas adequado, enquanto um avalia como passível de melhoras. Na questão sete, a E-ciber foi bem avaliada, ainda que tenha sido considerada, em uma das respostas, teórica. Na questão oito, a atuação internacional brasileira no campo recebeu boas avaliações. Nas questões nove e dez, a participação da iniciativa privada foi considerada importante, particularmente no que diz respeito à inovação tecnológica. Finalmente, na questão onze, houve unanimidade entre os entrevistados em relação à relevância da sociedade civil para o âmbito cibernético. O exercício foi interessante para confirmar o elevado grau de consciência das autoridades em posição de liderança sobre o tema.

4.2 HAVIA DUAS PEDRAS NO CAMINHO

4.2.1 Inflação normativa

Dado que a tendência no Brasil é gerenciar problemas de toda sorte por intermédio de vigorosa e irrefreável atividade normativa, cumpre tecer brevíssimo comentário sobre a efetividade dessa abordagem. Oliveira (2009) argumenta que flexibilizar o direito por causa de evoluções socioeconômicas pode ser contraproducente, pois "(…) tende a criar uma situação de crise dentro do ordenamento jurídico o qual não conseguiria manter imperatividade concomitante à universalidade. O resultado seria um direito efêmero e impossível de ser assimilado pelo sujeito de direitos", (OLIVEIRA, 2009, p. 21).

Expressaram preocupações similares em artigos publicados em sítios eletrônicos voltados para o meio jurídico Martorelli (2009), Clemente Junior (2018) e Maia (2009). Em comum, os autores criticam o furor legiferante e suas consequências para a efetividade das normas jurídicas brasileiras.

Não se pretende aqui adentrar os meandros dos debates jurídicos travados no Brasil sobre o tema; ao contrário, o que se busca é apenas pontuar que o recurso à produção normativa não necessariamente produz soluções eficientes e duradouras. Quando se considera questões cibernéticas em sentido amplo, e adicionando-se a dimensão do direito à privacidade[65] e à livre expressão assegurados no artigo 5º da Constituição vigente (Brasil, 1988), que podem ser facilmente violados sob pretensões legítimas de se manejar a segurança e a defesa do país[66], vê-se que há importante nuance sobre a questão. Com efeito, qualquer empreendimento normativo que se queira erigir deve ser produto de profunda reflexão sobre os efeitos colaterais que tal medida pode ter, bem como sobre a possível atenuação de sua eficácia no frutífero contexto normativo brasileiro.

4.2.2 Relações civis-militares

A verdade é que a participação das forças armadas na vida política do Brasil antecede a própria fundação do país enquanto entidade política independente, dizem Mathias e Guzzi (2010, p. 41), em referência à confrontação entre D. Pedro I e o comandante de tropa Jorge de Avilez acerca da deposição do Conde de Arcos e da nomeação do desembargador Álvares Diniz para o cargo de Ministro do Reino. A construção do Estado nacional, argumentam, deu-se em paralelo à ascensão da autonomia militar que "até hoje não se decidiu pela completa subordinação das armas aos civis, mitigando a democracia no país", (MATHIAS; GUZZI, 2010, p. 41).

Na Constituição de 1988, apontam Mathias e Guzzi, a definição do que seriam forças armadas e as funções a elas atribuídas são o produto de uma solução de compromisso entre constituintes e militares, entre outros atores. Os termos eram claros, para os autores: "os militares continuavam como guardiões dos valores nacionais e os civis poderiam continuar com seu projeto democrático", (MATHIAS; GUZZI, 2010, p. 50). Citando o ex-ministro da Defesa da Espanha Narcís Serra, eles problematizam o arranjo. A questão é que as forças armadas que se veem como guardiãs de valores permanentes representam perigo para regimes

[65] Importantes reflexões sobre a questão da privacidade na era digital e o modelo do consentimento adotado na legislação brasileira foram trazidas por Mendes e Fonseca (2020). Mendes, aliás, tem produzido um interessante arco de argumentações sobre o tema desde 2008, ao menos, quando defendeu dissertação de Mestrado sobre a proteção de dados pessoais (MENDES, 2008).

[66] Não seria a primeira vez que direitos humanos seriam flexibilizados em razão de questão urgente de segurança nacional. Sobre esse processo no contexto da guerra ao terror, ver Alto Comissário das Nações Unidas para Direitos Humanos (2008).

democráticos, uma vez que o que é permanente pode passar a ser considerado superior com relativa facilidade. Assim, enquanto guardiões desses valores, os militares converter-se-iam em essenciais para o país, na visão de Serra.

Para Mathias e Guzzi, a Constituição de 1988 transformou as forças armadas propriamente em um valor, colocando-as em posição superior, acima, inclusive, da nacionalidade. O caráter nacional das forças armadas, aliás, também é considerado delicado pelos autores, pois estas seriam a única instituição profissional que representa toda a nação.

> Ao defini-las como "nacionais e permanentes", transformaram-nas legalmente em uma entidade superior aos legítimos representantes do povo na democracia e, quiçá, em algo superior ao próprio povo. (…) a manutenção da responsabilidade das Forças Armadas sobre a ordem interna auxiliou na falta de definição das missões militares e na permanência de ênfase nas chamadas "atividades subsidiárias", justamente o que não está realmente adstrito à lida castrense e pelas quais elas, em particular o Exército, não querem responder. Parece que, neste caso, prevaleceu o receio corporativo de perder o que eles chamam de "representação da nacionalidade". (MATHIAS; GUZZI, 2010, p. 51)

De acordo com os autores, a questão foi parcialmente resolvida com a Lei Complementar nº 69, publicada em 30 de julho de 1991. Nela, estabelece-se que o emprego das forças armadas para ações de defesa da pátria, dos poderes constitucionais, da lei e da ordem, está sob autoridade do presidente da República. Mas, à luz do exemplo de democracias reestabelecidas, prosseguem Mathias e Guzzi, afastar as forças armadas de ações de segurança pública é fundamental para que se assegure sua subordinação às autoridades civis. Não é o que o governo brasileiro tem feito – vide as operações de garantia da lei e da ordem (GLO). O resultado, para os autores, foi a banalização do uso das forças armadas no país, empregadas como fiadoras da segurança interna.

De modo complementar, Costa (2015) compreende a relação civil-militar como "fluxo cooperativo dialético e dialógico de poder entre os dirigentes políticos e os dirigentes militares (ambos obedecendo às diretrizes de segurança emanadas do seio da população), tendo em vista a obtenção de (…) a segurança do Estado e/ou comunidade política", (COSTA, 2015, p. 113). Para o autor, o controle civil seria o elemento central da relação civil-militar, pois asseguraria, em tese, que as possibilidades de guerra ou até mesmo de golpe de Estado sejam atenuadas. A questão é que, prossegue, o controle civil implica relegar o Estado enquanto objeto de segurança a plano secundário. Assim, "cada vez mais, os Estados de segurança nacional desaparecem e, em seu lugar, as populações emergem com suas demandas de segurança em relação a privações diversas causadas por guerras civis, catástrofes naturais,

mudança climática, escravidão, crime organizado, entre outras tantas", (COSTA, 2015, p. 126).

Nesse contexto, requerer-se-ia da relação civil-militar propostas de segurança que fortalecessem a prestação de contas dos contingentes militares, participação da população e primado da segurança da população quando da elaboração de propostas de treinamento e profissionalização militar. Ausente o controle civil, seja por qual motivo, lega-se "às elites políticas ou militares na determinação do inimigo contra quem se quer sentir segurança, e esse inimigo pode ser, como a história demonstra, a própria população nacional", (COSTA, 2015, p. 127).

Trata-se de contextualização histórica para as relações entre civis e militares no Brasil, necessária para a compreensão dos limites e condições que devem informar a navegação desse tema. Eis o porquê de inspirar cuidados o alerta de Diniz, Muggah e Glenny (2014), particularmente à luz da baixa coordenação dentro do governo brasileiro sobre o tema, da concentração de atribuições no GSI e no Ministério da Defesa e da inexistência de mecanismos que construam pontes com a sociedade em geral sobre segurança e defesa cibernética. Ainda que a E-ciber seja adequada na ênfase em coordenação entre governo, sociedade e iniciativa privada, e em que pese o diagnóstico parcial focado em infraestrutura crítica, suas recomendações não foram implementadas – sequer parece haver movimento no sentido de que o sejam.

É preciso reforçar que, conquanto o objeto de análise aqui seja a República Federativa do Brasil, a problemática das relações entre civis e militares não se restringe ao território nacional. Com efeito, Diamint (2015) enxerga na América Latina dificuldades comuns em relação ao controle civil sobre as forças armadas. No entanto, assevera a autora, "*a democracy, it is generally agreed, cannot be considered consolidated unless its armed forces are firmly under the control of duly constituted civilian authorities*", (DIAMINT, 2015, p. 155). Isso significa que o papel das forças armadas na região segue como um quebra-cabeças para as democracias latino-americanas. Face à emergência de novas manifestações de poderio militar, Diamint coloca em questão se as ideias tradicionais sobre o que sejam as relações civis-militares sequer podem ainda ser aplicadas à América Latina. A multiplicação de regimes democráticos na região foi acompanhada, talvez de maneira contraintuitiva, por incremento do poder das forças armadas, na avaliação da autora,

principalmente enquanto fiadoras de autoridades civis eleitas[67], o que é prejudicial não apenas para a preservação dos direitos dos civis, mas também para a própria identidade institucional das forças armadas. É verdade que a pluralidade de experiências dificulta o desenvolvimento de uma teoria explicativa abrangente sobre relações entre civis e militares; mas o ponto em comum é que

> *The military is now a central ally not of democracy's losers (the predemocratic old guard), but of its winners: Soldiers are serving election victors as police officers, as praetorian guards, and even as leaders of what amounts to a political party. In this new state of things, civil-military relations are thinly institutionalized at best. Following the transition, the military was sent back to its barracks, but civilian authorities failed to focus on reforming defense ministries. Instead, it seems, civilians have opted to give the soldiers more tasks to keep them busy, not only in the field of domestic order-keeping but also in terms of social-welfare projects. This may explain why Latin America's elected officials have become so prone to misuse the armed forces for ends that are far from their professional competence*. (DIAMINT, 2015, p. 157)

Não só no campo da segurança pública as forças armadas são chamadas à ação por dirigentes civis, mas também no da política. Para Diamint, as forças armadas se tornaram uma ferramenta para neutralização da oposição a políticas públicas. Em alguns países, há também certo componente de defesa da dignidade nacional contra os desígnios imperialistas de potências ocidentais. Como exemplo desse tipo de instrumentalização dos contingentes militares, a autora menciona Bolívia, Equador e Nicarágua. Os benefícios para as forças armadas têm sido a possibilidade de assegurar seus interesses corporativos e de auferir benefícios materiais. Ao fim e ao cabo, trata-se de controle civil subjetivo, segundo o qual um grupo específico de civis instrumentaliza as forças armadas para a consecução de seus próprios objetivos. O modelo ideal, diz Diamint, citando Huntington (1957), seria o controle civil objetivo, que só seria possível em países nos quais os contingentes militares se abstivessem de maneira sistemática e principiológica do envolvimento em assuntos políticos.

Interessante cotejar as observações de Diamint com as de Medeiros Filho (2010). Na América do Sul, a explicação para a dificuldade de preeminência civil sobre as instituições militares estaria no padrão de ameaças eminentemente internas, argumenta Medeiros Filho (2010, p. 108). Citando Desch (1996), o autor acrescenta que "ameaças externas tendem a

[67] Nas palavras de Diamint: "*this is most clearly the case in the five Spanish-speaking ALBA countries—Bolivia, Cuba, Ecuador, Nicaragua, and Venezuela—where civilian elites increasingly depend on the military to keep them in power. In the region's most notorious recent use of military power for domestic political purposes, Venezuela's President Nicolás Maduro—facing massive demonstrations fueled by public anger at basic consumer-goods shortages—has not only relied on the armed forces to suppress protests, but has several times even sent troops to take over stores*", (DIAMINT, 2015, p. 156).

incentivar as elites a adotarem o controle civil objetivo. (...) sem uma missão externa clara, os militares têm menos incentivos para subordinar-se à autoridade civil", (MEDEIROS FILHO, 2010, p. 108). Assim, continua o autor, o controle civil relativamente frágil e a autonomia dos militares estão assentados sobre

> (…) fatores históricos, como os inúmeros casos de intervenção militar (ou sua simples ameaça) nos governos nacionais, por um lado, e a relativa ausência de ameaças externas, por outro lado. Como consequência, quando os governos da região tratam de "questões militares", o tema dominante é o "lugar dos militares na política", e não o "lugar dos militares na defesa", como sugeriria o modelo huntingtoniano. Dessa forma, a preocupação central dos primeiros governos civis em relação aos militares não diz respeito à "política de defesa", mas à "política militar". (…) Nesse sentido, o próprio processo de integração regional dos países do Cone Sul, incluindo os acordos iniciais do Mercosul, pode ser visto como uma estratégia das elites políticas de colocarem sob seu controle as agências militares, consideradas naquele contexto uma ameaça à estabilidade da democracia nascente. (MEDEIROS FILHO, 2010, p. 112-113)

O *bottom line*, diz o autor, é que o "controle civil desejável" em um regime democrático exigiria o reconhecimento por parte das autoridades civis de um "espaço de competência profissional e autonomia" para os militares (MEDEIROS FILHO, 2010, p. 113). Além disso, tem-se a questão da capacitação de civis em gestão de defesa, pois

> A especialização funcional desenvolve entre os militares habilidades e conhecimentos específicos (…). A ausência de uma estrutura civil com conhecimento específico e capacidade de estabelecer diretrizes de defesa acaba por permitir a manutenção de espaços de autonomia aos militares (…). Segundo alguns especialistas, o quadro apresentado sugere um processo de "desmilitarização" de setores de defesa que passa necessariamente pela inclusão de civis nas esferas de decisão e de análise das questões de defesa. Diamint apresenta uma proposta de desenvolvimento de uma comunidade civil de defesa, condição considerada necessária pela autora para o controle civil. Enquanto isso não acontece, a tendência é que, por falta de conhecimento ou por simples desinteresse, os civis continuem a delegar aos militares a tomada de decisão nos diversos setores de defesa. Ao ignorar a política de defesa, as lideranças civis cedem autoridade aos militares, permitindo-lhes a possibilidade de autogestão. (MEDEIROS FILHO, 2010, p. 115-116).

4.3 PROPOSTAS PARA O FUTURO

O objetivo dessa seção do trabalho não é fornecer um passo a passo do que deve ser feito para ajustar o ecossistema de segurança e defesa cibernética do Brasil. O que se propõe é analisar, à luz do *National Cybersecurity Framework Manual* editado por Alexander

Klimburg para o *Cyber Defence Centre of Excellence* da OTAN (KLIMBURG, 2012), quais recomendações poderiam ser úteis para o caso brasileiro.

No manual, coloca-se que a segurança do ambiente *online* de um dado país depende de uma miríade de *stakeholders*. Cada um dos usuários de um sistema de informação influencia o nível de resiliência da infraestrutura de informação nacional a ameaças cibernéticas. É por isso que estratégias de segurança cibernética que pretendam ser bem-sucedidas devem necessariamente levar em consideração todos os *stakeholders* envolvidos, a necessidade de que eles compreendam sua importância na segurança cibernética do país e os meios de que esses *stakeholders* necessitam para executar seu papel. Assim, segurança cibernética não pode ser vista como uma atividade setorial, pois requer esforço coordenado de todos. Por isso que todas as estratégias analisadas neste trabalho – inclusive a brasileira, ainda que em menor medida –, falam em colaboração. Ademais, a segurança cibernética é um desafio internacional, que requer cooperação a fim de que um nível razoável de segurança seja atingido em escala global.

Tomando-se o governo como objeto, é comum e compreensível que diversos ministérios e departamentos arvorem para si responsabilidade sobre algum aspecto da segurança cibernética nacional. Ausente estratégia coerente, torna-se difícil estabelecer ações coesas. O desafio é melhorar a coordenação entre atores governamentais, por intermédio da criação de um grupo de trabalho abrangente – mesmo que este seja subdividido em eixos temáticos – ou da melhora de processos interdepartamentais sem que se criem novos órgãos. De suma importância é a constância da coordenação, que deve ser contínua. Encontros esparsos não são suficientes para que se atinja nível ótimo de interação. Agilidade é fundamental, posto ser atributo nevrálgico da questão cibernética. Há certo precedente, ainda que a escala seja distinta do que se propõe aqui. Basta recordar os casos de cooperação por ocasião de grandes eventos, como a Copa do Mundo FIFA de 2014 e os Jogos Olímpicos de 2016, sem mencionar o exemplo recente da Operação Fronteira Sul - Ágata 21, que congregou a 5ª Divisão do Exército e órgãos de segurança estaduais e federais.

Na arena internacional, "*the emphasis must be on relationships with all the relevant actors within specific systems (in particular, but not limited to the field of 'internet governance')*", (KLIMBURG, 2012, p. 31). Isso requer que o governo escolha um ponto focal, que pode não fazer parte da estrutura governamental. Esse ator deve ter liberdade para ser flexível o suficiente para se engajar com *stakeholders* ao redor do mundo. Respostas de política externa à ambiguidade das relações no espaço cibernético também devem ser

desenvolvidas. Não é possível prescindir do envolvimento massivo e focado do Ministério das Relações Exteriores no assunto. Não parece eficiente, ademais, delegar suas funções para outros órgãos do governo – como se sugere na E-ciber que se faça para o GSI, que teria no MRE mero auxiliar. A diplomacia brasileira deve estar intimamente envolvida em todos os temas e desdobramentos da questão cibernética. Naturalmente, a maneira como isso se dá é atrelada às instruções que o próprio MRE recebe da Presidência da República a respeito de diretrizes de Política Externa. É necessário, no entanto, que se crie consciência do papel fundamental que a diplomacia tem nessa seara, como visto nas soluções encontradas por Finlândia e Dinamarca.

No plano nacional, a construção de relacionamentos entre governo, fornecedores de serviço de segurança e empresas de infraestrutura crítica em tecnologia é importante. A abordagem *Whole of Nation*, ou *Whole of Society*, encoraja uma variedade de atores não-estatais – iniciativa privada, *think tanks* e sociedade civil – a cooperar com o governo em assuntos de segurança cibernética. Ainda que haja variações no estilo de cooperação a ser adotado, algum nível de interação deverá ser encorajado. No momento, não há iniciativas nesse sentido. Em que pese a incompletude do diagnóstico sobre as ameaças cibernéticas que se enfrenta atualmente, a E-ciber advoga a importância do envolvimento da sociedade como um todo, o que foi reconhecido pelas autoridades entrevistadas, aliás. É temerário negligenciar esse ponto. O Brasil dispõe de servidores públicos de inegável competência; eles sozinhos, no entanto, não podem dar conta da questão cibernética. Tampouco tem o governo brasileiro capacidade técnica para manter-se a par das inovações tecnológicas constantes e implementá-las, quando for o caso. A expertise e o *input* da iniciativa privada são fundamentais.

Ao fim e ao cabo, é preciso que haja ampla compreensão na sociedade como um todo sobre o que é o ciberespaço e qual é a natureza das ameaças à segurança cibernética para evitar falhas. Klimburg (2012, p. 141) menciona seis problemas a serem evitados: deixar um vácuo de políticas públicas com clara visão estratégica; permitir que o compartilhamento de informação dentro do governo em particular, e com *stakeholders* em geral seja atravancado; redigir legislação obsoleta, que não responda aos desafios colocados pelo ciberespaço; enrijecer a cooperação entre órgãos do governo e entre governo e sociedade; comunicar-se de maneira ineficiente; tolerar o analfabetismo cibernético de agentes públicos, tomadores de decisão, membros do poder judiciário, políticos em geral, academia, inciativa privada e

sociedade civil; negligenciar a dimensão internacional. É preciso implementar políticas públicas voltadas para o incremento da *digital literacy* da sociedade civil brasileira. A coordenação com a academia também se faz absolutamente necessária. Aqui, cumpre mencionar as considerações de Elisabeth Braw.

Sobre *deterrence by denial*, Braw (2021), ecoando Wigell (2019) e Estados Unidos da América (2020), considera que a sociedade civil tem papel nevrálgico na defesa contra as *gray zone aggressions* presentes e futuras exatamente porque esse tipo de ação é direcionado à sociedade civil. "*When trying to improve defense and deterrence while leaving society out, government practically guarantee they will be overstretched while leaving civil society* (…) *passive observers of their own fate*", (BRAW, 2021, p. 4). Ou seja, ainda que o governo quisesse tornar-se ubíquo em termos de dissuasão no campo cibernético, os custos seriam demasiadamente elevados – e o esforço ineficiente. Ora, se o propósito da defesa é também desencorajar ações hostis, a abordagem *whole of government* sinaliza a possíveis adversários que parte essencial da sociedade não será envolvida nesses esforços e é considerada um passivo por seu próprio governo. É quase um convite para atacar. Esclareça-se que, por sociedade, Braw entende não apenas cidadãos, mas também iniciativa privada. A alternativa, para Braw, é

> *By empowering the population, governments can achieve two goals. The public—both the private sector and the citizenry—assumes some of the duties the government would otherwise have to execute, which frees up the government to focus on duties it alone can perform. In addition, civil society becomes an integral part of national security, thereby reducing gaps adversaries would otherwise seek to exploit. This approach also creates reserves of experts, increases governments' freedom of action, and provides resource strategies the government may wish to pursue. This way, governments and their societies form a combined shield to deny adversaries the benefits they seek and negatively influence the adversaries' cost-benefit calculus. Such an approach clearly involves a major shift in both policy and practice*. (BRAW, 2021, p. 5)

A autora sugere, para envolvimento dos cidadãos, campanhas de conscientização, exercícios de *stress testing* da sociedade, cursos de treinamento de resiliência e a conscrição de estudantes egressos da educação secundária para servir em todos os setores do governo envolvidos no gerenciamento de crises. Para envolvimento da iniciativa privada, as principais sugestões de Braw são *briefings* entre governo e líderes da indústria, engajamento da classe artística na produção de conteúdos culturais – séries, filmes, etc – que aborde o tema,

exercícios conjuntos entre forças armadas e iniciativa privada sobre *grey zone aggressions* e cursos sobre segurança nacional.

A seara é grande. O Brasil dispõe de estratégia e recursos humanos para lidar com a questão; por isso, é preciso colocar em prática o que se tem, rever processos e investir na coordenação *whole of society*. O movimento deve ser constante.

4.4 Conclusão parcial

Neste capítulo, viu-se que, conquanto tenha consideráveis iniciativas estratégicas e legislativas atinentes à questão cibernética, o Brasil não dispõe de mecanismos de implementação desses documentos e normas. Não há sequer grupos de trabalho interministeriais sobre segurança e defesa cibernética além do Comitê Gestor de Segurança da Informação, cujos encontros se dão de maneira esparsa. No campo internacional, apenas um instrumento se detém exclusivamente sobre o assunto – os demais o abordam de maneira incidental, principalmente em contexto de assistência jurídica mútua. O reconhecimento da necessidade de envolvimento de outros setores da sociedade, ainda que exista, não se traduz em aplicação concreta. Além disso, em vista do delineamento teórico feito no primeiro capítulo deste trabalho, sustenta-se que o diagnóstico do governo brasileiro sobre a questão cibernética é parcial e não abrange a possibilidade de sua instrumentalização para ameaças híbridas ou *grey zone aggressions*, de maneira que o foco parece ser em proteção da informação e de infraestruturas críticas. Ressalte-se que tem sido dada auspiciosa atenção à inteligência artificial. Ao fim e ao cabo, o que se tem é a vulnerabilidade da posição brasileira frente às ameaças cibernéticas. A concentração de atribuições no GSI e no Ministério da Defesa coloca em pauta o risco de que a gestão de ameaças cibernéticas seja militarizada, na contramão das práticas *whole of society* dos países estudados neste trabalho e das observações postas na literatura. Coloca-se a proposta de que o governo empreenda mudanças não em sua estrutura organizacional, posto não ser esse um fator determinante, mas sim na forma como trabalha a questão e, principalmente, no modo de incluir atores não-governamentais em suas atividades. Iniciativas de incentivo à construção de resiliência societal também devem ser empreendidas.

5 CONCLUSÃO

Se apenas uma informação for lembrada neste trabalho, que seja a de que ameaças cibernéticas são eminentemente híbridas e têm desafiado a distinção entre tempos de conflito e tempos de paz. Vivemos na *grey zone* (BRAW, 2021). Isso significa que o *cyber* atravessa diversos domínios do conhecimento e da sociedade, de maneira que abordagens que não reconheçam esse fato fundamental não serão completas. A *internet* está por toda a parte, de modo que, na vida contemporânea, somos profundamente dependentes de dispositivos eletrônicos de comunicação para ampla gama de atividades, das mais corriqueiras às mais estratégicas. Assim, o *cyber* aumentou a possível superfície de ataque para atores maliciosos que se aproveitam dessas fragilidades para não apenas empreender ataques à infraestrutura crítica, mas também, e principalmente, à própria resiliência de dada população. Os conflitos modernos têm passado por mudanças que apontam no sentido do uso do contingente civil para desestabilizar adversários. Campanhas de desinformação são instrumento que serve a esse propósito, por exemplo, ao se aproveitar de fragilidades já existentes. Ressalte-se que não apenas atores estrangeiros podem fazer uso desse expediente.

Nesse diapasão, foram apresentados estudos que apontam serem ataques apocalípticos a infraestruturas críticas possíveis, mas raros e improváveis, pois a maior parte dos ataques cibernéticos são de baixa intensidade. Defende-se que o maior desafio trazido pela questão cibernética não é uma hipotética guerra disputada no ciberespaço, mas a corrosão do tecido social por meio de ataques híbridos.

A organização dos ecossistemas de segurança cibernética de em nível estratégico e tático de países nórdicos, Estônia e Estados Unidos também foi analisada. Os Estados Unidos adotaram abordagem *top-down* na elaboração de sua Estratégia, mas os demais envolveram representantes de diversos grupos de interesse. Todos, sem qualquer exceção, reconhecem ser importante envolver não apenas os ramos do governo diretamente associados a questões tradicionais de segurança e defesa, mas a sociedade como um todo. É importante notar que países nórdicos e Estônia destacam reiteradas vezes a importância da cooperação doméstica e internacional, com Dinamarca e Finlândia criando, inclusive, a figura do *Tech Ambassador*, no caso dinamarquês, e do *Ambassador of Hybrid Affairs*, no caso finlandês. Trata-se de solução inovadora.

A doutrina da Defesa Total informa parte da abordagem nórdica sobre o assunto, de maneira que se deve ter em consideração o caráter eminentemente cultural da maneira como

assuntos de segurança e defesa são tratados por esses países. Seja como for, os países estudados veem a questão cibernética como assunto demandante de níveis elevados de coordenação e cooperação com amplíssimo espectro de atores. Coordenação e cooperação de fato, não apenas nominal. Para tanto, são necessários arranjos que assegurem a interação entre esses atores.

O Brasil tem estratégias e leis que abordam a questão cibernética, mas não tem mecanismos de implementação das diretrizes estratégicas de que já dispõe, como grupos de trabalho interministeriais sobre segurança e defesa cibernética. A única instância é o Comitê Gestor de Segurança da Informação, cujos encontros não acontecem de maneira constante. No que diz respeito à diplomacia brasileira, dispõe-se de instrumentos que abordam o assunto tangencialmente, principalmente em contexto de assistência jurídica mútua.

O reconhecimento da necessidade de envolvimento de outros setores da sociedade, ainda que exista, não se traduz em aplicação concreta. Essa é a maior fragilidade do sistema brasileiro. Ademais, o diagnóstico do governo sobre a questão cibernética é parcial e, insista-se, não reconhece ameaças híbridas ou *grey zone aggressions*, apenas proteção da informação e de infraestruturas críticas. O país está vulnerável. É temerária, ainda, a concentração de atribuições no GSI e no Ministério da Defesa, pois a militarização da gestão de ameaças cibernéticas é possível nesse cenário. Por fim, diga-se que o governo brasileiro deve mudar não sua estrutura organizacional, mas o modo como trata a questão.

A hipótese com a qual se iniciou esse projeto foi parcialmente confirmada. A expectativa era de que a estratégia brasileira fosse de todo ineficiente, o que não é o caso. É incompleta, sim; não tem mecanismos sólidos de implementação, também. Mas há, para usar expressão em língua inglesa, encorajador *awareness* sobre a importância da questão. Isso é positivo. Se contarmos com o ativismo que o governo brasileiro tem demonstrado sobre a inteligência artificial, o cenário não é desolador, mas inspira cuidados.

Vaticinar diagnósticos e soluções nas páginas eletrônicas nas quais este trabalho foi escrito é relativamente simples se comparado à tarefa hercúlea que deve ser empreendida para que o Brasil se adapte aos desafios que já se fazem presentes. Com efeito, alterar processos e métodos de formulação de políticas públicas, ainda que de modo setorial e delimitado, bem como incluir segmentos da sociedade que normalmente não têm papel ativo em atividades governamentais de qualquer campo temático, seria, em uma comparação absolutamente rasteira, como mover um transatlântico “no braço”. Quanto mais quando o transatlântico é um

país com extenso território, enorme contingente populacional e uma máquina pública de proporções faraônicas. Nenhum dos países mencionados, à óbvia exceção dos Estados Unidos, teve de gerenciar esses fatores. No entanto, a argumentação que se construiu aqui buscou mostrar que os desafios são comuns a todos e, em seus contornos gerais, independem de características demográficas.

Esse campo de estudos está em franca expansão e carece de muita pesquisa ainda. Não se teve aqui ambição de preencher lacunas, mas espera-se que futuros leitores dessa dissertação reconheçam a necessidade de estudar segurança e defesa cibernética. Como foi dito na introdução do trabalho, mal cobrimos a superfície do oceano cibernético e de suas consequências em diversos campos da vida humana. Se há perspectiva de estudos mais empolgantes, esta autora a desconhece. Ao trabalho.

REFERÊNCIAS

ACORDO de Cooperação para o Combate à Criminalidade Organizada Transnacional e outras Modalidades Delituosas. 12 de novembro de 2004. Disponível em: https://concordia.itamaraty.gov.br/detalhamento-acordo/5248?TipoAcordo=BL%2CTL%2CML&TituloAcordo=cibern%C3%A9tico&page=2&tipoPesquisa=1. Acesso em: 18 abr. 2021.

ACORDO de Cooperação entre o Governo da República Federativa do Brasil e o Governo da República da Polônia no Campo da Luta Contra o Crime Organizado e outras Modalidades Delituosas. 09 de outubro de 2006. Disponível em: https://concordia.itamaraty.gov.br/detalhamento-acordo/5686?TituloAcordo=cibern%C3%A9tico&tipoPesquisa=1&TipoAcordo=BL,TL,ML. Acesso em: 18 abr. 2021.

ACORDO de Cooperação Estratégica entre a República Federativa do Brasil e o Serviço Europeu de Polícia. 11 de abril de 2017. Disponível em: https://concordia.itamaraty.gov.br/detalhamento-acordo/11999?TituloAcordo=cibernético&tipoPesquisa=1&TipoAcordo=BL,TL,ML. Acesso em: 18 abr. 2021.

ACORDO entre a República Federativa do Brasil e a República da Índia sobre assistência jurídica mútua em matéria penal. 25 de janeiro de 2020. Disponível em: https://concordia.itamaraty.gov.br/detalhamento-acordo/12374?TituloAcordo=cibernético&tipoPesquisa=1&TipoAcordo=BL,TL,ML. Acesso em: 18 abr. 2021.

ACORDO Complementar ao Acordo Básico de Cooperação Científica e Técnica entre o Governo da República Federativa do Brasil e o Governo da República do Suriname para a Execução do Projeto “Apoio à Criação do Centro de Resposta aos Incidentes de Segurança Cibernética no Suriname”. 24 de novembro de 2020. Disponível em: https://concordia.itamaraty.gov.br/detalhamento-acordo/12440?TituloAcordo=cibernética&tipoPesquisa=1&TipoAcordo=BL,TL,ML. Acesso em: 18 abr. 2021.

AJUSTE Complementar ao Acordo Básico de Cooperação Científica e Técnica entre o Governo da República Federativa do Brasil e o Governo da República do Suriname para a Implementação do Projeto “Capacitação Técnica para Repressão ao Crime Organizado”. 10 de setembro de 2009. Disponível em: https://concordia.itamaraty.gov.br/detalhamento-acordo/6487?TituloAcordo=cibernético&tipoPesquisa=1&TipoAcordo=BL,TL,ML. Acesso em: 18 abr. 2021.

AJUSTE Complementar ao Acordo Básico de Cooperação Científica e Técnica entre o Governo da República Federativa do Brasil e o Governo da República do Peru para a Implementação do Projeto “Capacitação Técnica para Repressão do Crime Organizado no Peru”. 31 de outubro de 2011. Disponível em: https://concordia.itamaraty.gov.br/detalhamento-acordo/7223?TituloAcordo=cibernético&tipoPesquisa=1&TipoAcordo=BL,TL,ML. Acesso em: 18 abr. 2021.

ALMEIDA, Carlos Wellington de. Política de defesa no Brasil: considerações do ponto de vista das políticas públicas. Opinião Pública, [S.l.], v. 16, n. 1, p. 220-250, jun. 2010. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s0104-62762010000100009.

ALSINA JUNIOR, João Paulo Soares. A síntese imperfeita: articulação entre política externa e política de defesa na era cardoso. Revista Brasileira de Política Internacional, [S.l.], v. 46, n. 2, p. 53-86, dez. 2003. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s0034-73292003000200003.

ALTO COMISSÁRIO DAS NAÇÕES UNIDAS PARA DIREITOS HUMANOS. **Human Rights, Terrorism and Counter-terrorism**. Genebra: Office Of The United Nations High Commissioner For Human Rights, 2008. Disponível em: https://ohchr.org/Documents/Publications/Factsheet32EN.pdf. Acesso em: 16 abr. 2021.

AMADO, Guilherme. Ameaças cibernéticas quintuplicam na pandemia: Levantamento registrou 75 milhões de ameaças em outubro. **Época**, [S.l.], ano 2021, p. 1-1, 25 jan. 2021. Disponível em: https://epoca.globo.com/guilherme-amado/ameacas-ciberneticas-quintuplicam-na-pandemia-24849183?versao=amp&%3Futm_source=twitter&utm_medium=social&utm_campaign=post&__twitter_impression=true. Acesso em: 29 mar. 2021.

ANDERSON, Janna; RAINIE, Lee. Concerns about democracy in the digital age. Disponível em: https://www.pewresearch.org/internet/2020/02/21/concerns-about-democracy-in-the-digital-age/. Acesso em: 21 fev. 2020.

ASSUMPÇÃO, Clara Ribeiro. Intelligence Oversight and Effectiveness in New Democracies. **Politikon**: The IAPSS Journal of Political Science, [S.l.], v. 45, p. 75-89, 29 jun. 2020. International Association for Political Science Students. http://dx.doi.org/10.22151/politikon.45.4.

BARBIÉRI, Luiz Felipe; D'AGOSTINO, Rosanne. **Tentativa de ataque a sistema do TSE partiu de diferentes países, diz Barroso**. 2020. Disponível em: https://g1.globo.com/politica/eleicoes/2020/noticia/2020/11/15/tentativa-de-ataque-a-sistema-do-tse-partiu-de-diferentes-paises-diz-barroso.ghtml. Acesso em: 12 abr. 2021.

BARR, Kasey; MINTZ, Alex. Public Policy Perspective on Group Decision-Making Dynamics in Foreign Policy. Policy Studies Journal, [S.l.], v. 46, p. 69-90, maio 2018. Wiley. http://dx.doi.org/10.1111/psj.12249.

BARTOLOMÉ, Mariano César. Una visión de América Latina desde la perspectiva de la agenda de la Seguridad Internacional contemporánea. Relaciones Internacionales, Madrid, v. 23, n. 2, p. 35-64, jun. 2013.

BAUMANN, Mario. 'Propaganda Fights' and 'Disinformation Campaigns': the discourse on information warfare in russia-west relations. **Contemporary Politics**, [S.l.], v. 26, n. 3, p. 288-307, 18 fev. 2020. Informa UK Limited. http://dx.doi.org/10.1080/13569775.2020.1728612.

BENNER, Thorsten. **Die autoritäre Herausforderung und die Selbstbehauptung liberaler Demokratien**. Disponível em:

https://www.gppi.net/2017/02/17/die-autoritaere-herausforderung-und-die-selbstbehauptung-liberaler-demokratien. Acesso em: 17 fev. 2017.

BENNER, Thorsten. **How To Fight China's Sharp Power**. Disponível em: https://www.gppi.net/2018/08/20/how-to-fight-chinas-sharp-power. Acesso em: 20 ago. 2018.

BENNER, Thorsten. **How Should Europe Handle Relations With China?** Disponível em: https://www.gppi.net/2019/04/09/how-should-europe-handle-relations-with-china. Acesso em: 09 abr. 2019.

BENNER, Thorsten. **The Future of Huawei in Europe**. Disponível em: https://www.gppi.net/2019/10/18/the-future-of-huawei-in-europe. Acesso em: 18 out. 2019.

BENNER, Thorsten. **Blinded By Rage Against US Digital Hegemony**: What Morozov Gets Wrong About "Technological Sovereignty". Disponível em: https://www.gppi.net/2015/01/05/blinded-by-rage-against-us-digital-hegemony-what-morozov-gets-wrong-about-technological-sovereig. Acesso em: 05 jan. 2015.

BENNER, Thorsten. **How Should Universities Respond to China's Growing Presence on Their Campuses?** Disponível em: https://www.gppi.net/2019/11/04/how-should-universities-respond-to-chinas-growing-presence-on-their-campuses. Acesso em: 04 nov. 2019.

BIDDLE, Tami Davis. Strategy and Grand Strategy: What Students and Practitioners Need to Know. Carlisle: Unites States Army War College Press, 2015. Disponível em: <https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1305>. Acesso em: 11 out. 2019.

BJOLA, Corneliu; PAPADAKIS, Krysianna. Digital propaganda, counterpublics and the disruption of the public sphere: the finnish approach to building digital resilience. **Cambridge Review Of International Affairs**, [S.I.], v. 33, n. 5, p. 638-666, 6 jan. 2020. Informa UK Limited. http://dx.doi.org/10.1080/09557571.2019.1704221.

BLEIKER, Roland. The Aesthetic Turn in International Political Theory. Millennium: Journal of International Studies, [S.L.], v. 30, n. 3, p. 509-533, dez. 2001. SAGE Publications. http://dx.doi.org/10.1177/03058298010300031001.

BOULANIN, Vincent; VERBRUGGEN, Maaike. **Article 36 Reviews**: Dealing with the challenges posed by emerging technologies. Solna: Stockholm International Peace Research Institute, 2017. Disponível em: <https://www.sipri.org/sites/default/files/2017-12/article_36_report_1712.pdf>. Acesso em: 20 nov. 2019.

BRADSHAW, Samantha; BAILEY, Hannah; HOWARD, Philip N.. **Industrialized Disinformation**: 2020 global inventory of organized social media manipulation. Oxford: Oxford Internet Institute, 2020. (Computational Propaganda Research Project). Disponível em: https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/#continue. Acesso em: 01 abr. 2021.

BRADSHAW, Samantha; HOWARD, Philip N.. **The Global Disinformation Order**: 2019 Global Inventory of Organised Social Media Manipulation. Oxford: University Of Oxford, 2019. Disponível em: <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf >. Acesso em: 09 out. 2019.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Centro Gráfico, 1988.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Lei de Acesso à Informação**. Brasília, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 19 abr. 2021.

BRASIL. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. 1. ed. Brasília: Ministério da Defesa, 2012. 41 p.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, ano 2012, 3 dez. 2012. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em: 29 mar. 2021.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, 3 dez. 2012. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: 29 mar. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. [S.l.], 24 abr. 2014. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 29 mar. 2021.

BRASIL. **Decreto nº 9.319, de 21 de março de 2018**. Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital. Brasília, ano 2018, 22 mar. 2018. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2018/Decreto/D9319.htm. Acesso em: 28 mar. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 15 ago. 2018. Disponível em:

http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 29 mar. 2021.

BRASIL. **Decreto nº 9.637, de 28 de dezembro de 2018**. Aprova a Estratégia Nacional Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. de Segurança Cibernética. **Política Nacional de Segurança da Informação**, Brasília, ano 2018, 28 dez. 2018. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2018/Decreto/D9637.htm. Acesso em: 24 mar. 2021.

BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, ano 2019, 10 out. 2019. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 28 mar. 2021.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. **Estratégia Nacional de Segurança Cibernética**: E-ciber, Brasília, ano 2020a, 5 fev. 2020. Disponível em: www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Decreto/D10222.htm. Acesso em: 24 mar. 2021.

BRASIL. **Decreto nº 10.332, de 28 de abril de 2020**. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Brasília, 29 abr. 2020. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Decreto/D10332.htm#art14. Acesso em: 28 mar. 2021.

BRASIL. **Livro Branco da Defesa Nacional**. 3. ed. Brasília: Ministério da Defesa, 2020b. 98 p. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_branco_congresso_nacional.pdf. Acesso em: 29 mar. 2021.

BRASIL. MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES. **Estratégia Brasileira de Inteligência Artificial**: Ebia. Brasília, 2021a. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial. Acesso em: 18 abr. 2021.

BRASIL. MINISTÉRIO DA DEFESA. **Sistema Militar de Defesa Cibernética entra em vigor nesta terça-feira**. 2020d. Disponível em: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/sistema-militar-de-defesa-cibernetica-entra-em-vigor-nesta-terca-feira. Acesso em: 08 abr. 2021.

BRASIL. MINISTÉRIO DA ECONOMIA. **Governo realiza seminário sobre Inteligência Artificial**. 2019. Disponível em: https://www.gov.br/economia/pt-br/canais_atendimento/imprensa/pautas/2019/05/governo-realiza-seminario-sobre-inteligencia-artificial. Acesso em: 18 abr. 2021.

BRASIL. MINISTÉRIO DAS RELAÇÕES EXTERIORES. **O Direito à Privacidade na Era Digital**. 2013a. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/o-direito-a-privacidade-na-era-digital. Acesso em: 18 abr. 2021.

BRASIL. MINISTÉRIO DAS RELAÇÕES EXTERIORES. **ONU aprova resolução sobre o Direito à Privacidade na Era Digital**. 2013b. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/resolucao-sobre-o-direito-a-privacidade-na-era-digital. Acesso em: 18 abr. 2021.

BRASIL. MINISTÉRIO DAS RELAÇÕES EXTERIORES. **Relatório da Alta Comissária para Direitos Humanos da ONU sobre "O Direito à Privacidade na Era Digital"**. 2014. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/relatorio-da-alta-comissaria-para-direitos-humanos-da-onu-sobre-o-direito-a-privacidade-na-era-digital. Acesso em: 18 abr. 2021.

BRASIL. MINISTÉRIO DAS RELAÇÕES EXTERIORES. **Criação da Relatoria Especial sobre "O Direito à Privacidade na Era Digital"**. 2015. Disponível em: http://antigo.itamaraty.gov.br/pt-BR/notas-a-imprensa/8460-criacao-da-relatoria-especial-sobre-o-direito-a-privacidade-na-era-digital. Acesso em: 19 abr. 2021.

BRASIL. MINISTÉRIO DAS RELAÇÕES EXTERIORES. **Direito à privacidade na era digital**. 2017. Disponível em: http://antigo.itamaraty.gov.br/pt-BR/notas-a-imprensa/15971-direito-a-privacidade-na-era-digital. Acesso em: 19 abr. 2021.

BRASIL. MINISTÉRIO DAS RELAÇÕES EXTERIORES. **IX Cúpula do BRICS – Declaração de Xiamen**. 2017. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/nona-cupula-do-brics-declaracao-de-xiamen-xiamen-china-4-de-setembro-de-2017. Acesso em: 18 abr. 2021.

BRASIL. MINISTÉRIO DAS RELAÇÕES EXTERIORES. **Comunicado Conjunto Brasil-Alemanha – Visita Oficial do Ministro Federal do Exterior da República Federal da Alemanha, Heiko Maas**. 2019. Nota à imprensa nº 106/2019. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/encontro-com-o-ministro-federal-do-exterior-da-republica-federal-da-alemanha-heiko-maas-brasilia-30-de-abril-de-2019. Acesso em: 18 abr. 2021.

BRASIL. MINISTÉRIO DAS RELAÇÕES EXTERIORES. **Declaração de Osaka dos Líderes do G20**. 2019. Nota à imprensa nº 170/2019. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/declaracao-de-osaka-dos-lideres-do-g20. Acesso em: 18 abr. 2021.

BRASIL. MINISTÉRIO DAS RELAÇÕES EXTERIORES. **Assinatura do Memorando de Entendimento entre o Brasil e o Chile sobre Cooperação na área de Telecomunicações e Economia Digital**. 2020. Nota à imprensa nº 82/2020. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2020/assinatura-do-memorando-de-entendimento-entre-o-brasil-e-o-chile-sobre-cooperacao-na-area-de-telecomunicacoes-e-economia-digital. Acesso em: 18 abr. 2021.

BRASIL. MINISTÉRIO DAS RELAÇÕES EXTERIORES. **Intervenções do Ministro das Relações Exteriores, Ernesto Araújo, na cerimônia de lançamento dos estudos da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) "A Caminho da Era Digital no Brasil" e "Telecomunicações e Radiofusão no Brasil"**. 2020. Disponível em: https://www.gov.br/mre/pt-br/centrais-de-conteudo/publicacoes/discursos-artigos-e-entrevistas/ministro-das-relacoes-exteriores/discursos-mre/intervencoes-do-ministro-das-relacoes-exteriores-ernesto-araujo-na-cerimonia-de-lancamento-dos-estudos-da-organizacao-para-a-cooperacao-e-desenvolvimento-economico-ocde-201ca-caminho-da-era-digital-no-brasil201d-e-201ctelecomunicacoes-e-radiofusao-no. Acesso em: 18 abr. 2021.

BRASIL. MINISTÉRIO DAS RELAÇÕES EXTERIORES. **Intervenção do Ministro Ernesto Araújo na Reunião Ministerial América Latina e Caribe – União Européia Painel temático III: Aliança Digital/ Cooperação Digital**. 2020. Disponível em: https://www.gov.br/mre/pt-br/centrais-de-conteudo/publicacoes/discursos-artigos-e-entrevistas/ministro-das-relacoes-exteriores/discursos-mre/intervencao-do-ministro-ernesto-araujo-na-reuniao-ministerial-america-latina-e-caribe-2013-uniao-europeia-painel-tematico-iii-alianca-digital-cooperacao-digital-14-de-dezembro-de-2020. Acesso em: 18 abr. 2021.

BRASIL. MINISTÉRIO DAS RELAÇÕES EXTERIORES. **Acervo de atos internacionais do Brasil**. Disponível em: https://concordia.itamaraty.gov.br/. Acesso em: 18 abr. 2021.

BRANNON, Valerie C.. Free Speech and the Regulation of Social Media Content. Washington: Congressional Research Service, 2019. Disponível em: https://fas.org/sgp/crs/misc/R45650.pdf. Acesso em: 24 jul. 2020.

BRAW, Elisabeth. **Building a Wall of Denial Against Gray-Zone Aggression**. Washington: American Enterprise Institute, 2021. Disponível em: https://www.aei.org/wp-content/uploads/2021/04/Building-a-Wall-of-Denial-Against-Gray-Zone-Aggression.pdf?x91208. Acesso em: 13 abr. 2021.

BRESSAN, Sarah; SULG, Mari-Liis. Welcome to the grey zone: future war and peace. **New Perspectives**, [S.l.], v. 28, n. 3, p. 379-397, 13 jul. 2020. SAGE Publications. http://dx.doi.org/10.1177/2336825x20935244.

BRICS. **Declaration of the 11th BRICS Summit**. Brasília: Brics, 2019. Disponível em: http://en.kremlin.ru/supplement/5458. Acesso em: 27 maio 2019.

BUCHAN, Russell. When More is Less: the us department of defense's statement on cyberspace. The US Department of Defense's Statement on Cyberspace. Disponível em:

https://www.ejiltalk.org/when-more-is-less-the-department-of-defenses-statement-on-cyberspace/. Acesso em: 01 jun. 2020.

BUZAN, Barry; WEAVER, Ole; WILDE, Jaap de. Security: A New Framework For Analysis. Boulder: Lynne Rienner Publishers, 1998.

CAMPOS, Ricardo; MARANHÃO, Juliano; ABRUSIO, Juliana. O impasse das contas inautênticas na regulação das redes sociais. Disponível em: https://www.conjur.com.br/2020-jun-09/direito-tecnologia-impasse-contas-inautenticas-regulacao-redes. Acesso em: 9 jun. 2020.

CARLSSON, Moa Peldán. Autonomous weapon systems and the impact on strategic stability. In: RIO SEMINAR ON AUTONOMOUS WEAPONS SYSTEMS, 1., 2020, Rio de Janeiro. **Apresentação**. Rio de Janeiro: Sipri, 2020. p. 1-8.

CARVALHO, Guilherme Otávio Godinho de. O papel da Diplomacia Militar e o Exército Brasileiro. Revista Artigos Estratégicos, Brasília, v. 7, n. 2, p. 7-20, jul. 2019.

CASA BRANCA (Estados Unidos da América). **International Strategy for Cyberspace**. Washington: Casa Branca, 2011. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf. Acesso em: 12 maio 2021.

CAVELTY, Myriam Dunn. Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. Journal Of Information Technology & Politics, [s.l.], v. 4, n. 1, p. 19-36, abr. 2008. Informa UK Limited. http://dx.doi.org/10.1300/j516v04n01_03.

CAVELTY, Myriam Dunn; WENGER, Andreas. Cyber security meets security politics: complex technology, fragmented politics, and networked science. Contemporary Security Policy, [s.l.], v. 41, n. 1, p. 5-32, 14 out. 2019. Informa UK Limited. http://dx.doi.org/10.1080/13523260.2019.1678855.

CHIUSI, Fabio *et al* (ed.). **Automating Society**: 2020 Report. Berlim: Algorithm Watch, 2020. Disponível em: https://automatingsociety.algorithmwatch.org/. Acesso em: 05 abr. 2021.

CLEMENTE JUNIOR, José Alberto. **A constante da incerteza no Direito brasileiro**. 2018. Disponível em: https://www.aasp.org.br/em-pauta/artigo-a-constante-da-incerteza/. Acesso em: 16 abr. 2021.

COMISSÃO EUROPEIA. União Europeia. **Digital Government Factsheet 2019**: Estonia. Bruxelas: Isa², 2019a. Disponível em: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Estonia_2019.pdf. Acesso em: 20 fev. 2021.

COMISSÃO EUROPEIA. **Digital Government Factsheet 2019**: Sweden. Bruxelas: Isa², 2019b. Disponível em: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Sweden_2019.pdf. Acesso em: 20 fev. 2021.

COMISSÃO EUROPEIA. **Digital Government Factsheet 2019**: Dinamarca. Bruxelas: Isa², 2019c. Disponível em: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Denmark_2019.pdf. Acesso em: 20 fev. 2021.

COMISSÃO EUROPEIA. **Digital Government Factsheet 2019**: Finlândia. Bruxelas: Isa², 2019d. Disponível em: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Finland_2019.pdf. Acesso em: 20 fev. 2021.

COMISSÃO EUROPEIA. **Digital Government Factsheet 2019**: Noruega. Bruxelas: Isa², 2019e. Disponível em: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Norway_2019.pdf. Acesso em: 20 fev. 2021.

COMISSÃO EUROPEIA. **Digital Government Factsheet 2019**: Estonia. Bruxelas: Isa², 2019f. Disponível em: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Estonia_2019.pdf. Acesso em: 09 fev. 2021.

CONVÊNIO entre a República Federativa do Brasil e o Reino da Espanha sobre Cooperação em Matéria de Combate à Criminalidade. 25 de junho de 2007. Disponível em: https://concordia.itamaraty.gov.br/detalhamento-acordo/5857?TituloAcordo=cibern%C3%A9tico&tipoPesquisa=1&TipoAcordo=BL,TL,ML. Acesso em: 18 abr. 2021.

COOK, Sarah. **Beijing's Global Megaphone**: the expansion of chinese communist party media influence since 2017. [S.l.]: Freedom House, 2020.

COSTA, Frederico Carlos de Sá. Estudos estratégicos, controle civil e identificação do inimigo. **Revista da Escola Superior de Guerra**, [S.l.], v. 30, n. 61, p. 112-127, jul. 2015. Disponível em: https://revista.esg.br/index.php/revistadaesg/article/download/154/131. Acesso em: 10 abr. 2021.

CRANDALL, Matthew; THAYER, Bradley. **The Balance of Cyberpower**. Disponível em: https://nationalinterest.org/feature/balance-cyberpower-36637. Acesso em: 25 nov. 2018.

CRUZ JÚNIOR, Samuel César da. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. Brasília: Ipea, 2013. (1850).

DAWDA, Sneha. **Exploring National Cyber Security Strategies**: policy approaches and implications. Londres: Royal United Services Institute For Defence And Security Studies, 2021.

DECLARAÇÃO sobre a Parceria Estratégica entre a República Federativa do Brasil e a República da Indonésia. 18 de novembro de 2008. Disponível em:

https://concordia.itamaraty.gov.br/detalhamento-acordo/6277?TituloAcordo=cibern%C3%A9tico&tipoPesquisa=1&TipoAcordo=BL,TL,ML. Acesso em: 18 abr. 2021.

DEMCHAK, Chris C.; DROMBROWSKI, Peter. Rise of a Cybered Westphalian Age. Strategic Studies Quarterly, [s.i.], v. 5, n. 1, p. 32-61, mar. 2011.

DIAMINT, Rut. A New Militarism in Latin America. **Journal Of Democracy**, [S.l.], v. 26, n. 4, p. 155-168, 2015. Project Muse. http://dx.doi.org/10.1353/jod.2015.0066.

DIJKSTRA, Hylke; PETROV, Petar; VERSLUIS, Esther. Governing risks in international security. Contemporary Security Policy, [S.l.], v. 39, n. 4, p. 537-543, 30 ago. 2018. Informa UK Limited. http://dx.doi.org/10.1080/13523260.2018.1503776.

DINAMARCA. **National Strategy for Cyber and Information Security 2015-2016**. Copenhague: Centre For Cyber Security, 2015. Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf. Acesso em: 08 fev. 2021.

DINAMARCA. **A Stronger and More Secure Digital Denmark**. Copenhague: The Danish Government, 2016. Disponível em: https://en.digst.dk/media/14143/ds_singlepage_uk_web.pdf. Acesso em: 08 fev. 2021.

DINAMARCA. **Danish Cyber and Information Security Strategy**. Copenhague: The Danish Government, 2018. Disponível em: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf. Acesso em: 08 fev. 2021.

DINAMARCA. **National Strategy for Artifcial Intelligence**. Copenhague: The Danish Government, 2019. Disponível em: https://en.digst.dk/media/19337/305755_gb_version_final-a.pdf. Acesso em: 08 fev. 2021.

DINAMARCA. **Strategy for Denmark's Tech Diplomacy**: 2021-2023. Copenhague: Ministry Of Foreign Affairs, 2021. Disponível em: https://t.co/mEeq0CohL7?amp=1. Acesso em: 22 fev. 2021.

DINIZ, Gustavo; MUGGAH, Robert; GLENNY, Misha. **Deconstructing Cyber Security in Brazil**: threats and responses. Rio de Janeiro: Instituto Igarapé, 2014. Disponível em: https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf. Acesso em: 08 abr. 2021.

DIRESTA, Renée; GROSSMAN, Shelby. Potemkin Pages & Personas: assessing gru online operations, 2014-2019. Stanford: Stanford Cyber Policy Center, 2019. 116 p. Disponível em: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/potemkin-pages-personas-sio-wp.pdf. Acesso em: 01 maio 2020.

DUQUE, Marina Guedes. O papel de síntese da Escola de Copenhague nos Estudos de Segurança Internacional. Contexto Internacional, Rio de Janeiro, v. 31, n. 3, p. 459-501, set. 2009.

E-ESTONIA. **I-Voting**. Disponível em: https://e-estonia.com/solutions/e-governance/i-voting/. Acesso em: 09 fev. 2021.

EGLOFF, Florian J.. Contested public attributions of cyber incidents and the role of academia. Contemporary Security Policy, [S.l.], v. 41, n. 1, p. 55-81, 12 out. 2019. Informa UK Limited. http://dx.doi.org/10.1080/13523260.2019.1677324.

ESCOSTEGUY, Diego. **Hacker criptografou todos os processos e emails do STJ**. 2020. Disponível em: https://obastidor.com.br/justica/hacker-criptografou-todos-os-processos-e-emails-do-stj-19. Acesso em: 12 abr. 2021.

ESTADOS UNIDOS DA AMÉRICA. **National Cyber Strategy of the United States of America**. Washington: The White House, 2018a. Disponível em: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Acesso em: 12 fev. 2021.

ESTADOS UNIDOS DA AMÉRICA. **Cyber Strategy**. Washington: Department Of Defense, 2018b. Disponível em: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF. Acesso em: 12 fev. 2021.

ESTADOS UNIDOS DA AMÉRICA. **Cybersecurity Strategy**. Washington: Department of Homeland Security, 2018c. Disponível em: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Fact-Sheet.pdf. Acesso em: 12 fev. 2021.

ESTADOS UNIDOS DA AMÉRICA. Daniel R. Coats. Director Of National Intelligence. **Worldwide threat assessment of the US Intelligence Community**: statement for the record. Washington: Senate Select Committee On Intelligence, 2019. Disponível em: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf. Acesso em: 7 jun. 2020.

ESTADOS UNIDOS DA AMÉRICA. **Report**. Washington: Cyberspace Solarium Commission, 2020. Disponível em: https://www.solarium.gov/report. Acesso em: 12 fev. 2021.

ESTÔNIA. **Cyber Security Strategy**. Tallinn: Ministry Of Defence, 2008. Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en. Acesso em: 09 fev. 2021.

ESTÔNIA. **Cyber Security Strategy**. Tallinn: Ministry Of Economic Affairs And Communications, 2014. Disponível em: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf. Acesso em: 09 fev. 2021.

ESTÔNIA. **Cyber Strategy**: Republic of Estonia. Tallinn: Ministry Of Economic Affairs And Communications, 2019. Disponível em: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf. Acesso em: 09 fev. 2021.

ESTÔNIA. **I-Voting**. Disponível em: https://www.valimised.ee/en/internet-voting/more-about-i-voting/introduction-i-voting. Acesso em: 09 fev. 2021.

FAZIO, Lisa K.; RAND, David G.; PENNYCOOK, Gordon. Repetition increases perceived truth equally for plausible and implausible statements. Psychonomic Bulletin & Review, [s.l.], p.1-6, 16 ago. 2019. Springer Science and Business Media LLC. http://dx.doi.org/10.3758/s13423-019-01651-4. Disponível em: <https://link.springer.com/epdf/10.3758/s13423-019-01651-4?shared_access_token=rd4epOc7BNGQLaIyFS5TYZAH0g46feNdnc402WrhzyppGle7MiYTBVZjyW6na73hYTrLoGHV2XTD6iHdqVlDUAvRMIByCynp0j8SdrNWT4N1LdMYYn_PoUwkkU3D2gKuozpiErC5UX4r6Bg5K571lA==>. Acesso em: 09 out. 2019.

FEAVER, Peter; INBODEN, Will. **Washington Needs a New Solarium Project To Counter Cyberthreats**. 2018. Disponível em: https://foreignpolicy.com/2018/06/26/washington-needs-a-new-solarium-project-to-counter-cyberthreats/. Acesso em: 13 fev. 2021.

FINLÂNDIA. **Finland's Cyber Security Strategy**. Helsinki: Secretariat Of The Security Committee, 2013. Disponível em: https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf. Acesso em: 02 fev. 2021.

FINLÂNDIA. **Implementation Programme for Finland's Cyber Security** Strategy for 2017–2020. Helsinki: The Security Committee, 2017. Disponível em: https://turvallisuuskomitea.fi/wp-content/uploads/2018/10/Implementation-programme-for-Finlands-Cyber-Security-Strategy-for-2017-2020-final.pdf. Acesso em: 03 fev. 2021.

FINLÂNDIA. **Security Strategy for Society**: government resolution. Helsinki: The Security Committee, 2017. Disponível em: https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf. Acesso em: 05 fev. 2021.

FINLÂNDIA. MINISTÉRIO DAS RELAÇÕES EXTERIORES. **Mikko Kinnunen appointed Finland's first Ambassador for Hybrid Affairs**. 2018. Disponível em: https://www.sttinfo.fi/tiedote/mfa-mikko-kinnunen-appointed-finlands-first-ambassador-for-hybrid-affairs?publisherId=1797&releaseId=67113810. Acesso em: 21 abr. 2021.

FISKVIK, Jannicke. Nordic Security: moving towards nato?. **Css Analyses In Security Policy**, Zurique, v. 189, n. 1, p. 1-4, abr. 2016. Disponível em: https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse-189-EN.pdf. Acesso em: 13 set. 2020.

FLEW, Terry. Social Media Governance. Social Media + Society, [S.L.], v. 1, n. 1, p. 205630511557813, 29 abr. 2015. SAGE Publications. http://dx.doi.org/10.1177/2056305115578136.

FOA, Roberto Stefan; MOUNK, Yascha. The Danger of Deconsolidation: the democratic disconnect. Journal Of Democracy. [S.l.], p. 5-17. jul. 2016.

FRANKE, Ulrike Esther. **Artificial divide**: how europe and america could clash over ai. [S.I.]: European Council On Foreign Relations, 2021. Disponível em: https://ecfr.eu/publication/artificial-divide-how-europe-and-america-could-clash-over-ai/. Acesso em: 05 abr. 2021.

GALLIOTT, Jai; WYATT, Austin. Risks and Benefits of Autonomous Weapon Systems: perceptions among future Australian Defence Force officers. **Journal Of Indo-Pacific Affairs**, Montgomery, p. 17-34, nov. 2020.

GARTZKE, Erik; LINDSAY, Jon R.. Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. Security Studies, [S.l.], v. 24, n. 2, p.316-348, 3 abr. 2015. Informa UK Limited. http://dx.doi.org/10.1080/09636412.2015.1038188.

GEORGIEVA, Ilina. The unexpected norm-setters: intelligence agencies in cyberspace. Contemporary Security Policy, [S.l.], v. 41, n. 1, p. 33-54, 9 out. 2019. Informa UK Limited. http://dx.doi.org/10.1080/13523260.2019.1677389.

GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE. **Advancing Cyberstability**. [S.I.]: Global Commission On The Stability Of Cyberspace, 2019. Disponível em: https://cyberstability.org/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf. Acesso em: 27 maio 2020.

GORWA, Robert. What is platform governance? Information, Communication & Society, [S.I.], v. 22, n. 6, p. 854-871, 11 fev. 2019. Informa UK Limited. http://dx.doi.org/10.1080/1369118x.2019.1573914.

GUITTON, Clement. Cyber insecurity as a national threat: overreaction from Germany, France and the UK?. European Security, [S.l.], v. 22, n. 1, p.21-35, mar. 2013. Informa UK Limited. http://dx.doi.org/10.1080/09662839.2012.749864.

HANSEN, Flemming Splidsboel. **Russian hybrid warfare**: a study of disinformation. Copenhague: Danish Institute For International Studies, 2017. Disponível em: https://www.econstor.eu/bitstream/10419/197644/1/896622703.pdf. Acesso em: 15 set. 2020.

HANSEN, Lene. How images make world politics: international icons and the case of Abu Ghraib. Review Of International Studies, [S.l.], v. 41, n. 2, p. 263-288, 2 set. 2014. Cambridge University Press (CUP). http://dx.doi.org/10.1017/s0260210514000199.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, [S.l.], v. 53, n. 4, p. 1155-1175, dez. 2009. Oxford University Press (OUP). http://dx.doi.org/10.1111/j.1468-2478.2009.00572.x.

HANSON, Fergus et al. Hacking democracies: Cataloguing cyber-enabled attacks on elections. [S.l.]: Australian Strategic Policy Institute, 2019. Disponível em: <https://www.aspi.org.au/report/hacking-democracies>. Acesso em: 26 ago. 2019.

HARE, Forrest B.. Precision cyber weapon systems: an important component of a responsible national security strategy?. Contemporary Security Policy, [S.l.], v. 40, n. 2, p. 193-213, 8 out. 2018. Informa UK Limited. http://dx.doi.org/10.1080/13523260.2018.1529369.

HELBERGER, Natali. On the Democratic Role of News Recommenders. Digital Journalism, [S.L.], v. 7, n. 8, p. 993-1012, 12 jun. 2019. Informa UK Limited. http://dx.doi.org/10.1080/21670811.2019.1623700.

HERZOG, Stephen. Revisiting the Estonian Cyber Attacks: digital threats and multinational responses. **Journal Of Strategic Security**, [S.l.], v. 4, n. 2, p. 49-60, jun. 2011. University of South Florida Libraries. http://dx.doi.org/10.5038/1944-0472.4.2.3.

HOFFMAN, Frank G.. **Conflict in the 21st century:** The rise of Hybrid Wars. Arlington: Potomac Institute For Policy Studies, 2007.

HOLLAND, Jake. **California Will Be First State With Its Own Privacy Regulator**: law will apply to data collected beginning in 2022. Law will apply to data collected beginning in 2022. 2020. Disponível em: https://news.bloomberglaw.com/tech-and-telecom-law/california-will-be-first-state-with-its-own-privacy-regulator?s=08. Acesso em: 12 fev. 2021.

HOROWITZ, Michael C.; SCHARRE, Paul. **AI and International Stability**: risks and confidence-building measures. Washington: Center For New American Security, 2021.

JÁCAMO, Ricardo Antonio Pravia. First steps in the study of cyber-psycho-cognitive operations. 2019. 202 f. Dissertação (Mestrado) - Curso de Relações Internacionais, Instituto de Relações Internacionais, Universidade de Brasília, Brasília, 2019.

JONES, Bryan D.; Thomas III, Herschel F.; WOLFE, Michelle. Policy Bubbles. Policy Studies Journal, Malden, v. 42, n. 1, p. 146-171, jan. 2014.

JONES, Calvert W.; PARIS, Celia. It's the End of the World and They Know It: how dystopian fiction shapes political attitudes. Perspectives On Politics, [S.l.], v. 16, n. 4, p. 969-989, 23 nov. 2018. Cambridge University Press (CUP). http://dx.doi.org/10.1017/s1537592718002153.

JØRGENSEN, Rikke Frank; ZULETA, Lumi. Private Governance of Freedom of Expression on Social Media Platforms. Nordicom Review, [S.l.], v. 41, n. 1, p. 51-67, 3 mar. 2020. Walter de Gruyter GmbH. http://dx.doi.org/10.2478/nor-2020-0003.

KALDOR, Mary et al. From Hybrid Peace to Human Security: Rethinking EU Strategy towards Conflict. Bruxelas: London School Of Economics And Political Science, 2016. Disponível em: <http://eprints.lse.ac.uk/84978/>. Acesso em: 11 out. 2019.

KELLO, Lucas. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. International Security, [S.l.], v. 38, n. 2, p.7-40, out. 2013. MIT Press - Journals. http://dx.doi.org/10.1162/isec_a_00138.

KLIMBURG, Alexander (ed.). **National Cybersecurity Framework Manual**. Talinn: Nato Cyber Defence Centre of Excellence, 2012. Disponível em: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf. Acesso em: 20 maio 2020.

KLIMBURG, Alexander. The Darkening Web: The War for Cybespace. [S.l.]: Penguin Random House, 2017.

KNIGHT, Will. **Military artificial intelligence can be easily and dangerously fooled**. 2019. Publicado no sítio eletrônico MIT Technology Review. Disponível em: https://www.technologyreview.com/2019/10/21/132277/military-artificial-intelligence-can-be-easily-and-dangerously-fooled/. Acesso em: 06 abr. 2021.

KUNZ, Barbara. **Northern Europe's strategic challenge from Russia**: what political and military responses?. Paris: Ifri, 2018. (Russie.Nei.Visions). Disponível em: https://www.ifri.org/sites/default/files/atoms/files/rnv_111_kunz_northern_europe_strategic_challenge_from_russia_2018.pdf. Acesso em: 15 set. 2020.

LANOZKA, Alexander. Russian hybrid warfare and extended deterrence in eastern Europe. **International Affairs**, [S.l.], v. 92, n. 1, p. 175-195, jan. 2016. Oxford University Press (OUP). http://dx.doi.org/10.1111/1468-2346.12509.

LAWAND, Kathleen. International humanitarian law (IHL) and 'LAWS': is there a need for a new protocol?. In: RIO SEMINAR ON AUTONOMOUS WEAPONS SYSTEMS, 1., 2020, Rio de Janeiro. **Apresentação**. Rio de Janeiro: ICRC, 2020. p. 1-8.

LAWSON, Sean. Beyond Cyber-Doom: assessing the limits of hypothetical scenarios in the framing of cyber-threats. Journal Of Information Technology & Politics, [s.l.], v. 10, n. 1, p. 86-103, jan. 2013. Informa UK Limited. http://dx.doi.org/10.1080/19331681.2012.759059.

LEUPRECHT, Christian; SZEMAN, Joseph; SKILLICORN, David B.. The Damoclean sword of offensive cyber: policy uncertainty and collective insecurity. Contemporary Security Policy, [S.l.], v. 40, n. 3, p. 382-407, 27 mar. 2019. Informa UK Limited. http://dx.doi.org/10.1080/13523260.2019.1590960.

LIMA, Mariana Fonseca. **Percepções sobre a interação entre defesa, diplomacia e inteligência no Brasil**. 2012. 174 f. Dissertação (Mestrado) - Curso de Relações Internacionais, Instituto de Relações Internacionais, Universidade de Brasília, Brasília, 2012. Disponível em: https://repositorio.unb.br/bitstream/10482/11615/1/2012_MarianaFonsecaLima.pdf. Acesso em: 05 jun. 2020.

LIND, William S. et al. The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette, [s.i.], v. 10, n. 73, p.22-26, out. 1989.

LINDNER, Ralf; AICHHOLZER, Georg. E-Democracy: conceptual foundations and recent trends. European E-Democracy In Practice, [S.l.], p. 11-45, 7 nov. 2019. Springer International Publishing. http://dx.doi.org/10.1007/978-3-030-27184-8_2.

LINDSAY, Jon R.. Stuxnet and the Limits of Cyber Warfare. Security Studies, [S.l.], v. 22, n. 3, p. 365-404, jul. 2013. Informa UK Limited. http://dx.doi.org/10.1080/09636412.2013.816122.

LUNDGREN, Per; BJERREGÅRD, Mogens Blicher (ed.). **Fighting Fakes - The Nordic Way**. Copenhagen: Nordic Council Of Ministers, 2018. Disponível em: http://dx.doi.org/10.6027/ANP2018-756. Acesso em: 17 fev. 2021.

LUPION, Bruno. The EU Framework Against Disinformation: What Worked, What Changed and The Way Forward. [S.l.]: Democracy Reporting International, 2019. Disponível em: <https://democracy-reporting.org/wp-content/uploads/2019/08/EU-Actions-Against-Disinformation-EP2019-Final-1.pdf>. Acesso em: 09 out. 2019.

MACKINTOSH, Eliza. **Finland is winning the war on fake news. What it's learned may be crucial to Western democracy**. 2019. Disponível em: https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/. Acesso em: 05 fev. 2021.

MAIA, Cesar. **Excesso de leis cria insegurança jurídica**. 2009. Disponível em: https://www.conjur.com.br/2009-set-05/excesso-leis-disfarca-problemas-cria-inseguranca-juridica. Acesso em: 14 abr. 2021.

MAIA, Gustavo. **Bolsonaro cria Centro de Inteligência Nacional na Abin para enfrentar 'ameaças à segurança do Estado'**. 2020. Disponível em: https://oglobo.globo.com/brasil/bolsonaro-cria-centro-de-inteligencia-nacional-na-abin-para-enfrentar-ameacas-seguranca-do-estado-1-24565334?versao=amp&s=08. Acesso em: 12 abr. 2021.

MANESS, Ryan C.; VALERIANO, Brandon. The Impact of Cyber Conflict on International Interactions. Armed Forces & Society, [S.l.], v. 42, n. 2, p.301-323, 25 mar. 2015. SAGE Publications. http://dx.doi.org/10.1177/0095327x15572997. Disponível em: <https://journals.sagepub.com/doi/abs/10.1177/0095327X15572997>. Acesso em: 16 ago. 2019.

MANESS, Ryan C.. Death by a thousand cuts: Is Russia winning the information war with the West?. In: KAROLWESKI, I. Pawel; CROSS, Maia D. (ed.). Security Challenges in the EU-Russia relations. Ann Arbor: University Of Michigan Press, 2019. p. 1-20.

MARIER, Patrik. The power of institutionalized learning: the uses and practices of commissions to generate policy change. Journal Of European Public Policy, [S.l.], v. 16, n. 8,

p.1204-1223, dez. 2009. Informa UK Limited. http://dx.doi.org/10.1080/13501760903332761.

MARTORELLI, João Humberto. **Revisão do CPC**. 2009. Disponível em: https://oabpe.org.br/revisao-do-cpc-joao-humberto-martorelli/. Acesso em: 16 abr. 2021.

MATHIAS, Suzeley Kalil; GUZZI, André Cavaller. Autonomia na lei: as forças armadas nas constituições nacionais. **Revista Brasileira de Ciências Sociais**, [S.l.], v. 25, n. 73, p. 41-57, jun. 2010. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s0102-69092010000200003.

MATOS, Sérgio Ricardo Reis; CRUZ, Manuel Adalberto Carlos Montenegro Lopes da. Temática de segurança sob o prisma das teorias das relações internacionais: um debate. : Um debate. Revista da Escola de Guerra Naval, Rio de Janeiro, v. 19, n. 2, p. 411-434, jul. 2013.

MCGWIN, Kevin. **In face of uncertainty about Russia, a Nordic gang of four emerges**: an increasingly uncertain security situation in Europe is driving Nordic countries towards closer military cooperation. 2019. Disponível em: https://www.arctictoday.com/in-face-of-uncertainty-about-russia-a-nordic-gang-of-four-emerges/. Acesso em: 12 set. 2020.

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. The Fundamental Conceptual Trinity of Cyberspace. **Contexto Internacional**, [S.l.], v. 42, n. 1, p. 31-54, abr. 2020. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s0102-8529.2019420100002.

MEDEIROS FILHO, Oscar. **Entre a cooperação e a dissuasão**: políticas de defesa e percepções militares na América do Sul. 2010. 240 f. Tese (Doutorado) - Curso de Ciência Política, Universidade de São Paulo, São Paulo, 2010. Disponível em: https://teses.usp.br/teses/disponiveis/8/8131/tde-16112010-105249/publico/2010_OscarMedeirosFilho.pdf. Acesso em: 02 mar. 2021.

MELLO, Patrícia Campos. **Brasil é único país onde fake news sobre cloroquina ainda circulam com frequência**. 2020. Disponível em: https://www1.folha.uol.com.br/equilibrioesaude/2020/11/brasil-e-unico-pais-onde-fake-news-sobre-cloroquina-ainda-circulam-com-frequencia.shtml. Acesso em: 12 abr. 2021.

MEMORANDO de Entendimento entre a República Federativa do Brasil e a República da Colômbia sobre Cooperação Policial. 14 de dezembro de 2005. Disponível em: https://concordia.itamaraty.gov.br/detalhamento-acordo/5531?TituloAcordo=cibern%C3%A9tico&tipoPesquisa=1&TipoAcordo=BL,TL,ML. Acesso em: 18 abr. 2021.

MEMORANDO de Entendimento entre o Governo da República Federativa do Brasil e o Governo do Reino Unido da Grã-Bretanha e Irlanda do Norte para Aprofundar a Cooperação nas Áreas de Segurança e Combate ao Crime. 27 de outubro de 2011. Disponível em: https://concordia.itamaraty.gov.br/detalhamento-acordo/7220?TituloAcordo=cibernético&tipoPesquisa=1&TipoAcordo=BL,TL,ML. Acesso em: 18 abr. 2021.

MEMORANDO de Entendimento entre o Governo da República Federativa do Brasil e o Governo da República do Chile sobre Cooperação na Área de Telecomunicações e Economia Digital. 24 de julho de 2020. Disponível em: https://concordia.itamaraty.gov.br/detalhamento-acordo/12416?TituloAcordo=inteligência artificial&tipoPesquisa=1&TipoAcordo=BL,TL,ML. Acesso em: 18 abr. 2021.

MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. 158 f. Dissertação (Mestrado) - Curso de Direito, Universidade de Brasília, Brasília, 2008. Disponível em: https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf. Acesso em: 16 abr. 2021.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **REI - Revista de Estudos Institucionais**, [S.l.], v. 6, n. 2, p. 507-533, 23 set. 2020. Revista Estudos Institucionais. http://dx.doi.org/10.21783/rei.v6i2.521.

MILLIKEN, Jennifer. The Study of Discourse in International Relations. European Journal Of International Relations, [S.l.], v. 5, n. 2, p. 225-254, jun. 1999. SAGE Publications. http://dx.doi.org/10.1177/1354066199005002003.

MOURY, Taciana. **Brazilian Army Invests in Cyber Defense**. 2017. Disponível em: https://dialogo-americas.com/articles/brazilian-army-invests-in-cyber-defense/. Acesso em: 12 abr. 2021.

MUNICH SECURITY CONFERENCE. **Munich Security Report 2020: Westlessness**. Munique: Munich Security Conference, 2020.

NIMMO, Ben. **Failures and adaptations: Kremlin propaganda in Finland and Sweden**. 2017. Disponível em: https://fpc.org.uk/failures-adaptations-kremlin-propaganda-finland-sweden/. Acesso em: 14 set. 2020.

NISSENBAUM, Helen. Hackers and the contested ontology of cyberspace. New Media & Society, [S.l.], v. 6, n. 2, p. 195-217, abr. 2004. SAGE Publications. http://dx.doi.org/10.1177/1461444804041445.

NEY JUNIOR, Paul C.. DOD General Counsel Remarks at U.S. Cyber Command Legal Conference. 2020. Disponível em: https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/. Acesso em: 01 jun. 2020.

NORUEGA. **Cyber Security Strategy for Norway**. Oslo: Norwegian Ministries, 2012. Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Norway_Cyber_Security_StrategyNO.pdf. Acesso em: 08 fev. 2021.

NORUEGA. **Official Norwegian Report (NOU 2015: 13) to the Ministry of Justice and Public Security**. Oslo: Committee Of Digital Vulnerabilities In Society, 2015. Disponível em:

https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/9.pdf. Acesso em: 08 fev. 2021.

NORUEGA. **Cyber Security**: a joint responsibility. Oslo: The Ministry Of Justice And Public Security, 2017a. Report to the Storting (white paper) No. 38. Disponível em: https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/en-gb/pdfs/stm201620170038000engpdfs.pdf. Acesso em: 08 fev. 2021.

NORUEGA. **International Cyber Strategy for Norway**. Oslo: Norwegian Ministries, 2017. Disponível em: https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategy_2017.pdf. Acesso em: 08 fev. 2021.

NORUEGA. **National Cyber Security Strategy for Norway**. Oslo: Norwegian Ministeries, 2019a. Disponível em: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf. Acesso em: 08 fev. 2021.

NORUEGA. **List of measures – National Cyber Security Strategy for Norway**. Oslo: Norwegian Ministeries, 2019b. Disponível em: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/list-of-measures--national-cyber-security-strategy-for-norway.pdf. Acesso em: 08 fev. 2021.

NYE, Joseph S.. Cyber Power. Cambridge: Belfer Center For Science And International Affairs, 2010. 30 p. Disponível em: <https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf>. Acesso em: 24 ago. 2019.

NYE JR, Joseph S.. The Regime Complex for Managing Global Cyber Activities. Paper Series, Londres, v. 1, n. 1, p.1-20, maio 2014. Disponível em: <https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf>. Acesso em: 16 ago. 2019.

NYE, Joseph S.. Normative Restraints on Cyber Conflict. Cambridge: Belfer Center For Science And International Affairs, 2018. Disponível em: <https://www.belfercenter.org/publication/normative-restraints-cyber-conflict>. Acesso em: 25 ago. 2019.

OAS. **NIST Cybersecurity Framework**: a comprehensive approach to cybersecurity. 5. ed. [S.l.]: Oas, 2019. Disponível em: http://www.cicad.oas.org/apps/ReadPublication.aspx?Id=5498. Acesso em: 30 maio 2020.

OLIVEIRA, Leonardo D'Avila de. **Inflação Normativa**: excesso e exceção. 2009. 180 f. Dissertação (Mestrado) - Curso de Direito, Universidade Federal de Santa Catarina, Florianópolis, 2009. Disponível em: https://core.ac.uk/download/pdf/30373682.pdf. Acesso em: 16 abr. 2021.

ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE. Tratado Constitutivo nº 1, de 1949. **The North Atlantic Treaty**. Washington, 04 abr. 1949. Disponível em: https://www.nato.int/nato_static_fl2014/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf. Acesso em: 17 fev. 2021.

ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE. **NATO's new atlantic command declared operational**. 2020. Disponível em: https://www.nato.int/cps/en/natohq/news_178031.htm. Acesso em: 17 fev. 2021.

ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE. **Collective defence**: article 5. Article 5. Disponível em: https://www.nato.int/cps/en/natohq/topics_110496.htm#:~:text=Collective%20defence%20means%20that%20an%20attack%20against%20one,the%209%2F11%20terrorist%20attacks%20against%20the%20United%20States.. Acesso em: 18 set. 2020.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Revisão Da Capacidade De Cibersegurança**: República Federativa do Brasil. [S.l.]: Comitê Interamericano contra o Terrorismo da Organização dos Estados Americanos, 2020. Disponível em: http://www.oas.org/pt/ssm/cicte/docs/PORT-Revisao-da-Capacidade-de-Ciberseguranca.pdf. Acesso em: 17 abr. 2021.

PAUWELS, Eleonore. The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI. Nova Iorque: United Nations University, 2019. Disponível em: <https://cpr.unu.edu/the-new-geopolitics-of-converging-risks-the-un-and-prevention-in-the-era-of-ai.html>. Acesso em: 31 jul. 2019.

PINTO, J. R. de Almeida; ROCHA, A. J. Ramalho da; SILVA, R. Doring Pinho da (org.). **O Brasil no cenário internacional de defesa e segurança**. Brasília: Ministério da Defesa, 2004. (Pensamento brasileiro sobre defesa e segurança).

PINTO, Renata Ávila. **Tech Power to the People!**: democratising cutting-edge technologies to serve society. Bonn: Development And Peace Foundation (Sef:), 2020. Disponível em: https://www.sef-bonn.org/en/publications/global-trends-analysis/032020/. Acesso em: 05 abr. 2021.

PLANO de Ação Conjunta entre o Governo da República Federativa do Brasil e o Governo da República Popular da China 2015-2021. 19 de maio de 2015. Disponível em: https://concordia.itamaraty.gov.br/detalhamento-acordo/11608?TituloAcordo=cibernética&tipoPesquisa=1&TipoAcordo=BL,TL,ML. Acesso em: 18 abr. 2021.

PYNNÖNIEMI, Katri. **Russia and the Nordic region**: challenges and prospects for cooperation between the EU and Russia. [S.I.]: Nordika Programme, 2013. Disponível em: https://www.files.ethz.ch/isn/175331/201329.pdf. Acesso em: 13 set. 2020.

PYNNÖNIEMI, Katri. The Asymmetric Approach in Russian Security Strategy: implications for the nordic countries. **Terrorism And Political Violence**, [S.l.], v. 31, n. 1, p. 154-167, 2 jan. 2019. Informa UK Limited. http://dx.doi.org/10.1080/09546553.2018.1555995.

REUTERS. **Germany, Brazil to propose anti-spying resolution at U.N.** 2013. Disponível em: https://www.reuters.com/article/us-usa-surveillance-un-idUSBRE99P01D20131026. Acesso em: 19 abr. 2021.

RID, Thomas. Cyber War Will Not Take Place. Journal Of Strategic Studies, [S.l.], v. 35, n. 1, p.5-32, fev. 2012. Informa UK Limited. http://dx.doi.org/10.1080/01402390.2011.608939.

RINGSMOSE, Jens. Investing in Fighters and Alliances. **International Journal**: Canada's Journal of Global Policy Analysis, [S.l.], v. 68, n. 1, p. 93-110, mar. 2013. SAGE Publications. http://dx.doi.org/10.1177/002070201306800107.

ROCHA, Antonio Jorge Ramalho da. Prioridades claras, necessidades ocultas e o Plano Estratégico Nacional de Defesa. Revista On-line Liberdade e Cidadania, [S.l.], v. 2, n. , p.1-1, dez. 2008. Disponível em: <https://www.flc.org.br/revista/materias_viewd17a.html?id=%7B3203F4E0-3260-4783-8F5B-B877B480E8A3%7D>. Acesso em: 18 nov. 2019.

ROCHA, Antonio Jorge Ramalho da. Política externa e política de defesa no Brasil: Civis e militares, prioridades e a participação em missões de paz. E-cadernos Ces, [S.l.], n. 06, p.142-158, 1 dez. 2009. OpenEdition. http://dx.doi.org/10.4000/eces.359. Disponível em: <https://journals.openedition.org/eces/359>. Acesso em: 18 nov. 2019.

ROCHEFORT, Alex. Regulating Social Media Platforms: a comparative policy analysis. Communication Law And Policy, [S.l.], v. 25, n. 2, p. 225-260, 2 abr. 2020. Informa UK Limited. http://dx.doi.org/10.1080/10811680.2020.1735194.

RUDZIT, Gunther. O debate teórico em segurança internacional: mudanças frente ao terrorismo?. Civitas, Porto Alegre, v. 5, n. 2, p. 297-323, jul. 2005.

RUDZIT, Gunther; NOGAMI, Otto. Segurança e Defesa Nacionais: conceitos básicos para uma análise. **Revista Brasileira de Política Internacional**, [S.l.], v. 53, n. 1, p. 5-24, jul. 2010. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s0034-73292010000100001.

RYAN, Mick. The Intellectual Edge: a competitive advantage for future war and strategic competition. Joint Force Quarterly, [S.l.], v. 96, n. 1, p. 6-11, jan. 2020.

SAMPLES, John. Why the Government Should Not Regulate Content Moderation of Social Media. Disponível em: https://www.cato.org/publications/policy-analysis/why-government-should-not-regulate-content-moderation-social-media. Acesso em: 09 abr. 2019.

SAMUEL J. BRANNEN. Global Security Forum. **Twin Pillars**: upholding national security and national innovation in emerging technologies governance. Washington: Center For Strategic And International Studies, 2019. Disponível em: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/200123_Brannen_TwinPillars_WEB_FINAL.pdf?eljUpAKOjVauOujYfnvuSGDK0xvsQGZF. Acesso em: 7 jun. 2020.

SAXI, Håkon Lunde; SUNDELIUS, Bengt; SWANEY, Brett. Baltics Left of Bang: nordic total defense and implications for the baltic sea region. Strategic Forum: National Defense University, [S.l.], v. 1, n. 304, p. 1-20, jan. 2020. Disponível em: https://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-304.pdf. Acesso em: 19 set. 2020.

SAYGIN, Ayse Pinar; CICEKLI, Ilyas; AKMAN, Varol. Turing Test: 50 years later. Minds And Machines, [s.l.], v. 10, n. 4, p. 463-518, 2000. Springer Science and Business Media LLC. http://dx.doi.org/10.1023/a:1011288000451.

SCHMIDT-FELZMANN, Anke. More than 'Just' Disinformation: Russia's information operations in the nordic region. In: ČIžIK, Tomáš (ed.). **Information Warfare**: new security challenge for europe. Bratislava: Centre For European And North Atlantic Affairs, 2017. p. 32-67. Disponível em: https://www.researchgate.net/profile/Anke_Schmidt-Felzmann/publication/316526667_More_than_'just'_disinformation_Russia's_information_operations_in_the_Nordic_region/links/590235e2a6fdcc8ed511850f/More-than-just-disinformation-Russias-information-operations-in-the-Nordic-region.pdf. Acesso em: 13 set. 2020.

SHABAZ, Adrian; FUNK, Allie. The Crisis of Social Media. [S.l.]: Freedom House, 2019. 32 p. (Freedom on the net 2019). Disponível em: https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf. Acesso em: 01 maio 2020.

SHIRES, James. Enacting Expertise: ritual and risk in cybersecurity. Politics And Governance, [S.l.], v. 6, n. 2, p. 31, 11 jun. 2018. Cogitatio. http://dx.doi.org/10.17645/pag.v6i2.1329.

SHIRES, James. Cyber-noir: cybersecurity and popular culture. Contemporary Security Policy, [S.l.], v. 41, n. 1, p. 82-107, 22 set. 2019. Informa UK Limited. http://dx.doi.org/10.1080/13523260.2019.1670006.

SILVA, Julio Cezar Barreto Leite da. Guerra Cibernética: a Guerra no Quinto Domínio, Conceituação e Princípios. Revista da Escola de Guerra Naval, Rio de Janeiro, v. 20, n. 1, p.193-211, jan. 2014. Disponível em: <file:///C:/Users/Raquel/Downloads/194-560-1-SM.pdf>. Acesso em: 21 set. 2019.

SIMÓN, Patrícia. '**A extrema-direita construiu as melhores máquinas de guerra digitais'**. 2020. Disponível em: http://www.ihu.unisinos.br/595971-a-extrema-direita-construiu-as-melhores-maquinas-de-guerra-digitais. Acesso em: 12 abr. 2021.

SINGLETON, F.. Finland after Kekkonen. **The World Today**, [S.l.], v. 38, n. 3, p. 90-96, mar. 1982. Published by the Royal Institute of International Affairs.

STEVENS, Clare. Assembling cybersecurity: the politics and materiality of technical malware reports and the case of stuxnet. Contemporary Security Policy, [S.l.], v. 41, n. 1, p.

129-152, 15 out. 2019. Informa UK Limited. http://dx.doi.org/10.1080/13523260.2019.1675258.

STRACHAN, Hew. The Changing Character of War. [S.l.]: Europaeum, 2006. Disponível em: <https://europaeum.org/wp-content/uploads/2017/09/The-Changing-Character-of-War-Hew-Strachan-Europaeum-Lecture-2006.pdf>. Acesso em: 11 out. 2019.

SUÉCIA. **A Completely Connected Sweden by 2025**: a broadband strategy. Estocolmo: Government Offices Of Sweden, 2016a. Disponível em: https://www.government.se/496173/contentassets/afe9f1cfeaac4e39abcdd3b82d9bee5d/sweden-completely-connected-by-2025-eng.pdf. Acesso em: 19 fev. 2021.

SUÉCIA. **Collaborating for Knowledge**. Estocolmo: Government Offices Of Sweden, 2016b.

SUÉCIA. **For sustainable digital transformation in Sweden**: a digital strategy. Estocolmo: Government Offices Of Sweden, 2017b. Disponível em: https://www.government.se/49c292/contentassets/117aec2b9bf44d758564506c2d99e825/2017_digitaliseringsstrategin_faktablad_eng_webb-2.pdf. Acesso em: 19 fev. 2021.

SUÉCIA. **National approach to artificial intelligence**. Estocolmo: Government Offices Of Sweden, 2018a. Disponível em: https://www.government.se/4a7451/contentassets/fe2ba005fb49433587574c513a837fac/national-approach-to-artificial-intelligence.pdf. Acesso em: 31 jan. 2021.

SUÉCIA. Ministry Of Enterprise And Innovation. **Sweden to lead AI cooperation in Nordic-Baltic region**. 2018b. Disponível em: https://www.government.se/press-releases/2018/05/sweden-to-lead-ai-cooperation-in-nordic-baltic-region/. Acesso em: 19 fev. 2021.

SUÉCIA. Prime Minister's Office. **New Nordic cooperation on 5G**. 2018c. Disponível em: https://www.government.se/press-releases/2018/05/new-nordic-cooperation-on-5g/. Acesso em: 19 fev. 2021.

SUÉCIA. **Comprehensive cyber security action plan 2019–2022**. Estocolmo: Swedish Civil Contingencies Agency (MSB), 2019a. Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjvu5L9hcfuAhVdHLkGHfG3B4AQFjAAegQIAhAC&url=https%3A%2F%2Frib.msb.se%2Ffiler%2Fpdf%2F28898.pdf&usg=AOvVaw2qxM85r9wOvo6qEUsfVeGU. Acesso em: 31 jan. 2021.

SUÉCIA. Lei nº 2018:585, de 01 de abril de 2019. **Protective Security Act**. Estocolmo: Riksdag, 2019b.

SUÉCIA. **Statement of Government Policy in the Parliamentary Debate on Foreign Affairs**. Estocolmo: Government Of Sweden, 2020. Disponível em: https://www.government.se/4914f9/contentassets/60b51f6b598a4874bbfb3b0074d48ad8/utriksesdeklarationen2020_eng.pdf. Acesso em: 31 jan. 2021.

SULTAN, Oz. Tackling Disinformation, Online Terrorism, and Cyber Risks into the 2020s. **The Cyber Defense Review**, West Point, v. 4, n. 1, p. 43-60, mar. 2019. Disponível em: https://www.jstor.org/stable/pdf/26623066.pdf. Acesso em: 01 abr. 2021.

SUZOR, Nicolas. Digital Constitutionalism: using the rule of law to evaluate the legitimacy of governance by platforms. Social Media + Society, [S.l.], v. 4, n. 3, p. 205630511878781, jul. 2018. SAGE Publications. http://dx.doi.org/10.1177/2056305118787812.

TAILLAT, Stéphane; DOUZET, Frédérick. Collective security and strategic instability in the digital domain. Contemporary Security Policy, [S.l.], v. 40, n. 3, p. 362-367, 9 abr. 2019. Informa UK Limited. http://dx.doi.org/10.1080/13523260.2019.1602693.

TAILLAT, Stéphane. Disrupt and restraint: the evolution of cyber conflict and the implications for collective security. Contemporary Security Policy, [S.l.], v. 40, n. 3, p. 368-381, 26 fev. 2019. Informa UK Limited. http://dx.doi.org/10.1080/13523260.2019.1581458.

TANNO, Grace. A contribuição da Escola de Copenhague aos Estudos de Segurança Internacional. Contexto Internacional, Rio de Janeiro, v. 25, n. 1, p.47-80, jan. 2003. Disponível em: <http://www.scielo.br/pdf/cint/v25n1/v25n1a02.pdf>. Acesso em: 22 set. 2019.

THOMAS, Timothy L.. Comparing US, Russian and Chinese information operations concepts. Fort Leavenworth: Foreign Military Studies Office, 2004.

TUATHAIL, Gearóid Ó. Understanding critical geopolitics: geopolitics and risk society. Journal Of Strategic Studies, [S.l.], v. 22, n. 2-3, p. 107-124, jun. 1999. Informa UK Limited. http://dx.doi.org/10.1080/01402399908437756.

TURNER, Graeme. The media and democracy in the digital era: is this what we had in mind?. Media International Australia, [S.l.], v. 168, n. 1, p. 3-14, 29 jun. 2018. SAGE Publications. http://dx.doi.org/10.1177/1329878x18782987.

TUSIKOV, Natasha; HAGGART, Blayne. It's time for a new way to regulate social media platforms. Disponível em: https://theconversation.com/its-time-for-a-new-way-to-regulate-social-media-platforms-109413. Acesso em: 16 jan. 2019.

UNESCO. **Elaboration of a Recommendation on the ethics of artificial intelligence**. 2021. Disponível em: https://en.unesco.org/artificial-intelligence/ethics. Acesso em: 19 abr. 2021.

UNIÃO EUROPEIA. **EU Cybersecurity plan to protect open internet and online freedom and opportunity**: cyber security strategy and proposal for a directive. Cyber Security strategy and Proposal for a Directive. 2013. Disponível em: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security. Acesso em: 19 fev. 2021.

UNIÃO EUROPEIA. **Directive (EU) 2016/1148**. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148. Acesso em: 19 fev. 2021.

UNIÃO EUROPEIA. **The EU's Cybersecurity Strategy for the Digital Decade**: Joint Communication to the European Parliament and the Council. Bruxelas: Comissão Europeia, 2020. Disponível em: file:///C:/Users/racri/Downloads/JointCommunicationTheEUsCybersecurityStrategyfortheDigitalDecadepdf.pdf. Acesso em: 17 fev. 2021.

UNIÃO EUROPEIA. **Laws about Cybersecurity**. Disponível em: https://ec.europa.eu/digital-single-market/en/laws/75984/3587. Acesso em: 17 fev. 2021.

UNITED NATIONS SECRETARY-GENERAL'S HIGH-LEVEL PANEL ON DIGITAL COOPERATION. **The age of digital interdependence**. [S.l.]: United Nations, 2019. Disponível em: https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-for-web.pdf. Acesso em: 30 maio 2019.

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH. United Nations. **The United Nations, Cyberspace and International Peace and Security**. Genebra: Unidir Resources, 2017. Disponível em: <http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf>. Acesso em: 13 ago. 2019.

VALERIANO, Brandon; MANESS, Ryan C. The dynamics of cyber conflict between rival antagonists, 2001–11. Journal Of Peace Research, [S.l.], v. 51, n. 3, p.347-360, abr. 2014. SAGE Publications. http://dx.doi.org/10.1177/0022343313518940.

VALERIANO, Brandon; MANESS, Ryan C.. How We Stopped Worrying about Cyber Doom and Started Collecting Data. Politics And Governance, [S.l.], v. 6, n. 2, p.49-60, 11 jun. 2018a. Cogitatio. http://dx.doi.org/10.17645/pag.v6i2.1368. Disponível em: <https://www.cogitatiopress.com/politicsandgovernance/article/view/1368>. Acesso em: 17 ago. 2019.

VALERIANO, Brandon; MANESS, Ryan C.. International Relations Theory and Cyber Security: Threat, Conflict, and Ethics in an Emergent Domain. In: BROWN, Chris; ECKERSLEY, Robyn (Ed.). The Oxford Handbook of International Political Theory. [S.l.]: Oxford Handbooks Online, 2018b. Cap. 20. p. 259-272. Oxford University Press. http://dx.doi.org/10.1093/oxfordhb/9780198746928.013.19.

VAN RYTHOVEN, Eric. Learning to feel, learning to fear? Emotions, imaginaries, and limits in the politics of securitization. Security Dialogue, [S.l.], v. 46, n. 5, p.458-475, 27 maio 2015. SAGE Publications. http://dx.doi.org/10.1177/0967010615574766. Disponível em: <file:///C:/Users/Raquel/Downloads/0967010615574766.pdf>. Acesso em: 18 nov. 2019.

VIEIRA, Heloise Guarise. **A identidade de segurança brasileira nas relações com a Colômbia**: do Plano Colômbia ao tratado de 2009. 2014. 221 f. Dissertação (Mestrado) -

Curso de Relações Internacionais, Universidade Federal de Santa Catarina, Florianópolis, 2014.

VIEIRA, Heloise. A identidade de Segurança e Defesa brasileira: os limites do princípio de autodeterminação e da integração sul-americana. In: SEMINÁRIO INTERNACIONAL DE CIÊNCIA POLÍTICA, 1., 2015, Porto Alegre. Anais [...] . Porto Alegre: Ufrgs, 2015. p. 1-25.

WALL, David S.. Cybercrime and the culture of fear. Information, Communication & Society, [s.l.], v. 11, n. 6, p. 861-884, set. 2008. Informa UK Limited. http://dx.doi.org/10.1080/13691180802007788.

WEIBLE, Christopher M.; HEIKKILA, Tanya; DELEON, Peter; SABATIER, Paul A.. Understanding and influencing the policy process. Policy Sciences, [S.l.], v. 45, n. 1, p. 1-21, 18 nov. 2011. Springer Science and Business Media LLC. http://dx.doi.org/10.1007/s11077-011-9143-5.

WENDT, Alexander. Anarchy is what States Make of it: The Social Construction of Power Politics. International Organization, [S.l.], v. 46, n. 2, p.391-425, set. 1992.

WIGELL, Mikael. Democratic Deterrence: How to dissuade Hybrid Interference. Helsinki: Finnish Institute For International Affairs, 2019. Disponível em: <https://www.fiia.fi/en/publication/democratic-deterrence>. Acesso em: 21 out. 2019.

WILLIAMS, Michael C.. Words, Images, Enemies: Securitization and International Politics. International Studies Quarterly, Storrs, v. 47, n. 4, p.511-531, dez. 2003.

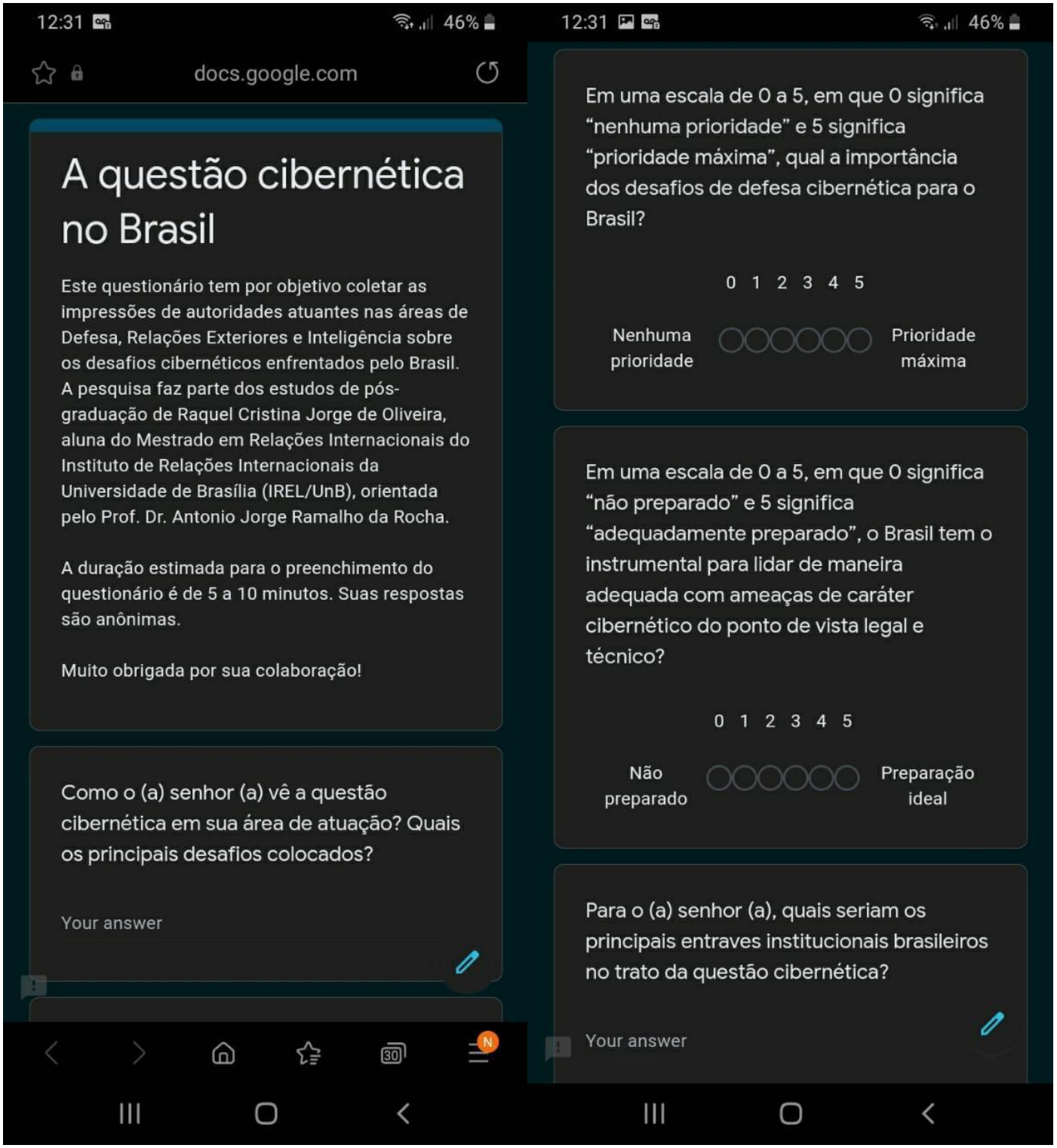
WITHER, James Kenneth. Back to the future? Nordic total defence concepts. **Defence Studies**, [S.L.], v. 20, n. 1, p. 61-81, 2 jan. 2020. Informa UK Limited. http://dx.doi.org/10.1080/14702436.2020.1718498.

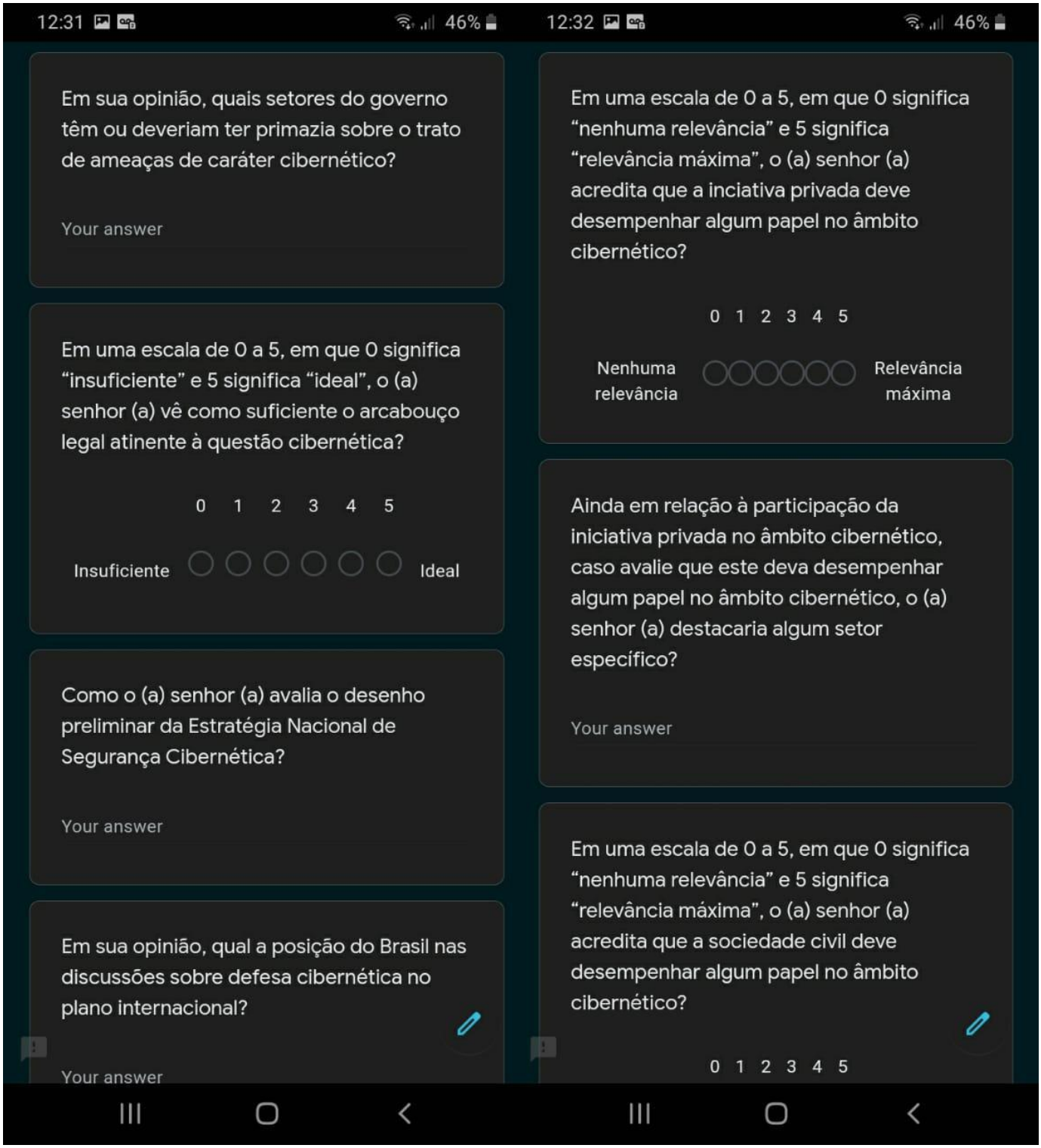
WONG, Yuna Huh *et al*. **Deterrence in the Age of Thinking Machines**. Santa Monica: Rand Corporation, 2020.

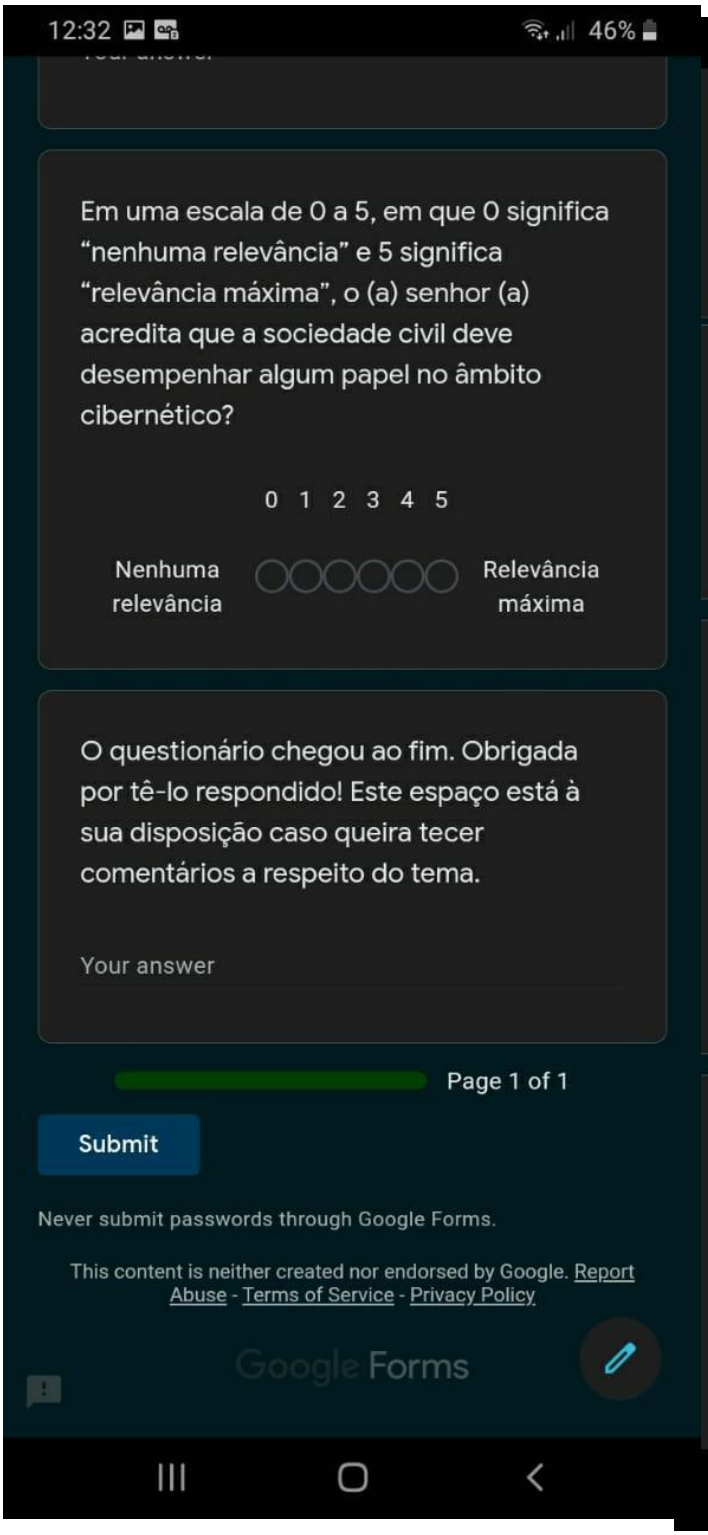
WORTZEL, Larry M.. China's Approach to Cyber Operations: Implications for the United States: Testimony before the Committee on Foreign Affairs. 2010. Disponível em: <https://www.uscc.gov/sites/default/files/Congressional_Testimonies/LarryWortzeltestimony-March2010.pdf>. Acesso em: 09 nov. 2019.

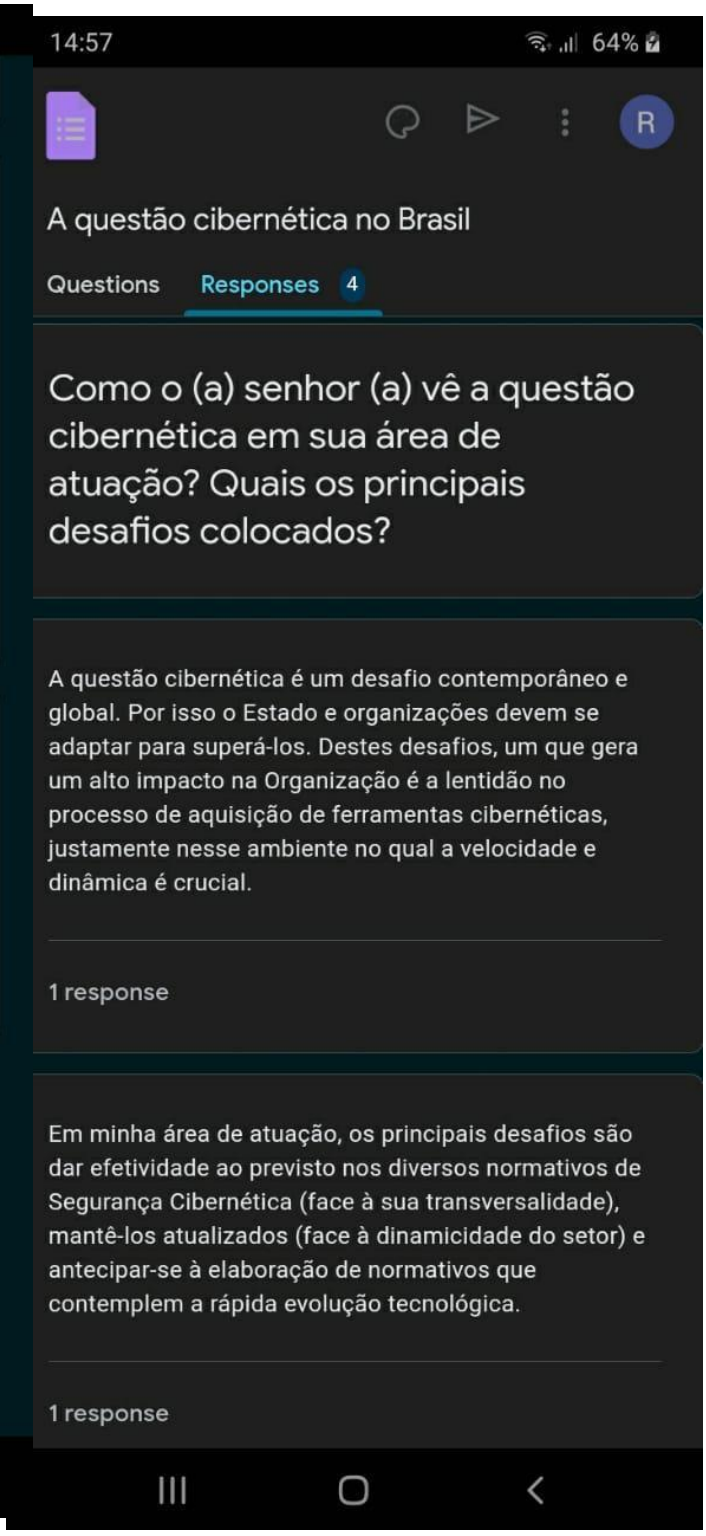
YOUNG, Kevin L; CARPENTER, Charli. Does Science Fiction Affect Political Fact? Yes and No: a survey experiment on "killer robots". International Studies Quarterly, [S.l.], v. 62, n. 3, p. 562-576, 20 ago. 2018. Oxford University Press (OUP). http://dx.doi.org/10.1093/isq/sqy028.

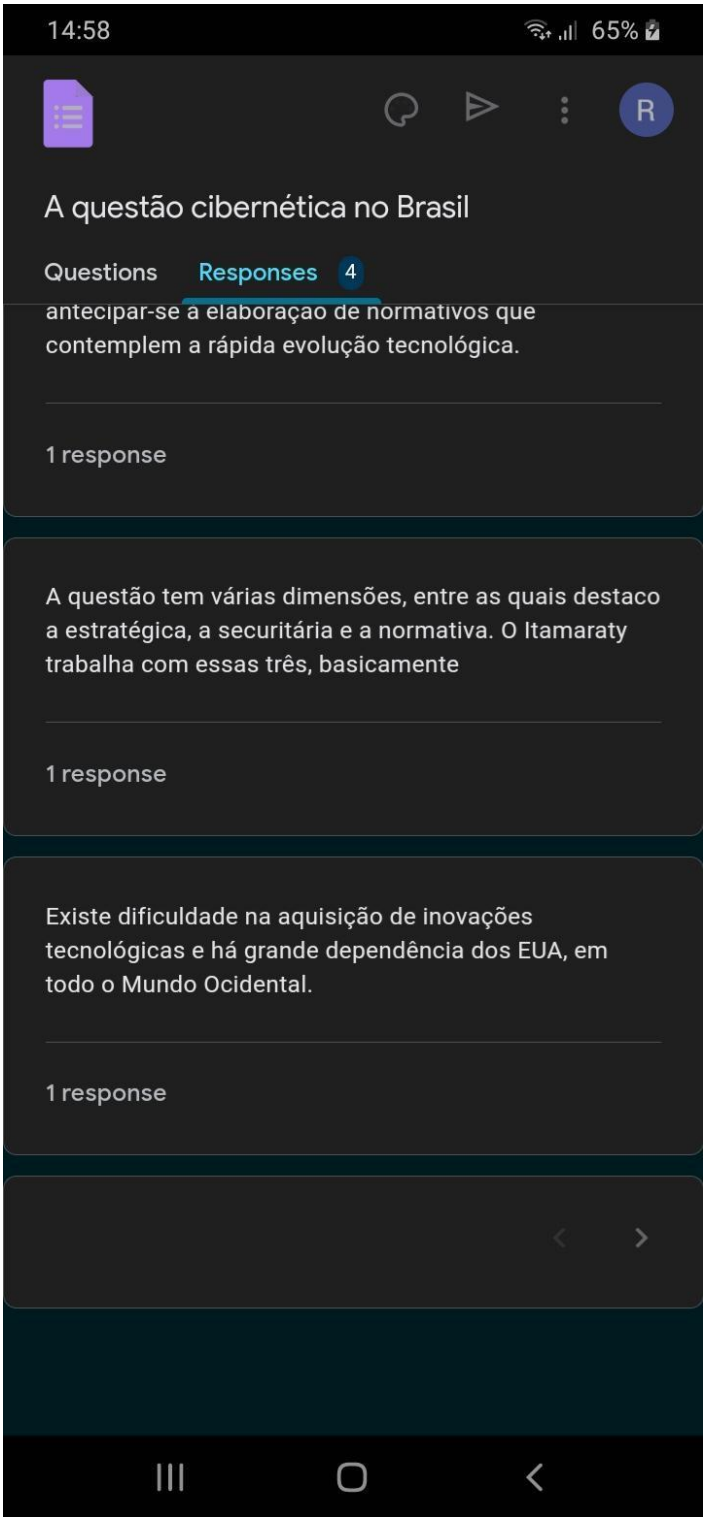
ANEXO A – Pesquisa via *Google Forms*

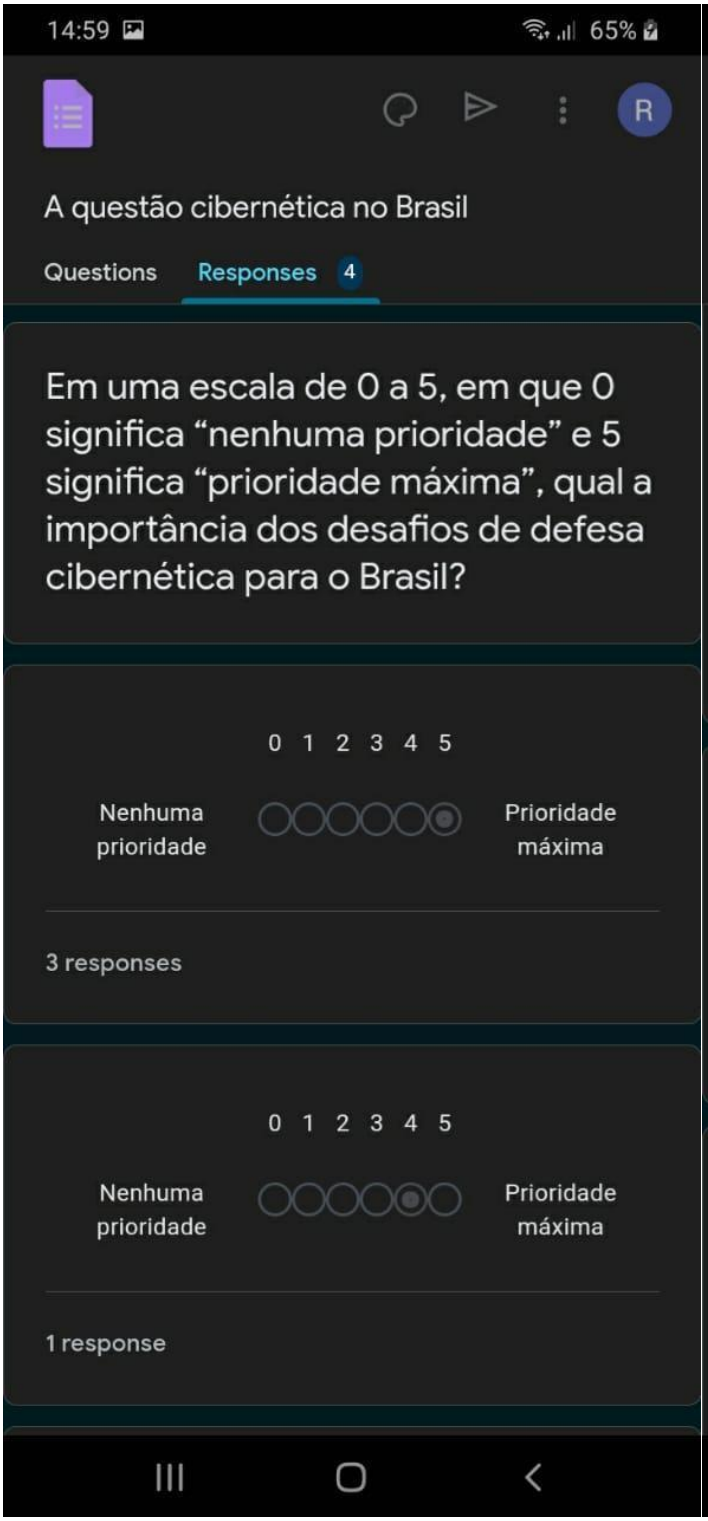


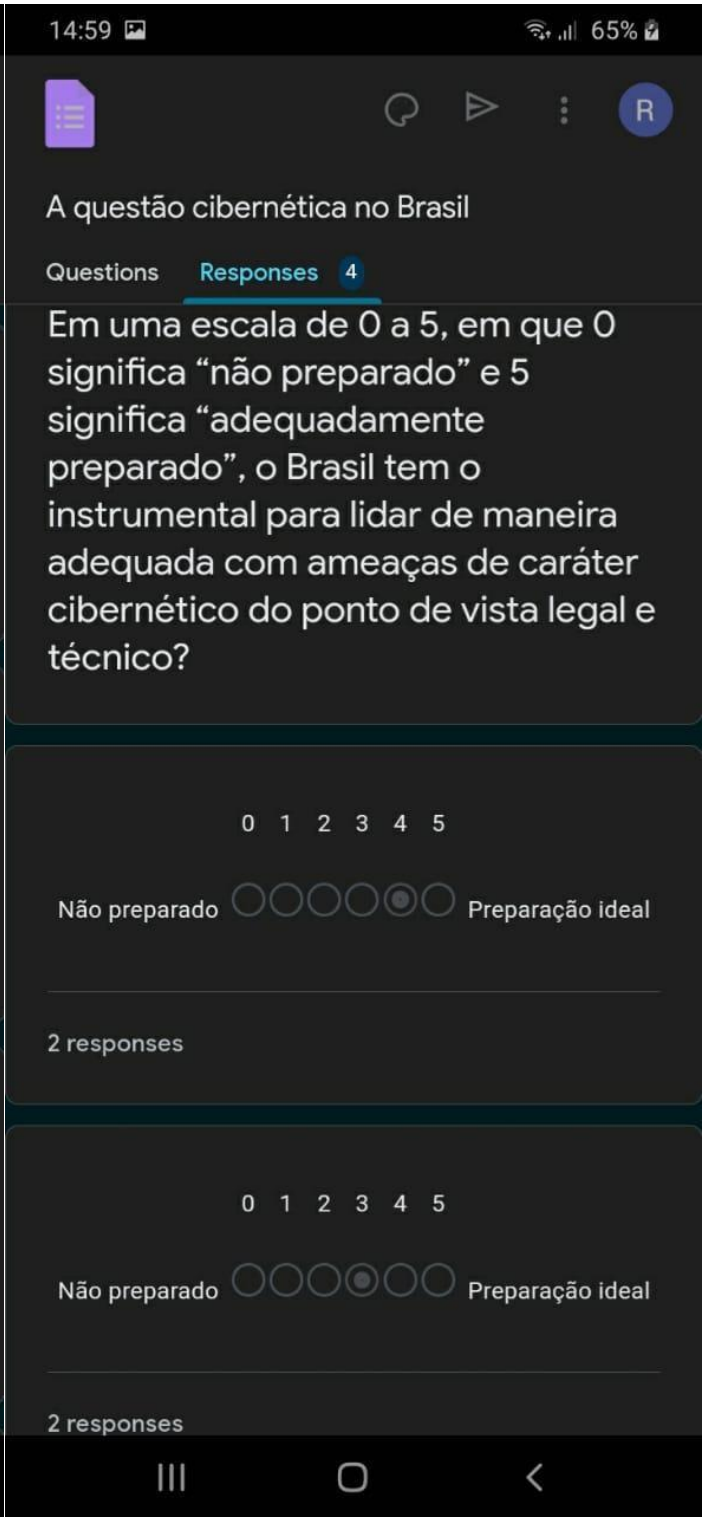

12:31
46%
Em sua opinião, quais setores do governo têm ou deveriam ter primazia sobre o trato de ameaças de caráter cibernético?
Your answer
Em uma escala de 0 a 5, em que 0 significa "insuficiente" e 5 significa "ideal", o (a) senhor (a) vê como suficiente o arcabouço legal atinente à questão cibernética?
0 1 2 3 4 5
Insuficiente
Ideal
Como o (a) senhor (a) avalia o desenho preliminar da Estratégia Nacional de Segurança Cibernética?
Your answer
Em sua opinião, qual a posição do Brasil nas discussões sobre defesa cibernética no plano internacional?
Your answer
12:32
46%
Em uma escala de 0 a 5, em que 0 significa "nenhuma relevância" e 5 significa "relevância máxima", o (a) senhor (a) acredita que a inciativa privada deve desempenhar algum papel no âmbito cibernético?
0 1 2 3 4 5
Nenhuma relevância
Relevância máxima
Ainda em relação à participação da iniciativa privada no âmbito cibernético, caso avalie que este deva desempenhar algum papel no âmbito cibernético, o (a) senhor (a) destacaria algum setor específico?
Your answer
Em uma escala de 0 a 5, em que 0 significa "nenhuma relevância" e 5 significa "relevância máxima", o (a) senhor (a) acredita que a sociedade civil deve desempenhar algum papel no âmbito cibernético?
0 1 2 3 4 5

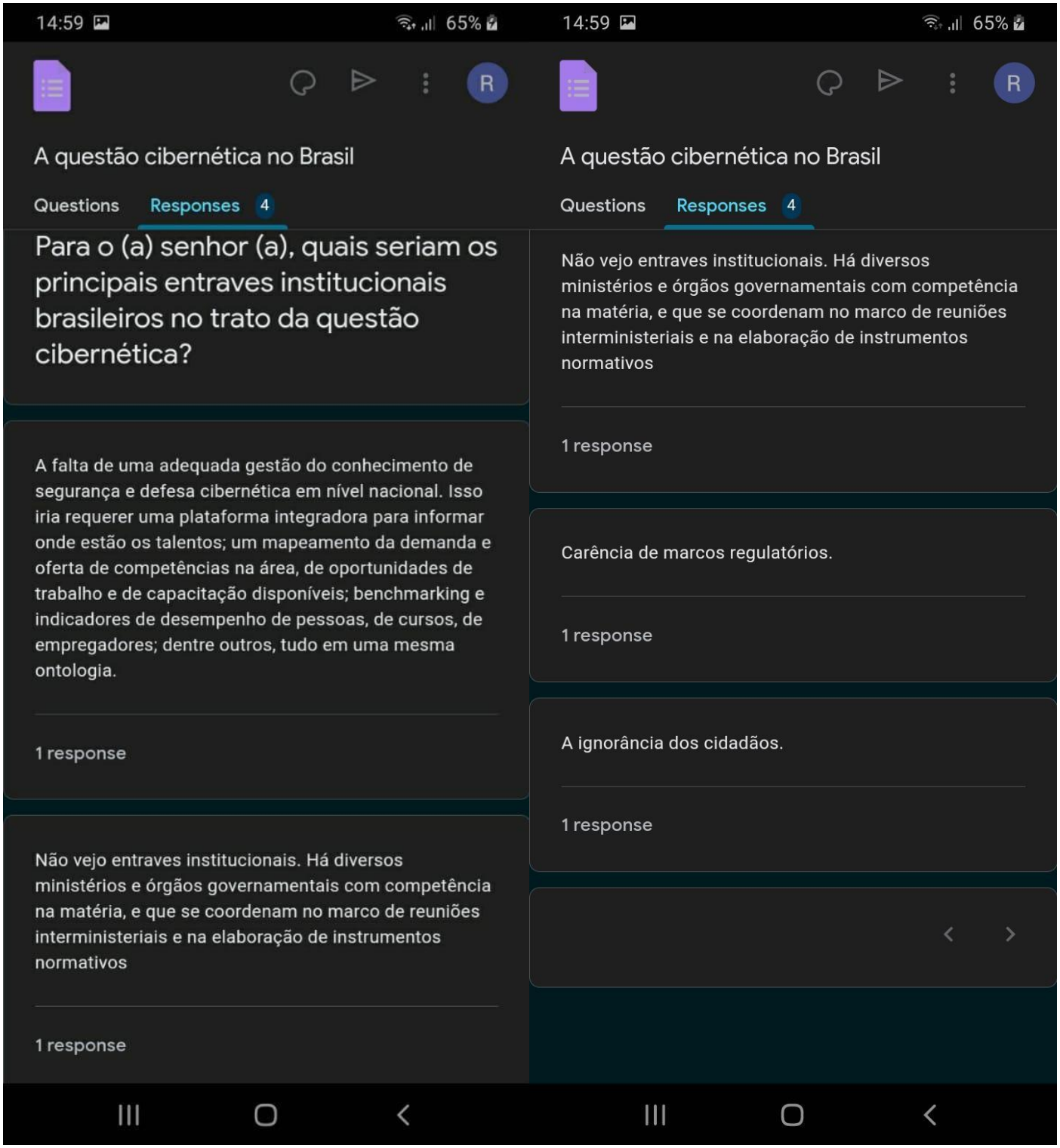

12:32
46%
Em uma escala de 0 a 5, em que 0 significa "nenhuma relevância" e 5 significa "relevância máxima", o (a) senhor (a) acredita que a sociedade civil deve desempenhar algum papel no âmbito cibernético?
0 1 2 3 4 5
Nenhuma relevância
Relevância máxima
O questionário chegou ao fim. Obrigada por tê-lo respondido! Este espaço está à sua disposição caso queira tecer comentários a respeito do tema.
Your answer
Page 1 of 1
Submit
Never submit passwords through Google Forms.
This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy
Google Forms

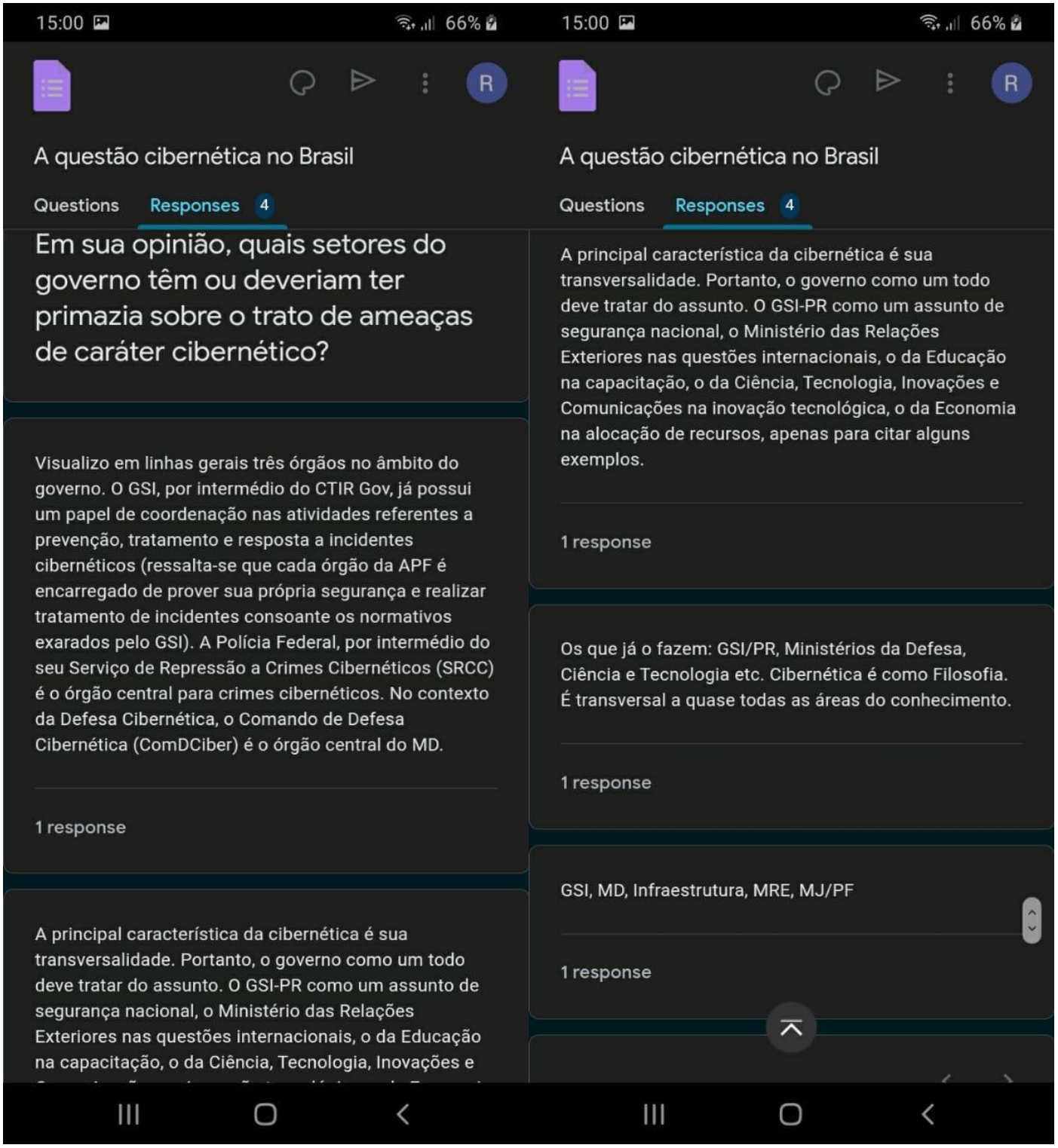

14:57
64%
A questão cibernética no Brasil
Questions
Responses 4
Como o (a) senhor (a) vê a questão cibernética em sua área de atuação? Quais os principais desafios colocados?
A questão cibernética é um desafio contemporâneo e global. Por isso o Estado e organizações devem se adaptar para superá-los. Destes desafios, um que gera um alto impacto na Organização é a lentidão no processo de aquisição de ferramentas cibernéticas, justamente nesse ambiente no qual a velocidade e dinâmica é crucial.
1 response
Em minha área de atuação, os principais desafios são dar efetividade ao previsto nos diversos normativos de Segurança Cibernética (face à sua transversalidade), mantê-los atualizados (face à dinamicidade do setor) e antecipar-se à elaboração de normativos que contemplem a rápida evolução tecnológica.
1 response

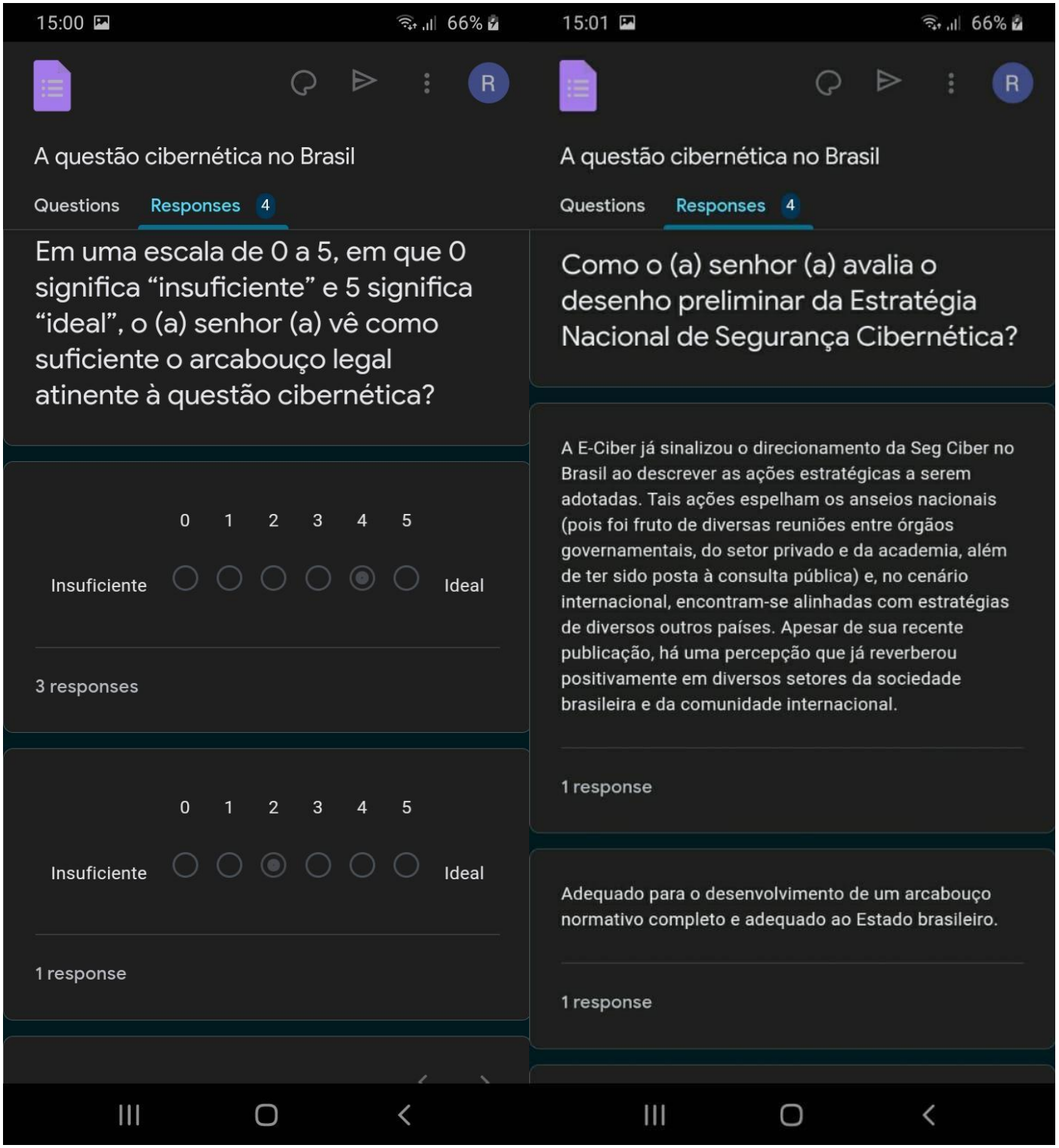

14:58
65%
R
A questão cibernética no Brasil
Questions
Responses 4
antecipar-se a elaboração de normativos que contemplem a rápida evolução tecnológica.
1 response
A questão tem várias dimensões, entre as quais destaco a estratégica, a securitária e a normativa. O Itamaraty trabalha com essas três, basicamente
1 response
Existe dificuldade na aquisição de inovações tecnológicas e há grande dependência dos EUA, em todo o Mundo Ocidental.
1 response

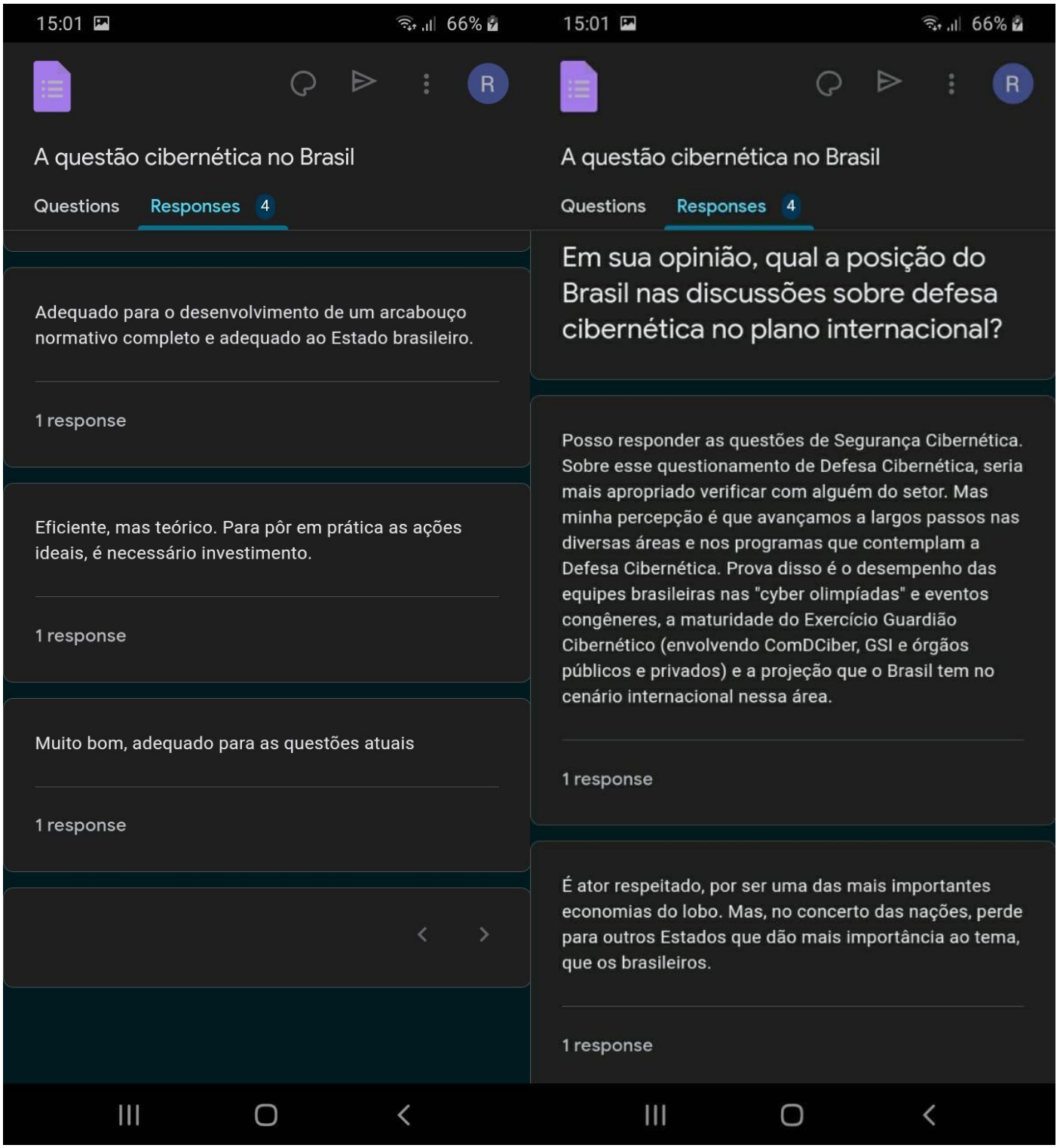

14:59
65%
R
A questão cibernética no Brasil
Questions
Responses 4
Em uma escala de 0 a 5, em que 0 significa “nenhuma prioridade” e 5 significa “prioridade máxima”, qual a importância dos desafios de defesa cibernética para o Brasil?
0 1 2 3 4 5
Nenhuma prioridade
Prioridade máxima
3 responses
0 1 2 3 4 5
Nenhuma prioridade
Prioridade máxima
1 response

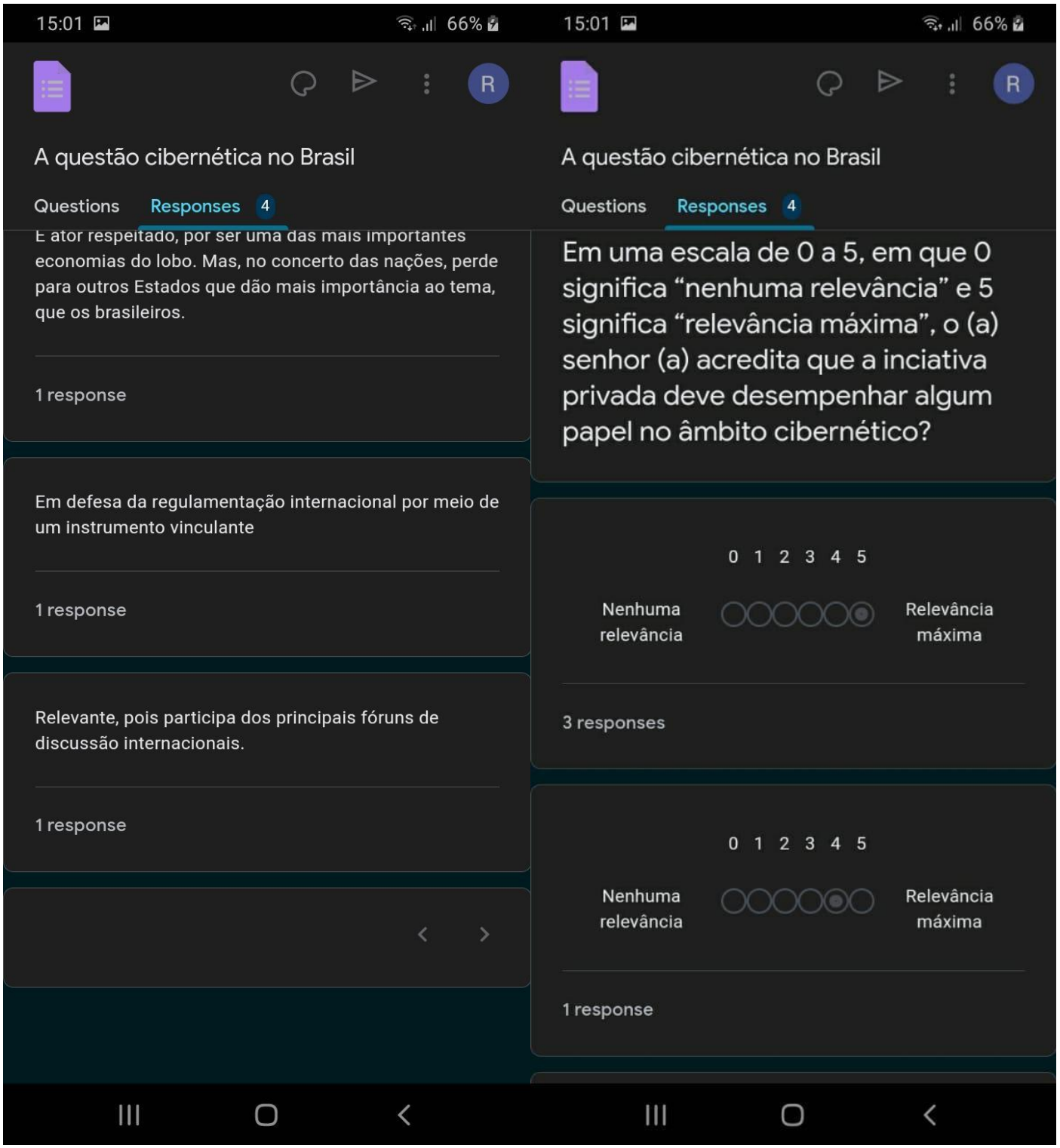

14:59
65%
R
A questão cibernética no Brasil
Questions
Responses 4
Em uma escala de 0 a 5, em que 0 significa “não preparado” e 5 significa “adequadamente preparado”, o Brasil tem o instrumental para lidar de maneira adequada com ameaças de caráter cibernético do ponto de vista legal e técnico?
0 1 2 3 4 5
Não preparado
Preparação ideal
2 responses
0 1 2 3 4 5
Não preparado
Preparação ideal
2 responses

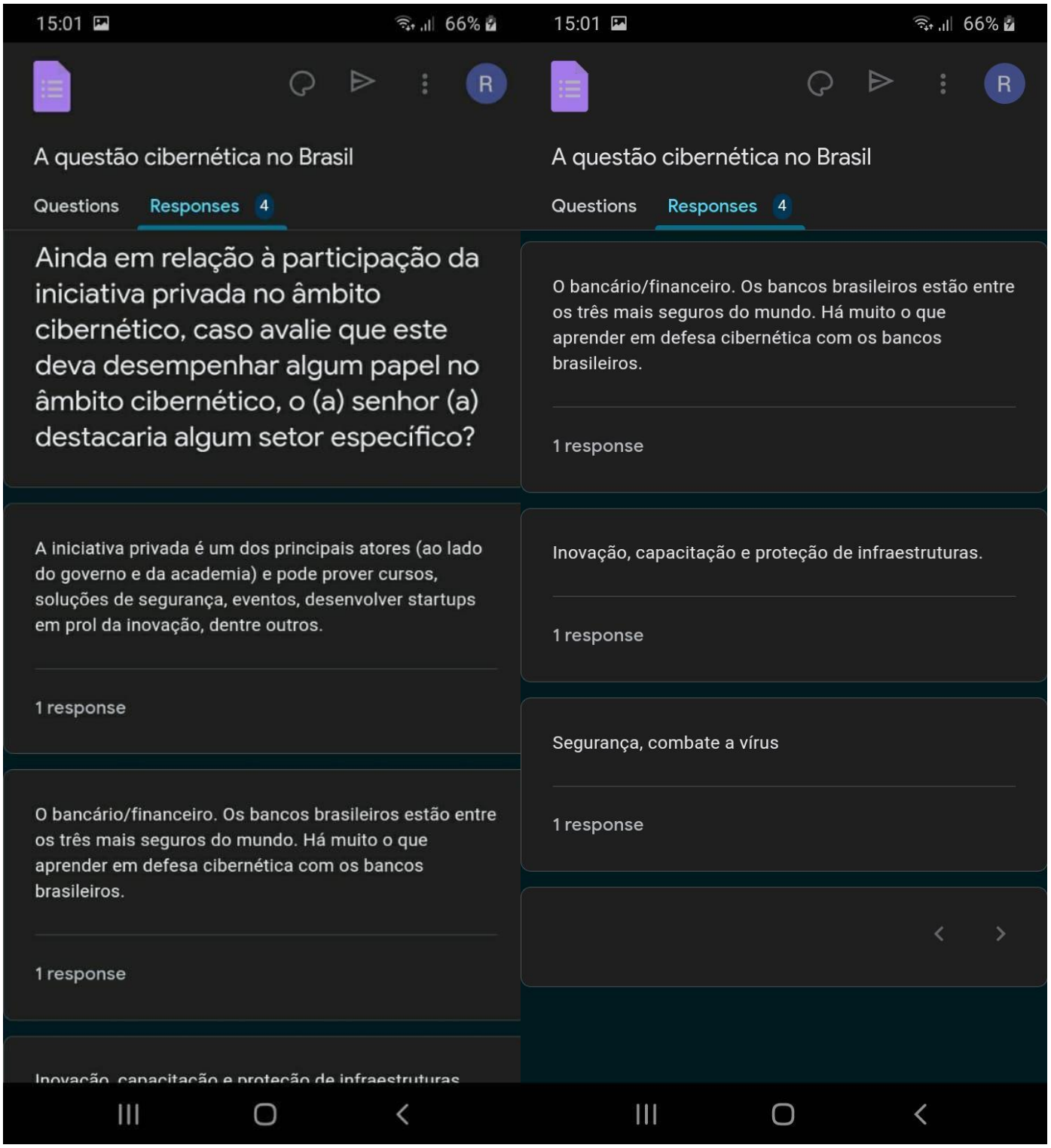

14:59
65%
A questão cibernética no Brasil
Questions
Responses 4
Para o (a) senhor (a), quais seriam os principais entraves institucionais brasileiros no trato da questão cibernética?
A falta de uma adequada gestão do conhecimento de segurança e defesa cibernética em nível nacional. Isso iria requerer uma plataforma integradora para informar onde estão os talentos; um mapeamento da demanda e oferta de competências na área, de oportunidades de trabalho e de capacitação disponíveis; benchmarking e indicadores de desempenho de pessoas, de cursos, de empregadores; dentre outros, tudo em uma mesma ontologia.
1 response
Não vejo entraves institucionais. Há diversos ministérios e órgãos governamentais com competência na matéria, e que se coordenam no marco de reuniões interministeriais e na elaboração de instrumentos normativos
1 response
14:59
65%
A questão cibernética no Brasil
Questions
Responses 4
Não vejo entraves institucionais. Há diversos ministérios e órgãos governamentais com competência na matéria, e que se coordenam no marco de reuniões interministeriais e na elaboração de instrumentos normativos
1 response
Carência de marcos regulatórios.
1 response
A ignorância dos cidadãos.
1 response

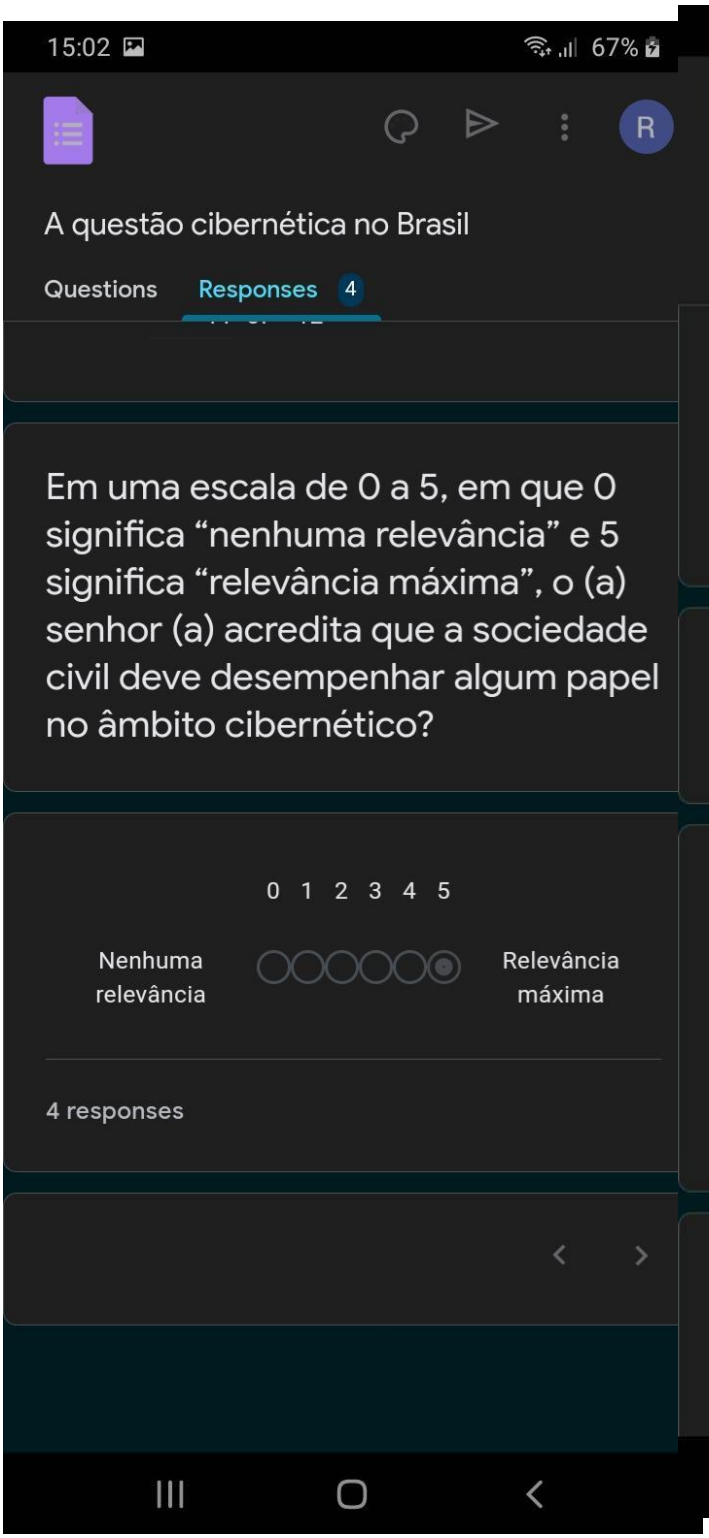

15:00
66%
A questão cibernética no Brasil
Questions
Responses 4
Em sua opinião, quais setores do governo têm ou deveriam ter primazia sobre o trato de ameaças de caráter cibernético?
Visualizo em linhas gerais três órgãos no âmbito do governo. O GSI, por intermédio do CTIR Gov, já possui um papel de coordenação nas atividades referentes a prevenção, tratamento e resposta a incidentes cibernéticos (ressalta-se que cada órgão da APF é encarregado de prover sua própria segurança e realizar tratamento de incidentes consoante os normativos exarados pelo GSI). A Polícia Federal, por intermédio do seu Serviço de Repressão a Crimes Cibernéticos (SRCC) é o órgão central para crimes cibernéticos. No contexto da Defesa Cibernética, o Comando de Defesa Cibernética (ComDCiber) é o órgão central do MD.
1 response
A principal característica da cibernética é sua transversalidade. Portanto, o governo como um todo deve tratar do assunto. O GSI-PR como um assunto de segurança nacional, o Ministério das Relações Exteriores nas questões internacionais, o da Educação na capacitação, o da Ciência, Tecnologia, Inovações e
15:00
66%
A questão cibernética no Brasil
Questions
Responses 4
A principal característica da cibernética é sua transversalidade. Portanto, o governo como um todo deve tratar do assunto. O GSI-PR como um assunto de segurança nacional, o Ministério das Relações Exteriores nas questões internacionais, o da Educação na capacitação, o da Ciência, Tecnologia, Inovações e Comunicações na inovação tecnológica, o da Economia na alocação de recursos, apenas para citar alguns exemplos.
1 response
Os que já o fazem: GSI/PR, Ministérios da Defesa, Ciência e Tecnologia etc. Cibernética é como Filosofia. É transversal a quase todas as áreas do conhecimento.
1 response
GSI, MD, Infraestrutura, MRE, MJ/PF
1 response

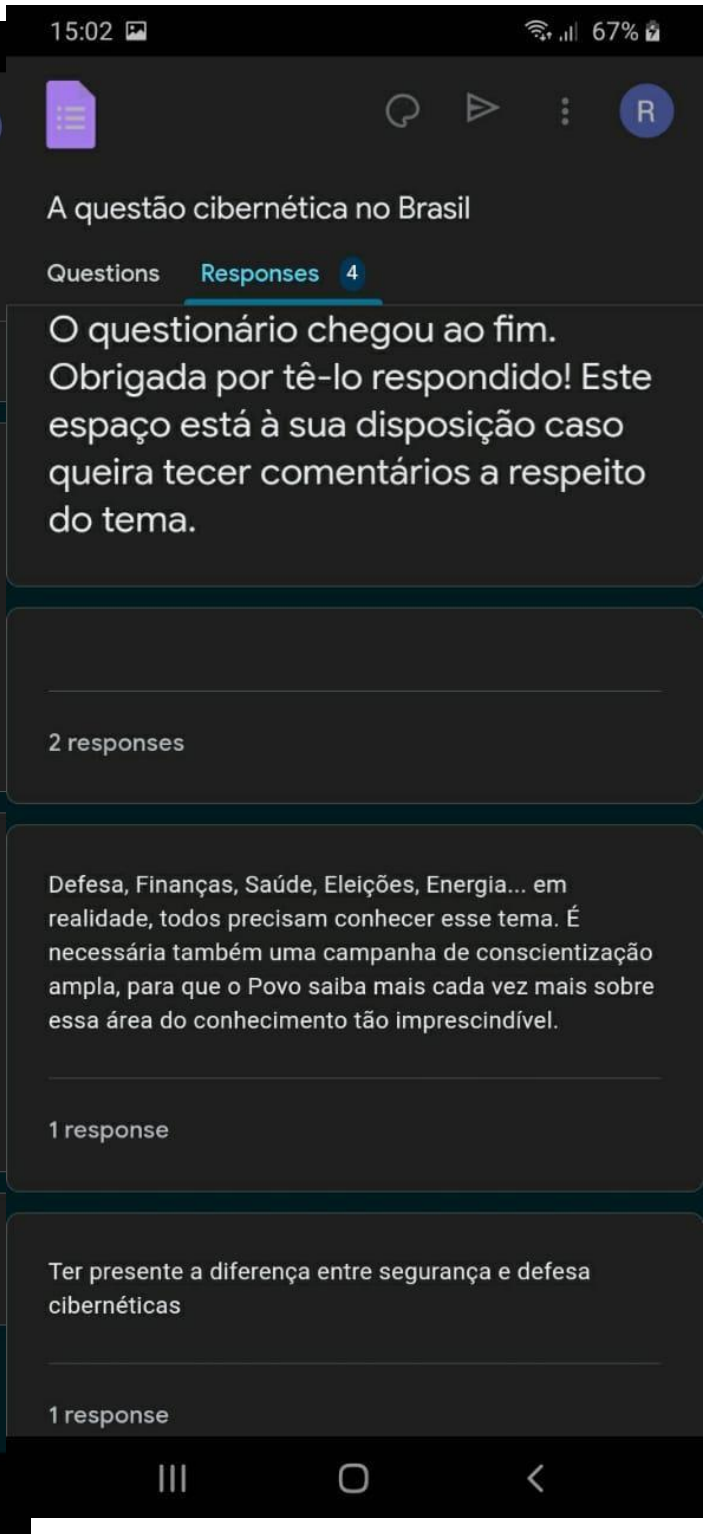

15:00
66%
A questão cibernética no Brasil
Questions
Responses 4
Em uma escala de 0 a 5, em que 0 significa "insuficiente" e 5 significa "ideal", o (a) senhor (a) vê como suficiente o arcabouço legal atinente à questão cibernética?
0 1 2 3 4 5
Insuficiente
Ideal
3 responses
0 1 2 3 4 5
Insuficiente
Ideal
1 response
15:01
66%
A questão cibernética no Brasil
Questions
Responses 4
Como o (a) senhor (a) avalia o desenho preliminar da Estratégia Nacional de Segurança Cibernética?
A E-Ciber já sinalizou o direcionamento da Seg Ciber no Brasil ao descrever as ações estratégicas a serem adotadas. Tais ações espelham os anseios nacionais (pois foi fruto de diversas reuniões entre órgãos governamentais, do setor privado e da academia, além de ter sido posta à consulta pública) e, no cenário internacional, encontram-se alinhadas com estratégias de diversos outros países. Apesar de sua recente publicação, há uma percepção que já reverberou positivamente em diversos setores da sociedade brasileira e da comunidade internacional.
1 response
Adequado para o desenvolvimento de um arcabouço normativo completo e adequado ao Estado brasileiro.
1 response


15:01
66%
A questão cibernética no Brasil
Questions
Responses 4
Adequado para o desenvolvimento de um arcabouço normativo completo e adequado ao Estado brasileiro.
1 response
Eficiente, mas teórico. Para pôr em prática as ações ideais, é necessário investimento.
1 response
Muito bom, adequado para as questões atuais
1 response
15:01
66%
A questão cibernética no Brasil
Questions
Responses 4
Em sua opinião, qual a posição do Brasil nas discussões sobre defesa cibernética no plano internacional?
Posso responder as questões de Segurança Cibernética. Sobre esse questionamento de Defesa Cibernética, seria mais apropriado verificar com alguém do setor. Mas minha percepção é que avançamos a largos passos nas diversas áreas e nos programas que contemplam a Defesa Cibernética. Prova disso é o desempenho das equipes brasileiras nas "cyber olimpíadas" e eventos congêneres, a maturidade do Exercício Guardião Cibernético (envolvendo ComDCiber, GSI e órgãos públicos e privados) e a projeção que o Brasil tem no cenário internacional nessa área.
1 response
É ator respeitado, por ser uma das mais importantes economias do lobo. Mas, no concerto das nações, perde para outros Estados que dão mais importância ao tema, que os brasileiros.
1 response


15:01
66%
A questão cibernética no Brasil
Questions
Responses 4
É ator respeitado, por ser uma das mais importantes economias do lobo. Mas, no concerto das nações, perde para outros Estados que dão mais importância ao tema, que os brasileiros.
1 response
Em defesa da regulamentação internacional por meio de um instrumento vinculante
1 response
Relevante, pois participa dos principais fóruns de discussão internacionais.
1 response
15:01
66%
A questão cibernética no Brasil
Questions
Responses 4
Em uma escala de 0 a 5, em que 0 significa "nenhuma relevância" e 5 significa "relevância máxima", o (a) senhor (a) acredita que a inciativa privada deve desempenhar algum papel no âmbito cibernético?
0 1 2 3 4 5
Nenhuma relevância
Relevância máxima
3 responses
0 1 2 3 4 5
Nenhuma relevância
Relevância máxima
1 response


15:01
66%
A questão cibernética no Brasil
Questions
Responses 4
Ainda em relação à participação da iniciativa privada no âmbito cibernético, caso avalie que este deva desempenhar algum papel no âmbito cibernético, o (a) senhor (a) destacaria algum setor específico?
A iniciativa privada é um dos principais atores (ao lado do governo e da academia) e pode prover cursos, soluções de segurança, eventos, desenvolver startups em prol da inovação, dentre outros.
1 response
O bancário/financeiro. Os bancos brasileiros estão entre os três mais seguros do mundo. Há muito o que aprender em defesa cibernética com os bancos brasileiros.
1 response
Inovação, capacitação e proteção de infraestruturas
15:01
66%
A questão cibernética no Brasil
Questions
Responses 4
O bancário/financeiro. Os bancos brasileiros estão entre os três mais seguros do mundo. Há muito o que aprender em defesa cibernética com os bancos brasileiros.
1 response
Inovação, capacitação e proteção de infraestruturas.
1 response
Segurança, combate a vírus
1 response


15:02
67%
R
A questão cibernética no Brasil
Questions
Responses 4
Em uma escala de 0 a 5, em que 0 significa “nenhuma relevância” e 5 significa “relevância máxima”, o (a) senhor (a) acredita que a sociedade civil deve desempenhar algum papel no âmbito cibernético?
0 1 2 3 4 5
Nenhuma relevância
Relevância máxima
4 responses


15:02
67%
R
A questão cibernética no Brasil
Questions
Responses 4
O questionário chegou ao fim. Obrigada por tê-lo respondido! Este espaço está à sua disposição caso queira tecer comentários a respeito do tema.
2 responses
Defesa, Finanças, Saúde, Eleições, Energia... em realidade, todos precisam conhecer esse tema. É necessária também uma campanha de conscientização ampla, para que o Povo saiba mais cada vez mais sobre essa área do conhecimento tão imprescindível.
1 response
Ter presente a diferença entre segurança e defesa cibernéticas
1 response