UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SOCIOECONÔMICO
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS
CURSO DE RELAÇÕES INTERNACIONAIS

Amanda de Brito

Estratégias de defesa cibernética: como Coreia do Sul e Brasil entendem poder cibernético

Florianópolis
2023

Amanda de Brito

Estratégias de defesa cibernética: como Coreia do Sul e Brasil entendem poder cibernético

Trabalho Conclusão do Curso de Graduação em Relações Internacionais do Centro de Socioeconômico da Universidade Federal de Santa Catarina como requisito para a obtenção do título de Bacharel em Relações Internacionais
Orientador: Profa. Dra. Danielle Jacon Ayres Pinto

Florianópolis
2023

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Brito, Amanda de
Estratégias de defesa cibernética : como Coreia do Sul e Brasil entendem poder cibernético / Amanda de Brito ; orientadora, Danielle Jacon Ayres Pinto , 2023.
99 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro Sócio Econômico, Graduação em Relações Internacionais, Florianópolis, 2023.

Inclui referências.

1. Relações Internacionais. 2. Poder cibernético. 3. Defesa cibernética. 4. Coreia do Sul. 5. Brasil. I. Ayres Pinto , Danielle Jacon . II. Universidade Federal de Santa Catarina. Graduação em Relações Internacionais. III. Título.

Amanda de Brito

Estratégias de defesa cibernética: como Coreia do Sul e Brasil entendem poder cibernético

Florianópolis, 16 de março de 2023.

O presente Trabalho de Conclusão de Curso foi avaliado e aprovado pela banca examinadora composta pelos seguintes membros:

Prof. Dra. Danielle Jacon Ayres Pinto (Orientadora)
Universidade Federal de Santa Catarina

Prof. Dra. Graciela de Conti Pagliari
Universidade Federal de Santa Catarina

Ma. Jéssica Maria Grassi
Universidade Federal de Santa Catarina (UFSC)

Certifico que esta é a **versão original e final** do Trabalho de Conclusão de Curso que foi julgado adequado para obtenção do título de Bacharel em Relações Internacionais por mim e pelos demais membros da banca examinadora.

ICP-Edu
Documento assinado digitalmente
Danielle Jacon Ayres Pinto
Data: 17/03/2023 16:02:25-0300
CPF: ***.367.488-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Dra. Danielle Jacon Ayres Pinto
Orientadora

Florianópolis, 2023

Este trabalho é dedicado à Deolinda Maria de Brito.

AGRADECIMENTOS

Gostaria de poder agradecer minha avó, Dona Nina, pessoalmente, mas tenho certeza, que onde ela está consegue sentir tamanha gratidão. Obrigada, Vó, por ter dedicado sua vida inteira à nossa família e ter construído uma base tão forte para que eu pudesse prosperar. Agradeço à minha mãe, Anita e às minhas tias, Ana e Arací, pelo apoio, pela confiança, pelo amor e por não medirem esforços para investirem na minha educação. À minha madrinha Andréia, que sempre esteve disponível nos momentos que precisei. Minha família é composta por mulheres fortes, espero conseguir carregar o legado de vocês.

À minha irmã de alma, Vithória. Seja na conclusão do ensino fundamental, do médio ou da universidade, crescer e compartilhar as conquistas da vida contigo é um privilégio. Não importa se estamos estudando no mesmo prédio ou a 18.000 quilômetros de distância, sempre te sinto ao meu lado. Às minhas amigas, Bruna, Eduarda, Lauana e Letícia, sei que cheguei por último no grupo e agradeço por me acolherem tão bem, pelas noites de fondue, pelas conversas, pelo companheirismo, a vida é muito mais divertida com vocês.

Agradeço imensamente à Ana Carolina, Giulia e Leonardo. Nossa ligação foi instantânea e tão forte que hoje mal consigo pensar como era antes de conhecer vocês. Viver a UFSC do lado de vocês fez tudo ser melhor, obrigada por acreditarem em mim, pelo carinho, pela companhia, pelo aconchego, pelos lanches e bolinhos com café. Vocês, acima de tudo, são meu lar em Florianópolis. À Júlia, Jota, Emanuel e Matheus, ter vocês no meu dia a dia durante a graduação foi um presente, obrigada.

À Universidade Federal de Santa Catarina, que sempre foi meu sonho, e à toda estrutura de ensino público de qualidade brasileiro, por me proporcionar uma formação tão completa e com tantas oportunidades, como o intercâmbio para a Sungkyunkwan University, a qual também agradeço, por ter me proporcionado estrutura para começar a pesquisa que é apresentada nesta monografia. Agradeço aos amigos que fiz na Coreia do Sul, Juliana, Miwa, Hanjae, Jason, Duda e Naz, vocês me mostraram que posso pertencer a qualquer lugar no mundo.

Agradeço ao GEPPIC e ao GESED, por terem me proporcionado um espaço para pesquisa e assim, fazer com que eu tivesse como retribuir pelo menos uma parcela do que a universidade me proporcionou à comunidade. Tanto quanto aos colegas de pesquisa, especialmente minha dupla Carol, que me acompanhou no meu primeiro processo de pesquisa. Agradeço às professoras orientadoras, Graciela e, especialmente Danielle, que me

acompanhou também no processo de escrita do TCC. Me inspiro imensamente em vocês. Além de todas e todos outros professores que tanto contribuíram para a minha formação, obrigada.

Por fim, meu muito obrigada a todas e todos que cruzaram meu caminho durante a graduação.

RESUMO

A Revolução da Informação transformou completamente a forma com que a sociedade opera, de maneira tão poderosa que até os Estados foram afetados. Um novo domínio operacional, caracterizado pelo uso de eletrônicos para armazenar e trocar informações entra no jogo de poder, o espaço cibernético. Os Estados utilizam o espaço cibernético para expressar seus interesses nacionais, que, mesmo não sendo um espaço físico, ainda está atrelado às noções geográficas humanas. Apresenta-se, então, um novo domínio de poder com espaço para conflito;os Estados, assim, preocupados com novas ameaças provindas do espaço cibernético, trazem a defesa e segurança cibernética para suas agendas políticas. Coreia do Sul e Brasil ocupam, respectivamente a 4ª e 18ª posição no Global Cybersecurity Index de 2020, mas não são comumente citados como grandes detentores de poder cibernético. Dessa forma, a partir do método hipotético dedutivo, o presente trabalho busca entender como Coreia do Sul e Brasil expressam poder cibernético através da análise e comparação das estratégias expostas em documentos oficiais. A pergunta que norteia a pesquisa é: Em que medida os documentos oficiais do Brasil e da Coreia do Sul consideram o espaço cibernético como um domínio de propagação de poder? Nesse sentido, a hipótese principal levantada é que se a Coreia do Sul e o Brasil constroem estratégias nacionais de defesa cibernética, então consideram o espaço cibernético como meio de propagação de poder no sistema internacional; de forma secundária, considerando que a Coreia do Sul recebe pontuação melhor que o Brasil no Global Cybersecurity Index 2020, levanta-se a hipótese que a Coreia do Sul tem estratégias de defesa cibernética mais robustas que o Brasil, pois se encontra em um entorno estratégico que lhe propõe mais ameaças.

Palavras-chave: Poder cibernético. Estratégia cibernética. Defesa Cibernética. Segurança Cibernética. Coreia do Sul. Brasil.

ABSTRACT

The Information Revolution has completely transformed the way society operates, even so powerfully that states have been affected. A new operational domain, characterized by the use of electronics to store and exchange information enters the power game, the so called cyberspace. States use cyberspace to express their national interests, and even though it is not a physical space, it is still linked to human geographic notions. A new domain of power presents itself with space for conflict, the States, thus, concerned with new threats coming from cyberspace, bring cyber defense and security to their political agendas. South Korea and Brazil rank 4th and 18th respectively in the 2020 Global Cybersecurity Index, but are not commonly cited as major cyber power holders. Thus, based on the hypothetical deductive method, this paper seeks to understand how South Korea and Brazil express cyber power through the analysis and comparison of strategies exposed in official documents. The question that guides the research is: To what extent do official documents from Brazil and South Korea consider cyberspace as a domain of power propagation? In this sense, the main hypothesis raised is that if South Korea and Brazil build national cyber defense strategies, then they consider cyber space as a means of propagating power in the international system; secondarily, considering that South Korea receives a better score than Brazil in the Global Cybersecurity Index 2020, it is hypothesized that South Korea has more robust cyber defense strategies than Brazil, as it is in a strategic environment that poses more threats.

Keywords: Cyber power. Cyber strategy. Cyber Defense. Cyber Security. South Korea. Brazil.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABIN Agência Brasileira de Inteligência

ADMM-Plus Grupo de Trabalho de Especialistas em Segurança Cibernética na Reunião de Ministros da Defesa da ASEAN-Plus

APF Administração Pública Federal

ASEAN Associação das Nações do Sudeste Asiático

BRICS Brasil, Rússia, Índia, China e África do Sul

CDCiber Centro de Defesa Cibernética

CERT.br Centro de Tratamento e Resposta

CGSI Comitê Gestor da Segurança da Informação

CSIRT Computer Security Incident Response Team

CT&I Ciência, Tecnologia e Inovação

DSIC Departamento de Segurança da Informação e Comunicações

E-Ciber Estratégia Nacional de segurança cibernética

END Estratégia Nacional de Defesa

EUA Estados Unidos da América

DCA Defense Cooperation Agreement

DoD Departamento de Defesa

DPRK Democratic People's Republic of Korea

FA Forças Armadas

FIRST Forum of Incident Response and Security Teams

GPS Sistema de Posicionamento Global

GSI/PR Gabinete de Segurança Institucional da Presidência da República

GSOMIA Acordo Geral sobre a Segurança de Informações Militares

ITU International Telecommunications Union

KHNP Korea Hydro and Nuclear Power

MDN Ministério da Defesa Nacional

MD Ministério da Defesa

MJ Ministério da Justiça

NCSC National Cybersecurity Center

NIS National Intelligence Service

NSS National Security Strategy

OCDE Organização para Cooperação e Desenvolvimento Econômico

OEA Organização dos Estados Americanos

ONU Organização das Nações Unidas

ONG Organizações Não Governamentais

OTAN Organização do Tratado do Atlântico Norte

PF Polícia Federal

PND Política Nacional de Defesa

P&D Pesquisa e desenvolvimento

RFID Radio Frequency Identification

ROK Republic of Korea

ROKA Republic of Korea Army

STIC2 Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle

TIC Tecnologias da Informação e Comunicação

TI Tecnologia da Informação

UE União Europeia

UN GGE Grupo de Especialistas Governamentais das Nações Unidas

SUMÁRIO

1 INTRODUÇÃO

Os avanços tecnológicos trazidos pela Revolução da Informação são uma espada de dois gumes, segundo Nye (2004). Trinta anos atrás existiam apenas 50 websites por todo o mundo e, hoje, com a queda brusca do custo de transmissão de informação, cerca de 3,5 bilhões de indivíduos estão conectados à internet, e o tamanho do mundo digital é estimado em 44 zettabytes (ITU, 2020). A Revolução da Informação, portanto, está transformando o mundo em rápida velocidade. Os Estados claramente são afetados por essa transformação. A Internet é um espaço que favorece a disseminação de diversas formas de interações sociais, transações e oportunidades, porém, também é um ambiente propenso a riscos e ameaças tanto para indivíduos quanto para Estados (SOUZA, 2013).

A tecnologia mudou as noções de poder tradicionais dos Estados-nação (BOLLIER, 2003), e a existência de um novo espaço para a operação de atividades relacionadas a eletrônicos, o espaço cibernético, significa novas oportunidades de desenvolvimento e execução de políticas nacionais. O ciberespaço, dessa forma, é global, mas de forma nenhuma é um local livre, sem regulamentação estatal; não é um bem comum. Está atrelado a humanos e infraestruturas humanas, estes, naturalmente estão sujeitos a suas delimitações geográficas e são subjugados a suas crenças e cultura (SINGER; FRIEDMAN, 2014). Os conflitos que se dão no espaço cibernético, portanto, são influenciados por limites estatais. Sendo assim, o espaço cibernético atualmente é o mais novo domínio de poder e guerra, junto dos domínios tradicionais: terrestre, marítimo, aéreo e espacial (SILVA, 2014).

Demanda, em vista disso, a criação de novas estratégias para que os Estados alcancem seus objetivos dentro dos elementos de poder nacional (KRAMER; STARR; WENTZ, 2009). O poder cibernético é a capacidade de chegar aos objetivos de política nacional por meio do espaço cibernético (NYE, 2010). Estabelecido como meio de propagação de poder, o espaco cibernetico se torna um novo *locus* de ameaças para os Estados e, assim, a segurança cibernética ganhou grande relevância e passou a ser considerada uma questão primordial nas agendas políticas de Estados, organizações internacionais e supranacionais (CAVELTY, 2018). Analisar as relações entre poder e espaço cibernético é importante para entender as aspirações dos Estados como atores no Sistema Internacional. Os Estados se utilizam de documentos oficiais, leis e diretrizes nacionais para publicizar seu entendimento, estratégias e traçar objetivos sobre o assunto (DE RÊ, 2021).

Cavelty (2018) cita que Estados Unidos e China são comumente mencionados por especialistas quando se trata de forte expressão de poder cibernético; Castro (2020) afirma

que estes países são os mais proeminentes na temática. A Coreia do Sul, porém, que ocupa a 4ª posição com a 98.52 de pontuação no *Global Cybersecurity Index 2020*[1] produzido pela *International Telecommunications Union (ITU)*, posição acima até da China, geralmente não é mencionada como grande expoente de poder cibernético, o que causa estranheza. O Brasil, que aparece na 18ª posição, pontuando 96.6 (ITU, 2020), também não é descrito como portador de capacidades cibernéticas para exercer poder (FAVERO, 2022).

A partir da inquietação causada pelo fato de que países com alto nível de segurança cibernética não serem considerados grandes portadores de poder cibernético, a presente monografia tem o objetivo, a partir de uma pesquisa exploratória e comparativa, entender como Coreia do Sul e Brasil expressam poder cibernético por meio da análise e comparação das estratégias expostas em documentos oficiais. E é guiada pela pergunta central: *Em que medida os documentos oficiais do Brasil e da Coreia do Sul consideram o espaço cibernético como um domínio de propagação de poder?* Nesse sentido, a hipótese principal levantada é que se a Coreia do Sul e o Brasil constroem estratégias nacionais de defesa cibernética, então consideram o espaço cibernético como meio de propagação de poder no sistema internacional; de forma secundária, considerando que a Coreia do Sul recebe pontuação melhor que o Brasil no *Global Cybersecurity Index 2020*, levanta-se a hipótese que a Coreia do Sul tem estratégias de defesa cibernética mais robustas que o Brasil, pois se encontra em um entorno estratégico[2] que lhe propõe mais ameaças. Assim, as variáveis independente e dependente são: o entorno estratégico e as estratégias de defesa construídas, respectivamente.

Este trabalho adota a diferenciação de Pagliari, Ayres Pinto e Barroso (2020) para segurança e defesa cibernética, em que defesa cibernética é uma resposta para ameaças ao setor público e infraestruturas críticas, e segurança cibernética, corresponde a ameaças onde o alvo principal é a área privada e sociedade civil. Uma vez que, os documentos sul-coreanos analisados se encontram em língua inglesa e coreana, por questões de adaptação semântica na tradução para a língua portuguesa, os termos às vezes se confundem. O trabalho, portanto, tem a premissa que assuntos públicos são relacionados à defesa e privados à segurança, desconsiderando o termo utilizado na tradução literal.

O primeiro capítulo busca conceituar poder, entender o papel do poder nas relações internacionais e dimensões de poder; entender como o advento da Internet alterou as relações

[1] O index considera as medidas legais, técnicas, organizacionais, de desenvolvimento de capacidades e de cooperação como metodologia na construção de seu ranking (ITU, 2020).
[2] Serão consideradas as definições próprias de cada país por seus documentos oficiais como entorno estratégico.

de poder entre os Estados e definir poder cibernético, espaço cibernético e domínio cibernético. Por fim, tipificar os conflitos cibernéticos e discutir governança e defesa cibernética. Para isso será feito uma revisão teórica dos trabalhos clássicos no campo dos estudos cibernéticos dentro das Relações Internacionais.

O segundo capítulo propõe expor a situação geopolítica da Coreia do Sul e do Brasil, entender o que consideram ameaças em seu entorno estratégico e transcrever de forma resumida o conteúdo de seus principais documentos estratégicos oficiais. A situação geopolítica é analisada antes dos documentos com o intuito de se entender em que contexto foram produzidos, já que a geografia influencia nos planejamentos e decisões políticas dos Estados (MAFRA, 2006). Foram escolhidos os documentos oficiais que, em alguma medida, versam sobre questões de defesa cibernética e são satisfatórios em quesitos de comparação, como o "Livro Branco de Defesa Nacional" brasileiro e o "Livros Branco de Defesa" sul coreano.

Por fim, o terceiro capítulo tem o objetivo de entender como Coreia do Sul e Brasil expressam poder cibernético a partir de Klimburg (2014) e como seu entorno estratégico influencia nessa expressão. Para tal fim, o capítulo apresentará o "Modelo de Capacidades Integradas" de Klimburg (2014), bem como argumentos que pretendem demonstrar que essa é a melhor perspectiva para se mensurar e comparar as capacidades de poder cibernético da Coreia do Sul e Brasil e assim, responder a pergunta de partida da pesquisa. A partir dos resultados dessa comparação, o trabalho abordará de que forma o entorno estratégico de cada país pode influenciar suas estratégias de defesa.

2 INTERNET E NOVAS PERSPECTIVAS DE PODER

Antes de qualquer análise sobre as estratégias de defesa cibernética, é necessário discutir o poder nas Relações Internacionais e como este se adaptou às novas tecnologias, como a Internet. Este primeiro capítulo busca entender o processo de securitização da Internet, e assim, a ascensão da defesa cibernética nas agendas de segurança. Além disso, expor conceitos que envolvem segurança e defesa cibernética, como: guerra cibernética, terrorismo cibernético, crime cibernetico sob diferentes perspectivas.

2.1 O PODER NAS RELAÇÕES INTERNACIONAIS

A conceituação de poder é descrita por Elster (1976) como a ideia mais importante no campo da teoria política (*apud* BALDWIN, 2016). Baldwin (2016) afirma que um pensamento claro sobre as implicações do poder em um mundo onde países podem não apenas destruir uns aos outros, mas a vida como conhecemos, é necessário.

É consenso que os estudos de poder são o cerne das Relações Internacionais, "o estudo da política internacional, centrado “em torno de uma análise do poder nacional” deve ser o “núcleo” intelectual do campo das relações internacionais" (KIRK, 1947 *apud* BALDWIN, 2016, p. 96, *tradução nossa*)[3], nesse mesmo cenário, Morgenthau (1948) solidificou a centralidade do poder como objetivo final de política externa das nações e o principal conceito para o entendimento da política internacional.

Dada a importância, o conceito de poder é discutido e revisitado por muitos acadêmicos. Dahl (1957) define poder nos termos de "a capacidade de A de conseguir que B faça algo que de outra forma não faria tem sido amplamente aceita e amplamente criticada por B" (*apud* BALDWIN, 2016, p. 12, *tradução nossa*)[4]. Nye (2004) aprofunda essa definição ao dizer que o poder não deve ser pensado de forma restrita, apenas em termos de coerção, há muitas formas de influenciar o comportamento do outro para receber resultados benéficos. O autor elenca "Você pode coagi-los com ameaças; você pode induzi-los com pagamentos; ou você pode atrair e cooptá-los para querer o que você quer." (NYE, 2004, p.2, *tradução*

[3] No original: "*around an analysis of national power” should be the intellectual “nucleus” of the field of international relations.*" (KIRK, 1947 *apud* BALDWIN, 2016, p. 96).
[4] No original: "*A’s ability to get B to do something that would not otherwise do has been both B widely accepted and widely criticized*. " (DAHL, 1957 *apud* BALDWIN, 2016, p. 12).

nossa)[5]. Sendo assim, percebe-se que o poder pode ser expresso de muitas formas que não são necessariamente subordinadas uma à outra, como: riqueza, armamentos, autoridade civil, influência de opinião (RUSSELL, 1938 *apud* LASSWELL, KAPLAN, 1950).

De acordo com a perspectiva do poder relacional, o poder é multidimensional. Ou seja, o poder pode aumentar em uma dimensão enquanto, ao mesmo tempo, diminui em outra (BALDWIN, 2016). Aqui, citaremos algumas dimensões que Baldwin (2016) elenca como as mais importantes: escopo, peso, base, meios, custos, tempo, lugar e domínio. Para promover uma boa especificação de relações de poder, deve-se considerar essas dimensões, principalmente escopo e domínio:

Quadro 1 - Dimensões de poder segundo Baldwin (2016).

Dimensão	Definição
Escopo	Se refere a quais aspectos um ator influencia no outro, é possível que o poder desse ator varie de um escopo para outro.
Peso	O quanto um ator A pode alterar a probabilidade que o ator B mude suas ações, essa dimensão é útil para separar poder real de poder aparente
Base	Se refere aos recursos em que as relações de poder são baseadas. Concerne o mecanismo causal subjacente à relação de poder entre A e B. É importante ressaltar que não há hierarquia sobre esses recursos de poder, ou seja, todos possuem a mesma fundamentalidade. Além disso, quase tudo pode ser considerado um recurso de poder dependendo do contexto.
Meios	Os meios de poder são utilizados para ativar a base de poder, são uma técnica de influência. Propaganda, diplomacia, sanções econômicas, discurso e força militar são exemplos.
Custos	Compete o quanto custa para A influenciar B e quanto custa para B atender às demandas de A. Um ator que consegue influenciar outro a um custo mais barato possui mais poder, por exemplo.
Quando	Alguns recursos de poder, como energia, são afetados pelo tempo. Petróleo e urânio são recursos de poder que se tornaram mais importantes ao longo do tempo.
Onde	A localização é uma variante de recursos de poder.
Domínio	Domínio de poder se refere a importância dos atores sujeitos à influência.

Fonte: Baldwin (2016)

[5] No original: "*You can coerce them with threats; you can induce them with payments; or you can attract and co-opt them to want what you want*" (NYE, 2004, p.2).

Joseph Nye (2004), traz a dimensão de *soft power*[6] para a discussão. Enquanto seu oposto, *hard power*[7] está relacionado a ameaças ou recompensas tangíveis para obter os resultados esperados, soft power está relacionado a habilidade de moldar as preferências dos outros:

> Um país pode obter os resultados que deseja na política mundial porque outros países - admirando seus valores, imitando seu exemplo, aspirando ao seu nível de prosperidade e abertura - querem segui-lo. Nesse sentido, também é importante definir a agenda e atrair outros na política mundial, e não apenas para forçá-los a mudar ameaçando com força militar ou sanções econômicas. Esse poder sutil, fazendo com que os outros desejem os resultados que você deseja, coopta as pessoas em vez de coagi-las. (NYE, 2004, p.5, *tradução nossa*)[8].

É importante ressaltar que soft power não é o mesmo que influência, já que hard power também pode influenciar através de ameaças e pagamentos. O soft power é mais que a persuasão, é também a habilidade de atrair, portanto a distinção entre os dois é em termos de grau da natureza do comportamento e da tangibilidade dos recursos. Hard e soft power interagem, às vezes de forma convergente, às vezes divergente. Por exemplo, um país popular no sistema internacional, com fama de pacifico, é relutante em usar o hard power para conseguir seus objetivos (NYE, 2004).

A ciência e a tecnologia adicionaram novas dimensões aos recursos de poder. A Revolução da Informação, citada na introdução deste trabalho, fez com que instrumentos de destruição em massa estejam cada vez mais baratos e de fácil acesso, dessa forma, o poder como conhecemos está mudando a passos rápidos, poder atualmente é muito menos tangível e coercivo (NYE, 2004).

Assim, Nye (2004) elenca três tipos de poder relevantes para o mundo moderno, são eles: poder militar, poder econômico e soft power. Levando em consideração, porém, a revolução digital, o soft power se torna o principal entre eles:

---

[6] Em tradução literal: poder sutil

[7] Em tradução literal: poder duro

[8] No original: "*A country may obtain the outcomes it wants in world politics because other countries-admiring its values, emulating its example, aspiring to its level of prosperity and openness-want to follow it. In this sense, it is also important to set the agenda and attract others in world politics, and not only to force them to change by threatening military force or economic sanctions. This soft power-getting others to want the outcomes that you want-co-opts people rather than coerces them*." (NYE, 2004, p.5).

Quadro 2 - Os três tipos de poder segundo Nye (2004).

	Comportamentos	Ocorrências primárias	Políticas governamentais
Poder Militar	Coerção Dissuasão Proteção	Ameaças Força	Diplomacia coerciva Guerra Alianças
Poder Econômico	Indução Coerção	Pagamentos Sanções	Ajuda Barganha Sanções
Soft Power	Atração Definição de agenda	Valores Cultura Políticas Instituições	Diplomacia pública Diplomacia bilateral e multilateral

Fonte: Nye (2004)

Pode-se, portanto, inferir que o poder no mundo moderno passa por duas grandes transformações: a transição de poder e a difusão de poder (NYE, 2011).

2.1.1 O Poder na Era da Informação

Uma Terceira Revolução Industrial, também chamada de Revolução da Informação, acontece entre o século vinte e vinte e um. Se resume à queda brusca dos custos de criar, processar, transmitir e procurar por informação, e é baseada em um aumento nas tecnologias de computador, software e comunicação. Esse aumento acontece muito rápido: em 1993, por exemplo, existiam cerca de 50 websites em todo mundo; sete anos depois, o número passava 5 milhões (NYE, 2011). Além disso,

> Ainda em 1980, as chamadas telefônicas por fio de cobre podiam transportar apenas 1 página de informação por segundo; hoje um fio fino de fibra óptica pode transmitir 90.000 volumes em um segundo. Em 1980, 1 gigabyte de armazenamento ocupava um quarto; agora 200 gigabytes de armazenamento cabem no bolso da sua camisa. A quantidade de informação digital aumenta dez vezes a cada cinco anos (NYE, 2011, p. 119, *tradução nossa*)[9].

Essa redução crucial nos custos de transmitir informação está mudando a natureza do poder e aumentando sua difusão. Os Estados não deixam de ser os atores dominantes no sistema internacional, mas encontram mais dificuldades em controlar os outros atores. Uma

[9] No original: "*As recently as 1980, phone calls over copper wire could carry only 1 page of information per second; today a thin strand of optical fiber can transmit 90,000 volumes in a second. In 1980, 1 gigabyte of storage occupied a room; now 200 gigabytes of storage fit in your shirt pocket. The amount of digital information increases tenfold every five years*" (NYE, 2011, p. 119).

parte muito maior da população de dentro e fora de suas fronteiras tem acesso ao poder que vem com a informação. Por população, diz-se novos atores que vão desde Organizações Não Governamentais (ONG) até grupos terroristas, que agora têm menos barreiras para participarem da política mundial, fazendo com que líderes políticos tenham a tomada de decisão cada vez mais influenciada por atores não formais (NYE, 2011).

Entretanto, Nye (2011) aponta que o poder militar, ou seja, poder tradicional como visto acima, ainda possui controle sobre os domínios críticos na política global. O parágrafo anterior mostra os benefícios que a Revolução da Informação traz a atores informais, já que a "disponibilidade comercial imediata de tecnologias militares outrora caras beneficia pequenos estados e atores não governamentais e aumenta a vulnerabilidade de grandes estados" (NYE, 2011, p. 121, *tradução nossa*)[10]. Por outro lado, os atores formais também são beneficiados por terem acesso a recursos muito maiores (NYE, 2011).

2.2 CIBER PODER, CIBERESPAÇO E DOMÍNIO CIBERNÉTICO

Aqui serão definidos conceitos relacionados a cibernética, como poder cibernético, espaço cibernético e domínio cibernético, conflitos cibernéticos e governança cibernética. O objetivo é trazer uma discussão com a contribuição de diversos atores sobre o assunto.

2.2.1 Poder cibernético

Como visto, o poder é relacional às mais variadas circunstâncias. Ou seja, depende do contexto no qual é analisado (NYE, 2010). O contexto eminente aqui, desta forma, é o surgimento da cibernética.

Mais recente que a própria Terceira Revolução Industrial, que trouxe o destaque ao poder baseado em informação, é o poder cibernético. O que difere, então, o poder cibernético dos outros tipos de poder? Em linhas gerais, quando utilizado como prefixo, "ciber" é relacionado a assuntos eletrônicos e computacionais (NYE, 2011). Para além, "o baixo preço de entrada, o anonimato e as assimetrias na vulnerabilidade significam que os atores menores

[10] No original: "*availability of formerly costly military technologies benefits small states and nongovernmental actors and increases the vulnerability of large states*." (NYE, 2011, p. 121).

têm mais capacidade de exercer hard e soft power no ciberespaço do que em muitos domínios mais tradicionais da política mundial"[11] (NYE, 2010, p. 1, *tradução nossa*).

Kramer, Starr e Wentz (2009) trazem uma sólida definição de poder cibernético, depois repetida e aprimorada dentro da academia. Para eles, e consequentemente para a agenda de defesa dos Estados Unidos, poder cibernético é a habilidade em "usar o ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais e nos instrumentos de poder"[12] (KRAMER; STARR; WENTZ, 2009, p. 38, *tradução nossa*).

Logo depois, Nye (2010) traz uma nova definição. Poder cibernético é como uma expressão de poder que se ancora nos recursos de criação, controle e comunicação de informações que circulam por meio eletrônico e de computadores, cita-se: "infraestrutura, redes, software, habilidades humanas. Isso inclui a Internet de computadores em rede, mas também intranets, tecnologias celulares e comunicações baseadas no espaço"[13] (NYE, 2010, p. 2, *tradução nossa*). Nye (2010) amplia a definição para os moldes do conceito clássico de poder, como descrito na seção anterior, "poder cibernético é a capacidade de obter resultados preferenciais através do uso dos recursos de informação interconectados eletronicamente do domínio cibernético"[14] (NYE, 2010, p. 3, *tradução nossa*). É importante destacar que o poder cibernético pode ser usado para produzir resultados favoráveis dentro do seu espaço de propagação, o ciberespaço, ou fora dele (NYE, 2010).

Nye (2011) aponta que o poder cibernético se difunde dentro de ambas esferas, soft e hard power. A informação é um instrumento que resulta em soft power dentro do espaço cibernético, por gerar definição de agenda, atração ou persuasão. Se a informação cibernética causar danos físicos a outros países, passa então a atuar como propagação de hard power. De outra forma, o hard power também é produzido quando atores, que podem ser estatais ou não, causam a interrupção da distribuição de algum serviço em um ciberataque por meio de botnets[15].

O contrário também pode acontecer, recursos físicos também podem causar danos no espaço cibernético. Os roteadores, os cabos de fibra óptica que provêm internet estão

---

[11] No original: "*The low price of entry, anonymity, and asymmetries in vulnerability means that smaller actors have more capacity to exercise hard and soft power in cyberspace than in many more traditional domains of world politics*. (NYE, 2010, p. 1).

[12] No original: *"the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power.*" (KRAMER; STARR; WENTZ, 2009, p. 38).

[13] No original: "*infrastructure, networks, software, human skills. This includes the Internet of networked computers, but also intranets, cellular technologies and space based communications*." (NYE, 2010, p. 2).

[14] No original: "*cyber power is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain*." (NYE, 2010, p. 3).

[15] Botnet é "uma rede de bots gerenciada pelo botmaster através do servidor de comando e controle, que coordena todos os dispositivos" (PRADO, 2018, p. 17).

localizados em terras dentro de fronteiras estatais, portanto, sobre a jurisdição destes Estados (NYE, 2011). Um ataque que visa prejudicar as infraestruturas cibernéticas, portanto, é uma forma de hard power.

Instrumentos físicos também têm a capacidade de prover recursos de soft e hard power para serem usados contra o domínio cibernético:

> A camada de ciber informação repousa sobre uma infraestrutura física que é vulnerável a ataques militares diretos ou sabotagem por governos e atores não estatais, como terroristas ou criminosos. Os servidores podem explodir e os cabos podem ser cortados. E no domínio do soft power, atores não estatais e ONGs podem organizar manifestações físicas para nomear e envergonhar empresas (e governos) que consideram abusar da Internet[16] (NYE, 2011, p. 131, *tradução nossa*).

Para além das esferas de hard e soft power, a difusão do poder cibernético também ocorre pela vasta quantidade de atores e a redução relativa de recursos de poder entre eles. Qualquer pessoa, desde que tenha acesso à Internet, o recurso mais simples do domínio cibernético, pode causar danos e ser um ator propagante de poder cibernético. Nye (2010) divide esses atores em três categorias: governos, organizações e redes altamente estruturadas e indivíduos e redes levemente estruturadas.

Os governos, como esperado, têm a maior quantidade de recursos para atuação no espaço cibernético. São responsáveis pelo desenvolvimento de infraestruturas, educação e de propriedade intelectual, e pelos recursos e inteligência para ataques e defesa cibernéticos; podem coagir legalmente e controlar outros atores dentro de suas fronteiras, como outros países e instituições - mercado, por exemplo; devem se preocupar, porém, com sua legitimidade, estabilidade política e reputação, a fim de continuar produzindo soft power. Atores governamentais sofrem uma série de vulnerabilidades no âmbito cibernético, são altamente dependentes de sistemas complexos que podem ser corrompidos com uso de vírus, a título de exemplo (NYE, 2010).

Organizações e redes altamente estruturadas, indivíduos e redes levemente estruturadas, por serem atores não tradicionais, passam por processos diferentes. Os primeiros são beneficiados por uma flexibilidade transnacional, ou seja, não precisam seguir a mesma série de protocolos formais que governos, mesmo que tenham grandes orçamentos e recursos

---

[16] No original: "T*he cyberinformation layer rests upon a physical infrastructure that is vulnerable to direct military attack or sabotage by both governments and nonstate actors such as terrorists or criminals. Servers can be blown up, and cables can be cut. And in the domain of soft power, nonstate actors and NGOs can organize physical demonstrations to name and shame companies (and governments) that they regard as abusing the Internet.*" (NYE, 2011, p. 131).

humanos à disposição. Sofrem, porém, de forma igual com riscos de reputação, e comprimento de sistemas. Um novo risco a ser adicionado é o perigo de roubo de propriedade intelectual. Na base encontram-se indivíduos e redes pouco estruturadas, que precisam de pouco investimento para atuação, são providos de anonimidade e podem ter seus rastros e feitos facilmente apagados, o que os deixa menos suscetíveis a sanções. Se pegos, entretanto, podem sofrer coerções legais e ilegais dos outros dois atores, apresentam, portanto, uma vulnerabilidade assimétrica em relação a esses (NYE, 2010).

2.2.2 Espaço Cibernético e Domínio Cibernético

Ventre (2012) define terra, ar, mar e espaço como domínios tradicionais de poder. O poder do mar, por exemplo, é ligado ao uso do domínio dos oceanos para vencer batalhas marítimas, controlar pontos estratégicos no mar, batalhas, e, de forma mais abstrata, influenciar no comércio e pensamentos em terra. Os domínios são mutáveis, são descobertos como meio de propagação de poder e ganham popularidade de acordo com a história. O domínio aéreo ganhou popularidade apenas depois da Primeira Guerra Mundial, quando aeronaves foram utilizadas pela primeira vez para atacar centros urbanos sem a necessidade de exércitos marchando em terra e conquistando fronteiras (NYE, 2010).

Dentro de tantas definições para espaço cibernético, cita-se a de Kramer, Starr e Wentz:

> O ciberespaço é um domínio caracterizado pelo uso da eletrônica e do espectro eletromagnético para armazenar, modificar e trocar informações por meio de sistemas de informação em rede e infra estruturas físicas[17] (KRAMER; STARR; WENTZ, 2009, p. 26, *tradução nossa*).

Kuehl (2009), por sua vez, define o espaço cibernético como "um domínio operacional enquadrado pelo uso de eletrônicos para explorar informações por meio de sistemas interconectados e sua infraestrutura associada." (*apud* NYE, 2010, p. 3, *tradução nossa*). As duas definições concordam que o espaço cibernético é muito mais que a internet, e que a troca de informações tem um papel de destaque.

O espaço cibernético se difere dos outros pois é o único que apresenta uma mistura de propriedades virtuais e físicas. A camada física se refere a infraestruturas que seguem leis

[17] No original: "Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked information systems and physical infrastructures." (KRAMER; STARR; WENTZ, 2009, p. 26).

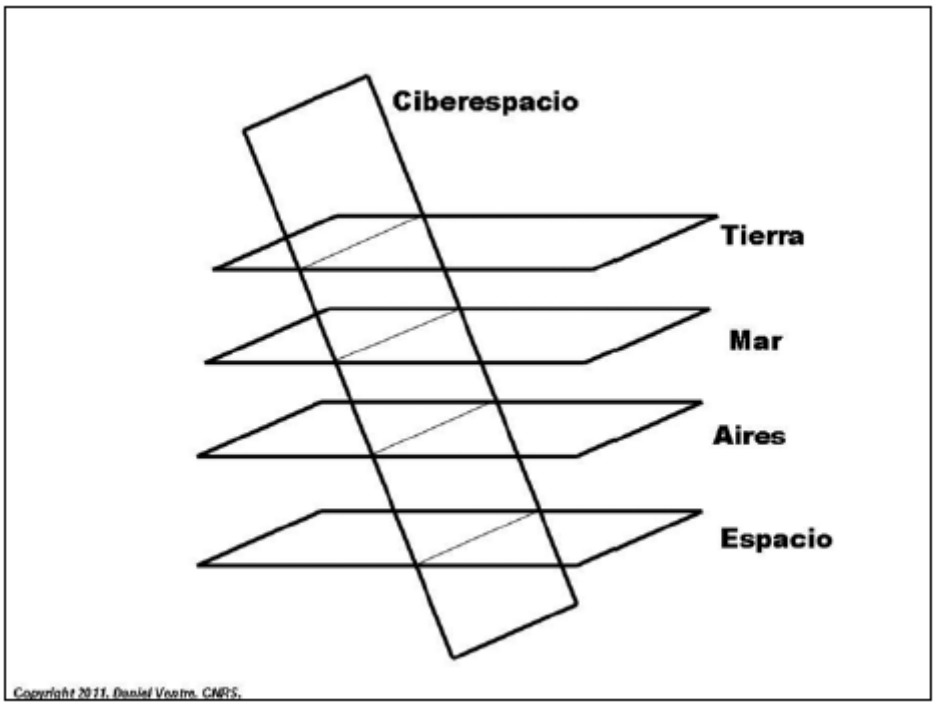
econômicas, custos tradicionais e está sob controle e jurisdição de Estados soberanos, já a camada virtual apresenta características que fogem do controle jurisdicional tradicional. Há a possibilidade de ataques que saem da camada virtual, onde os custos são baixos, prejudicarem a camada física, que tem recursos escassos e custos altos. Outra característica é que o controle da camada física gera efeitos territoriais e extra-territoriais na camada virtual (NYE, 2011).

O espaço cibernético é novo, em tempo cronológico. Mesmo com pouco tempo de criação, o crescimento do espaço cibernético é exponencial, em 1992 existiam um milhão de usuários de Internet, esse número cresceu para um bilhão em 15 anos (NYE, 2010).

Mesmo que muitos pensem que o espaço cibernético se resuma à internet, Ventre (2012) expõe que vai muito além disso. Espaço cibernético é, portanto, o conjunto de "satélites, drones, RFID, computadores conectados ou não, sistemas industriais informatizados"[18] (VENTRE, 2012, p. 34, *tradução nossa*). Para Ventre (2012), o espaço cibernético é representado em três camadas distintas: uma camada inferior, que representa as características materiais, ou seja, a infra estrutura (hardwares, por exemplo); a camada do meio indica as características não materiais, como softwares e aplicativos; por fim, a camada superior representa o espectro cognitivo. Outra característica significante do espaço cibernético é sua transversalidade. Quer dizer que ultrapassa todos os domínios tradicionais de poder, como terrestre, aéreo, marítimo e espacial. Como pode ser observado na figura abaixo:

[18] No original: "*los satélites, los drones, el RFID, los ordenadores conectados o no, los sistemas industriales informatizados*" (VENTRE, 2012, p. 34).

Figura 1 - Domínios de poder.



Fonte: VENTRE, 2012, p. 34

O domínio cibernético, em comparação com os outros, é único. Ser feito pelo ser humano é sua primeira especificidade, isso faz com que seja recente e que tenha mudanças tecnológicas fáceis e rápidas. Além disso, o domínio cibernético contribuiu para a difusão de poder, já que há poucas barreiras de entrada e pouco custo de operação, "é mais barato e mais rápido mover elétrons pelo globo do que mover grandes navios por longas distâncias através do atrito da água salgada"[19] (NYE, 2011, p. 128, *tradução nossa*).

Tais características fazem com que o espaço cibernético, diferente dos outros domínios, possa apresentar apenas fronteiras artificiais, pois é criado pelo e manipulado pelo homem. Contudo, mesmo sendo um espaço não material, ainda é mutável de acordo com características e vontades humanas, como língua e cultura (MEIRA MATTOS, 1990 *apud* FERREIRA NETO, 2014).

Em consequência do surgimento do domínio cibernético, países importantes, como os Estados Unidos, se veem agora dividindo recursos de poder de forma equivalente com novos atores e apresentando problemas em definir suas fronteiras dentro do novo domínio. Nye (2010), no entanto, deixa a ressalva que, mesmo considerando toda revolução informacional e tecnologia, o espaço cibernético não "substituirá o espaço geográfico e não abolirá a soberania

[19] No original: "*It is cheaper and quicker to move electrons across the globe than to move large ships long distances through the friction of saltwater*" (NYE, 2011, p. 128).

estatal"[20] (NYE, 2010, p. 2, *tradução nossa*). A novidade é que a facilidade de difusão de poder alterará o que era conhecido como exercer poder nos domínios tradicionais.

2.2.3 Conflitos cibernéticos

O Brasil sofreu 3,4 bilhões de ataques cibernéticos no ano de 2020 (FORTIGUARD, 2021). Da mesma forma, todos os países conectados ao espaço cibernético são alvo desses ataques, os números subindo ano após ano (VENTRE, 2012). O escopo desses ataques variam atualmente entre conflitos políticos, econômicos e até mesmo militares, que podem ser conduzidos no domínio cibernético (CAVELTY, 2010).

Conflitos extremos no domínio cibernético são chamados de guerra cibernética. Diferente de conflitos tradicionais, onde o governo detém o monopólio do uso da força, onde recursos e mobilidade são custosos, nos conflitos dentro do domínio cibernético, os atores são diversos - algumas vezes anônimos - e a distância física é inexistente. E o mais importante, os custos de ofensa são baixíssimos, se não gratuitos, já que "a Internet foi projetada para facilidade de uso em vez de segurança, o ataque atualmente tem a vantagem sobre a defesa"[21] (NYE, 2011, p. 128, *tradução nossa*).

As particularidades do espaco cibernetico, fazem com que as ameaças conduzidas nesse domínio sejam cada vez mais difíceis de conter, uma vez que as "armas" de ataque, como descreve Ventre (2012), estejam cada vez mais democratizadas, consequentemente, é muito mais fácil conduzir essa forma de ataque, por qualquer que seja o ator.

Cavelty (2010) categoriza os ataques cibernéticos pelo dano resultante do ato. Apresenta-se tal categorização no quadro abaixo, em ordem crescente de gravidade:

---

[20] No original: "*replace geographical space and will not abolish state sovereignty*" (NYE, 2010, p. 2).
[21] No original: "*Because the Internet was designed for ease of use rather than security, the offense currently has the advantage over the defense*." (NYE, 2011, p. 128).

Quadro 3 - Ameaças cibernéticas.

Cyberhacking ou vandalismo cibernético	É limitado ao tempo e relativamente inofensivo.
Crimes na internet ou ciberespionagem	Relacionado ao setor privado. As vítimas mais recorrentes são os setores empresariais.
Ciberterrorismo	"Usado para descrever ataques ilegais por atores não estatais contra computadores, redes e as informações neles armazenadas, realizados com o objetivo de intimidar um governo ou população, ou para compelir determinado comportamento. Um ciberataque só é classificado como ciberterrorismo se resultar em violência física contra pessoas ou propriedade, ou pelo menos causar danos suficientes para criar medo considerável. O alcance potencial dos danos é considerado muito alto, embora não tenha havido nenhum caso real de ciberterrorismo até o momento"[22].
Guerra cibernética	"O termo se refere ao conflito bélico no espaço virtual que envolve principalmente meios de tecnologia da informação. O termo "guerra cibernética" refere-se a uma subseção da guerra de informação. Como parte deste conceito mais amplo, que visa influenciar a vontade e as capacidades de tomada de decisão da liderança política do inimigo e das forças armadas e/ou as atitudes da população civil no teatro de operações ao nível dos sistemas de informação e informação (cf. Análise CSS nº 34), a ciberguerra inclui atividades no ciberespaço. Conceitualmente, portanto, a guerra cibernética reflete a natureza cada vez mais tecnologizada da guerra na era da informação, baseada na informatização, eletronização e no funcionamento da rede de quase todas as áreas e aspectos das forças armadas."[23]

Fonte: Elaboração própria com base em CAVELTY, 2010

[22] No original: "*used to describe illegal attacks by non-state actors against computers, net-works, and the information stored therein,carried out with the aim of intimidating a government (or population) or to compel certain behaviour. A cyberattack is there-fore only categorised as cyberterrorism if it results in physical violence against per-sons or property, or at least causes suffi-cient damage to create considerable fear.The potential scope of damage is regarded as very high, although there have been noreal-life cases of cyberterrorism to date"* (CAVELTY, 2010, p. 2).

[23] No original: "r*efers to a sub-section of information warfare. As part of this broader concept, which aims at influencing the will and decisionmak-ing capabilities of the enemy's politi-cal leadership and armed forces and/or the attitudes of the civilian popu-lation in the theatre of operations at the level of information and informa-tion systems (cf. CSS Analysis no. 34),cyberwar includes activities in cyber-space. Conceptually, therefore, cyberwar reflects the increasingly technologies nature of war in the information age based on computeri-sation, electronisa-tion, and the net-working of nearly all areas and aspects of the military*" (CAVELTY, 2010, p. 2)

Nye (2010) classifica ciberataques de uma forma diferente. Para ele, cyberhacking ou hacktivismo é apenas uma forma de incômodo, não uma ameaça propriamente dita. Dessa forma, existem outras quatro grandes ameaças: espionagem econômica, crime cibernético, guerra cibernética e terrorismo cibernético.

Conclui-se, desta forma, que as ameaças cibernéticas, dependendo da tipologia, resultam em atos de violência e agressão no mundo real:

> Governos e exércitos devem levar em conta esta nova realidade que surgiu no campo das relações internacionais: as operações no ciberespaço provavelmente afetarão seu equilíbrio, sua operação, suas capacidades, sua liberdade de ação, sua eficiência e a capacidade. Na verdade, os ataques cibernéticos também são uma arma com a qual eles precisam aprender a manejar.[24] (VENTRE, 2012, p. 33, *tradução nossa*).

Mesmo que ataques cibernéticos não tenham as mesmas dimensões que ataques nucleares, ainda há dissuasão entre Estados (NYE, 2010). Logo, presume-se que as forças armadas dos Estados, gradativamente, passarão a se engajar em defender seu espaço cibernético e se defender de ataques provenientes do espaço cibernético.

2.2.4 Governança e defesa cibernética

É papel dos estados nacionais cuidar de problemas que ameaçam a segurança de seus habitantes dentro do espectro de leis internas. Como visto anteriormente, tudo que envolve o espaço cibernético é novo e, consequentemente, conceitos e determinações mudam de acordo com a evolução de conhecimento e da própria tecnologia. A governança para o espaço cibernético, naturalmente, segue essa tendência:

> A governança imperfeita do ciberespaço pode ser categorizada como um "complexo de regimes" de normas e instituições fracamente acopladas em algum lugar entre uma instituição integrada que impõe regulação por meio de regras hierárquicas e práticas e instituições altamente fragmentadas sem núcleo identificável e vínculos inexistentes[25] (NYE, 2010, p. 15*, tradução nossa*)

---

[24] No original: " *Los gobiernos y los ejércitos deben tomar en cuenta esa nueva realidad que ha surgido en el campo de las relaciones internacionales: las operaciones en el ciberespacio son susceptibles de afectar su equilibrio, su funcionamiento, sus capacidades, su libertad de acción, su eficiencia y el poder. De hecho, los ataques cibernéticos también son un arma que tienen que aprender a manejar*." (VENTRE, 2012, p. 33).

[25] No original: "*The imperfect governance of cyberspace can be categorized as a "regime complex" of loosely coupled norms and institutions somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages.*" (NYE, 2010, p. 15).

As características específicas do domínio cibernético desenham, então, um cenário desfavorável para a auto governança, já que favorecem as ameaças. Por consequência, têm-se Estados buscando incessantemente formas de regular e governar o espaço cibernético a fim de preservar sua segurança (NYE, 2010).

Ou seja, ainda é cedo para traçar um plano forte e acordado no Sistema Internacional para governança do espaço cibernético. Parte dessa dificuldade vem de uma característica única do domínio cibernético: este não pode ser dado com um bem público. Os domínios tradicionais, como terra e mar, têm acesso facilitado e por serem físicos, claramente pertencem a este ou aquele estado dentro de fronteiras terrestres e marítimas. Nye (2010) define o espaço cibernético como "imperfeito comum", pertencente a muitos proprietários sem regras bem elaboradas.

Este capítulo, portanto, trouxe discussões clássicas dentro do campo das Relações Internacionais sobre poder e as consequências trazidas pelas novas tecnologias trazidas pela Revolução da Informação ao Sistema Internacional, com a criação do espaço cibernético e, consequentemente, um novo domínio de poder para os Estados alcançarem seus objetivos. No próximo capítulo será exposto como Coreia do Sul e Brasil constroem estratégias para expressarem poder cibernético a partir de seus documentos oficiais.

3 DOCUMENTOS OFICIAIS DE BRASIL E COREIA DO SUL

Dada a relação entre poder e cibernética, o próximo passo para entender como Coreia do Sul e Brasil exprimem e pensam poder cibernético é mapear e transcrever seus documentos oficiais em defesa, já que são fontes primárias. Dessa forma, este capítulo busca analisar os documentos oficiais da Coreia do Sul e do Brasil que tratam de cibernética. A escolha de Coreia do Sul e Brasil, como mencionado anteriormente, se dá por conta da discrepância na pontuação destes no *Global Cybersecurity Index* 2020 produzido pela *International Telecommunications Union.* A Coreia do Sul ocupa a 4ª posição, com 98.52 de pontuação, enquanto o Brasil aparece na 18ª posição, pontuando 96.6 (ITU, 2020), além do questionamento causado pela falta de literatura que considere Brasil e Coreia do Sul grandes portadores de poder cibernético mesmo com suas posições altas no ranking (CAVELTY, 2018; CASTRO, 2020; FAVERO, 2022).

3.1 COREIA DO SUL

Nesta seção os seguintes documentos de defesa e segurança cibernética sul coreanos serão mapeados e transcritos: Plano Diretor Nacional de Segurança Cibernética (2011); Regulamentos Nacionais de Gerenciamento de Segurança Cibernética (2013); Estratégia Nacional de Segurança Cibernética (2019); Livros Branco de Defesa (2006 - 2020) e Livros Branco de Segurança Cibernética Nacional. Além disso, oferece uma visão sobre a estrutura de governança interna em cibernética da Coreia do Sul e sua situação geopolítica.

3.1.1 Geopolítica

Antes de apresentar os documentos, é importante entender em que contexto foram produzidos. Assim, primeiro se apresentará o contexto geopolítico em que a Coreia do Sul está inserida.

Chung-In e Lee (2022) apontam como a posição da península coreana é, ao mesmo tempo, uma maldição e uma benção por colidir poder terrestre e marítimo. Toda a história do território é carregada de conflitos pela sua posição geográfica estratégica. Os impérios continentais, como Han, Mongol e Manchu, tentaram utilizar a península para expandir seus territórios e como meio de chegar ao Japão. Anos depois, no século XIX , a Coreia foi usada

como porta de entrada do império japonês para a Ásia continental durante a Guerra Sino-Japonesa. Em 1945, logo após sua independência do colonialismo japonês, instantaneamente se tornou vítima da rivalidade geopolítica das potências Estados Unidos e União Soviética, que dominaram sul e norte, respectivamente, e causaram a Guerra da Coreia.

Atualmente, a Coreia do Sul continua dividida em dois lados, tendo os Estados Unidos como seu maior aliado e a China como grande parceira comercial e de cooperação internacional, como observa-se:

> Washington tem pressionado Seul para endossar sua estratégia Indo-Pacífico e participar de atividades militares relacionadas; juntar-se aos esforços americanos de dissociação em comércio e investimento; formar uma aliança tecnológica para enfrentar os desafios da China; e para apoiar a campanha da América para criticar a violação da democracia e dos direitos humanos por Pequim. Pequim tem enviado um aviso sutil a Seul de que, embora não queira que a Coreia do Sul fique do lado da China, ela deve permanecer neutra. Se Seul permitir que os EUA reforcem seus meios de defesa antimísseis na Coreia do Sul, como o aumento de seu sistema de mísseis THAAD (Terminal High Altitude Area Defense) e/ou a implantação de mísseis balísticos americanos de alcance intermediário, a China tratará a Coreia do Sul como inimiga e tomar medidas correspondentes (CHUNG-IN; LEE, 2022, p.4, *tradução nossa*)[26].

A constante divisão e ameaça ficam claras pelo posicionamento da Coreia do Sul em seus documentos de defesa oficiais. No *2020 Defense White Paper* é defendido que a geopolítica, junto de território e religião, são as razões fundamentais dos conflitos atuais, principalmente na região da Ásia, onde Estados Unidos e China continuam disputando poder com atividades militares. Além disso, o conflito entre os dois países se expande para além do militar e entra em aspectos políticos e econômicos. Dessa forma, as incertezas no nordeste asiático se expandem devido à dinâmica conflituosa entre China e Estados Unidos, que envolve fortemente Rússia e Japão. O documento elenca duas causas principais para isso: a primeira são as atividades militares dos EUA e da China no Mar da China Meridional, e a segunda são as tensões causadas pela pandemia do COVID-19 (SOUTH KOREA, 2020).

Pode-se concluir, portanto, que a prioridade da Coreia do Sul em questão de geopolítica sob a península é observar o comportamento de Estados Unidos, China, Rússia e

---

[26] No original: *Washington has been pressing Seoul to endorse its Indo-Pacific strategy and participate in related military activities; to join American decoupling efforts in trade and investment; to form a technological alliance to cope with China's challenges; and to support America's campaign to criticise Beijing's violation of democracy and human rights. Beijing has been sending a subtle warning to Seoul that although it does not want South Korea to take sides with China, it should stay neutral. If Seoul allows the U.S. to strengthen its missile defence assets in South Korea such as augmenting its THAAD (Terminal High Altitude Area Defence) missile system and/or the deployment of American intermediate-range ballistic missiles, China will treat South Korea as an enemy and take corresponding measures (CHUNG-IN; LEE, 2022, p.4)*

Japão, citando, por exemplo os gastos, efetivo e capacidades militares em seus documentos de defesa oficiais, como observa-se no quadro seguinte:

Quadro 4 - Forças militares das quatro maiores potências que cercam a Península Coreana.

	Rússia	China	Estados Unidos	Japão
Orçamento militar	48.2 bilhões de dólares	181 bilhões de dólares	738 bilhões de dólares	48,6 bilhões de dólares
Nº de tropas	900.000	2.035.000	1.380.000	247.000
Submarinos	49	59	67	21
Porta-aviões/Tanques de guerra	1 porta-avião	2 porta-aviões	11 porta-aviões	51 tanques de guerra
Forças Militares	Melhoria da capacidade nuclear, desenvolvimento de caças furtivos e mísseis estratégicos, modernização de armas convencionais	Aquisição de novos mísseis estratégicos, caças furtivos e porta-aviões; fortalecimento da guerra cibernética e das forças espaciais	Melhoria e modernização da capacidade nuclear, desenvolvimento de bombardeiros estratégicos de longa distância, fortalecimento da defesa antimísseis, guerra cibernética e espaço	Aquisição de mais F-35s, novas aeronaves de alerta, contratorpedeiros Aegis e submarinos; reforço das forças de guerra espacial, cibernética e eletrônica

Fonte: Elaboração própria com base em SOUTH KOREA, 2020.

Seria de causar estranheza que a Coreia do Norte não tenha sido citada até agora. Isso se dá porque o país tem uma sessão especial inteira no documento, intitulada "Situação Norte Coreana". A seção traz os destaques da relação entre os países:

> Desde que (...) Kim Jong-un, assumiu o cargo em 2011, a Coreia do Norte declarou a conclusão da "capacidade nuclear estatal" em 2017, concentrando suas capacidades no avanço das capacidades nucleares e de mísseis, defendendo a política "Byungjin" de desenvolver simultaneamente sua economia e armas nucleares. Em 2018, a Coreia do Norte introduziu a "linha para concentrar todos os esforços na construção econômica" como uma nova linha estratégica e buscou uma diplomacia de cúpula ativa, defendendo o objetivo da desnuclearização da Península Coreana. No entanto, o impasse nas negociações de desnuclearização foi prolongado desde o colapso da Cúpula EUA-Coreia do Norte em Hanói em 2019. Enquanto em 2020, mesmo em uma situação de aprofundamento das dificuldades econômicas devido ao COVID-19 e às sanções, a Coreia do Norte busca fortalecer sua postura operacional por meio do aprimoramento de suas capacidades nucleares e de mísseis e reforço de

> forças convencionais seletivas a pretexto de fortalecer seu poderio militar autodefensivo. (SOUTH KOREA, 2020, p. 25, *tradução nossa*)[27]

Internamente, a administração de Moon Jae-in (2017-2022) tinha como visão de estratégia nacional em defesa "uma Nação das Pessoas, uma República da Coreia Justa" e o objetivo de manter a Península Coreana próspera e pacífica e proteger a segurança e vida de seus cidadãos. O maior feito do governo Moon foi estabelecer a Estratégia de Segurança Nacional[28] a fim de realizar esse objetivo principal e resolver a questão nuclear com a Coreia do Norte sem perder uma postura robusta de segurança nacional. O documento expressa que a administração de Moon fortalecerá a aliança República da Coreia e Estados Unidos da América (ROK-USA) para aumentar suas capacidades em defesa e estabelecer a paz na península e cooperará internacionalmente para manter a paz do Nordeste Asiático (SOUTH KOREA, 2020).

3.1.2 Governança interna

O governo sul-coreano começou a promover a informatização da economia, administração estatal e sociedade no começo dos anos 1980, e junto a essas ações começaram também os esforços para a segurança cibernética. No entanto, até os anos 2000 os empenhos eram focados somente em segurança e proteção de informação (KIM; BAE, 2021).

Neste primeiro momento, a estrutura de governança em segurança cibernética da Coreia do Sul era divida em três agências: o Centro Nacional de Cibersegurança[29], criado em 2004, que respondia ao Serviço de Inteligência Nacional[30] e era responsável tanto pelo setor público quanto pelo privado; o Ministério da Ciência e Tecnologia da Informação e Comunicação, que tratava apenas de assuntos privados; e o Ministério da Defesa Nacional (MDN) para assuntos de defesa cibernética ligados ao setor militar. Esse sistema foi

---

[27] No original: "*Since (...) Kim Jong-un took office in 2011, North Korea has declared the completion of "state nuclear capability" in 2017 by focusing its capabilities on advancing nuclear and missile capabilities, advocating the "Byungjin" policy of simultaneously developing its economy and nuclear weapons. In 2018, North Korea introduced the "line to focus all efforts on economic construction" as a new strategic line and pursued active summit diplomacy, advocating the goal of denuclearization of the Korean Peninsula. However, the deadlock in denuclearization negotiations has been prolonged since the breakdown of the US–North Korea Hanoi Summit in 2019. While in 2020, even in a situation of deepening economic difficulties due to COVID-19 and sanctions, North Korea is seeking to strengthen its operational posture through the enhancement of its nuclear and missile capabilities and reinforcement of selective conventional forces on the pretext of strengthening its self-defensive military power.*" (SOUTH KOREA, 2020, p. 25)

[28] Tradução literal de National Security Strategy (NSS); no original: 국가안보전략.

[29] No original: 국가사이버안전센터; em inglês: National Cybersecurity Center (NCSC).

[30] No original: 국가정보원; em inglês: National Intelligence Service (NIS).

primordial para os primeiros avanços do país em matéria de defesa cibernética, principalmente na dissuasão dos primeiros ataques cibernéticos, como a criação do Manual Nacional de Gerenciamento de Crises Cibernéticas em resposta ao ataque de disrupção da Internet em janeiro de 2003 (KIM; BAE, 2021).

O escopo atual de atuação do Serviço de Inteligência Nacional foi determinado pela revisão da Lei do Serviço Nacional de Inteligência e definiu três tarefas principais:

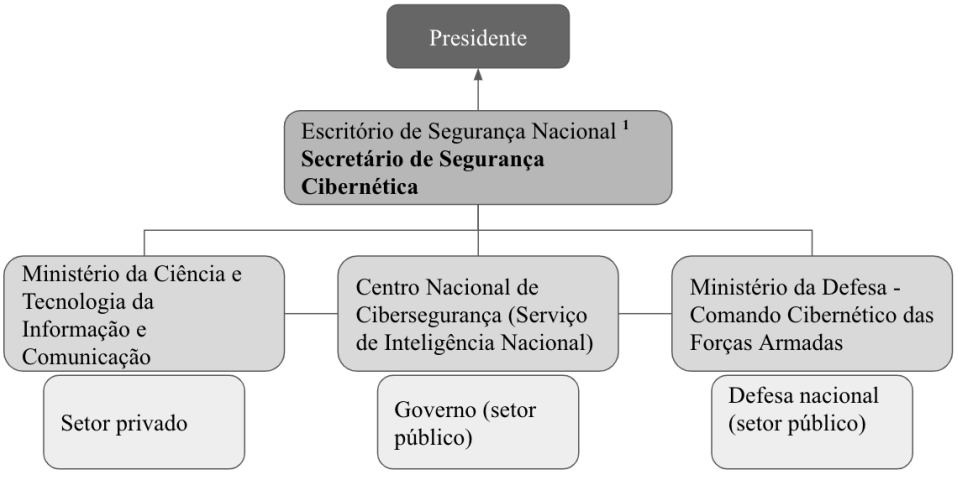
1. coleta, análise e distribuição de informações relacionadas à segurança cibernética;
2. contramedidas relacionadas ao desempenho da segurança cibernética;
3. prevenir e responder a ataques cibernéticos e ameaças contra agências governamentais e instituições do setor público (KIM; BAE, 2021).

Da mesma forma, atualmente, o Centro Nacional de Cibersegurança tem 5 funções-chave:

1. Estabelecimento de políticas públicas e consultoria;
2. Detecção de ameaças e resposta;
3. Investigação de incidentes e controle de danos;
4. Compartilhamento de informações e cooperação;
5. Educação e treinamento (SOUTH KOREA, 2021).

Por fim, o Livro Branco de Segurança Informacional de 2018 traz o esquema mais atualizado de governança interna em cibernética da Coreia do Sul:

Figura 2 - Estado do Sistema Nacional de Implementação de Segurança Cibernética.



[1] No original: 국가안보실, em inglês: National Security Office

Fonte: Elaboração própria com base em SOUTH KOREA, 2018b, p. 52.

Na nova formação, o órgão mais importante em questões de cibernética passa a ser o Escritório de Segurança Nacional, o que demonstra clara mudança na percepção da Coreia sobre o espaço cibernético como domínio de poder. Além disso, percebe-se que o país divide claramente as questões de defesa e segurança entre espaços públicos e privados, respectivamente.

3.1.3 Plano Diretor Nacional de Segurança Cibernética (2011)

O Plano Diretor é uma estratégia de resposta abrangente ao nível nacional para lidar efetivamente com as ameaças cibernéticas nacionais, que estão se tornando cada vez mais sofisticadas e inteligentes. O documento foi escrito pela Comissão de Comunicações Coreana durante o encontro "Conselho Nacional de Contramedidas de Segurança Cibernética". Os pontos-chave do documento são juntar o setor público, o privado e o militar para estabelecer um sistema de resposta conjunta; reforçar a segurança de infraestruturas críticas; estabelecer a dissuasão de ataques por cooperação internacional, construir infraestruturas de segurança cibernética e deter e bloquear ataques cibernéticos ao nível nacional (SOUTH KOREA, 2011).

A "Equipe nacional de resposta conjunta a ameaças cibernéticas" é um grupo focal criado em 2012[31] do setor privado, público e militar sob o Centro Nacional de Cibersegurança para fortalecer os laços de cooperação internos. O grupo visa prioritariamente a criação de um sistema para detecção e resposta antecipada às ameaças cibernéticas. Para isso, será estabelecido o "Sistema de Defesa em 3 Camadas" que conectará gateways internacionais, provedores de serviços de Internet e usuários finais para identificar e impedir ataques cibernéticos com antecedência. Além disso, há um fortalecimento do sistema de resposta no setor financeiro, que inclui a melhoria da segurança nas instituições financeiras e a ampliação dos serviços de monitoramento de segurança para seguradoras e corporações de cartão de crédito. Por fim, está sendo reforçado o sistema de restauração cibernética, através do desenvolvimento e distribuição de softwares antivírus (SOUTH KOREA, 2011).

A segunda prioridade é melhorar o nível de segurança de informações e instalações críticas. Para isso, a criptografia será amplamente utilizada para proteger informações oficiais. As medidas de segurança para as infraestruturas críticas, como centrais elétricas e meios de

[31] A versão atualizada do documento conta notas com as ações de resposta aos pontos planejados em 2011.

transporte, também serão reforçadas e será estabelecido um sistema para diagnóstico de vulnerabilidades de segurança do software do governo. Para além, o grupo busca o desenvolvimento de uma nova plataforma para melhorar a segurança cibernética. A esfera jurídica também sofrerá alterações para acomodar os planos de melhoria da segurança cibernética através da promulgação de novas leis. O documento promete criar armas exclusivas para segurança cibernética e fornecer suporte para a exportação de produtos de proteção de informações e aumentar o orçamento para P&D de proteção de informações (SOUTH KOREA, 2011).

Por fim, fortalecendo a dissuasão contra ataques cibernéticos e aumentando a colaboração internacional, a junta ampliará as relações de cooperação com outras potências e organizações internacionais no campo de segurança cibernética e estabelecerá sistemas de compartilhamento de informações. Implementando, assim, um "esquema de verificação privada" para lidar com a suspeita pública sobre perpetradores e para construir confiança junto ao público e promovendo treinamentos conjuntos entre organizações relacionadas para aumentar sua capacidade de lidar de forma eficaz com crises cibernéticas (SOUTH KOREA, 2011).

3.1.4 Regulamentos Nacionais de Gerenciamento de Segurança Cibernética[32] (2013)

Essa ordem presidencial publicada pelo Serviço de Inteligência Nacional[33] tem o objetivo de "proteger a rede nacional de informações e comunicações de ataques cibernéticos que ameacem a segurança nacional, fortalecendo a cooperação"[34] e "estipula o sistema organizacional e operacional relacionado à segurança cibernética nacional"[35] (SOUTH KOREA, 2013, p.1). Ou seja, traz a definição de termos relacionados à cibernética para a Coreia do Sul, principalmente para conhecimento e informação dos órgãos públicos centrais afiliados à presidência da Coreia do Sul. Como se observa no quadro:

[32] No original: "국가사이버안전관리규정".
[33] No original: 국가정보원.
[34] No original: " 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로 한다" (SOUTH KOREA, 2013, p.1).
[35] No original: "국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간" (SOUTH KOREA, 2013, p.1).

Quadro 5 - Conceitos e definições presentes em "Regulamentos Nacionais de Gerenciamento de Segurança Cibernética".

Rede de informação e comunicações (정보통신망)	"Uso de equipamentos de telecomunicações e computadores e sistemas de informação e comunicação que coletam, processam, armazenam, pesquisam, transmitem ou recebem informações utilizando tecnologia de computador."[36]
Ataque cibernético (사이버공격)	"O termo "todos os atos de ataque" significa intrusão ilegal, perturbação, paralisia, destruição ou roubo ou destruição de informações por meios eletrônicos, como hacking, vírus de computador, bombas lógicas, bombas de correio e obstrução de serviço."[37]
Segurança cibernética (사이버안전)	"O estado de manutenção da segurança, como a confidencialidade, integridade e disponibilidade das redes nacionais de informação e comunicação, protegendo as redes nacionais de informação e comunicação de ataques cibernéticos."[38]
Crise cibernética (사이버위기)	"Uma situação na qual informações distribuídas e armazenadas através de redes de informação e comunicação vazam, mudam ou são destruídas, afetando a segurança nacional, causando confusão social e econômica, ou danificando ou paralisando funções essenciais do sistema nacional de informação e comunicação"[39]
Instituição pública (공공기관)	"Outras instituições públicas estabelecidas sob outras leis e regulamentos designados pela Reunião Nacional de Estratégia de Segurança Cibernética (...) como necessárias para garantir a segurança da rede de informação e comunicação."[40]

Fonte: Elaboração própria com base em SOUTH KOREA, 2013. p.1.

[36] No original: "전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다" (SOUTH KOREA, 2013, p.1).
[37] No original: "이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망 을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말한다″ (SOUTH KOREA, 2013, p.1).
[38] No original: "사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성 ·가용성 등 안전성을 유지하는 상태를 말한다" (SOUTH KOREA, 2013, p.1).
[39] No original: "사이버공격으로 정보통신망을 통해 유통·저장되는 정보를 유출·변경·파괴함으로써 국가안보에 영향을 미치거나 사회·경제적 혼란을 발생시키거나 국가 정보통신시스템의 핵심기능이 훼손·정지되는 등 무력화되는 상황을 말 한다" (SOUTH KOREA, 2013, p.1).
[40] No original: "그 밖에 다른 법령의 규정에 의하여 설립된 공공기관 중 제*6*조의 규정에 의한 국가사이버안전전략회의에서 정보통신 망의 안전성 확보가 필요하다고 지정한 기관" (SOUTH KOREA, 2013, p.1).

3.1.5 Estratégia Nacional de Segurança Cibernética (2019)

Em 2019 o Escritório de Segurança Nacional publicou o mais recente e importante documento de estratégia em segurança cibernética da Coreia do Sul: a Estratégia Nacional de Segurança Cibernética (2019). Esse documento visa enfrentar crescentes ameaças cibernéticas, proteger a segurança, os direitos e o interesse das pessoas em face ao crime cibernético e detectar e bloquear de forma rápida e eficaz as ameaças cibernética a fim de proteger as operações vitais do governo, bem como promover e estimular talentos em cibernética e apoiar o desenvolvimento da indústria de segurança cibernética. Reconhece as ameaças cibernéticas como ameaças à segurança nacional, sendo, portanto, elaborado em linha de congruência com as estratégias de segurança nacional (SOUTH KOREA, 2019).

No prefácio escrito pelo então presidente Moon Jae-In é reafirmada a posição de liderança tecnológica, de informação e infraestrutura, que a Coreia do Sul apresenta no mundo. Traz também a importância do ciberespaço como base da estrutura do governo e como o domínio que fornece serviços administrativos e opera as infraestruturas críticas do país. As ameaças cibernéticas, como ciber crime e ciber terrorismo colocam em risco a vida da população civil, fazendo com que ataques cibernéticos sejam um desafio a segurança nacional. A garantia da segurança cibernética é, então, prioridade para o governo, que não poupa esforços para criar um ambiente online seguro e livre (SOUTH KOREA, 2019).

Dessa forma, a visão principal da República da Coreia é "criar um ciberespaço livre e seguro para apoiar a segurança nacional, assim como promover a prosperidade econômica e contribuir para a paz internacional"[41] (SOUTH KOREA, 2019, p. 12). Para isso, elenca três objetivos e três princípios básicos:

[41] No original: "*Create a free and safe cyberspace to support national security, promote economic prosperity, and contribute to international peace*" (SOUTH KOREA, 2019, p. 12).

Quadro 5: Objetivos e princípios básicos em segurança cibernética da Coreia do Sul

Objetivos	Garantir operações estáveis do estado: fortalecer a segurança e a resiliência da infraestrutura central do país para permitir a operação contínua, apesar de quaisquer ameaças cibernéticas
	Responder a ataques cibernéticos: fortalecer os recursos de segurança para deter ameaças cibernéticas, detectá-las e bloqueá-las rapidamente e responder a qualquer incidente prontamente
	Construa uma base sólida de segurança cibernética: fomente um ecossistema justo e autônomo onde a tecnologia de segurança cibernética, os recursos humanos e os setores sejam competitivos
Princípios básicos	Equilibre os direitos individuais com a segurança cibernética: encontre um equilíbrio entre proteger o ciberespaço e salvaguardar os direitos fundamentais das pessoas, por exemplo, privacidade.
	Realizar atividades de segurança com base no Estado de Direito: Executar as políticas e atividades de segurança cibernética do governo de maneira transparente e em conformidade com as leis nacionais e internacionais
	Construa um sistema de participação e cooperação: incentive indivíduos, empresas e o governo a participarem de atividades de segurança cibernética e busque uma cooperação estreita com a comunidade internacional

Fonte: Elaboração própria com base em SOUTH KOREA, 2019, p. 12.

O documento admite que, mesmo sendo um dos ambientes cibernéticos mais prósperos, a República da Coreia ainda está suscetível a ameaças cibernéticas, que podem afetar o ambiente físico, já que as tecnologias estão presentes no dia a dia dos cidadãos coreanos e pontua-se que a severidade dessas ameaças evoluíram com o tempo. No passado, os ataques cibernéticos sofridos pela Coreia se resumiam a grupos de indivíduos maliciosos e hackers, às vezes apoiados por setores estatais. Agora, os ataques sofridos estão cada vez mais organizados e em maior escala, desde roubo de dados pessoais, informaçõesconfidenciais e dinheiro, até causar agitação social com fins políticos e terrorismo cibernético, que resultam em destruição de infraestruras críticas. O documento não descarta a possibilidade de uma guerra cibernética, já que as disputas tradicionais entre os estados estão escalando para o espaço cibernético (SOUTH KOREA, 2019).

É importante para a Coreia do Sul reconhecer as capacidades cibernéticas de outros países e, para isso, o estado fomenta a formação de especialistas em cibernética e expande as organizações focadas em segurança cibernética. O governo também aumentou o orçamento de forma substancial para o desenvolvimento de tecnologias cibernéticas, como inteligência

artificial e análise de dados. Admite-se, porém, que a "proporção do orçamento de cibersegurança do governo em proporção ao orçamento nacional ainda fica aquém da dos países desenvolvidos"[42] (SOUTH KOREA, 2019, p. 9).

Outra crítica é que mesmo possuindo medidas eficazes, como um sistema automático de identificação e resposta a ataques cibernéticos, o foco é aumentar a resiliência de serviços nacionais e infraestruturas críticas. Demonstra que as ações governamentais de publicação de leis e decretos são pouco proveitosas enquanto não houver investimento substancial em pesquisa e inovação. Ainda há a visão de segurança cibernética como custo, o que limita o país em tentar diminuir a lacuna com outros países desenvolvidos (SOUTH KOREA, 2019).

Traz-se a visão sul coreana sobre cooperação internacional em cibernética. Para responder às ameaças externas, o governo busca cooperar com aliados e com organizações internacionais, como as Nações Unidas e a UIT, o propósito é promover "cooperação internacional sistemáticas e práticas, como a adesão a convenções internacionais, o compartilhamento de informações e tecnologia e a elaboração de regras internacionais sobre segurança cibernética" [43] (SOUTH KOREA, 2019, p. 9).

Por fim, apresentam-se as estratégias táticas para atingir os objetivos citados previamente. Para garantir o fornecimento de serviços, a Coreia planeja reforçar a segurança e resiliência da infraestrutura central nacional contra ataques cibernéticos, reforçando a segurança das redes nacionais de informação e comunicação e desenvolvendo infraestruturas de segurança cibernética de última geração. Expandindo a capacidade de deter ataques cibernéticos o mais cedo possível e com eficiência, a Coreia do Sul planeja melhorar sua capacidade de resposta a esses ataques. Para isso, deve-se garantir a dissuasão, aprimorar recursos de resposta ao crime cibernético e elaborar contramedidas eficientes (SOUTH KOREA, 2019).

Outra estratégia é estabelecer uma governança baseada na confiança e cooperação. O país prioriza a confiança interna para facilitar a cooperação público, privada e militar através de "segurança cibernética voltada para o futuro com base na confiança mútua e na cooperação entre indivíduos, empresas e o governo, abrangendo os setores público, privado e militar"[44]

---

[42] No original: "*ratio of the government's cybersecurity budget in proportion to the national budget still falls short that of developed countries, and there remains a shortage of talented cybersecurity experts*" (SOUTH KOREA, 2019, p. 9)

[43] No original: "*systematic and practical international cooperative activities, such as joining international conventions, sharing information and technology, and drawing up international rules on cybersecurity"* (SOUTH KOREA, 2019. p. 9).

[44] No original: "Execute a future-oriented cybersecurity framework based on mutual trust and cooperation among individuals, businesses, and the government, encompassing the public, private, and military sectors" (SOUTH KOREA, 2019. p. 18).

(SOUTH KOREA, 2019, p. 18). A cooperação internacional também é citada como uma estratégia. A Coreia pretende tornar-se um líder em segurança cibernética no sistema internacional, participando de sistemas de cooperação multi e bilaterais e contribuindo para a formação de regras internacionais (SOUTH KOREA, 2019).

Aumentar o investimento em segurança cibernética para construir uma base sólida para o crescimento do setor cibernético também é um fator listado, além de favorecer a competitividade da força de trabalho em tecnologia. A próxima estratégia é adotar uma cultura em cibersegurança e, para isso, deve-se aumentar a conscientização e fortalecer práticas de segurança cibernética, a fim de equilibrar os direitos individuais com a segurança cibernética (SOUTH KOREA, 2019).

3.1.6 Livros Branco de Defesa (2006 - 2020)

A primeira vez que a palavra cibernética é citada em um livro branco de defesa da Coreia do Sul é em referência à digitalização das Forças Armadas, na edição de 2006. O documento afirma que a digitalização da defesa tem por objetivo aprimorar as capacidades militares, por meio da automatização dos sistemas de comando e controle e pelo gerenciamento do campo de batalha. Ademais, busca a realização de gestão de defesa e operação de baixo custo, bem como alta eficiência com base na digitalização e transações eletrônicas de gestão de recursos de defesa. Para atingir esses objetivos, três estratégias foram apresentadas: expandir as infraestruturas de digitalização; construir políticas governamentais para digitalização da defesa e investir em educação para a digitalização (SOUTH KOREA, 2006).

Dentro da estratégia de expansão de infraestruturas de digitalização, é citado pela primeira vez o termo segurança cibernética. Antes mesmo da publicação do Livro Branco, um manual prático para confrontos que ameaçam a segurança cibernética foi publicado, e uma "Equipe de Resposta a Emergências de Computador"[45] que:

> estabeleceram o sistema básico de combate às ameaças cibernéticas, desenvolvendo um sistema integrado de controle de segurança, sistema de prevenção de vírus de computador e sistema de certificação militar. Além disso, eles serão organizados para ter mais funções de acordo com o estabelecimento do sistema de informações de gerenciamento do campo de batalha e do escritório integrado de gerenciamento de informações de defesa. O MND planeja atualizar o sistema de proteção de

[45] No original: "*Computer Emergency Response Team (CERT)"*

> informações para futuras **guerras centradas na rede** (SOUTH KOREA, 2006, p. 185, *tradução nossa, grifo nosso*)[46].

Essa necessidade de digitalização era baseada no conceito de campo de batalha do futuro, ou seja, os conflitos ocorrerão com um sistema de gestão do campo de batalha automatizado, capaz de integrar e operar todos os componentes de força, como controle e comando e inteligência militar (SOUTH KOREA, 2006).

No documento publicado em 2008, os ataques cibernéticos são listados pela primeira vez como ameaças não militares e, além disso, guerra cibernética, defesa cibernética e ameaças cibernéticas são citadas pela primeira vez. Declara-se, que a Coreia do Norte segue a tendência de modernização global e está reforçando a capacidade de executar a guerra moderna e "isso é evidenciado pela construção de um sistema de automação de comando e pelo cultivo de hackers de computador para guerra cibernética"[47] (SOUTH KOREA, 2008, p. 27, *tradução nossa*).

A Coreia do Sul estava atenta às mudanças nas tecnologias de informação e comunicação em 2008, portanto, planejava criar um ambiente para informatização centrada em rede, com o objetivo de responder eficazmente às guerras do futuro. A estratégia de informatização da defesa foi aprimorada de acordo com a política nacional de defesa e a infraestrutura foi reforçada para garantir o compartilhamento de informações. O Ministério da Defesa também objetivava integrar as tecnologias de informação e comunicação com as questões de defesa do país (SOUTH KOREA, 2008).

O documento segue listando ações do Ministério da Defesa para maximizar o cumprimento de suas missões em tempos de guerra e paz, enfrentando ameaças cibernéticas cada vez mais rebuscadas e malignas. Em 2007, adicionou um manual de regulações e respostas às ameaças cibernéticas no "Condição de Operações de Informação"[48] (SOUTH KOREA, 2008).

Em 2010 é publicizada a formação do Comando Cibernético dentro das Forças Armadas da República da Coreia a fim de estabelecer um Centro de Resposta à Guerra Cibernética. Todos os computadores conectados com a Rede de Informação de Defesa foram,

---

[46] No original: "*have set up the basic system tackling cyber threats by developing an integrated security control system, computer virus prevention system, and military certification system. In addition, they will be organized to have more duties according to the establishment of the battlefield management information system and the defense integrated information management office. The MND plans on upgrading the information protection system for future NCW*" (SOUTH KOREA, 2006, p. 185).

[47] No original: "*This is evidenced by the construction of a command automation system and by the cultivation of computer hackers for cyber warfare*" (SOUTH KOREA, 2008, p. 27).

[48] No original: *"Information Operations Condition (INFOCON)*" é um sistema de defesa baseado principalmente no status dos sistemas de informação e é um método usado pelos militares para se defender contra um ataque à rede de computadores (USA, 2006).

assim, equipados com um sistema antivírus, um sistema próprio de identificação e detenção de hackers. Os sistemas de informação e comunicação usados em campo de batalha agora são operados em redes criptografadas para reduzir as chances de sofrerem ataques cibernéticos (SOUTH KOREA, 2010). Outra inovação foi a criação do Sistema de Proteção Distribuída de Negação de Serviço[49] no qual:

> O direito de acesso a dados importantes foi classificado em vários níveis para garantir a operação estável do ambiente de compartilhamento de informações, protegido pelo Gerenciamento de Dados Classificados Sistema. Sistemas para diagnosticar e prevenir a liberação de informações pessoais foram implementados para proteger melhor as informações pessoais[50] (SOUTH KOREA, 2010, p. 165, *tradução nossa*).

No Livro Branco de Defesa, publicado em 2014, é divulgado o Plano Básico de Reforma da Defesa das Forças Armadas da Coreia, tendo em vista que o contexto atual de segurança interna e externa está em constante evolução, exige adaptações no ambiente de defesa. Com base na política de reforma da defesa, as diretrizes do plano asseguram que a estrutura militar esteja pronta para lidar com qualquer situação de conflito no futuro, e que o sistema de gerenciamento de defesa opere com eficiência. O encaminhamento principal da reforma é buscar o desenvolvimento da ciência e tecnologia de defesa, ao mesmo tempo em que revitaliza a cooperação civil-militar por meio da transferência de tecnologias de defesa para o setor privado (SOUTH KOREA, 2014).

É importante destacar a presença da estratégia de cooperação internacional em assuntos cibernéticos nesta edição. É necessário, para a Coreia do Sul, que a comunidade internacional tome medidas conjuntas, uma vez que os perpetradores de ataques cibernéticos estão organizados e ampliando seus alvos, atacando não somente nações, mas também indivíduos e empresas. Como resultado, as ameaças de ataques cibernéticos têm aumentado. Traz-se evidência para a posição de destaque da Coreia para os esforços de cooperação, citando a terceira Conferência Global sobre Espaço Cibernético, realizada em Seul em outubro de 2013, que reuniu participantes de 87 nações e 18 instituições internacionais. O evento ofereceu uma oportunidade para que os participantes discutissem maneiras de colaboração entre as nações para garantir a segurança cibernética, contribuindo para o

---

[49] Em inglês: Distributed Denial of Service (DDoS) Protection System.

[50] No original: "*The right to access important data has been classified in various levels to ensure stable operation of the information sharing environment, which is protected by the Classified Data Management System. Systems to diagnose and prevent the release of personal information have been implemented to better protect of personal information.*" (SOUTH KOREA, 2010, p. 165)

aprimoramento do sistema de cooperação internacional contra as ameaças cibernéticas (SOUTH KOREA, 2014).

Por fim, o documento de 2014 trata detalhadamente sobre a necessidade de se preparar para guerras do futuro e reconhece o espaço cibernético como futuro campo de batalha. O Ministério da Defesa Nacional afirma que, à medida que o tempo avança, enquanto a guerra convencional perdura, uma infinidade de novos tipos de guerra surgirá devido aos avanços tecnológicos. Os países dominantes travarão a guerra por meio de tecnologia e guerra de informação, implantando armamento avançado para ataques de precisão de longo alcance e operações secretas para minimizar as perdas. Os futuros campos de batalha abrangerão o espaço sideral e o ciberespaço, apresentando tanto a guerra cinética por meio de forças militares quanto a guerra não cinética, como a guerra cibernética (SOUTH KOREA, 2014).

O documento de 2016 inicia alertando sobre a quantidade e seriedade de ataques cibernéticos conduzidos pela Coreia do Norte, na mensagem inicial do então ministro da defesa, que afirma que o foco do preparo será para dissuadir as ameaças do país vizinho, principalmente os ataques cibernéticos (SOUTH KOREA, 2016).

A seriedade de ataques cibernéticos é destacada como uma ameaça transnacional. Numerosos casos surgiram onde os sistemas de computador, não apenas os de empresas privadas, mas também os de organizações governamentais foram infiltrados, levando a graves problemas de funcionamento do sistema ou falhas completas do sistema. A partir do final de outubro, a Coreia do Norte iniciou uma campanha de propaganda e guerra ciberpsicológica em um esforço para fomentar a agitação civil na Coreia do Sul (SOUTH KOREA, 2016).

A fim de obter uma vantagem militar sobre a República da Coreia, a Coreia do Norte está alocando recursos significativos para capacidades assimétricas, como armas nucleares e mísseis de destruição em massa, artilharia de longo alcance, capacidades subaquáticas, unidades de forças especiais, e **unidades cibernéticas**, ao mesmo tempo em que aumenta a eficácia de seu armamento convencional. Vale notar que a Coréia do Norte estabeleceu uma equipe de 6.800 especialistas em guerra cibernética, altamente treinados, que estão conduzindo uma variedade de ataques cibernéticos. É enfatizado que vindo da Coreia do Norte os "ataques cibernéticos (...) representam grandes ameaças à nossa segurança nacional"[51] (SOUTH KOREA, 2016, p.41, *tradução nossa*).

A República da Coreia novamente dá destaque a avanços em cooperação internacional em cibernética e aponta que assuntos públicos - de governo - e privados estão em espaços diferentes de negociação. Durante a quinta assembleia do UN GGE (Grupo de Especialistas

[51] No original: "*cyber-attacks (...) pose major threats to our national security"* (SOUTH KOREA, 2016, p.41)

Governamentais) sobre Segurança da Informação, em 2016, os participantes examinaram as ameaças cibernéticas e deliberaram sobre os regulamentos e padrões internacionais relevantes para o domínio cibernético. Além disso, o Forum of Incident Response and Security Teams[52] (FIRST), um consórcio consultivo do setor privado, está se esforçando para reforçar a colaboração global no domínio da segurança da Internet (SOUTH KOREA, 2016). Outro destaque em cooperação é a aliança em defesa da Coreia do Sul com os Estados Unidos para amenizar os desafios que ameaças cibernéticas causam à segurança coreana:

> A República da Coreia e os Estados Unidos estão construindo um sistema de defesa combinado de amplo espectro para manter a paz e a estabilidade na Península Coreana acima de tudo. Ao manter diálogos de defesa de forma regular e ad hoc, os dois países coordenarão políticas de perto, administrarão com eficácia questões importantes para a Aliança ROK-EUA, garantirão as condições necessárias para o desdobramento de forças rotativas e realizarão exercícios combinados continuamente e formação. A transição do controle operacional em tempo de guerra ocorrerá de maneira estável, avaliando periodicamente se as condições exigidas são atendidas e os dois países ampliarão o nível e o escopo da cooperação para incluir a cooperação espacial **e cibernética** (SOUTH KOREA, 2016, p.45, *tradução nossa, grifo nosso)*.[53]

No capítulo intitulado "Estabelecendo uma postura de defesa robusta"[54] é exposto como as forças armadas operam ativos de vigilância com os esforços de cooperação para combater ataques cibernéticos, além de aumentar a capacidade de resposta aos ataques, desenvolvendo políticas e sistemas de cibersegurança, fomentando especialistas cibernéticos , adquirindo tecnologias e sistemas para responder a ciberameaças (SOUTH KOREA, 2016).

O documento de 2018 destaca as tensões elevadas por um teste nuclear conduzido pela Coreia do Norte em 2017, sendo o foco desse documento os esforços para a desnuclearização da Coreia do Norte; outro assunto relevante é a conclusão da Reforma de Defesa 2.0. Por fim, o ministro da defesa promete criar um "exército inteligente", adotando ativamente as principais tecnologias da Quarta Revolução Industrial no campo da defesa para uma gestão eficiente do orçamento de defesa (SOUTH KOREA, 2018a).

---

[52] Fórum de Resposta a Incidentes e Equipes de Segurança.

[53] No original: "*The ROK and the United States are building a full-spectrum combined defense system to maintain peace and stability on the Korean Peninsula above all else. By holding defense dialogues both on a regular and ad-hoc basis, the two countries will closely coordinate policies, effectively manage issues of importance to the ROK-U.S. Alliance, ensure conditions necessary for the deployment of rotational forces, and continuously carry out combined exercises and training. The transition of the wartime operational control will proceed in a stable manner by periodically evaluating whether the required conditions are met and the two countries will broaden the level and scope of cooperation to include space and cyber cooperation"* (SOUTH KOREA, 2016, p.45).

[54] No original: "*Establishing a Robust Defense Posture*"

Dentro das políticas de estratégia de defesa e segurança nacional é citado como papel do governo da República da Coreia é o de proteger a segurança e privacidade individual dos seus habitantes contra ataques cibernéticos. Para além, ressalta-se o compartilhamento de informações civil-governo-militar-policial que foi construído e operado como uma postura de prontidão para estabelecer respostas robustas contra ameaças à segurança cibernética. As Forças Armadas também instituíram um sistema de cooperação com o Ministério da Tecnologia da Informação e Comunicação e revisaram o manual de prontidão para situações de interrupção do sinal de GPS para enfrentar as investidas de interferência do sistema de posicionamento global provenientes da Coreia do Norte (SOUTH KOREA, 2018a).

Como citado anteriormente, no ano de 2010, as Forças Armadas da República da Coreia (ROKA) fundaram o Comando Cibernético das Forças Armadas para criar uma estrutura institucional e organizacional capaz de conduzir operações de guerra cibernética. Desde então, têm respondido ativamente às ameaças cibernéticas em constante crescimento. Entretanto, houve preocupações em relação à segurança cibernética após o incidente de invasão de rede de defesa e a polêmica sobre a suposta interferência política ilegal do Comando Cibernético em 2016. A necessidade de ampliar continuamente as capacidades de resposta contra ameaças cibernéticas cada vez mais sofisticadas e inteligentes também aumentou (SOUTH KOREA, 2018a).

O Ministério da Defesa Nacional planejava classificar a resposta militar a uma violação do espaço cibernético como um domínio de "operações cibernéticas" e criar um sistema de execução de operações cibernéticas liderado pelo Estado-Maior Conjunto. As missões e estrutura de trabalho sob essa estratégia ampla foram definidas da seguinte forma: o ministério atua como centro de controle das políticas cibernéticas, enquanto o Estado-Maior Conjunto comanda as operações cibernéticas de todo o exército. O Comando Cibernético assume o papel de unidade responsável pela implementação e execução final de todas as operações e pela segurança cibernética das Forças Armadas. As sedes de cada ramo e as unidades de cada nível são encarregadas da segurança cibernética e das operações defensivas relacionadas à área e aos ativos sob sua responsabilidade (SOUTH KOREA, 2018a).

A última novidade é uma reforma em escala total da organização e funções do comando cibernético. O Comando Cibernético como "Comando de Operações Cibernéticas" foi estabelecido como uma unidade conjunta capaz de realizar operações cibernéticas sob a autoridade do Presidente do Estado-Maior Conjunto. Houve uma controvérsia sobre a possível interferência política ilegal por parte do Comando Cibernético, resolvida, em grande

parte, com a eliminação de sua função controversa de guerra psicológica, permitindo-o focar exclusivamente em sua missão original: operações cibernéticas (SOUTH KOREA, 2018a).

O último documento disponível é o Livro Branco de Defesa de 2020. A situação conflituosa com a Coreia do Norte não apresentou grande melhora desde o documento anterior, segundo o Ministro da Defesa Suh Wook (2020), que agora acrescenta a China como perigo a segurança cibernética coreana, afirmando que "os países vizinhos da Península Coreana continuam a reforçar suas capacidades militares (...) expandem seus domínios militares (...) no ciberespaço"[55] (SOUTH KOREA, 2020, p. 3, *tradução nossa*).

A pandemia do COVID-19 foi um fator facilitador para ameaçar a segurança cibernética do país, já que muitas tarefas primordiais para a sociedade passaram a ser realizadas a distância. Com a dependência de tecnologias digitais se intensificando na tentativa de combater a propagação do COVID-19, o aumento dos ataques cibernéticos está diretamente relacionado com o avanço das tecnologias de informação e comunicação (SOUTH KOREA, 2020).

Mudanças contínuas nas condições de segurança levaram a repetidos ajustes e atrasos da efetivação da Reforma de Defesa sul coreana. As ameaças à segurança, como exemplo dessas mudanças, tornaram-se mais abrangentes, incluindo o aumento da instabilidade no Nordeste da Ásia, ameaças da Coreia do Norte e ameaças transnacionais e não militares, como desastres naturais, terrorismo e ataques cibernéticos. Devido à rápida deterioração das condições para a implementação das políticas de defesa, como a escassez de recursos do serviço militar devido ao declínio populacional e a demanda crescente por direitos humanos e bem-estar, a reforma da defesa nacional não pode mais ser adiada (SOUTH KOREA, 2020).

As forças armadas continuam considerando e se preparando para uma guerra de grande escala, por meio de exercícios conjuntos com os Estados Unidos. Em caso de emergência, as forças militares empregarão táticas combinadas e conjuntas para finalizar o conflito o mais rápido possível e obter vitórias decisivas em todas as áreas de atuação, como terrestre, aérea, marítima, espacial e cibernética. Além disso, melhorar as capacidades de defesa cibernética nacionais continua sendo listada como uma estratégia para estabelecer um sistema de resposta para ameaças de segurança transnacionais e não militares. O desenvolvimento de políticas e estratégias de segurança cibernética de defesa e sistema de

[55] No original: "*Neighboring countries of the Korean Peninsula continue to reinforce their cutting-edge military capabilities, pushing their own priorities while expanding their military domains (...) cyber.*" (SOUTH KOREA, 2020, p. 3)

execução de missões de guerra cibernética é uma forma de melhorar as capacidades (SOUTH KOREA, 2020).

Com o avanço das Tecnologias da Informação e Comunicação (TIC)e Infraestrutura, as ameaças no ciberespaço se tornaram cada vez mais sofisticadas e diversificadas. Como resultado, o sucesso das operações militares está altamente relacionado ao ciberespaço. Com isso em mente, as Forças Armadas da República da Coreia estão reforçando seus recursos de segurança cibernética para estabelecer e manter um ciberespaço de defesa preciso e seguro, garantindo assim uma vantagem estratégica nessa área. Um exemplo desses esforços foi a publicação da Estratégia Nacional de Segurança Cibernética em 2019, promovida pelo Escritório de Segurança Nacional (SOUTH KOREA, 2020).

Com o objetivo de aprimorar a postura de operações cibernéticas e responder de maneira efetiva às ameaças de segurança cibernética, o Ministério da Defesa estabeleceu, em 2019, um sistema centralizado de execução de operações cibernéticas, sob a supervisão do Estado-Maior Conjunto. Além disso, um sistema orgânico de controle e relatórios de operações cibernéticas foi implementado entre o Estado-Maior Conjunto o Comando de Operações Cibernéticas e cada serviço militar. Em fevereiro do mesmo ano, o "Comando Cibernético da República da Coreia"[56] foi reorganizado como "Comando de Operações Cibernéticas"[57] e designado como uma força conjunta sob o comando do Presidente do Estado-Maior Conjunto. O Ministério da Defesa também reorganizou o "Centro de Proteção Cibernética"[58] de cada serviço para "Centro de Operações Cibernéticas"[59] e aumentou o seu efetivo, transformando a estrutura organizacional para ser mais adequada à realização de operações cibernéticas (SOUTH KOREA, 2020).

Expõe-se que, no campo das operações cibernéticas, a capacidade operacional é altamente dependente da habilidade e experiência dos especialistas, mais do que em outras áreas de batalha. Portanto, outra estratégia é aprimorar o conhecimento dos especialistas cibernéticos. Dessa forma, a Coreia do Sul está desenvolvendo um sistema integrado de gerenciamento de especialistas, que abrange todo o processo de aquisição, treinamento, nomeação e promoção. Em 2019 foi criada a especialização em cibernética para oficiais e suboficiais e em 2020, a designação de cargos cibernéticos para funcionários civis militares, estabelecendo assim, uma sólida base para aquisição e gerenciamento estável de especialistas em segurança cibernética (SOUTH KOREA, 2020).

---

[56] *the ROK Cyber Command*
[57] *Cyber-Operations Command*
[58] *Cyber-Protection Center*
[59] Cyber-Operations Center

Outra novidade é a criação de um sistema ciber operacional que integra e visualiza vários tipos de informações necessárias às operações cibernéticas, permitindo aos comandantes uma rápida tomada de decisão e um controle mais eficaz. Além disso, estão sendo construídas ciber forças especializadas em sistemas de detecção e análise que identificam comportamentos anômalos na rede, como códigos maliciosos. Para se adaptar ao ambiente cibernético em constante mudança, o Ministério da Defesa tem planos de melhorar continuamente sua capacidade de resposta a ataques cibernéticos não estruturados com a ajuda de tecnologias avançadas, como a inteligência artificial, e reforçar ainda mais as funções e o desempenho do sistema de operação cibernética (SOUTH KOREA, 2020).

Em assuntos de cooperação cibernética, a Coreia do Sul planeja manter os Estados Unidos como seu maior aliado. O Ministério da Defesa Nacional e o Departamento de Defesa dos EUA (DoD) têm colaborado no Grupo de Trabalho de Cooperação Cibernética desde 2014, por meio do qual compartilham informações sobre ameaças cibernéticas e discutido planos de cooperação e intercâmbio nas áreas de tecnologia, recursos humanos e organizações. A Coreia do Sul tem planos de desenvolver esse grupo para um importante órgão consultivo multilateral no campo da cooperação cibernética em defesa, fortalecendo as capacidades cibernéticas dos países participantes e construindo confiança entre eles (SOUTH KOREA, 2020).

Ademais, desde 2018, o Ministério da Defesa Nacional tem participado do Grupo de Trabalho de Especialistas em Segurança Cibernética no âmbito do Grupo de Trabalho de Especialistas em Segurança Cibernética na Reunião de Ministros da Defesa da ASEAN-Plus (ADMM-Plus), que envolve 10 países da Associação das Nações do Sudeste Asiático (ASEAN), mais 8 países, incluindo os Estados Unidos e a Coreia do Sul. O objetivo deste grupo é compartilhar informações e políticas de segurança cibernética e realizar exercícios para melhorar a capacidade de gestão de crises diante de ameaças cibernéticas. A Coreia do Sul assumirá, entre 2020 e 2023, a tarefa de co-presidir o grupo com a Malásia, a fim de identificar as capacidades políticas e tecnológicas dos membros e fortalecer as parcerias internacionais com os países ASEAN e ASEAN Plus (SOUTH KOREA, 2020).

Pela primeira vez, é discutido sobre orçamento militar em questões cibernéticas. O Ministério da Defesa desenvolveu um orçamento integrado para todos os aspectos das operações cibernéticas, que incluem a vigilância e defesa no ciberespaço, bem como um orçamento específico para preparar as forças de reserva para a força de elite. Esse orçamento foi ajustado para garantir uma taxa de compensação realista para o treinamento de

mobilização, e foi introduzido ciência e tecnologia para o treinamento militar de reserva, além do fornecimento adequado de equipamentos e materiais para as unidades de mobilização (SOUTH KOREA, 2020). Observa-se que o Ministério da Defesa Nacional alocou

> KRW 209,9 bilhões para responder a diversas ameaças, incluindo **ameaças cibernéticas** e espaciais e terrorismo e para aprimorar as capacidades de apoio a desastres do país, KRW 1,47 trilhão para aumentar a capacidade de desenvolver armas avançadas, como futuras tecnologias estratégicas e sistemas complexos tripulados e não tripulados que liderará a era da Quarta Revolução Industrial e outros KRW 96,8 bilhões para promover e construir a base da indústria de defesa para apoiar a transformação da indústria de defesa doméstica em uma estrutura voltada para a exportação e para criar empregos de alta qualidade (SOUTH KOREA, 2020, p. 193, *tradução nossa, grifo nosso*)[60].

3.1.7 Livros Branco de Segurança Cibernética Nacional

Os Livros Branco de Segurança Cibernética Nacional não traçam estratégias de defesa cibernética, apenas de segurança cibernética, merecem menção pois são documentos produzidos por uma parceria entre Serviço de Inteligência Nacional, Ministério da Ciência, Comunicações, Tecnologia e Informação, Ministério do Interior e Segurança, Comissão de Proteção de Informação Pessoal, Comissão de Serviços de Finanças e Ministério dos Assuntos Internacionais. É publicado anualmente desde 2008, o último sendo lançado em 2022.

Trata de assuntos internos de segurança cibernética, como as mudanças no ambiente de segurança cibernética e tendências em ameaças cibernéticas internas, hackers e distribuição de pornografia, lida com mudanças no ambiente de segurança cibernética na Coreia e mudanças em ataques e ameaças cibernéticas. Elabora uma análise das políticas, sistemas e práticas relacionadas à segurança cibernética em áreas como a salvaguarda da rede nacional de informação e comunicação, governança digital, proteção da infraestrutura crítica de informação e comunicação, serviços de informação e comunicação e serviços financeiros. Por fim, trata do aprimoramento da indústria de segurança cibernética, avanços em tecnologia de segurança cibernética, capacitação de profissionais em segurança cibernética, garantia da privacidade de informações pessoais, promoção de segurança cibernética para a sociedade em geral e colaboração internacional na área de segurança cibernética (SOUTH KOREA, 2022).

---

[60] No original: "*KRW 209.9 billion to respond to diverse threats including cyber and space threats and terrorism and to enhance the country's disaster support capabilities, KRW 1.47 trillion to increase the capability to develop advanced weapons such as future strategic technologies and manned and unmanned complex systems that will lead the era of the Fourth Industrial Revolution, and another KRW 96.8 billion to foster and build the defense industry base to support the transformation of the domestic defense industry into an export-oriented structure and to create high-quality jobs*" (SOUTH KOREA, 2020, p. 193).

3.2 BRASIL

Esta seção tratará da situação geopolítica brasileira, além de descrever a governança cibernética interna do país. Por fim, serão mapeados os seguintes documentos: Livro Verde: Segurança Cibernética no Brasil (2010); Doutrina militar de defesa cibernética (2014); Política Nacional de Defesa & Estratégia Nacional de Defesa; Estratégia Nacional de Segurança Cibernética (2020) e Livro Branco de Defesa Nacional (2012 e 2020).

3.2.1 Geopolítica

As questões de geopolítica brasileiras são marcadas desde os primórdios por duas grandes prioridades: defesa da soberania nacional e formação de território (FREITAS, 2004 *apud* CAMILO, 2019). Segundo Lira (2013) , os dois pensadores em geopolítica sul americana, Travessos e Golbery, concordam que a montagem geográfica da América do Sul determina as questões políticas do continente. Travassos se preocupa, em sentido de firmação do território brasileiro, com o avanço argentino sobre o interior:

> no pensamento de Travassos, a disputa pela hegemonia regional praticada por Brasil e Argentina em seus ensejos expansivos se daria pelo domínio da região central do subcontinente, de onde um pudesse, além de anular o outro, se expandir para todas as direções (TRAVASSOS, 1935 *apud* LIRA, 2013, p. 57).

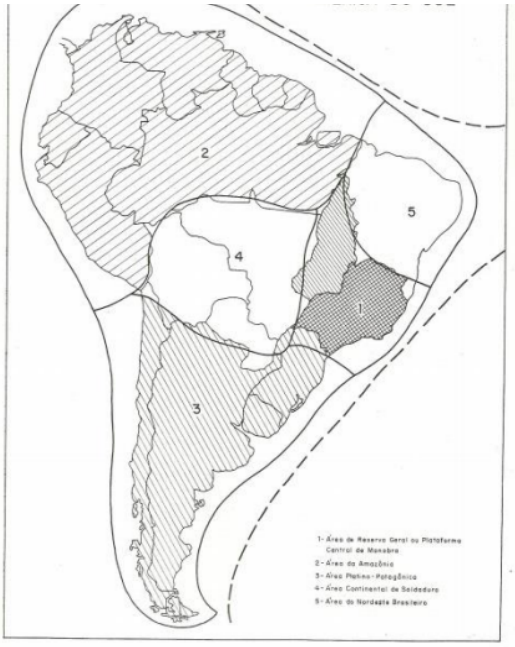
Não se pode descartar também as influências de países fora da região, como os Estados Unidos. Travassos (1935 *apud* LIRA, 2013) chama de "influência yankee" os casos de instabilidade resultantes disso, sendo um exemplo a preocupação com a Bolívia.

A integração nacional é o preceito para que a segurança nacional fosse completa para Golbery (COUTO e SILVA, 1981), já que todas as partes do território brasileiro eram vulneráveis a pressões externas de suas fronteiras (*apud* LIRA, 2013). De maneira ampla, a falta de uniformidade no processo de integração regional na América do Sul indica que os níveis de estabilidade e instabilidade também variam de forma desigual no espaço (NASSER; MORAES, 2014).

Como se observa na Figura 3 foram apresentadas as regiões geopolíticas que compõem o subcontinente sul-americano e evidenciam a importância central do Brasil nesse

território. Ademais, as zonas de conexão, tanto no centro quanto no nordeste do Brasil, permitem que o país exerça influência tanto no interior do continente quanto além, em relação à segurança do Atlântico Sul (LIRA, 2013), demonstrando, assim, a centralidade do Brasil na América do Sul, como se observa na figura abaixo, que demonstra que o Brasil faz parte de todas as compartimentações das áreas geopolíticas:

Figura 3 - Compartimentação Geopolítica da América do Sul.



Fonte: SODRÉ, 1965 *apud* LIRA, 2013, p. 88.

A dinâmica entre Brasil e Argentina era caracterizada pelo sentimento de "vizinho-inimigo"; cada ação ou gesto do vizinho era interpretado como hostil ou pouco confiável (MEDEIROS FILHO, 2014). Nos últimos anos da década de 1940, houve um aumento significativo da influência dos Estados Unidos no pensamento estratégico do Brasil. Isso se deveu, em grande parte, à criação da Escola Superior de Guerra (ESG) em 1948, que consolidou a relação entre os dois países. Durante a década seguinte, a ESG desenvolveu a Doutrina de Segurança Nacional (DSN), o que levou a uma reflexão sobre o papel do Brasil no cenário internacional, baseada na aliança com os Estados Unidos (LIRA, 2013).

Houve uma mudança de prioridades em 2005, quando o Brasil indicou que pretendia colocar em primeiro plano uma agenda que levasse em conta seus interesses nacionais. Foi assim que surgiu a Política Nacional de Defesa (PND), que estabeleceu diretrizes gerais, aprofundadas posteriormente na Estratégia Nacional de Defesa (END) de 2008. Apesar da maior atenção dada às ameaças externas, ambos os documentos revelaram o dilema em torno

da dissuasão externa e das novas ameaças surgidas na década de 1990, como as ameaças internas (LIRA, 2013).

Atualmente, a prioridade estratégica brasileira é se cercar de "um cinturão de paz e boa vontade", além de continuar a proteger suas fronteiras terrestres e cooperar com seus vizinhos. Enquanto isso, é necessário que o país esteja preparado para proteger-se contra possíveis ameaças provenientes de diferentes direções. É imprescindível estabelecer capacidades dissuasórias apropriadas nos domínios marítimo, terrestre e aéreo; essa medida é fundamental para desencorajar eventuais ataques à soberania brasileira e, consequentemente, garantir a inserção pacífica do Brasil no cenário mundial (AMORIM, 2014, p. 9).

Especificamente sobre a situação do Brasil na América do Sul, Filho (2014) apresenta a região dividida em dois arcos, um estável e outro instável; "o primeiro corresponde à faixa atlântica (...), o segundo se refere à porção onde persistem zonas potenciais de conflitos armados, notadamente Amazônia e Andes" (MEDEIROS FILHO, 2014, p. 30). Observa-se a seguir:

Figura 4 - Arcos de estabilidade e instabilidade.

Fonte: FILHO, 2014, p. 31.

Essa grande zona de estabilidade faz com que a América do Sul seja a região com menos gastos em defesa do mundo, representando apenas 4% do total mundial (FILHO, 2014). Conclui-se, portanto, que, em comparação, a nível global, o Brasil enfrenta uma situação de defesa peculiar. Há ausência de guerras formais e as ameaças à segurança vem da fragilidade do império da lei e do alto grau de violência nacional:

> Os principais problemas não seriam "de" fronteira – questão de defesa –, mas estariam "na" fronteira – questão de segurança. Sob tal inversão, a ameaça passaria a ser o vizinho fraco, incapaz de controlar seu próprio território, e não o vizinho forte (VILLA E MEDEIROS FILHO, 2007 *apud* MEDEIROS FILHO, 2014, p. 23).

Dessa forma, de acordo com a Política Nacional de Defesa (PND) de 2020, os interesses prioritários do Brasil são seu entorno estratégico, ou seja, a América do Sul, o Atlântico Sul, a costa ocidental da África e a Antártica. O Brasil segue sua tradição pacífica e preza pela convivência harmônica entre todos os países sem deixar de exprimir seu poder no Sistema Internacional (BRASIL, 2020c).

3.2.2 Governança interna

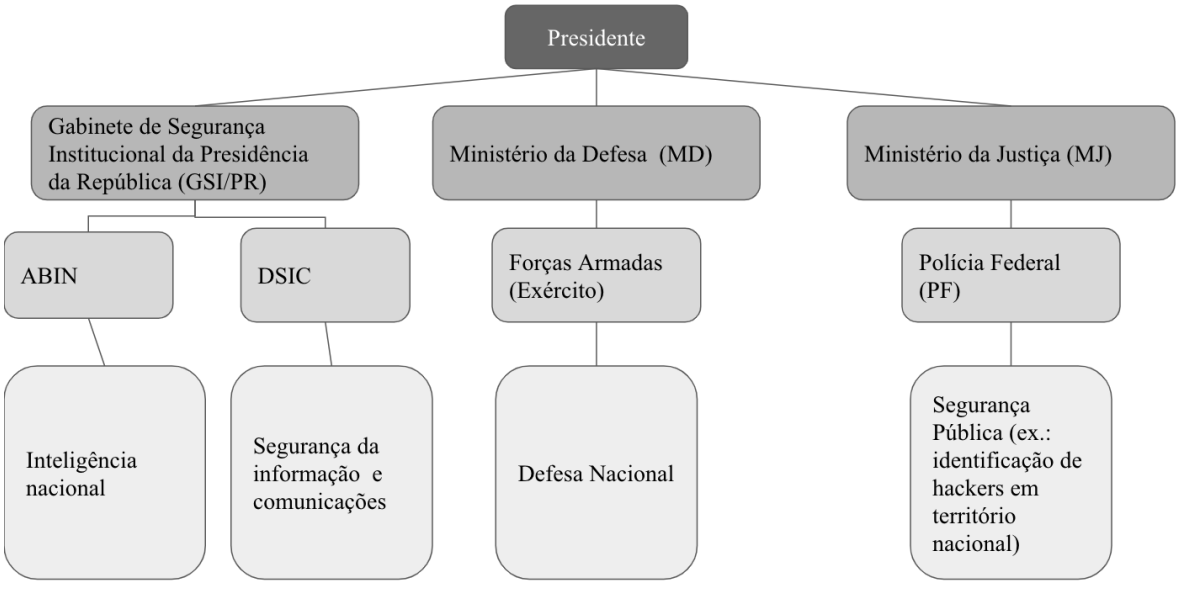
O Brasil não produziu conhecimento significativo sobre cibernética até o final dos anos 1990. No entanto, à medida que o Estado brasileiro reconheceu a importância e necessidade dessa tecnologia, houve uma institucionalização da questão, alocando recursos e delineando conceitos. Dessa forma, a partir dos anos 2000 o Brasil começou o processo de institucionalização e politização das questões de segurança e defesa cibernética com a produção do Livro Verde Sociedade da Informação no Brasil pelo Ministério da Ciência e Tecnologia. O documento, porém, era restrito a limitar diretrizes para a informatização do Brasil (SOUZA; ALMEIDA, 2016).

Em primeiro momento, foi instituído o Comitê Gestor da Segurança da Informação (CGSI), subordinado à Secretaria-Executiva do Conselho de Defesa Nacional, responsável por garantir a segurança da informação do Estado brasileiro. Logo em seguida, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) foi promulgado pela Lei Federal No 10.683, de 28 de maio de 2003, com funções relacionadas à inteligência, planejamento e coordenação da segurança da informação. Sob o guarda chuva de atuação do GSI foram criados dois órgãos que simbolizavam os esforços para a construção de uma estratégia de segurança cibernética (SOUZA; ALMEIDA, 2016), cita-se:

> O Decreto Presidencial No. 5.772 de 08 de maio de 2006 criou o Departamento de Segurança da Informação e Comunicações (DSIC), com o objetivo de exercer exatamente as atividades de segurança da informação. O segundo órgão é a Agência Brasileira de Inteligência (ABIN), o qual atua nas vertentes de inteligência e contra inteligência em prol do Estado, tendo como função, entre outras, "avaliar as ameaças internas e externas à ordem constitucional". (SOUZA; ALMEIDA, 2016, p. 392).

Nos próximos cinco anos, consequentemente, o que era entendido apenas como segurança da informação sofreu um processo de politização e passou a ser compreendido como uma questão de segurança cibernética. Órgãos foram criados, documentos oficiais escritos e recursos oficiais foram alocados. É importante destacar que mesmo com esforços de securitização, a questão cibernética ainda não era vista como uma ameaça existencial. Foi a partir da Política Nacional de Defesa de 2005, que menciona o termo "ataque cibernético" pela primeira vez, que se institucionaliza e aumenta a produção de materiais em questões de defesa cibernética propriamente dita. Como resultado, o Estado brasileiro passou a reconhecer a possibilidade de ataques cibernéticos contra infraestruturas críticas e a segurança da informação no país (SOUZA; ALMEIDA, 2016).

Figura 5 - Governança Cibernética interna do Brasil.



Fonte: Elaboração própria com base em SOUZA; ALMEIDA, 2016 e BRASIL, 2014.

A Figura 5 representa a constituição atual em defesa e segurança cibernética no Brasil. Nesse sentido, o Gabinete de Segurança Institucional da Presidência da República, a Polícia

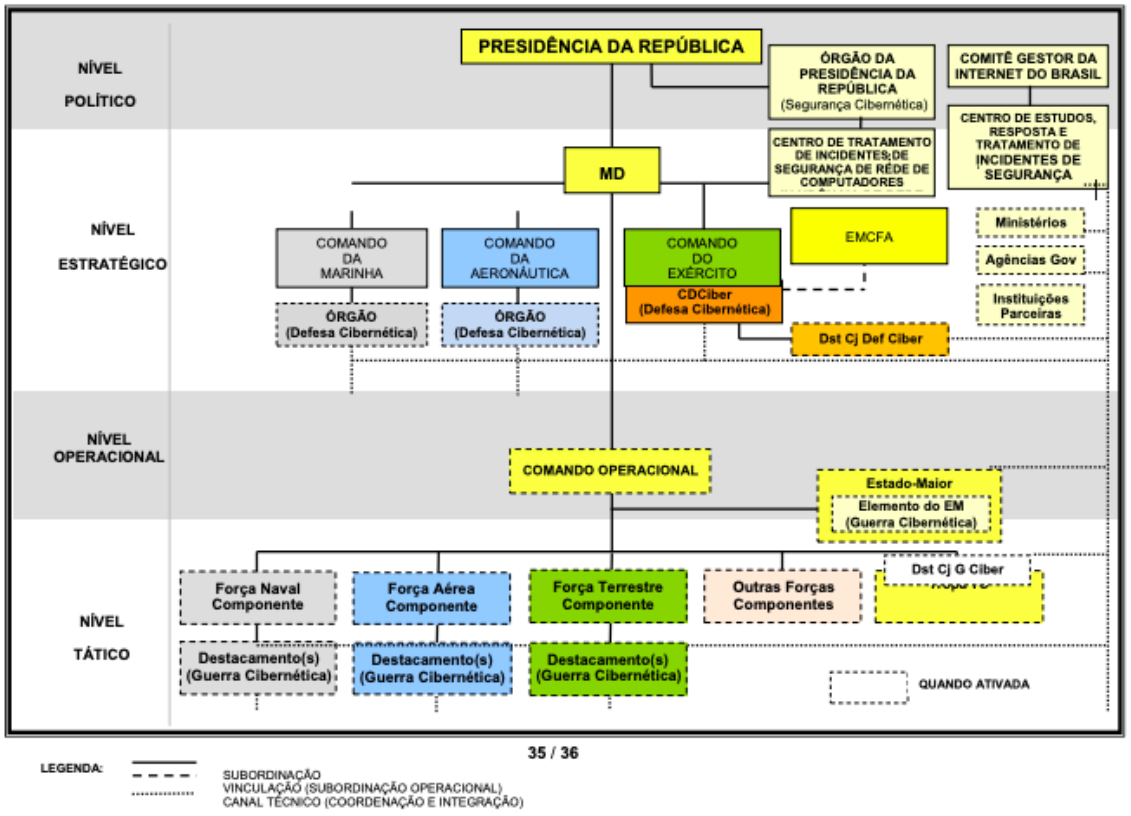
Federal e o Exército Brasileiro se tornaram os principais órgãos responsáveis pelas atividades relacionadas à segurança e defesa cibernética (BRASIL, 2014).

Quando se trata de garantir a segurança pública, é incumbência da Polícia Federal (PF), que está subordinada ao Ministério da Justiça, identificar os hackers que operam em território nacional. Esse tipo de ação é considerado um crime comum, o que significa que a PF é responsável por prevenir incidentes e reprimi-los também no âmbito cibernético. Uma das atribuições do GSI/PR é a coordenação da inteligência e segurança da informação, convertendo-a na principal ferramenta para a organização da estratégia nacional de segurança cibernética (SOUZA; ALMEIDA, 2016). Subordinados ao GSI/PR encontram-se o DSIC e a ABIN.

O DSIC é encarregado de regular a segurança da informação e das comunicações em toda a Administração Pública Federal (APF), estabelecer acordos internacionais para a troca de informações sigilosas, atuar como ponto de contato com a Organização dos Estados Americanos (OEA) em questões relacionadas ao terrorismo cibernético e manter o Centro de Tratamento e Resposta (CERT.br) para lidar com incidentes nas redes de computadores da APF. Já a ABIN é responsável por diversas tarefas de inteligência, as quais envolvem a produção de informações relevantes para o processo decisório, bem como a salvaguarda da sociedade e do Estado. Além disso, a agência atua em atividades de contrainteligência, tomando medidas para proteger informações sigilosas que sejam importantes para o Estado e a sociedade, neutralizando assim ações de inteligência executadas em benefício de interesses estrangeiros (SOUZA; ALMEIDA, 2016).

Tratando especificamente de defesa cibernética, objeto principal desta monografia, tem-se o Ministério da Defesa. A estrutura de governança militar cibernética interna pode ser observada na figura 6:

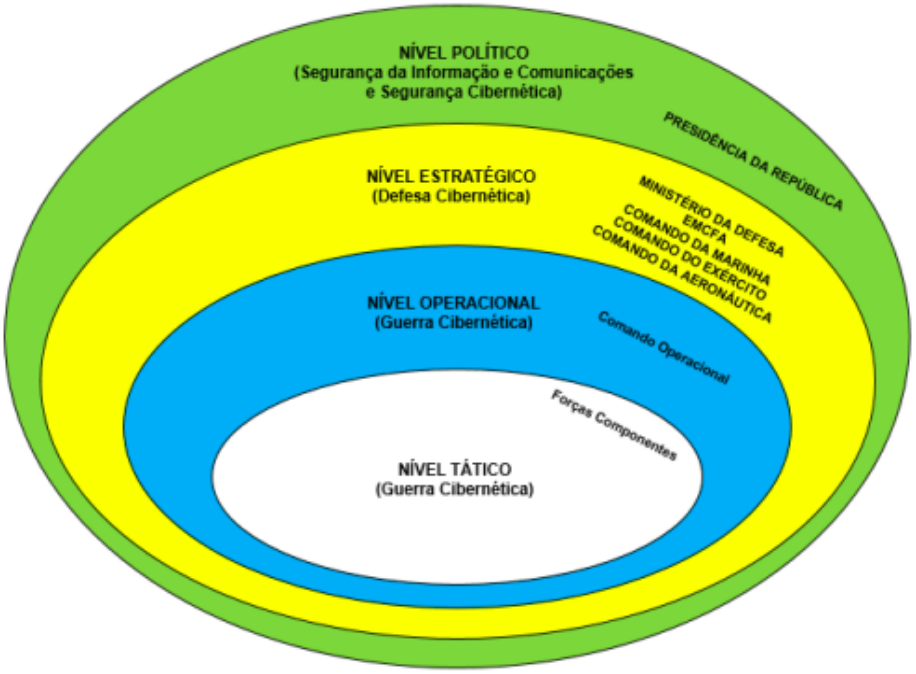
Figura 6 - Sistema Militar em defesa cibernética.



Fonte: BRASIL, 2014, p. 35.

As ações militares em defesa cibernética acontecem nas seguintes esferas:

Figura 7 - Níveis de decisão no Ministério da Defesa .



Fonte: BRASIL, 2014, p. 17

Os níveis tático e operacional, menos abrangente, respondem somente pelas questões de Guerra Cibernética e estão nas mãos das Forças Armadas. O nível estratégico fica a cargo do Ministério da Defesa, Estado Maior Conjunto das Forças Armadas e Comandos das Forças Armadas, interagindo com a Presidência da República e a Administração Pública Federal. E o nível político, operacionalizado pela presidência da república, engloba todos os outros (BRASIL, 2014).

Subordinado ao exército, é essencial citar o Comando de Defesa Cibernética. Ativada em 15 de abril de 2016, a organização militar conjunta que faz parte da estrutura organizacional do Comando do Exército atua em conjunto com as organizações governamentais já existentes, somando esforços em prol da defesa cibernética. Suas principais responsabilidades incluem o planejamento, orientação, supervisão e controle de atividades operacionais, de inteligência, doutrinárias, científicas e tecnológicas; além da capacitação no setor cibernético de defesa (OLIVEIRA; PORTELA, 2017).

3.2.3 Livro Verde: Segurança Cibernética no Brasil (2010)

Documento pertencente ao Gabinete de Segurança Institucional o Livro Verde: Segurança Cibernética no Brasil tem o objetivo de

> expressar potenciais diretrizes estratégicas para o estabelecimento da Política Nacional de Segurança Cibernética, articulando visão de curto (2 - 3 anos), médio (5 – 7 anos), e longo (10 – 15 anos) prazo no tema, abrangendo, como ponto de partida, os seguintes vetores: Político Estratégico, Econômico, Social e Ambiental, CT&I, Educação, Legal, Cooperação Internacional, e Segurança das Infraestruturas Críticas (BRASIL, 2010, p. 17).

O Livro Verde elenca a Segurança Cibernética como o desafio do século XXI, e afirma que esta se destaca cada vez mais como uma função estratégica estatal, essencial para a manutenção das infraestruturas críticas do país. Portanto, o reconhecimento da relevância da segurança cibernética está se tornando cada vez mais indispensável para o progresso, exigindo a implementação de diversas medidas, incluindo a promoção de discussões e intercâmbios de ideias, iniciativas, dados e informações, bem como das melhores práticas, para fomentar a cooperação no assunto, tanto nacionalmente quanto internacionalmente (BRASIL, 2010).

Este documento adotou como ponto de partida para abordar a segurança cibernética a seguinte definição: "a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas" (BRASIL, 2010, p. 19).

Destaca o interesse do Brasil de, no futuro, dirigir fóruns internacionais sobre cibernética e se tornar um player no assunto no Sistema Internacional. A segurança cibernética apresenta diversos desafios, por isso é essencial que sejam estabelecidas ações conjuntas envolvendo governo, empresas privadas, instituições acadêmicas, organizações do terceiro setor e sociedade em geral, a fim de lidar com a complexidade de fatores que permeiam a segurança cibernética (BRASIL, 2010).

O GSI aponta, neste livro, que economias desenvolvidas, como Estados Unidos e Japão, estão revisando ou lançando seus próprios documentos de “Estratégias nacionais de segurança cibernética”. O Brasil não fica para trás, em 2010 Salvador sediou a Convenção do Crime Cibernético e o governo federal conta com especialistas em segurança cibernética que desempenham um papel fundamental na área, além de participarem ativamente de diferentes redes de contatos e fóruns nacionais e internacionais. Como resultado, o país é reconhecido globalmente como um dos principais atores em diversos temas, incluindo a segurança cibernética (BRASIL, 2010).

O Brasil enfrenta muitos desafios relacionados à cibernética, como a falta de clareza sobre a relevância e a verdadeira magnitude da problemática relacionada à segurança cibernética, tanto direta quanto indiretamente, como um tema de grande importância para o Estado. É percebida tanto pela alta cúpula do governo quanto pelos pensadores e formadores

de opinião. Além disso, havia diversos atores governamentais envolvidos na segurança cibernética, o que pode levar a uma superposição de responsabilidades institucionais e, consequentemente, gerar deficiências na estruturação de uma governança adequada. Aproximadamente 80% dos serviços de rede são controlados por empresas privadas e internacionais. E não há um orçamento específico destinado ao desenvolvimento de ações e atividades voltadas à segurança cibernética em todas as esferas do governo, bem como não há uma carreira oficial de Estado destinada exclusivamente à atuação na área de segurança cibernética (BRASIL, 2010).

Por fim, conforme o Livro Verde, não há leis claras e precisas tanto no âmbito nacional quanto internacional que tratem especificamente da segurança cibernética e combatam efetivamente os crimes cibernéticos. Além disso, não existem regulamentações e sistemas de certificação que garantam a segurança cibernética. Há também uma variedade de termos e suas respectivas definições, que precisam ser harmonizados em nível nacional e internacional para se estabelecer uma linguagem comum e coerente no campo da segurança cibernética (BRASIL, 2010).

No âmbito político-estratégico e econômico, o Livro anuncia o plano de lançar, no curto prazo, uma Política Nacional de Segurança Cibernética capaz de melhorar a capacidade de dissuasão da Defesa brasileira frente a ameaças cibernéticas. Ademais, cita a importância de ter um programa específico para conhecer e mapear o nível de vulnerabilidade do país em relação aos seus sistemas de informação e infraestruturas críticas de informação, tanto a médio como a longo prazo. Esse programa deve envolver a macro-coordenação do mapeamento dos ativos de informação das infraestruturas críticas e apoiar o processo de auditoria de segurança das mesmas, estabelecendo requisitos mínimos de segurança (BRASIL, 2010).

3.2.4 Doutrina militar de defesa cibernética (2014)

A Doutrina militar de defesa cibernética tem o objetivo de:

> Estabelecer os fundamentos da Doutrina Militar de Defesa Cibernética, proporcionando unidade de pensamento sobre o assunto, no âmbito do Ministério da Defesa (MD), e contribuindo para a atuação conjunta das Forças Armadas (FA) na defesa do Brasil no espaço cibernético (BRASIL, 2014, p. 13).

O documento começa com uma linha do tempo sobre as questões cibernéticas no Brasil;e cita a criação do DSIC sob o GSI/PR em 2006, que tem a função de executar atividades de Segurança da Informação e Comunicações. Em 2008, a Estratégia Nacional de

Defesa (END) reconheceu, portanto, o cibernético como um setor estratégico para a Defesa Nacional,e os outros setores prioritários eram o nuclear e o espacial. Nesse mesmo ano, o exército foi incumbido pelo Ministério da Defesa a partir da Portaria nº 3.405/MD as atividades de Defesa Cibernética do país. Por fim, o Livro Branco de Defesa Nacional e a atualização da Estratégia Nacional de Defesa versam sobre a proteção do espaço cibernético, o novo domínio de poder "abrange um grande número de áreas, como: capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional e gestão de pessoal" (BRASIL, 2014, p. 14).

O Ministério da Defesa elenca quatro princípios relevantes no emprego da Defesa Cibernética. O **Princípio do Efeito**, em que, no âmbito do Espaço Cibernético, as ações realizadas devem resultar em benefícios estratégicos, operacionais ou táticos que tenham impactos concretos no mundo real, ainda que tais efeitos não sejam físicos. No **Princípio da Dissimulação**, com o intuito de ocultar a autoria e a origem das ações ofensivas e exploratórias no Espaço Cibernético, é preciso adotar medidas ativas que dificultem a rastreabilidade dessas atividades em sistemas de tecnologia da informação e comunicações do adversário, dissimulando, assim, a identidade e localização dos perpetradores dessas ações. O **Princípio da Rastreabilidade** versa que para identificar e prevenir ações ofensivas e exploratórias no Espaço Cibernético contra sistemas de tecnologia da informação e comunicações próprios, é necessário implementar medidas eficazes de detecção. Tais medidas devem permitir identificar possíveis ameaças e agir de forma preventiva para evitar danos ou perdas. Por fim, o **Princípio da Adaptabilidade** argumenta que a adaptabilidade é uma característica fundamental da Defesa Cibernética para lidar com a natureza mutável do Espaço Cibernético. É essencial manter a proatividade mesmo diante de mudanças repentinas e imprevisíveis para garantir a capacidade de resposta rápida e eficaz contra ameaças cibernéticas (BRASIL, 2014, *grifo nosso*). O quadro abaixo demonstra as definições presentes no documento de termos relacionados a cibernética:

Quadro 6 - Conceitos e definições presentes em "Doutrina militar de defesa cibernética".

Ameaça Cibernética	"Causa potencial de um incidente indesejado, que pode resultar em dano ao Espaço Cibernético de interesse"
Cibernética	"Comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação. No campo da Defesa Nacional, inclui os recursos de tecnologia da informação e comunicações de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle (SISMC2), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais"
Defesa Cibernética	"Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente"
Espaço Cibernético	"Espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas"
Guerra Cibernética	"Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2"
Infraestrutura Crítica da Informação	"Subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade"
Poder Cibernético	"Capacidade de utilizar o Espaço Cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder"
Operação de Informação	"Ações coordenadas sobre o ambiente de informação e executadas, com o apoio da inteligência, para influenciar um oponente real ou potencial, diminuindo sua combatividade, coesão interna e externa e capacidade de tomada de decisão,

	bem como para a proteção do próprio processo decisório, concorrendo, assim, para a consecução dos objetivos políticos e militares"
Resiliência Cibernética	"capacidade de manter as infraestruturas críticas de tecnologia da informação e comunicações operando sob condições de ataque cibernético ou de restabelecê-las após uma ação adversa"
Segurança Cibernética	"Arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas"
Segurança da Informação e Comunicações (SIC)	"Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações"

Fonte: Elaboração própria com base em BRASIL, 2014, p. 18-19.

Para o Brasil, as maneiras de operar no espaço cibernético podem diferir com base na escala dos objetivos a serem alcançados (sejam eles políticos, estratégicos, operacionais ou táticos), no grau de envolvimento nacional, no contexto de aplicação, no nível de tecnologia utilizada, na coordenação e no tempo de planejamento. A operação cibernética com finalidade política ou estratégica é executada em períodos de paz e tem como objetivo alcançar um resultado político ou estratégico específico, geralmente como parte de uma Operação de Informação ou Inteligência. Esse tipo de atuação visa alcançar uma vantagem ou objetivo estratégico para a nação ou organização que está conduzindo a operação, utilizando recursos cibernéticos para alcançar seus objetivos. A operação cibernética ao nível operacional ou tático é normalmente utilizada em um ambiente militar, a fim de contribuir para a realização de um efeito desejado em uma Operação Militar. Nesse contexto, a ação cibernética é empregada como um meio para apoiar as atividades operacionais ou táticas no campo de batalha, auxiliando na conquista de objetivos militares específicos (BRASIL, 2014).

Considera-se ataques cibernéticos, proteção cibernética e exploração cibernética como ações a serem realizadas pelo exército brasileiro. As ações de ataque cibernético compreendem "interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente" (BRASIL, 2014, p. 23). A proteção cibernética é uma atividade permanente e refere-se às medidas adotadas para combater ataques e explorações cibernéticas em nossos sistemas de computadores e redes de comunicação, reforçando as atividades de Segurança,

Defesa e Guerra Cibernética em situações de crise ou conflito. A exploração, enfim, trata-se de uma série de atividades voltadas para a busca e coleta de informações em sistemas de tecnologia da informação relevantes, com o objetivo de obter uma compreensão situacional do ambiente cibernético (BRASIL, 2014).

O documento admite limitações que a área de Defesa Cibernética apresenta no Brasil. Expõe-se capacidades limitadas de identificação da origem de ataques cibernéticos, há vulnerabilidades nos sistemas computacionais do país e dificuldade de identificação de talentos humanos. As questões de poder assimétrico colocam o Brasil em uma posição vulnerável no Sistema Internacional nas questões de cibernética, gerando dificuldades no acompanhamento de novas tecnologias (BRASIL, 2014).

3.2.5 Política Nacional de Defesa & Estratégia Nacional de Defesa[61]

A Política Nacional de Defesa (PND) e Estratégia Nacional de Defesa (END) constroem a noção de Segurança Nacional, que se refere à capacidade de manter a soberania e a integridade territorial, bem como a defesa dos interesses nacionais, apesar de pressões e ameaças de diversas origens, é reforçada pela contribuição de determinados fatores (BRASIL, 2020c).

A primeira vez que a Política Nacional de Defesa cita diretamente o tema cibernética, com o termo "ataque cibernético" é em sua versão de 2005:

> Para minimizar os danos de possível ataque cibernético, é essencial a busca permanente do aperfeiçoamento dos dispositivos de segurança e a adoção de procedimentos que reduzam a vulnerabilidade dos sistemas e permitam seu pronto restabelecimento. (...) XII - aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso permita seu pronto restabelecimento (BRASIL, 2005).

Na edição de 2020, além da proteção dos espaços tradicionais, como ar, mar, terra e espaço, o documento traz atenção especial a necessidade de garantir a segurança e defesa do espaço cibernético brasileiro uma vez que são cruciais para assegurar o adequado funcionamento dos sistemas de informações, gerenciamento e comunicações de interesse nacional (BRASIL, 2020c).

---

[61] O Livro Branco de Defesa Nacional de 2020 diferencia a Política Nacional de Defesa da Estratégia Nacional de Defesa. A PND é o principal documento que guia o planejamento das ações voltadas para a defesa do país, principalmente contra ameaças externas. Por meio da PND, são estabelecidos objetivos que orientam o preparo e a utilização de todos os setores do Poder Nacional em prol da Defesa Nacional. Por sua vez, a END direciona as diversas áreas do governo para implementar as medidas necessárias para alcançar tais objetivos. Assim, a END serve como uma ponte entre a posição do país nas questões de Defesa e as ações necessárias para efetivamente capacitar o Estado a proteger seus interesses (BRASIL, 2020b).

O Sistema de Defesa Cibernética, junto do Sistema Integrado de Monitoramento de Fronteira – SISFRON, o Sistema de Mísseis e Foguetes, o Sistema de Defesa Antiaérea colabora diretamente para a capacidade de dissuasão brasileira. Operam aumentando a mobilidade, intensificando a vigilância e o controle das fronteiras, e desenvolvendo capacidades para impedir o acesso não autorizado a áreas ou sistemas específicos (BRASIL, 2020c).

Três segmentos tecnológicos são considerados fundamentais para a Defesa Nacional: o setor nuclear, o **setor cibernético** e o setor espacial. Tais setores são classificados como estratégicos, visto que extrapolam a distinção entre desenvolvimento e defesa, bem como entre as esferas civil e militar. É importante que o país se capacite como um todo e que o Poder Nacional esteja preparado para adaptar-se às circunstâncias e explorar o potencial desses setores. No entanto, dada a complexidade desses segmentos, é necessário que haja liderança centralizada e coordenação estreita entre diversos atores e áreas de conhecimento. Nesse sentido, na área de Defesa, a Marinha é responsável pelo Setor Nuclear, o Exército pelo Setor Cibernético e a Força Aérea pelo Setor Espacial (BRASIL, 2020c, *grifo nosso*).

No que diz respeito ao Setor Cibernético, as capacitações serão destinadas a uma ampla gama de usos, tanto militares quanto civis. É fundamental que as Forças Armadas possuam tecnologias de comunicação que garantam a interoperabilidade e a capacidade de atuar de forma integrada e segura. Para alcançar esse objetivo, é preciso aprimorar a segurança da informação e das comunicações e a segurança cibernética, com especial atenção à proteção das estruturas críticas. Torna-se primordial, então, fomentar a pesquisa, o desenvolvimento e a inovação, é necessário concentrar esforços em tecnologias que permitam o planejamento e a execução de atividades cibernéticas no Setor de Defesa e que contribuam para a segurança cibernética em âmbito nacional. Para tanto, é importante fortalecer a colaboração entre as Forças Armadas, a comunidade acadêmica, os setores público e privado e a Base Industrial de Defesa. Ademais, é fundamental intensificar parcerias estratégicas e o intercâmbio com as Forças Armadas de outros países (BRASIL, 2020c).

3.2.6 Estratégia Nacional de Segurança Cibernética (2020)

O DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020 intitulado de Estratégia Nacional de Segurança Cibernética - E-Ciber, elaborado pelo GSI/PR, tem por objetivos específicos: 1. Tornar o Brasil mais próspero e confiável no ambiente digital; 2. Aumentar a

resiliência brasileira às ameaças cibernéticas; e 3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional. Em longo prazo, o documento busca contribuir para tornar o Brasil um país de excelência em segurança cibernética. É o primeiro módulo da Estratégia Nacional de Segurança da Informação, a ser futuramente elaborada (BRASIL, 2020a).

O decreto estabelece que a área sistêmica de Segurança da Informação está acima de qualquer outro debate sobre segurança cibernética já que se liga diretamente com "proteção de um conjunto de informações e ao valor que estas possuem para um indivíduo ou para uma organização" (BRASIL, 2020a, p. 2). Dessa forma, o decreto estabelece que a área de Segurança da Informação abrange as áreas de: segurança cibernética, defesa cibernética, segurança física e proteção de dados organizacionais (BRASIL, 2020a).

Desempenha uma função importante no conjunto de normas nacionais de segurança cibernética, estabelecendo medidas para mudar, de forma cooperativa e em nível nacional, as atitudes de indivíduos e instituições sobre o assunto. As iniciativas de gestão na área são fragmentadas e pontuais, o que dificulta a convergência de esforços no setor. Há, também, falta de alinhamento normativo, estratégico e operacional, o que frequentemente resulta em retrabalho e na formação de forças-tarefa para ações pontuais, prejudicando a absorção de lições aprendidas e colocando em risco a eficácia prolongada dessas ações. Por fim, há diferentes níveis de maturidade da sociedade em relação à segurança cibernética, o que resulta em percepções variadas sobre a importância real do tema (BRASIL, 2020a).

Infere-se, portanto, que a grande novidade é a busca por um modelo centralizado de governança no âmbito nacional. Para isso, um sistema nacional de segurança cibernética será criado, com as seguintes atribuições: promover a coordenação entre diversos atores relacionados com a segurança cibernética, não apenas a nível federal, mas também em outros setores e estabelecer rotinas de verificação de conformidade internamente nos órgãos públicos e nas entidades privadas. É importante permitir a convergência dos esforços e iniciativas, atuando de forma complementar para receber denúncias, apurar incidentes e promover a conscientização e educação da sociedade sobre o tema (BRASIL, 2020a).

É prioritário, também, incentivar a concepção de soluções inovadoras em segurança cibernética. Para isso, o governo propõe a inclusão de assuntos de segurança cibernética em programas de fomento à pesquisa e busca estimular a criação de startups na área. O documento busca expandir o protagonismo brasileiro em cooperação internacional na área de segurança cibernética. Para obter os resultados mais efetivos, é essencial que os atores ajam em conjunto, mantendo sempre em mente que nenhuma entidade individual poderá enfrentar

sozinha todos os desafios apresentados pelas tecnologias emergentes. A cooperação interna é citada na forma de parcerias entre setor público, privado, academia e sociedade (BRASIL, 2020a).

Nesse contexto, é necessário que as instituições implementem programas de segurança cibernética baseados em modelos reconhecidos. Esses modelos devem fornecer uma avaliação adequada do estágio atual de segurança, identificar os pontos mais vulneráveis dos sistemas, as ameaças cibernéticas mais prováveis e os principais fatores de risco. É fundamental considerar a implementação de medidas de proteção apropriadas, mecanismos eficazes de detecção de ataques, metodologias para responder a incidentes e procedimentos para restaurar o ambiente computacional. O Brasil tem dificuldades na análise do grau de maturidade em segurança cibernética, pois esses mecanismos são adotados de forma distinta em entidades públicas e pelo setor privado, isso demonstra a necessidade de uma lei que "regule as ações de segurança cibernética, que especifique atribuições, que aponte mecanismos de diálogo com a sociedade" (BRASIL, 2020a, p. 16).

Para o GSI/PR, é imprescindível que todas as organizações, sejam elas públicas ou privadas, possuam uma equipe de tratamento e resposta a incidentes cibernéticos, também conhecida como Computer Security Incident Response Team (CSIRT). É fundamental que essa equipe seja capacitada e tenha acesso a ferramentas computacionais apropriadas para atender às suas necessidades. Além disso, é importante que os sistemas utilizados sejam baseados em tecnologias emergentes e estejam em conformidade com os padrões internacionais de segurança. Esses centros devem atuar em constante comunicação e compartilhar seus registros de incidentes nacionais (BRASIL, 2020a).

O decreto recomenda que a segurança crítica esteja em conformidade com os padrões nacionais e internacionalmente reconhecidos. Isso garante que os processos de certificação sejam justos e transparentes. É importante que haja um equilíbrio nesses processos para garantir que as empresas e organizações possam obter a certificação necessária para operar com segurança, enquanto atendem aos requisitos de segurança cibernética (BRASIL, 2020a).

Segue uma sessão específica para a promoção da pesquisa, desenvolvimento e inovação em cibernética,

> O Brasil possui um cenário diversificado no que tange à pesquisa e ao desenvolvimento em tecnologia. Identificam-se centros de excelência altamente capacitados e reconhecidos por suas atividades, mas que produzem pouca inovação ou tecnologia aplicável ao ambiente cibernético. É preciso que o País disponha de uma 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 (BRASIL, 2020a, p. 26).

Por fim, retrata as dificuldades brasileiras na educação cibernética. Foram identificadas algumas deficiências no país: a falta de profissionais capacitados em segurança cibernética, uma baixa conscientização por parte dos usuários e uma oferta limitada de programas educacionais voltados para a área. Ademais, é importante ressaltar que a construção de uma cultura sólida de segurança cibernética, baseada em conscientização, treinamento e capacitação, depende de uma gestão eficiente do conhecimento. É necessário garantir a continuidade dos processos envolvidos, formar profissionais com habilidades atualizadas de acordo com a evolução constante das competências em segurança cibernética e a obsolescência das mesmas (BRASIL, 2020a).

3.2.7 Livro Branco de Defesa Nacional (2012 e 2020)

Os Livros Brancos de Defesa Nacional são de responsabilidade intelectual do Ministério da Defesa.

Na edição de 2012, as ameaças cibernéticas são citadas como uma preocupação real, pois têm o potencial de comprometer a integridade de infraestruturas críticas que são essenciais para a operação e controle de diversos sistemas e órgãos ligados à segurança nacional. Essas infraestruturas sensíveis podem ser prejudicadas por ações maliciosas, representando um risco significativo para a segurança nacional. Dessa forma, a proteção do espaço cibernético se faz necessária, e envolve diversas áreas, tais como a formação de profissionais capacitados, inteligência, pesquisa científica, elaboração de doutrinas, preparação e operação efetiva, além da gestão de recursos humanos. Também inclui a proteção de ativos cibernéticos e a habilidade de operar em rede de forma segura e eficiente (BRASIL, 2012).

Apresenta a implantação do Setor Cibernético como um projeto de longo prazo que tem como objetivo principal garantir que os dados que são processados e armazenados em suas redes sejam confidenciais, estejam disponíveis quando necessários, mantenham sua integridade e sejam autênticos. Além disso, planeja "produzir componentes críticos nacionais. O Centro de Defesa Cibernética do Exército vem somar esforços com as organizações governamentais já existentes" (BRASIL, 2012, p. 127).

O Sistema de Proteção Cibernética – Defesa Cibernética é citado como projeto prioritário para transformação da Força Terrestre é garantir que suas brigadas tenham os meios de transporte, equipamentos, armamentos e suprimentos necessários para atender às demandas operacionais e níveis de modernização desejados. Essa transformação tem como objetivo equipar as brigadas de forma adequada para aumentar suas capacidades operacionais, tornando-as mais eficientes e eficazes em suas missões (BRASIL, 2012).

É responsabilidade do Exército cuidar do Setor Estratégico Cibernético, o que inclui várias medidas pontuais, articulação e equipamentos necessários para consolidar esse setor. Preservar a integridade de estruturas estratégicas que possam ser alvo de diferentes modalidades de ataques cibernéticos é fundamental para o país. Para proteger contra ameaças cibernéticas, algumas ações de curto prazo foram identificadas, tais como: construir a sede definitiva do Centro de Defesa Cibernética (CDCiber) e adquirir a infraestrutura de apoio necessária, adquirir equipamentos e capacitar recursos humanos, obter soluções de hardware e software de defesa cibernética e implementar projetos estruturais no Setor Cibernético para ampliar a capacidade de resposta às ameaças (BRASIL, 2012). O Livro, por fim, estima o orçamento de defesa cibernética em 895,40 mi de reais para o período de 2010 a 2023 (BRASIL, 2012).

No apêndice, trata-se sobre capacitações oferecidas a fim de fomentar os setores estratégicos espacial, cibernético e nuclear. Tem-se como prioridades: fortalecer o Centro de Defesa Cibernética; estimular o avanço da investigação científica na área da cibersegurança, com a participação da comunidade acadêmica nacional e internacional, estabelecendo a criação da Escola Nacional de Defesa Cibernética e desenvolver e capacitar para o emprego na área de cibernética (BRASIL, 2012).

Em 2020, é destacado como novas abordagens de temas tradicionais e novos temas têm influenciado o cenário internacional. Essas mudanças têm implicações significativas para a Defesa Nacional, especialmente no que diz respeito ao problema global do tráfico de drogas e armas, à necessidade de proteger a biodiversidade, aos **possíveis ataques cibernéticos**, à crescente escassez de recursos, às pandemias, aos crimes transnacionais, ao terrorismo internacional, à pirataria, e outros. Isso demonstra que os temas relacionados à Defesa Nacional são cada vez mais transversais, ultrapassando a visão convencional de ameaças potenciais ou manifestas focadas exclusivamente em tensões ou crises entre Estados (BRASIL, 2020b, *grifo nosso*).

No entanto, o Brasil aposta que haverá a prevalência da cooperação internacional sobre o conflito e que o Brasil tem o dever de promover a criação de um mundo multipolar baseado na cooperação, em consonância com sua histórica e tradicional postura de defender a integridade das normas do sistema internacional (BRASIL, 2020b).

Sobre espaço cibernético, o documento admite a possibilidade do acontecimento de guerras cibernéticas e que esse é o desafio mais importante para a Defesa Nacional e para a segurança internacional no século XXI,

> A possibilidade de o País sofrer um ataque cibernético de origens das mais diversas e de difícil identificação, que poderão causar danos consideráveis a estruturas estratégicas ou mesmo a outros setores de importâncias vitais para a nação brasileira, faz com que a Defesa Cibernética passe a ter importância fundamental para a Defesa Nacional (BRASIL, 2020b, p. 23).

Por fim, cita a colaboração entre instituições de pesquisa civis e militares, universidades e empresas é essencial para unir esforços na formação de centros de excelência em alta tecnologia em diversas áreas (BRASIL, 2020b).

4 ANALISANDO O PODER CIBERNÉTICO DA COREIA DO SUL E BRASIL

Visto que a cibernética é um grande instrumento de poder nacional e entendendo como Coreia do Sul e Brasil se posicionam em assuntos dessa natureza por meio de seus documentos oficiais, resta analisar como as estratégias de defesa cibernéticas documentadas no capítulo anterior mensuram o exercício de poder de ambos no espaço cibernético. Por fim, as características geopolíticas serão ligadas aos resultados obtidos através da análise a fim de entender em que medida a geopolítica influencia os resultados observados.

4.1 O MODELO DE KLIMBURG

Motivada por preocupações contínuas com as ameaças no ciberespaço, a defesa cibernética tornou-se um assunto relevante nas agendas políticas de governos, organizações internacionais e supranacionais (CAVELTY, 2018). Os países estão empenhados em reduzir os riscos que os ataques cibernéticos apresentam para suas economias digitais, infraestruturas críticas e cidadãos, incorporando, por consequência, estratégias cibernéticas em doutrinas militares, planos de governo e diretrizes nacionais. A inclusão da cibernética nas políticas de governo, portanto, levanta uma série de questões relevantes. A questão central, consequentemente, é se o poder cibernético emergente dos Estados pode ser objetivamente quantificado e medido, e se é possível classificar os Estados de acordo com esse poder (WILLETT, 2011).

Para Willett (2011), mensurar o poder nacional é um processo já familiar. É comum que países sejam classificados com base no tamanho de suas economias, nas capacidades militares e no investimento em defesa como percentual do PIB. No entanto, criar uma metodologia eficaz para medir o poder cibernético apresenta algumas novas dificuldades, já que se trata de um campo de estudo novo e complexo. Além disso, para Cavelty (2018), a complexidade do conceito de poder cibernético reside no fato de que ainda não há análises empíricas suficientes sobre o assunto. A literatura sobre poder cibernético ainda é pequena e fragmentada, o que torna a compreensão do tema ainda mais desafiadora.

Para além das definições clássicas de poder cibernético expostas no Capítulo 1, Willett (2011, p. 88, *tradução nossa*) argumenta que "um ator cibernético poderoso precisa ser capaz de usar o ciberespaço para conduzir operações de influência contra, ou atacar diretamente,

alvos designados"[62]. Cavelty, no entanto, cita Haugaard (2012) ao criticar a visão ofensiva para entender e mensurar o poder cibernético: "todas as variantes de poder agora discutidas são formas de dominação (ou “poder sobre”) em contraste com o poder como empoderamento (ou “poder para”)"[63] (*apud* CAVELTY, 2018, p. 6).

Ou seja, a proposta é afastar a ideia de que o poder cibernético está relacionado exclusivamente à projeção coercitiva de interesses nacionais e acrescentar a noção de uma forte defesa cibernética baseada em modelos de melhores práticas de política de defesa cibernética. Nessa visão, o poder cibernético e a defesa cibernética estão interligados. Uma entidade política é capaz de exercer o poder cibernético quando possui a capacidade de influenciar o cenário global de segurança cibernética. No entanto, um poder cibernético efetivo também deve ser capaz de se defender contra ameaças cibernéticas e gerenciá-las de forma adequada. As necessidades de resiliência cibernética interna e poder cibernético externo se complementam: nesta visão, não pode existir um verdadeiro poder cibernético sem uma política de defesa sólida, e vice-versa (CAVELTY, 2018).

Cavelty (2018) argumenta que o único autor que inclui os elementos de "poder para" é Klimburg, com o Modelo de Capacidades Integradas. Klimburg (2011) mesura poder de acordo com um resultado de forças distribuídas, mais precisamente como a força de elementos, humanos e organizacionais, existentes em relação ao espaço cibernético para produzir defesa cibernética. Dessa forma, no Modelo de Capacidades Integradas o poder cibernético tem três dimensões: "coordenação de aspectos operacionais e políticos em estruturas governamentais, coerência de políticas por meio de alianças internacionais e estruturas legais e cooperação de atores cibernéticos não estatais" ou "'capacidade de governo integrada', 'capacidade de sistemas integrados' e 'capacidade nacional integrada', respectivamente" (KLIMBURG, 2011, p. 43).

Cavelty (2018) atribui definições mais aprofundadas para as dimensões: a capacidade de governo integrada significaria a habilidade dos governos de entregarem ações conjuntas, como atacar e se defender no domínio cibernético e compartilhar recursos operacionais. Capacidade de sistemas integrados versa sobre as capacidades de cooperação do Estado em assuntos de cibernética e, por fim, capacidade nacional integrada é a habilidade que um país tem de usar atores não estatais para apoiar suas políticas nacionais; importante frisar que através da cooperação e não da coerção (*apud* KLIMBURG, 2011).

---

[62] No original: "*a powerful cyber actor needs to be able to use cyberspace to conduct influence operations against, or directly attack, designated targets"* (WILLETT, 2011, p. 88).

[63] No original: "*All variants of power now discussed are forms of domination (or ‘power over’) in contrast to power as empowerment (or ‘power to’)*" (CAVELTY, 2018, p. 6).

Carrapicho e Barrinha (2018) e Cavelty (2018) afirmam que o melhor modelo para mensurar o poder cibernético da União Europeia a partir da análise de seus documentos é o de Klimburg, por três razões:

> Um cânone comum na literatura é criticar a União Europeia por não ter poder cibernético suficiente (Klimburg & Tirmaa-Klaar, 2011; Sliwinski, 2014a, 2014b), em linha com críticas semelhantes para todos os tipos de tópicos de Segurança e Defesa Comuns. No entanto, essa afirmação é muito simplista, pois iguala o poder simplesmente à 1ª face ou poder compulsório ou, ainda mais estreitamente, ao poder militar. Em primeiro lugar, como mostrado acima, o poder cibernético é muito multifacetado para fazer uma afirmação tão geral (como é o poder em geral). Em segundo lugar, medir as capacidades de poder da UE em uma compreensão instrumental do poder como "projeção de interesses nacionais" é questionável por padrão, dado o projeto político especial da União Europeia. Em terceiro lugar, as noções atuais de quem tem poder cibernético (a maioria dos especialistas mencionaria os Estados Unidos e talvez a China, ver Rowland, Rice, & Shenoi, 2014a, 2014b) são baseadas em "conjecturas" em vez de empíricas. Muito mais trabalho conceitual e empírico é necessário sobre esta questão[64] (CAVELTY, 2018. p. 7).

Portanto, o modelo de Klimburg tem vantagens para a comparação proposta por essa monografia quando comparado, por exemplo, aos argumentos que prezam pelas capacidades ofensivas de poder cibernética, pois, como exposto no capítulo anterior, Coreia do Sul e Brasil não possuem, ou não publicizam, capacidades cibernéticas ofensivas.

4.1.1 Capacidade de governo integrada

A Coreia do Sul demonstra grande coesão no aparato governamental para a construção de estratégias de defesa e segurança cibernética. Um exemplo são os Livros Branco de Segurança Cibernética Nacional, que são escritos de forma conjunta pelo Serviço de Inteligência Nacional, Ministério da Ciência, Comunicações, Tecnologia e Informação, Ministério do Interior e Segurança, Comissão de Proteção de Informação Pessoal, Comissão de Serviços de Finanças e Ministério dos Assuntos Internacionais. Outra forma de identificar tal coesão é pelo Livro Branco de Defesa (2020), que adota os objetivos da Estratégia de Segurança Cibernética Nacional (2019), escrita pelo Escritório de Segurança Nacional, como

[64] No original: "*A common canon in the literature is to criticize the European Union for not having enough cyber-power (Klimburg & Tirmaa-Klaar, 2011; Sliwinski, 2014a, 2014b), in line with similar critique for all kinds of Common Security and Defence topics. However, that statement is far too simplistic, as it equates power simply with 1st face or compulsory power or even more narrowly, with military power. First, as shown above, cyber-power is too multifaceted to make such a general statement (as is power more generally). Second, measuring the EU's power capabilities on an instrumental understanding of power as 'projecting national interests' is questionable by default, given the special political project of the European Union. Third, current notions of who has cyber-power (most experts would mention the United States and maybe China, see Rowland, Rice, & Shenoi, 2014a, 2014b) are based on 'guesstimates' rather than empirics. Much more conceptual and empirical work is needed on this issue."* (CAVELTY, 2018. p. 7).

diretriz máxima da política nacional de cibersegurança. A própria estrutura de governança interna em cibernética mostra concordância entres os órgãos, onde todas as decisões são centradas no Escritório de Segurança Nacional[65] e o país se divide claramente em questões do setor privado, público e de defesa nacional.

Nesse quesito, o Brasil admite falha em seus próprios documentos apenas durante a elaboração da Estratégia Nacional de Segurança Cibernética, em 2020. Onde foi apurado que o Brasil não possuía um "arcabouço autóctone e abrangente de segurança cibernética que contribua para o fortalecimento da resiliência cibernética nacional" (BRASIL, 2020a, p. 22). Portanto, a E-Ciber visa preencher essa importante lacuna no arcabouço normativo nacional sobre segurança cibernética (BRASIL, 2020a). O Brasil também não possui nenhum órgão que unifique a governança interna em cibernética do país[66], uma vez que o GSI/PR, o Ministério da Defesa e o Ministério da Justiça respondem apenas ao presidente. Grande exemplo disso é a falta de acordo na definição de termos relevantes em defesa cibernética nos documentos construídos no Brasil. Guerra cibernética é definida de formas diferentes no Livro Verde de Segurança Cibernética (2010)[67], produzido pelo GSI/PR e na Doutrina Militar de Defesa Cibernética[68] (2014) produzido pelo Ministério da Defesa.

A Coreia do Sul começou a se preocupar com questões de automatização do campo de batalha e digitalização das forças armadas em 2006 (SOUTH KOREA, 2006). Tais tecnologias ganharam cada vez mais espaço nos documentos de defesa, até sua versão mais atual (2020), que cita questões de cibernética, como espaço cibernético e guerra cibernética, mais de 150 vezes (SOUTH KOREA, 2020). Desde de 2009, o país vem tentando estabelecer uma única contramedida nacional de segurança cibernética e ataques cibernéticos (KIM; BAE, 2021), no entanto, somente em 2011 foi publicado a primeira resposta nacional com diretrizes para lidar com ameaças cibernéticas: o Plano Diretor Nacional de Segurança Cibernética (SOUTH KOREA, 2011). A Estratégia Nacional de Segurança Cibernética pelo Escritório de Segurança Nacional foi amplamente considerada como o documento de política

---

[65] Ver Figura 2

[66] Ver Figura 5

[67] "Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil. (Glossário MD35-G-01, 2007)." (BRASIL, 2010, p. 54)

[68] “Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2” . (BRASIL, 2014, p.19).

mais importante e eficaz sobre segurança cibernética produzido em mais de trinta anos na Coréia (KIM; BAE, 2021). Desde 2008 a Coreia do Sul publica anualmente um Livro Branco de Segurança Cibernética Nacional.

A produção brasileira de documentos referentes à segurança e defesa cibernética, qualitativa e quantitativamente, é inferior à da Coreia do Sul. Estrategicamente, a documentação oficial da concepção estratégica do ciberespaço no Brasil evoluiu desde as primeiras iterações da Política Nacional de Defesa (PND), quando o termo ataque cibernético é citado pela primeira vez. Em 2010, o GSI/PR publicou um Livro Verde e quatro anos depois uma doutrina militar. Os documentos que não são específicos de cibernética, como o Livro Branco e as PND e END, citam estratégias de defesa cibernética de forma superficial e insuficiente (FAVERO, 2022).

Tanto o Ministério da Defesa Nacional da Coreia do Sul quanto o Escritório de Segurança Nacional elencam o fortalecimento da segurança e capacidades de defesa cibernética como prioridade. Dentro disso está o desenvolvimento de políticas e estratégias de segurança cibernética de defesa e sistema de execução de missões de guerra cibernética. Mesmo sendo de forma não explícita, "execução de missões de guerra cibernética" é a única forma que uma estratégia cibernética ofensiva é mencionada. Os recursos das forças armadas coreanas, portanto, estão sendo fortalecidos e destinados à área de segurança e defesa cibernética de forma uniforme (SOUTH KOREA, 2020). Não há questionamentos sobre a efetividade de diversas medidas implementadas por entidades governamentais. Tanto o setor público quanto estatal têm conduzido ativamente políticas relacionadas à segurança cibernética, e estendido a aplicação delas para o setor privado, favorecendo o desenvolvimento de habilidades técnicas e gerenciais (KIM; BAE, 2021).

A Estratégia de Segurança Cibernética Nacional (2019) cita um ponto crucial na análise de suas capacidades de governo integradas: "O governo tem aprimorado continuamente o sistema nacional de segurança cibernética, estabelecendo e implementando medidas abrangentes em conjunto com os ministérios e agências relevantes **sempre que ocorre um grande incidente**"[69] (SOUTH KOREA, 2019, p. 8, *tradução nossa*, *grifo nosso*). Esse é um expressivo ponto de crítica de acadêmicos coreanos. As estratégias coreanas, a construção de estratégias de defesa, políticas e instituições atuais, são voltadas somente para a

[69] No original: "The government has continuously enhanced the national cybersecurity system by establishing and implementing comprehensive measures in concert with relevant ministries and agencies whenever a massive incident occurred."

recuperação contra ataques cibernéticos graves. Após cada ataque, foram adotadas mudanças restritas de política para melhorar a resposta a incidentes, com base na análise e nas experiências com o ataque recente, sem se concentrar em melhorias fundamentais na base legal ou em questões constitucionais relacionadas (KIM; BAE, 2021).

O Brasil também considera as questões de defesa cibernética como prioridade nos seus debates de defesa e segurança, relevantes em diferentes elementos do poder nacional – militar, político, econômico e tecnológico, mesmo afirmando que não existam evidências que o Brasil já tenha usado capacidades cibernéticas ofensivas (DEVANNY *et al*., 2022). As estratégias e recursos voltados para o Brasil na área cibernética são, portanto, puramente defensivos. Tanto em perspectiva militar, na Doutrina Militar de Defesa Cibernética, "contribuindo para a atuação conjunta das Forças Armadas (FA) **na defesa do Brasil no espaço cibernético**" (BRASIL, 2014, p. 13), quanto na área pública e privada, na Estratégia Nacional De Segurança Cibernética: “1. Tornar o Brasil mais próspero e confiável no ambiente digital; 2. Aumentar a resiliência brasileira às ameaças cibernéticas; e 3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional” (BRASIL, 2020a, p. 5).

O Brasil se inspira nas estratégias de seus aliados internacionais para a implementação e planejamento das suas próprias estratégias de defesa cibernética, considerando uma redução brusca no orçamento (DEVANNY *et al*., 2022). O estabelecimento, por exemplo, da Segurança da Informação como uma área sistemática acima de defesa cibernética faz a estratégia brasileira se aproximar do modelo britânico, além de fazer com que a prioridade seja a segurança cibernética, sendo a defesa uma preocupação em segundo quadro (BRASIL, 2020a; DEVANNY *et al*., 2022).

Em comparação com o Brasil, a Coreia do Sul demonstra grande capacidade de governo integrada, ao redigir documentos robustos e completos, promover a parceria de vários atores governamentais para a escrita de um documento e construir estratégias puramente de defesa, o Livro Branco, por exemplo, baseadas em uma estratégia nacional cibernética escrita por um outro órgão governamental. Além de ter uma divisão clara e efetiva de governança interna cibernética, onde os interesses privados, públicos e de defesa respondem ao mesmo órgão e este responde ao presidente, sendo um agente focalizador que não assume interesses. Falhando, no entanto, ao ponto de construir estratégias de defesa apenas como respostas a ataques já sofridos.

Em comparação, o Brasil se encontra um passo atrás da Coreia do Sul em suas capacidades de governo integradas. Em vista que, ainda há muito ruído de comunicação entre os órgãos do governo responsáveis pela criação e implantação das estratégias, podendo citar a

falta de unidade nas definições de conceitos como exemplo. O primeiro passo para o avanço foi dado pela E-Ciber, que é o reconhecimento da falha, o documento visa aumentar sua expressão de poder no espaço cibernético através da coordenação de aspectos operacionais e políticos em estruturas governamentais. É necessário que o Brasil continue a construir documentos com estratégias robustas, sistematizadas e acordadas por todas as partes do governo para expressar de forma mais efetiva suas capacidades de governo integradas.

4.1.2 Capacidade de sistemas integrados

A base para as estratégias de cooperação internacional da Coreia do Sul parte do reconhecimento que a sua "situação de segurança é extremamente complexa e grave (...). Os países vizinhos da Península Coreana continuam a reforçar suas capacidades militares de ponta, impulsionando suas próprias prioridades enquanto expandem seus domínios militares (...) no ciberespaço"[70] (SOUTH KOREA, 2020, p. 3, *tradução nossa*). À vista disso, os esforços de cooperação internacional em cibernética são uma questão prioritária na Coreia e foram objeto de empenho mesmo antes da construção de documentos estratégicos.

A Estratégia de Segurança Cibernética Nacional de 2019 conta com um capítulo dedicado à promoção de cooperação internacional onde estabelece que, com o objetivo de enfrentar as ameaças cibernéticas transnacionais, o governo está empenhado em estabelecer um mecanismo de cooperação com aliados e organizações internacionais, tais como a ONU e a UIT. Para alcançar esse objetivo, é necessário buscar atividades de cooperação internacional sistemáticas e práticas, tais como adesão a convenções internacionais, compartilhamento de informações e tecnologias, bem como a elaboração de regras internacionais sobre segurança cibernética (SOUTH KOREA, 2019).

Mesmo com uma tentativa falha de publicar uma estratégia de defesa cibernética em 2009, a Coreia do Sul já estava engajando em esforços internacionais para tratar de ameaças cibernéticas e se articulava com parcerias intergovernamentais em cibernética (KIM; BAE, 2021).

---

[70] No original: "*situation is extremely complex and grave, both internally and externally. Neighboring countries of the Korean Peninsula continue to reinforce their cutting-edge military capabilities, pushing their own priorities while expanding their military domains not only in the sea and air but also to space and cyber."* (SOUTH KOREA, 2020, p. 3).

O país tomou parte nos primeiros e segundos Grupos de Especialistas Governamentais[71] da Organização das Nações Unidas sobre segurança cibernética, participou do Processo de Londres e foi anfitriã da Reunião Ministerial sobre a Economia da Internet da Organização para Cooperação e Desenvolvimento Econômico (OCDE) em 2008. Durante o encontro, foi produzida a Declaração de Seul para o Futuro da Economia da Internet[72]. Por essa declaração entende-se que a Coreia do Sul está disposta a cooperar com Austrália, Áustria, Bélgica, Canadá, Chile, República Tcheca, Dinamarca, Egito, Estônia, Finlândia, França, Alemanha, Grécia, Hungria, Islândia, Índia, Indonésia, Irlanda, Israel, Itália, Japão, Coréia, Letônia, Luxemburgo, México, Holanda, Nova Zelândia, Noruega, Polônia, Portugal, Senegal, República Eslovaca, Eslovênia, Espanha, Suécia, Suíça, Turquia, Reino Unido, Estados Unidos da América e Comunidade Européia (OECD, 2008).

O encontro resultou na expressão pública de interesse conjunto em fomentar o desenvolvimento da Economia da Internet e encorajar o crescimento econômico sustentável e a prosperidade por meio de regulamentações e ambientes normativos que apoiem a inovação, o investimento e a concorrência no setor de Tecnologia da Informação e Comunicação. Outros objetivos seriam colaborar com a indústria privada, a sociedade civil e a comunidade virtual para salvaguardar as redes de TIC que sustentam a Economia da Internet e adotar medidas para garantir a proteção dos usuários da Economia da Internet, incluindo a necessária cooperação internacional (OECD, 2008).

Ainda em âmbito multilateral, o governo sul coreano manteve os esforços de conversas e negociações que resultaram na Conferência de Seul sobre Ciberespaço, ocorrida em 2013. Foi considerado pelas Nações Unidas como um momento significativo para avaliar a relevância das questões digitais no âmbito diplomático e de segurança. Durante o evento, foi elaborada a Estrutura e Diretrizes de Seul para um Ciberespaço Aberto e Seguro. O tema desta conferência, Prosperidade Global através de um Ciberespaço Aberto e Seguro - Oportunidades, Ameaças e Cooperação, onde foi discutido uma agenda de desenvolvimento global para o período pós-2015, com o desenvolvimento sustentável em seu centro (UNITED NATIONS, 2013).

Ademais, cita-se o Grupo de Trabalho Cibernético criado em 2014 no Diálogo de Defesa de Seul[73] onde todos os anos cerca de 20 a 30 países se reúnem para compartilhar o status de ameaças cibernéticas e também para manter intercâmbios ativos, como a introdução

[71] Groups of Governmental Experts (GGE).
[72] THE SEOUL DECLARATION FOR THE FUTURE OF THE INTERNET ECONOMY.
[73] Diálogo de Defesa de Seul é um órgão consultivo de segurança multilateral anual no nível vice-ministerial sob o domínio do Ministério da Defesa Nacional (SOUTH KOREA, 2020)

de políticas e sistemas de segurança cibernética de cada país. A Coreia do Sul se compromete em continuar a desenvolver o espaço para cooperação, a fim de ser um órgão consultivo multilateral no campo da cooperação cibernética de defesa, fortalecendo as capacidades cibernéticas dos países participantes e construindo confiança entre eles. Por fim, desde 2018, o Ministério da Defesa conduz um Grupo de Trabalho de Especialistas em Segurança Cibernética na Reunião de Ministros da Defesa da ASEAN-Plus (ADMM-Plus), que consiste em 10 países da ASEAN mais 8 países adjuntos[74] (ASEAN, 2023). Nas reuniões são realizados exercícios simulados para compartilhar políticas nacionais de segurança cibernética e aprimorar as habilidades de gerenciamento de crises diante de ameaças cibernéticas. Durante o período de 2020 a 2023, a Coreia do Sul co-presidirá o Grupo de Trabalho de Especialistas em Segurança Cibernética com a Malásia, cujo objetivo é identificar áreas de cooperação para o desenvolvimento de capacidades políticas e tecnológicas relacionadas à segurança cibernética entre os estados membros. Essa iniciativa tem como propósito fortalecer as parcerias internacionais com os países da ASEAN e ASEAN Plus, e gerar resultados positivos para todos os envolvidos (SOUTH KOREA, 2020).

Não se pode falar de cooperação internacional sem citar o maior parceiro estratégico da Coreia do Sul, os Estados Unidos. O Ministério da Defesa define que as Forças Armadas da Coreia do Sul "mantêm uma postura de defesa combinada com base na robusta aliança ROK-EUA que é capaz de combater as provocações de guerra locais e em grande escala da Coréia do Norte"[75] (SOUTH KOREA, 2020, p. 63) e afirma que os Estados Unidos é o país mais ativo e avançado em assuntos de cibernética (SOUTH KOREA, 2020).

Em reunião bilateral, representantes da Coreia do Sul e Estados Unidos reafirmaram seus valores de cooperação na área cibernética a fim de garantir uma resposta eficaz contra novas ameaças emergentes e reforçar as capacidades de resposta abrangentes. Ambas as partes concordaram em manter uma comunicação e coordenação estreitas no que se refere ao ciberespaço, por meio do compartilhamento de informações sobre tendências de ameaças cibernéticas, bem como de discussões sobre as mudanças políticas correspondentes. Além disso, foi acordado que seria necessário estabelecer um canal de comunicação entre os respectivos comandos cibernéticos, com o intuito de discutir e promover interesses mútuos (USA, 2020).

---

[74] Austrália, China, Índia, Japão, Nova Zelândia, República da Coreia, Rússia e Estados Unidos.
[75] No original: "*maintains a combined defense posture based on the robust ROK–US alliance that is capable of countering local and full scale war provocations from North Korea*" (SOUTH KOREA, 2020, p. 63).

Cibernética é assunto das reuniões entre os presidentes Yoon e Biden, que trataram de defesa cibernética em um encontro em 2022. Como resultado, fica evidente que o motivo central da cooperação ROK-EUA é deter a Coreia do Norte, ficou decidido que os países irão expandir "a cooperação para enfrentar uma série de ameaças cibernéticas da RPDC, incluindo, mas não se limitando a, ataques cibernéticos patrocinados pelo Estado"[76] (USA, 2022, não paginado).

A aliança ROK-EUA se fortalece cada vez mais. Os líderes Yoon e Biden planejam continuar trabalhando juntos para abordar desafios regionais e globais de segurança cibernética. Isso inclui colaboração na dissuasão de adversários cibernéticos, garantindo a segurança da infraestrutura crítica, combatendo o crime cibernético e a lavagem de dinheiro relacionados, protegendo criptomoedas e aplicativos blockchain, realizando treinamentos e exercícios cibernéticos, compartilhando informações relevantes e promovendo a cooperação cibernética entre militares (EUA, 2022).

Pouco se diz sobre cooperação em defesa cibernética nos documentos oficiais brasileiros previamente analisados. O Brasil tem se concentrado em questões relacionadas às Tecnologias da Informação e Comunicação, bem como em diálogos de desenvolvimento econômico com organizações como o Mercosul, OEA, BRICS e União Europeia (UE), no que se refere à diplomacia cibernética. Embora haja cooperação em matéria de segurança, esta tem se limitado à capacitação, formação e profissionalização em níveis técnicos. No entanto, o aumento do interesse em segurança cibernética como uma agenda estratégica dentro do governo tem levado a alguns esforços iniciais. Exemplos incluem os recentes diálogos Brasil-UE, o grupo de trabalho da OEA para medidas de construção de confiança e a cooperação cibernética dentro do grupo BRICS (HUREL, 2020).

Devanny *et al.* (2022) afirma que a habilidade do Brasil em lidar com questões cibernéticas é reforçada através da realização de exercícios colaborativos com seus parceiros históricos e aliados, incluindo a Organização do Tratado do Atlântico Norte (OTAN). Em 2019, o Brasil participou de um exercício da OTAN como parte integrante da equipe do Exército espanhol demonstrando que o país está bem posicionado para liderar a cooperação horizontalmente através de acordos de entendimento bilateral e também multilateralmente, através do Conselho de Defesa Sul-Americano ou outros acordos ad hoc. A cooperação regional pode incluir: integração de inteligência para identificação de ameaças cibernéticas,

[76] No original: "*will significantly expand cooperation to confront a range of cyber threats from the DPRK, including but not limited to, state-sponsored cyber-attacks"* (USA, 2022).

avaliação e compartilhamento de dados, desenvolvimento conjunto de capacidades de defesa cibernética e coordenação de estratégias para combater crimes cibernéticos.

No âmbito multilateral, o Brasil é ativo em fóruns e está envolvido na diplomacia relacionada à governança da internet. Um representante brasileiro liderou as atividades do Grupo de Especialistas Governamentais da ONU entre 2019 e 2021, com o objetivo de promover um comportamento responsável dos estados no ciberespaço no contexto da segurança internacional (DEVANNY *et al*., 2022). O Brasil, no entanto, é visto com a imagem de um Estado oscilante[77], com uma diplomacia ambígua no que tange governança cibernética (HUREL, 2020).

Em âmbito bilateral, entre 2011 e 2020 o Brasil assinou sete acordos internacionais bilaterais que versam sobre cibernética com Reino Unido, Peru, China, Europol, Chile, Índia e Suriname. Em apenas um desses acordos, o com o Suriname, a questão da segurança cibernética é o tema central abordado pelas partes; nos demais a segurança cibernética é apenas um componente secundário em meio a uma cooperação mais ampla na repressão de diversos tipos de crimes internacionais, sendo os crimes cibernéticos apenas um dentre vários outros abordados (FEITOSA, 2021). Infere-se, portanto, que o Brasil não trata assuntos de cibernética como maior prioridade em cooperação bilateral.

Os Estados Unidos também é aliado do Brasil em defesa. O ex-presidente dos Estados Unidos, Barack Obama, e a ex-presidente brasileira, Dilma Rousseff, saudaram em 2015 a entrada em vigor do Acordo Bilateral sobre Cooperação em Matéria de Defesa (Defense Cooperation Agreement - DCA), que estabelece um quadro institucional para a cooperação em defesa entre os dois países. Além disso, o Acordo Geral sobre a Segurança de Informações Militares (GSOMIA) permitiu o aprofundamento da parceria Brasil-EUA na área de defesa, possibilitando o fluxo bilateral de informações, bens, serviços e tecnologias em benefício da segurança de ambos os países (FAGUNDES *et al*., 2019)[78].

Diante do exposto, percebe-se que Brasil e Coreia do Sul apresentam esforços um tanto parecidos em suas capacidades de sistemas integrados. Ambos países apresentam forte coerência de políticas por meio de alianças internacionais e estruturas legais, e atuam fortemente em âmbito multilateral para ajudar a construir políticas de governança cibernética. A maior diferença é no âmbito bilateral, uma vez que o Brasil assina acordos onde o assunto

[77] Swing State
[78] Uma fonte secundária foi utilizada neste caso pois os documentos originais não se encontravam disponíveis no site do Ministério das Relações Exteriores no momento da pesquisa.

principal é o combate a crimes e a cibernética muitas vezes é apenas um assunto tangente. Já a Coreia coopera de forma estratégica com os Estados Unidos a fim de deter um inimigo em comum e cibernética é um assunto principal nas reuniões bilaterais.

4.1.3 Capacidade nacional integrada

Os discursos oficiais sul-coreanos destacam que a prioridade máxima do país é proteger a segurança e os direitos dos seus cidadãos de ameaças cibernéticas, dentre outros riscos (SOUTH KOREA, 2020). Uma das formas de garantir essa prioridade é envolver civis nas questões de defesa. O Ministério da Defesa, por exemplo, cita a transferência de tecnologia de defesa para o setor privado por meio de cooperação civil-militar como uma resolução da reforma de defesa (SOUTH KOREA, 2014). Os documentos seguintes citam o termo "cooperação civil-governo-militar-policial", um sistema de compartilhamento de informações construído para estabelecer respostas rápidas a ameaças cibernéticas (SOUTH KOREA, 2018a; SOUTH KOREA, 2020). Os documentos não oferecem detalhes de como o sistema funciona, ainda que a Estratégia de Segurança Cibernética Nacional encoraje que civis, empresas e o governo trabalhem juntos e engajem em atividades de segurança cibernética (SOUTH KOREA, 2019).

Feigenbaum e Nelson (2021) afirmam que o Escritório de Segurança Nacional tem a responsabilidade de implementar esse planejamento. Para isso, é fundamental que o Escritório atue como uma torre de controle para coordenar políticas em todo o governo e entre os setores público e privado. No entanto, essa não é uma tarefa fácil, é necessário adotar uma abordagem multissetorial que leve em consideração não apenas as necessidades dos órgãos governamentais envolvidos, mas também as diversas necessidades das empresas e dos cidadãos coreanos. Os autores acreditam que a Coreia do Sul tem a capacidade de liderar o caminho nesse aspecto.

No Brasil, é possível afirmar que a E-Ciber traz como tema principal a cooperação público-privada como estratégia de Segurança da Informação. O documento traz como objetivo principal centralizar a governança cibernética do país, pela criação de um sistema nacional de segurança cibernética. Uma atribuição desse sistema será promover a cooperação com atores não estatais: "promover a coordenação dos diversos atores relacionados com a segurança cibernética, além da esfera federal" (BRASIL, 2020a, p. 5). Uma ação prevista é fomentar a criação de um espaço seguro, colaborativo e participativo entre os setores público e privado, bem como a sociedade em geral. Para atingir essa meta, planeja-se monitorar

constantemente possíveis ameaças e ataques cibernéticos e incentivar o compartilhamento de informações sobre vulnerabilidades e incidentes entre os atores. Além disso, realizar exercícios cibernéticos que envolvam diversos atores, incluindo organizações públicas, instituições privadas, a academia e a sociedade em geral (BRASIL, 2020a).

O Brasil aponta como falha estratégica exatamente essa falta de comunicação entre atores internos. A falta de uniformidade nos critérios e requisitos das normas de segurança cibernética dificulta a avaliação do nível de maturidade em segurança cibernética do país como um todo. É essencial padronizar as melhores práticas e estabelecer diretrizes claras para que até mesmo pequenas organizações possam adotar medidas eficazes de proteção de suas informações. À vista disso, a avaliação e a gestão de riscos em segurança cibernética surgem como fatores fundamentais para garantir a proteção do espaço cibernético, dos serviços e das informações que nele circulam (BRASIL, 2020a).

Nesse sentido, o Brasil tem como objetivo desenvolver um programa parecido com o que a Coreia do Sul implementa desde 2018, já que salienta a importância de que as organizações adotem programas eficazes, utilizando modelos reconhecidos que permitam avaliar o nível de segurança dos seus sistemas. Esses programas devem identificar os pontos mais vulneráveis dos sistemas, bem como as ameaças cibernéticas mais prováveis e os principais fatores de risco. Para garantir uma proteção adequada, é fundamental que sejam adotados mecanismos de detecção de ataques, metodologias eficientes de resposta a incidentes e procedimentos para a restauração do ecossistema informático (BRASIL, 2020a).

Uma crítica pertinente à Coreia do Sul é que, embora a conscientização sobre a importância da segurança cibernética tenha aumentado e esforços têm sido feitos para cooperação com atores internos, a pesquisa realizada por cientistas sociais coreanos sobre a evolução das instituições e práticas relacionadas à segurança cibernética no país tem sido muito limitada e não é levada em consideração para a escrita de documentos oficiais. Até o momento, a pesquisa sobre segurança cibernética tem se concentrado principalmente em aspectos jurídicos restritos, abordados por alguns juristas, e em discussões altamente técnicas sobre práticas de segurança cibernética, lideradas por engenheiros, tecnólogos e profissionais de segurança. Essa abordagem estreita, voltada para soluções tecnológicas, ressalta a necessidade de um trabalho político mais aprofundado para garantir a efetiva implantação e gestão dessas soluções (KIM; BAE, 2021).

Mesmo com a defasagem na esfera acadêmica, empresas coreanas e agências governamentais intensificaram seus esforços para proteger seus sistemas de Tecnologia da

Informação (TI) contra ataques de negação de serviço. Além disso, muitas delas passaram a implementar sistemas para backup de dados e recuperação de informações após um ataque, o que ajuda a reduzir significativamente a quantidade de danos causados. Apesar dos desafios constantes, as empresas e agências coreanas têm se mantido vigilantes e investindo cada vez mais em medidas de segurança cibernética para proteger suas operações e informações (FEIGENBAUM; NELSON, 2021).

Na Coreia do Sul, grande parte das instalações críticas, como energia, água e transporte, são operadas centralmente pelo estado, representando quase 70% dessas instituições públicas. Isso significa que, embora o setor privado tenha um papel importante no fortalecimento da segurança cibernética, seu envolvimento é menor em comparação com outros países. A coleta e o compartilhamento de informações sobre ameaças relacionadas à infraestrutura continuam liderados pelo governo, permitindo uma resposta rápida a ataques cibernéticos em instalações críticas e a implementação de políticas de segurança cibernética para essas instalações com cooperação ativa e sem a necessidade de negociações prolongadas ou oposição significativa (KIM; BAE, 2021).

No Brasil também existe um problema com pesquisa científica em cibernética, segundo a E-Ciber. De acordo com o documento, foram identificadas falhas no que diz respeito à cooperação público privada em cibernética, como a escassez de profissionais qualificados nessa área, a falta de consciência por parte dos usuários e a insuficiência de programas educacionais voltados para o assunto. As instituições de ensino superior e outras organizações não estão formando profissionais em número suficiente para atender à crescente demanda por especialistas em segurança cibernética. Para o GSI/PR, é fundamental que todos os níveis de ensino estejam envolvidos na disseminação do conhecimento sobre segurança cibernética. Por fim, para garantir a efetividade do desenvolvimento de uma cultura de segurança cibernética, é necessária uma gestão de conhecimento bem estruturada, que permita a continuidade dos processos envolvidos, a formação de profissionais atualizados em relação às competências em constante mudança e a adaptação às mudanças dinâmicas no campo (BRASIL, 2020).

A Coreia do Sul se encontra em um estágio avançado nesse quesito, tendo ações concretas para a promoção de mão de obra qualificada em cibernética. O país também vê a área como um campo onde a capacidade de atuação depende fortemente da experiência dos especialistas, mais até do que em outras áreas de conflito. Com o objetivo de aprimorar a habilidade dos especialistas em cibersegurança, o Ministério da Defesa Nacional está implementando um sistema abrangente de gerenciamento que engloba as etapas de

"aquisição-treinamento-nomeação-promoção". Ao identificar as habilidades e conhecimentos necessários para executar tarefas de segurança cibernética, o ministério incorporará essas competências em cada posição no "Sistema de Tarefas Cibernéticas de Defesa". A partir disso, espera-se uma melhora nos padrões de qualificação, planos de carreira e sistemas de educação e treinamento para especialistas em cibersegurança que atuam em defesa nacional (SOUTH KOREA, 2020).

Observa-se que os esforços brasileiros de cooperação interna para aumentar suas capacidades nacionais integradas são recentes, de acordo com os documentos analisados. A E-ciber faz um trabalho satisfatório de identificar a falta anterior desses esforços e apontá-los como foco de atenção e trabalho. Mesmo que ambos países apresentem defasagem no sentido de produção acadêmica em cibernética, a Coreia do Sul possui maior habilidade em usar atores não estatais para apoiar suas políticas nacionais, já que apresenta estratégias claras e resultados satisfatórios no quesito e, como visto ao longo do item, pode ser exemplo de sucesso em construir capacidades nacionais integradas.

4.2 RELACIONANDO GEOPOLÍTICA E PODER CIBERNÉTICO

Entendendo, a partir das conclusões do subtópico anterior, que a Coreia do Sul apresenta mais capacidades de expressão de poder cibernético a partir do Modelo de Klimburg, nos resta explorar quais influências as condições geopolíticas que cada país se encontra têm em determinar tal resultado. É importante explicitar que a intenção dessa pesquisa não é encontrar causalidades, apenas ligar os fatos expressos nos documentos com ameaças cibernéticas reais.

Como visto no capítulo anterior, a Coreia do Sul define sua situação securitária como grave e complexa por considerar alguns países de seu entorno estratégico como inimigos, vide Coreia do Norte e Rússia. Esse ambiente de ameaça constante é visto também nas ameaças e ataques cibernéticos sofridos pela Coreia do Sul:

Quadro 7 - Maiores ataques cibernéticos à Coreia do Sul.

Ataque distribuído de negação de serviço (2009)	Três ataques distribuídos de negação de serviço de 7 a 10 de julho paralisaram os principais sites do governo, incluindo o do Gabinete do Presidente.
Ataque distribuído de negação de serviço (2011)	Ataques a quarenta sites locais, incluindo os de grandes portais, repartições públicas, Ministério da Defesa Nacional e instituições financeiras.
Incidente do Banco NH[79] (2011)	Os dados internos e o sistema do servidor do NH Bank foram danificados. O acesso ao serviço foi paralisado total ou parcialmente.
Terror cibernético de 20 de março (2013)	As principais emissoras locais e os sistemas de tecnologia da informação de seis instituições financeiras caíram devido a um malware destrutivo. O site do Gabinete do Presidente, os principais sites do governo, a mídia e os sites dos partidos políticos estavam sob ataque cibernético.
Incidente KHNP (2014)	A Korea Hydro and Nuclear Power foi chantageada pelo chamado Grupo Contra as Usinas Nucleares. Os chantagistas ameaçaram que, se as usinas do KHNP não fossem detidas, o grupo as destruiria.
Incidente da Olimpíada de Inverno de PyeongChang	No dia da cerimônia de abertura, centenas de computadores do Comitê Olímpico Internacional foram hackeados, causando falhas de conexão em seus sites

Fonte: JANG; LIM, 2021, p. 16

A Coreia do Sul, portanto, sofre ataques cibernéticos constantes a infraestruturas críticas de governo, presumidamente, oriundos da Coreia do Norte, com exceção do ataque cibernético das Olimpíadas de PyeongChang em 2018, no qual a Rússia era suspeita de atacar o Comitê Olímpico Internacional em razão de um escândalo nacional de doping (JANG; LIM, 2021). Os ciberataques perpetrados pela Coreia do Norte costumam se encaixar em categorias principais. A primeira envolve atividades de espionagem, bem como ataques disruptivos e destrutivos, como uma operação de espionagem na qual a Coreia do Norte derrubou estações de transmissão, sites do governo e bancos sul-coreanos, além de roubar informações. Por fim, há os roubos cibernéticos a bancos e trocas de criptomoedas, que ajudam a manter a economia da Coreia do Norte em funcionamento, apesar das sanções internacionais (LEE, 2022).

[79] Anteriormente Federação Nacional de Cooperativas Agrícolas

Apesar de possuir uma infraestrutura digital altamente avançada, a Coreia ainda enfrenta inúmeros desafios quando se trata de proteção cibernética. Especificamente, a Coreia do Norte tem executado frequentes ataques cibernéticos devastadores contra organizações governamentais e empresas sul-coreanas. Dado que a Coreia do Sul é extremamente dependente da tecnologia da informação e comunicação, os prejuízos financeiros resultantes desses ataques atingiram cifras bilionárias, além de provocarem a interrupção generalizada de serviços vitais (JANG; LIM, 2021).

As robustas capacidades de poder cibernético da Coreia tem ligação, então, com essa ameaça cibernética constante. Como visto anteriormente, a maior estratégia nacional de segurança cibernética afirma que seu objetivo é capacitar e preparar medidas sempre que ocorre um ataque cibernético. Kim e Bae (2021) afirmam que apenas se preparar para o combate, no entanto, não oferece uma defesa adequada contra novas e distintas ameaças. Para as autoras, muitas vezes parece que as novas políticas coreanas são projetadas principalmente para responder ao sentimento e à opinião pública, e para demonstrar que os responsáveis pela formulação de políticas aprenderam com as análises realizadas após os incidentes ocorridos.

O Brasil se encontra em situação bem diferente da Coreia do Sul no que se trata de entorno estratégico, como visto no capítulo anterior, já que a América do Sul é frequentemente descrita como uma "zona unipolar de paz", na qual o Brasil é a principal potência econômica e militar, e não há grandes rivalidades agressivas entre o país e outras potências secundárias. Durante mais de 20 anos, o Brasil tem desfrutado de uma posição geoestratégica relativamente favorável, fortalecida por uma estratégia diplomática que destaca o papel do país como membro cooperativo do sistema internacional (DEVANNY *et al.*, 2022).

O Brasil sofre, porém, majoritariamente com crimes cibernéticos. Os números aumentaram exponencialmente desde 2010, o que levou o país a receber o título de "epicentro da onda global de crimes cibernéticos". O caráter das ameaças sofridas pelo Brasil é privado, por exemplo: em 2018, cerca de 70 milhões de pessoas foram vítimas de crimes cibernéticos no Brasil, resultando em perdas econômicas na ordem de US$ 20 bilhões (BNAmericas 2019). Esses números colocam o Brasil como o segundo país mais afetado por crimes cibernéticos em todo o mundo (BNAmericas, 2020 *apud* DEVANNY *et al.*, 2022). Mesmo quando os ataques são direcionados ao governo, como o ataque que o Ministério da Saúde sofreu em 2012, onde seus sistemas foram derrubados por hackers, tende-se a considerar as agressões como hacking cibernético (DEVANNY *et al*., 2022). A Estratégia Nacional de Segurança Cibernética traz um diagnóstico das principais ameaças cibernéticas sofridas pelo

Brasil, que é o segundo país com mais prejuízos provenientes de crimes cibernéticos, além de ser o maior alvo de ataques onlines da América do Sul. É importante mencionar, que cerca de 54% desses ataques são oriundos de dentro do próprio país, ou seja, o Brasil sofre mais com ameaças cibernéticas internas do que internacionais (BRASIL, 2020a).

A junção desses fatos, posição geopolítica pacífica e crimes cibernéticos majoritariamente direcionados à rede privada, entende-se melhor a posição estratégica brasileira. O documento mais recente e completo, a E-ciber, representa um avanço significativo e coerente na consolidação de uma abordagem coesa em relação à segurança cibernética no Brasil. Esse plano define três objetivos estratégicos que guiam a abordagem do país: fortalecer a segurança digital e a prosperidade, aumentar a resiliência diante de ameaças cibernéticas e consolidar o papel do Brasil na segurança cibernética internacional (HUREL, 2020).

5 CONCLUSÃO

Esta monografia teve como objetivo entender como Coreia do Sul e Brasil expressam poder cibernético através da análise e comparação das estratégias expostas em documentos oficiais. Para tal fim, foi construída uma revisão teórica que traçou uma linha contínua de pensamento, que vai desde as primeiras e clássicas definições de poder em ciência política, como a de Dahl (1957), em que poder é definido pela capacidade de A de conseguir fazer com que B faça algo diferente de sua vontade; até as consequências que a Revolução da Informação trouxe para as relações internacionais. Logo depois, apresentou-se o poder como um fator multidimensional, mostrando a evolução do pensamento; agora, além de A conseguir moldar as ações de B é importante considerar quando, onde e quais meios foram usados por A, por exemplo. Na esfera do sistema internacional, Nye (2010) aponta como as habilidades de persuasão e força são importantes para que os Estados consigam obter seus objetivos. Foi considerado também as mudanças trazidas pela Revolução da Informação a perspectiva de poder. Em um mundo informatizado, o poder se torna muito mais difuso e propõe dificuldades para os Estados afirmarem sua posição de principais atores internacionais.

Conclui-se que, com as novas tecnologias, os Estados expressam seus interesses e objetivos em um novo domínio de poder, o espaço cibernético. Os países agora passam a considerar o espaço cibernético para propagarem poder, e, por consequência lógica, sofrem ameaças dentro deste. Tendo em vista que não há leis de governança internacional estabelecidas sobre o espaço cibernético, a única alternativa é que os Estados construam estratégias ofensivas ou defensivas, para expressar seus interesses no domínio.

O capítulo seguinte apresentou os objetos de estudo deste trabalho. Coreia do Sul e Brasil foram analisados, primeiramente a partir do contexto geopolítico que estão inseridos. O primeiro ponto relevante para chegar ao objetivo proposto vem da diferença entre o entorno estratégico de Brasil e Coreia do Sul. Enquanto o Brasil está dentro de um cinturão de paz e coopera com todos os países que o cerca, a Coreia define sua situação geopolítica como perigosa e ameaçadora. Apresentou-se, também, as estruturas de governança interna em cibernética dos países. Como o capítulo não se propôs a análises, é exposto o conteúdo dos documentos selecionados apenas em forma de transcrição até esse ponto.

Retomando a diferenciação de defesa e segurança de Pagliari, Ayres Pinto e Barroso (2020), percebe-se que ambos se organizam de forma similar, tanto Coreia do Sul quanto Brasil atribuem órgãos diferentes para segurança e defesa cibernética. Nos dois países, o Ministério da Defesa cuida dos assuntos de defesa cibernética nacional; o NIS e o GSI/PR,

órgãos de inteligência nacional com atribuições parecidas, são responsáveis pela segurança da informação dos governos. O Ministério da Justiça, no Brasil, e o de Tecnologia e Informação, na Coreia, tratam de assuntos privados. A conclusão a ser tirada deste ponto vem justamente da diferença entre os sistemas internos. O da Coreia se apresenta melhor organizado, por possuir um órgão que atua como intermediário entre os ministérios e o presidente, o Escritório de Segurança Nacional, que não representa interesses de nenhum grupo social, seja civil ou militar, e apresenta condições estruturais para coordenar questões de defesa e segurança cibernética. No Brasil, a falta desse órgão implica que o GSI/PR, o MD e o MJ advoguem por seus interesses diretamente com o presidente e construam suas estratégias de forma independente.

No decorrer da pesquisa para construção do trabalho, foi percebido que, salvo as diferenças que serão pontuadas a seguir, as estratégias apontadas nos documentos de Brasil e Coreia do Sul não se encaixavam nas definições de poder clássicas do primeiro capítulo. Nenhum dos países analisados demonstra pretensão de mudar o comportamento de outros atores do sistema internacional, seja por força (hard power) ou persuasão (soft power), o que estavam sendo expostas eram estratégias puramente defensivas. Visto que os objetivos dos documentos principais em estratégia dos dois países elencam apenas questões de defesa: a Estratégia Nacional de Segurança Cibernética (2019) da Coreia do Sul tem como missão construir uma base sólida de segurança cibernética para o país, responder a ataques cibernéticos e fortalecer as infraestruturas centrais (SOUTH KOREA, 2020). A Estratégia Nacional de Segurança Cibernética brasileira, do mesmo modo, objetiva: 1. Tornar o Brasil mais próspero e confiável no ambiente digital; 2. Aumentar a resiliência brasileira às ameaças cibernéticas; e 3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional (BRASIL, 2020a).

Pode-se explicitar, portanto, as primeiras respostas relacionadas à hipótese proposta: a partir dos documentos oficiais de Brasil e Coreia do Sul, entende-se que os países propagam poder pelo espaço cibernético reconhecendo as ameaças presentes e construindo estratégias defensivas, confirmando a hipótese principal. É necessário, porém, levantar um ponto de dúvida em decorrência da natureza da pesquisa, é fato que os documentos analisados não apresentam capacidades ofensivas, isso significa que Brasil e Coreia do Sul não possuem interesses ofensivos? Ou não deixam explícitas seus interesses e capacidades ofensivas como mais uma estratégia?

Por fim, no último capítulo, concordando com a crítica proposta por Cavelty (2018) às variantes clássicas - as mesmas expostas no primeiro capítulo - para entender e mensurar

poder cibernético, que consideram o poder como uma forma de dominação "poder sobre" e não uma forma de empoderamento "poder para". Observou-se, portanto, que Brasil e Coreia do Sul buscam, a partir das estratégias expostas em seus documentos, poder no espaço cibernético para construir capacidades de defesa. Foi então proposto o Modelo de Capacidades Integradas de Kimburg (2014), considerado mais adequado para comparar as estratégias construídas pelos países.

Como resultados da comparação, aponta-se que a Coreia do Sul possui melhores capacidades de governo integradas por construir documentos mais robustos e coesos entre si, por promover parcerias entre atores governamentais e por apresentar uma estrutura de governança interna melhor organizada. Sobre as capacidades de sistemas integrados, ambos países honram suas tradições diplomáticas e apresentam esforços parecidos para cooperar internacionalmente em assuntos de cibernética. Enfim, é apontado que o interesse brasileiro em aumentar suas capacidades nacionais integradas ainda é recente, enquanto a Coreia apresenta mais eficiência em utilizar atores não estatais para construir suas políticas nacionais.

Ligando as conclusões tiradas a partir da comparação com um breve histórico de ataques cibernéticos sofridos pelos dois países ao retomar as condições geopolíticas que se encontram, é possível inferir que a Coreia do Sul considera as ameaças sofridas pelo seu entorno estratégico ao confeccionar suas estratégias de defesa. Mas não é possível confirmar a hipótese secundária de que a Coreia do Sul tem estratégias de defesa cibernética mais robustas que o Brasil, pois se encontra em um entorno estratégico que lhe propõe mais ameaças, em vista de que as informações presentes sobre os responsáveis pelos ataques cibernéticos sofridos pela Coreia do Sul serem baseadas apenas em presunções do próprio governo sul coreano. Como próximo passo de pesquisa, é necessário entender os objetivos de poder cibernético dos países presentes no entorno estratégico da Coreia do Sul e Brasil, a fim de possuir evidências suficientes para confirmar a segunda hipótese.

REFERÊNCIAS

AMORIM, Celso. **PREFÁCIO**. In: NASSER, Reginaldo Mattar; MORAES, Rodrigo Fracalossi de (org.). O Brasil e a segurança no seu entorno estratégico: américa do sul e atlântico sul. Brasília: Ipea, 2014. p. 9-10. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/3075/1/Livro_O%20Brasil%20e%20a%20seguran%C3%A7a%20no%20seu%20entorno%20estrat%C3%A9gico_Am%C3%A9rica%20do%20Sul%20e%20Atl%C3%A2ntico%20Sul.pdf. Acesso em: 20 fev. 2023.

ASEAN. About the ASEAN Defence Ministers' Meeting Plus. 2023. Disponível em: https://admm.asean.org/index.php/about-admm/about-admm-plus.html. Acesso em: 02 fev. 2023.

BALDWIN, David A.. **Power and International Relations**. Princeton University Press. 2016.

BOLLIER, David. **THE RISE OF NETPOLITIK:** how the internet is changing international politics and diplomacy. How the Internet Is Changing International Politics and Diplomacy. 2003. Disponível em: http://www.bollier.org/files/aspen_reports/NETPOLITIK.PDF. Acesso em: 11 set. 2022.

BRASIL. **Estratégia Nacional de Segurança Cibernética** – E-Ciber. Presidência da República. Brasília, Decreto nº 10.222, Brasil, 2020a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm>. Acesso em: ago de 2022.

____. Gabinete De Segurança Institucional. **Livro Verde – Segurança Cibernética no Brasil**. Gabinete de Segurança Institucional da Presidência da República. Brasília, Brasil. 2010.

____. **Livro Branco de Defesa Nacional**. Brasília, DF, 2012.

____. **Livro Branco de Defesa Nacional**. Brasília, DF, 2020b.

___. **Política Nacional de Defesa**. Brasília, DF, 2005.

____. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, DF, 2020c.

____. Portaria Normativa No 3010, de 18 de novembro de 2014. Aprova a **Doutrina Militar de Defesa Cibernética**. 2014. Portaria Normativa no 3.010/Md. Brasília, DF: Diário Oficial da União, 19 nov. v. 224. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf. Acesso em: fev de 2021.

CAMILO, Maj Inf Luiz Angelo Pelinsari. A **Geopolítica brasileira e sua influência para as iniciativas nacionais**. 2019. 51 f. TCC (Graduação) - Curso de Especialista em Ciências Militares, Com Ênfase em Defesa Nacional, Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2019. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/5780/1/MO%206114%20-%20PELINSARI.pdf. Acesso em: 19 fev. 2023.

CAVELTY, Myriam Dunn. **CYBERWAR**: concept, status quo, and limitations. Center For Security Studies (Css), Zurich, v. 71, n. , p. 1-3, abr. 2010.

CAVELTY, Myriam Dunn. 2018. **Europe's cyber-power, European Politics and Society**. DOI: 10.1080/23745118.2018.1430718.

CARRAPICO, H.; BARRINHA, A.. 2018. **European Union cyber security as an emerging research and policy field. European Politics and Society**, 19(3), 299–303. doi:10.1080/23745118.2018.1430.

CASTRO, Maria Carolina. **As competências brasileiras na produção de recursos para o setor de defesa cibernética e suas implicações**. TCC (graduação) - Universidade Federal de Santa Catarina. Centro Sócio-Econômico. Relações Internacionais. 2020. Disponível em: <https://repositorio.ufsc.br/handle/123456789/218387>. Acesso em agosto de 2022

CHUNG-IN, Moon; LEE, Sung-Won. **South Korea's geopolitics**: challenges and strategic choices. Melbourne Asia Review, [S.L.], v. 9, p. 1-11, 18 mar. 2022. Asia Institute, University of Melbourne. http://dx.doi.org/10.37839/mar2652-550x9.11. Disponível em: https://melbourneasiareview.edu.au/south-koreas-geopolitics-challenges-and-strategic-choices/?print=pdf. Acesso em: 23 dez. 2022.

DE RÊ, Eduardo. **Ciberespaço e segurança cibernética: as estratégias cibernéticas de EUA, China e Israel e as suas relações com a estratégia cibernética do Brasil**. TCC (graduação) - Universidade Federal de Santa Catarina. Centro Sócio-Econômico. Relações Internacionais. 2021. Disponível em: <https://repositorio.ufsc.br/handle/123456789/223136>. Acesso em agosto de 2022

DEVANNY, Joe et al. **The rise of cyber power in Brazil**. Revista Brasileira de Política Internacional, [S.L.], v. 65, n. 1, p. 1-21, 2022. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/0034-7329202200113.

FAGUNDES, George Harrison Gonçalves *et al*. **A COOPERAÇÃO INTERNACIONAL ENTRE BRASIL E ESTADOS UNIDOS EM MATÉRIA DE SEGURANÇA E DEFESA CIBERNÉTICA**. 2019. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/aa_cooperaaoa_internacionala_entrea_brasila_ea_estadosa_unidosa_ema_materiaa_dea_segurana.pdf. Acesso em: 10 fev. 2023.

FAVERO, Pedro Henrique Paulette. **O amanhecer do poder cibernético brasileiro?** Uma análise documental sobre defesa e segurança cibernética no Brasil de 2018 a 2020. TCC (graduação) - Universidade Federal de Santa Catarina. Centro Sócio-Econômico. Relações Internacionais. 2022. Disponível em: <https://repositorio.ufsc.br/handle/123456789/237203>. Acesso em agosto de 2022.

FEIGENBAUM, E.; NELSON, Michael R.. **The Korean Way With Data: how the world's most wired country is forging a third way.** Carnegie Endowment For International Peace, 2021.

FEITOSA, Lucas Marques. **Cooperação Cibernética Brasileira:** observando os atos internacionais (2010-2020). Observando os Atos Internacionais (2010-2020). 2021. Rede CTIDC. Disponível em: https://redectidc.com.br/assets/files/set-2021-cooperacao-cibernetica-brasileira.pdf. Acesso em: 10 fev. 2023.

FERREIRA NETO, W. B. **Territorializando o "Novo" e (Re)territorializando os Tradicionais: A Cibernética como Espaço e Recurso de Poder**. Coleção Meira Mattos, Rio de Janeiro, v. 8, n. 31, p. 7-18, abr./2014.

FORTIGUARD. **Fortinet**. 2021. Disponível em: https://www.fortiguard.com/encyclopedia/ips/43963/backdoor-doublepulsar. Acesso em: 14 maio 2021.

HUREL, L. **Brazil's first national cybersecurity strategy: an analysis of its past, present and future**. Atlanta: Internet Governance Project, 2020. Disponível em: https://www.internetgovernance.org/2020/04/05/brazils-first-national-cybersecurity-strategy-an-analysis-of-its-pastpresent-and-future/. Acesso em: 02 fev. 2023.

ITU. United Nations. **Global Cybersecurity Index 2020**: measuring commitment to cybersecurity. 2020. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. Acesso em: 08 fev. 2023.

JANG, Gyehyun; LIM, Jong-In. **Technologies of Trus**t: Online Authentication and Data Access Control in Korea. In: FEIGENBAUM, Evan A.; NELSON, Michael R.. The Korean Way With Data: how the world's most wired country is forging a third way. Carnegie Endowment For International Peace, 2021. p. 11-37.

KIM, So Jeong; BAE, Sunha. **Korean Policies of Cybersecurity and Data Resilience**. In: FEIGENBAUM, Evan A.; in NELSON, Michael R.. The Korean Way With Data: how the world's most wired country is forging a third way. Carnegie Endowment For International Peace, 2021. p. 39-60.

KLIMBURG, Alexander. **Mobilising Cyber Power**. Survival, vol 53 (1), p. 41-60, 2011.

KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K.. **Cyberpower and National Security**. Washington: University Of Nebraska Press, Potomac Books, 2009. p. 24-42.

LASSWELL, Harold D.; KAPLAN, A.. **Power and Society**: A Framework for Political Inquiry. New Haven, CT: Yale University Press. 1950.

LEE, Seungmin. **The Future of South Korea-US Cyber Cooperation**: North Korea's reliance on cyberattacks is growing, but the South Korea-U.S. alliance has yet to catch up. 2022. The Diplomat.. Disponível em: https://thediplomat.com/2022/10/the-future-of-south-korea-us-cyber-cooperation/. Acesso em: 23 fev. 2023.

LIRA, Paulo Vitor Sanches. **AGENDA DE SEGURANÇA BRASILEIRA**: o dilema entre a ameaça interna e externa. 2013. 112 f. Dissertação (Mestrado) - Curso de Programa de

Pós-Graduação em Economia Política Internacional, Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2013. Disponível em: https://www.ie.ufrj.br/images/IE/PEPI/disserta%C3%A7%C3%B5es/2013/Paulo%20Vitor%20Sanches%20Lira.pdf. Acesso em: 19 fev. 2023.

MAFRA, Roberto Machado de Oliveira. **Geopolític**a: Introdução ao Estudo. São Paulo: Sicurezza, 2006.

MEDEIROS FILHO, Oscar. **BREVE PANORAMA DE SEGURANÇA NA AMÉRICA DO SUL**. In: NASSER, Reginaldo Mattar; MORAES, Rodrigo Fracalossi de (org.). O Brasil e a segurança no seu entorno estratégico: américa do sul e atlântico sul. Brasília: Ipea, 2014. p. 9-10. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/3075/1/Livro_O%20Brasil%20e%20a%20seguran%C3%A7a%20no%20seu%20entorno%20estrat%C3%A9gico_Am%C3%A9rica%20do%20Sul%20e%20Atl%C3%A2ntico%20Sul.pdf. Acesso em: 20 fev. 2023.

MORGENTHAU, Hans J. **A política entre as nações**: a luta pelo poder e pela paz. Brasília. Editora Universidade de Brasília. 1948.

NYE, Joseph S.. **Cyber Power.** Belfer Center For Science And International Affairs, Cambridge, p. 1-30, maio 2010.

____. **The Future of Power**. Public Affairs, 2011.

____. **Soft Power: The Means to Success in World Politics**. New York, Public Affairs Press. 2004.

OECD, **Declaration for the Future of the Internet Economy (The Seoul Declaration)**. OECD/LEGAL/0366, adotada em 17 de junho de 2008.

OLIVEIRA, Marcos Aurélio Guedes de; PORTELA, Lucas Soares. **As camadas do espaço cibernético sob a perspectiva dos documentos de defesa do Brasil**. Revista Brasileira de Estudos de Defesa, Porto Alegre, v. 4, n. 2, p. 77-99, dez./2017.

PAGLIARI, Graciela de Conti; AYRES PINTO, Danielle Jacon; BARROSO, Juliana L. Viggiano. **Mobilização nacional, ameaças cibernéticas e redes de interação num modelo de tríplice hélice estratégica**: um estudo prospectivo. In: Marcos Guedes de Oliveira. (Org.). Defesa Cibernética e Mobilização Nacional. 1ed.Recife: UFPE, 2020, v. 1, p. 153-174.

PRADO, Marcelo Alves. **Análise experimental da botnet IoT Mirai**. 2018. 69 f. TCC (Graduação) - Curso de Sistemas de Informação., Universidade Federal de Uberlândia, Urbelândia, 2018. Disponível em: https://repositorio.ufu.br/bitstream/123456789/24053/1/AnaliseExperimentalBotnet.pdf. Acesso em: 10 dez. 2022.

SILVA J. C. B. L. 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./jun. 2014. Disponível em: https://revista.egn.mar.mil.br/index.php/revistadaegn/article/download/194/156. Acesso 04 maio 2021.
SINGER, P.W; FRIEDMAN, Allan. **Cybersecurity and Cyberwar**: What Everyone Needs to Know. 1. ed. Oxford: Oxford University Press, 2013.

SOUTH KOREA. **Annual Report**. National Cybersecurity Center. 2021.

____. **Defense White Paper**. Ministry of National Defense. 2020.

____. **Defense White Paper**. Ministry of National Defense. 2006.

____. **Defense White Paper**. Ministry of National Defense. 2008.

____. **Defense White Paper**. Ministry of National Defense. 2010.

____. **Defense White Paper**. Ministry of National Defense. 2014.

____. **Defense White Paper**. Ministry of National Defense. 2016.

____. **Defense White Paper**. Ministry of National Defense. 2018a.

____. **National Cybersecurity Strategy**. 2019. National Security Office.

____. **National Cybersecurity Master Plan**. 2011.

____. **National Cybersecurity White Paper**. National Intelligence Service. 2022.

____. 국가정보보호백서. National Intelligence Service. 2018b.

____. 국가사이버안전관리규정. 대통령훈령 제316호, 2013. 9. 2., 일부개정. 2013.

SOUZA, G. L. Mâcedo. **Reflexos da digitalização da Guerra na Política Internacional do Século XXI**: Uma análise exploratória da securitização do Ciberespaço nos Estados Unidos, Brasil e Canadá. 2013. 129f. Dissertação (Mestrado em Ciência Política) - Centro de Filosofia e Ciências Humanas, Universidade Federal de Pernambuco, Recife, 2013.

UNITED NATIONS. 2013. **Seoul Framework for and Commitment to Open and Secure Cyberspace**. Disponível em: <https://www.un.org/en/desa/seoul-conference-cyberspace-2013>. Acesso em dezembro de 2022.

USA. **INFORMATION OPERATIONS CONDITION (INFOCON) SYSTEM PROCEDURES**. 2006. Department of Defense. Disponível em: https://info.publicintelligence.net/StrategicCommandDirective527-1_27JAN2006InformationOperationsCondition-INFOCON-System.pdf. Acesso em: 10 fev. 2023.

USA. **Joint Communique of the 52nd U.S.-Republic of Korea Security Consultative Meeting**. 2020. Disponível em:

https://www.defense.gov/News/Releases/Release/Article/2381879/joint-communique-of-the-52nd-us-republic-of-korea-security-consultative-meeting/. Acesso em: 02 fev. 2023.

USA. **United States-Republic of Korea Leaders' Joint Statemen**t. 2022. Disponível em: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/21/united-states-republic-of-korea-leaders-joint-statement/. Acesso em: 02 fev. 2023.

VENTRE, Daniel. 2012. **Ciberguerra**. In: Academia General Militar. Seguridad Global y Potencias Emergentes en un Mundo Multipolar. XIX Curso Internacional de Defensa. Zaragoza: Universidad Zaragoza.

WILLETT, Marcus. 2019. **Assessing Cyber Power**. Survival, 61:1, 85-90. DOI: 10.1080/00396338.2019.1569895.