ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO
ESCOLA MARECHAL CASTELLO BRANCO

Maj Com **Asael** da Silva Vaz

Uma análise comparada dos modelos de governança cibernética adotados no Canadá, Reino Unido e Japão com o modelo adotado no Brasil.

Rio de Janeiro
2024

Maj Com **Asael** da Silva Vaz

Uma análise comparada dos modelos de governança cibernética adotados no Canadá, Reino Unido e Japão com o modelo adotado no Brasil.

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Defesa Nacional.

Orientador: Maj Com Leandro **Kuhn**

Rio de Janeiro

2024

V393a Vaz, Asael da Silva

Uma análise comparada dos modelos de governança cibernética adotados no Canadá, Reino Unido e Japão com o modelo adotado no Brasil. / Asael da Silva Vaz. - 2024.

71 f. il. 30 cm.

Orientador : Leandro Kuhn

Trabalho de Conclusão de Curso (Especialização em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2024.

Bibliografia: f. 67 - 71.

1. Governança Cibernética. 2. Reino Unido. 3. Canadá. 4. Japão. 5. Brasil. I Título

CDD 658.4

“Compreensão exige teoria; teoria exige abstração; e abstração exige simplificação e ordenamento da realidade. Teoria alguma pode explicar todos os fatos” (Samuel P. Huntington).

Maj Com **Asael** da Silva Vaz

Uma análise comparada dos modelos de governança cibernética adotados no Canadá, Reino Unido e Japão com o modelo adotado no Brasil.

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Defesa Nacional.

Aprovado em 04 de outubro de 2024.

COMISSÃO AVALIADORA

Maj Com LEANDRO KUHN – Presidente
Escola de Comando e Estado-Maior do Exército

Maj Com QEMA WAGNER DE MATOS SALUSTRIANO – Membro
Escola de Comando e Estado-Maior do Exército

Maj Art QEMA CARLOS EDUARDO DA SILVA LOURENÇO – Membro
Escola de Comando e Estado-Maior do Exército

RESUMO

O espaço cibernético tornou-se tão relevante para a sociedade contemporânea que a Organização do Tratado do Atlântico Norte (OTAN), em 2017, considerou-o mais um domínio, junto ao terrestre, marítimo, aéreo e espacial. Reino Unido, Canadá e Japão estão entre os países mais dependentes de redes de dados e da Internet, tanto que consideraram a proteção desse ambiente virtual essencial para a segurança de suas nações e atribuíram tarefas para a Defesa. No Brasil, não foi diferente. Diante de tal relevância e do fato de que a maioria dos serviços modernos utilizam esse espaço, a governança torna-se essencial para organizar sua exploração e segurança. Mas, como os modelos se relacionam quando comparados? São similares, podemos dizer que um é mais adequado que outro? O objetivo desse trabalho é encontrar respostas verificando se a estrutura da governança cibernética do Brasil está adequada para garantir sua liberdade de ação. O assunto de governança tem sido amplamente estudado, assim como a cibernética, sendo o estudo da governança aplicada ao setor cibernética é algo mais recente. O espaço cibernético cresceu à medida que a Internet expandiu-se pelo globo tornando-o conectado, mas as questões de segurança e as estratégias de segurança do setor foram, em sua maioria, apresentadas a partir do início da década de 2010. Como exemplo, a mudança de Estratégia de Segurança Cibernética para Estratégia Nacional de Cibernética no Reino Unido ocorreu em 2021, assim como a Política Nacional de Cibersegurança do Brasil foi publicada em 2023. Logo, o problema apresentado foi como a organização da governança cibernética do Brasil apresenta-se, quando comparada aos modelos do Canadá, Reino Unido e Japão? Para chegar a uma resposta, foi realizada uma pesquisa bibliográfica para levantar os dados sobre governança cibernética e como está estruturada nos países selecionados. A comparação dos dados compilados foi realizada por análise de conteúdo. A investigação oferece dados centralizados sobre as legislações acerca da cibernética e da organização das estruturas que atuam no setor na esfera nacional e na Defesa. Tais dados permitem a visualização da posição do Brasil em relação a países considerados do arco do conhecimento. Os resultados podem contribuir para a evolução organizacional do espaço cibernético do Brasil, apresentando possibilidades de arranjos.

Palavras-chave: governança cibernética, Reino Unido, Canadá, Japão, Brasil.

ABSTRACT

The cyberspace has become so relevant to contemporary society that the North Atlantic Treaty Organization (NATO) considered it an additional domain in 2017, alongside land, maritime, aerial, and space domains. The United Kingdom, Canada, and Japan are among the countries most dependent on data networks and the Internet, to the extent that they consider the protection of this virtual environment essential for the security of their nations and have assigned tasks to their Defense sectors. In Brazil, it is no different. In light of such relevance and the fact that most modern services utilize this space, governance becomes essential for organizing its exploration and security. But how do the models relate when compared? Are they similar, or can we say that one is more suitable than the other? The objective of this work is to find answers by verifying whether the structure of Brazil's cyber governance is adequate to ensure its freedom of action. The topic of governance has been extensively studied, as has cybernetics, with the study of governance applied to the cyber sector being a more recent development. Cyberspace has grown as the Internet has expanded globally, connecting it, but security issues and strategies for the sector were mostly presented from the early 2010s. For example, the transition from Cyber Security Strategy to National Cyber Strategy in the United Kingdom occurred in 2021, just as Brazil's National Cybersecurity Policy was published in 2023. Therefore, the presented problem is how Brazil's cyber governance organization compares to those of Canada, the United Kingdom, and Japan. To reach an answer, a bibliographic research was conducted to gather data on cyber governance and how it is structured in the selected countries. The comparison of the compiled data was conducted through content analysis. The investigation provides centralized data on the legislation regarding cybernetics and the organization of structures operating in the sector at the national level and in Defense. Such data allows for visualization of Brazil's position in relation to countries considered part of the knowledge arc. The results may contribute to the organizational evolution of Brazil's cyberspace, presenting possibilities for arrangements.

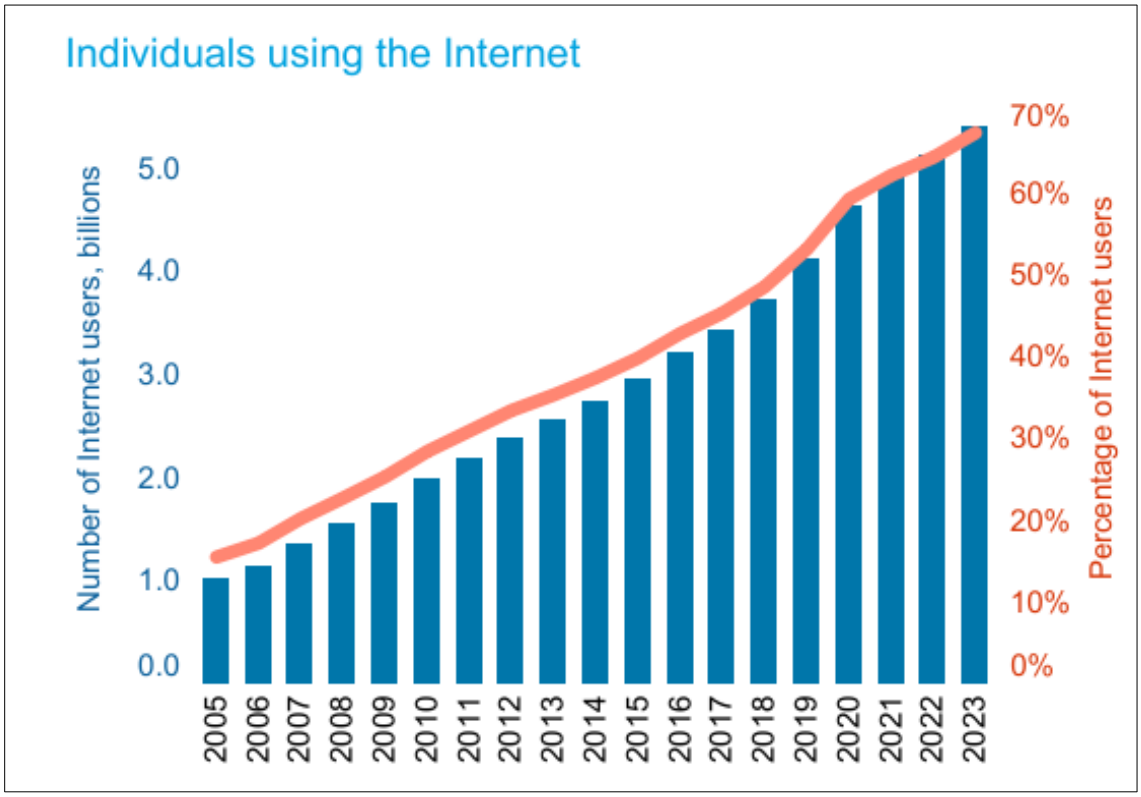
Keywords: cyberspace governance, United Kingdom, Canada, Japan, Brazil.

SUMÁRIO

1. INTRODUÇÃO

O setor cibernético tornou-se essencial para a maioria das sociedades. Setores essenciais (como o elétrico, de saneamento, transporte, segurança pública e de saúde), as infraestruturas críticas (como usinas de geração de energia, plantas nucleares ou estações de tratamento de água), além dos sistemas financeiros, bancários e de investimento estão conectados a redes de dados e à Rede Mundial de Computadores (Internet) e dependem destas para suas operações. Podemos observar o aumento de pessoas conectadas à Internet na Figura 1:

Figura 1. Evolução do número de usuários na Internet.



Fonte: ITU, 2024

Segundo o gráfico acima, 5,4 bilhões de pessoas, 67% da população mundial, estavam conectadas à Internet em 2023, um aumento de 45% desde 2018. Quanto maior o número de usuários, maior a necessidade de manter o ciberespaço em segurança.

Além disso, tal dependência aumenta à medida que os países se desenvolvem e a infraestrutura da Internet expande-se pelo espaço geográfico e em número de usuários. O controle remoto dos serviços, mesmo os críticos,

e o acesso *on-line* a eles faz parte da vida moderna e facilita nossas atividades diárias. Ainda, a pandemia de Covid-19 popularizou, por imposição da necessidade, ainda mais os acessos remotos, como trabalho, consultas médicas a distância e o *Internet Banking.* Como afirmou Doreen Bogdan-Martin, atual secretária-geral da União Internacional de Telecomunicações, com tradução do autor, a necessidade de um cibererpaço seguro e protegido torna-se mais importante à medida que nos tornamos cada vez mais dependentes de "recursos digitais essenciais".

Essa condição atrai o espaço cibernético para a área de interesse da Defesa:

> O fato de nossos sistemas vitais serem tão vulneráveis à guerra cibernética também aumenta a instabilidade de crise. Enquanto nossos sistemas econômicos e militares forem tão obviamente vulneráveis à guerra cibernética, nossos oponentes se sentirão instigados a nos atacar em períodos de tensão. Os oponentes podem pensar que têm uma oportunidade de fazer uma reforma no balanço político, econômico e militar, demonstrando ao mundo o que eles podem fazer com os EUA. Eles podem acreditar que a ameaça de um dano ainda maior dará maior credibilidade e prevenirá uma resposta dos Estados Unidos. No entanto, depois que uma ataque cibernético for lançado, a liderança norte-americana poderá se sentir obrigada a responder. E essa resposta pode não estar limitada ao ciberespaço, fazendo o conflito escalar rapidamente e ficar fora de controle (CLARK e KNAKE, 2015, p. 128).

O funcionamento da maioria dos Estados e seus governos depende diretamente de redes de dados e do acesso à Internet. Além disso, é por meio da rede mundial que os cidadãos têm acesso a informações e serviços disponibilizados por instituições e organizações estatais. Tal condição gera vulnerabilidades que ameaçam os Estados e seus povos, como descrito na seguinte análise sobre os EUA:

> Na verdade, devido à sua maior dependência a sistemas controlados de forma cibernética e à sua incapacidade, até o momento, de criar defesas cibernéticas nacionais, os Estados Unidos estão atualmente muito mais vulneráveis à guerra cibernética do que a Rússia ou a China e possuem um maior risco de guerra cibernética do que estados menores, como a Coreia do Norte. Podem até mesmo, em algum momento, estar em risco diante de nações ou personagens não estatais que, apesar de não possuírem capacidade de guerra cibernética, podem contratar equipes de *hackers* altamente capacitados (CLARK e KNAKE, 2015, p. 127).

Quando busca-se demonstrar a importância do ambiente cibernético para um país, os exemplos mais comuns estão relacionados à possibilidade de

interrupção de serviços básicos em caso de um ataque. As chamadas infraestruturas críticas, como sistemas de geração e distribuição de energia, de transportes, saúde, bancário e financeiro funcionam por meio de redes de dados e estão conectadas à Internet, logo estão vulneráveis a ataques com origem no ambiente cibernético.

Podemos exemplificar tal possibilidade por meio de uma operação dos Estados Unidos da América no ambiente cibernético a uma instalação nuclear iraniana. Na primeira década do século XXI, agências americanas criaram um artefato cibernético (um *worm)* chamado *Stuxnet.* Essa arma foi desenhada para atacar os sistemas de controle de centrífugas iranianas para enriquecimentos de Urânio-235 em Natanz, o que ocorreu em 2009. Como resultado do sucesso do ataque, centenas de centrífugas quebraram totalmente, atrasando o programa nuclear iraniano. Ou seja, como afirmou Clarke (2012), o *Stuxnet* representou um ataque cibernético de um país a outro, causando danos a uma infraestrutura crítica.

Isso demonstra a necessidade de uma governança de Estado para o ambiente cibernético, a fim de garantir a segurança do país. A governança cibernética cria uma estrutura nos níveis político e estratégico, que envolve legislação, regulamentação e fiscalização, capaz de atuar ativamente no espaço virtual.

A análise e comparação dos sistemas de governança cibernética de diferentes países pode ajudar-nos a avaliar a organização em vigor no Brasil.

1.1 PROBLEMA E OBJETIVOS

O presente estudo pretende relacionar modelos de governança cibernética e buscará responder o seguinte problema: **como a organização da governança cibernética do Brasil apresenta-se, quando comparada a países do arco do conhecimento, especificamente, Canadá, Reino Unido e Japão?**

Com vistas à resolução de tal problemática, com fundamentação teórica e adequada profundidade de investigação, foi definido o seguinte objetivo geral: **comparar os modelos de governança cibernética adotados no Canadá, Reino Unido e Japão com o aplicado no Brasil.**

Para viabilizar a consecução do objetivo geral de estudo, foram propostos os seguintes objetivos específicos, que permitirão o encadeamento lógico do raciocínio investigativo:

a. Refinar o conceito de governança cibernética;
b. explicar a seleção dos países para comparação;
c. descrever os modelos de governança dos países selecionados;
d. descrever o modelo de governança do Brasil;
e. comparar os modelos analisados.

1.2 DELIMITAÇÃO E QUESTÕES DE ESTUDO

Para verificar as condições da governança cibernética no Brasil, é necessário compará-las às de outros países. Para definir quais seriam escolhidos para tal comparação, foram definidos alguns parâmetros. O primeiro quesito é que fosse países considerados desenvolvidos, por estes serem mais dependentes do espaço cibernético. O segundo é que estivessem localizados em diferentes continentes, a fim de garantir a maior diversidade de influências possível.

As características a serem analisadas devem estar em vigor no ano de 2024. Ou seja, as regulamentações, organizações, instituições e órgãos dos Estados devem estar em vigor ou ativos no presente ano.

Em relação ao nível analisado, estaremos limitados aos níveis político e estratégicos dos Estados. Isso deve-se ao fato de a governança estar localizada em tais níveis, principalmente no político.

QUADRO 1 – Questões de Estudo

Questões de Estudo	Objetivos
1) O que é governança cibernética?	a.
2) Como a governança cibernética está organizada no Brasil?	d.
3) Como a governança cibernética está organizada em países desenvolvidos do arco do conhecimento?	c.
4) Como tais países serão selecionados para a pesquisa?	b.
5) Como a organização da governança cibernética do Brasil está quando comparada a outros países?	e.

Fonte: elaborado pelo autor

1.3 RELEVÂNCIA DO ESTUDO

O setor cibernético foi considerado estratégico e essencial para a Defesa na Estratégia Nacional de Defesa de 2008 (END 2008). A Diretriz Ministerial nº 14 do Ministério da Defesa (MD), de 09 de novembro de 2009, definiu providências para o cumprimento da END 2008 nos setores estratégicos da defesa, definindo ao Exército a responsabilidade pela coordenação e pela integração do Setor Cibernético (BRASIL, 2014).

Entretanto, o domínio cibernético transpassa todos os setores da sociedade e adquiriu caráter essencial para elas. Considerando que a segurança cibernética envolve atores estatais e não-estatais sem relação hierárquica, a governança torna-se ainda mais relevante, pois o povo, principal usuário dessa tecnologia, demandará gestão em todos os níveis a fim de garantir seu pleno funcionamento.

Uma forma de verificar o nível de organização da governança do setor cibernético no Brasil é compará-lo com o sistema adotado em outros países, observando as diferenças entre os Estados. Dessa forma poderemos verificar como o Estado brasileiro e outros organizaram sua governança cibernética.

Estudos sobre o assunto já foram realizados, mas a composição com diferentes países pode enriquecer o conhecimento e levantar novas possibilidades de organização desse setor estratégico.

2. REFERENCIAL TEÓRICO-CONCEITUAL

O conceito de governança cibernética ainda está em desenvolvimento. A expansão do acesso à Internet e do uso de redes de dados em geral aconteceu em ritmo acelerado, e a preocupação com a segurança do ambiente cibernético foi um fenômeno recente. Isso levou a uma falta de padronização de requisitos e procedimentos.

A necessidade de uma organização da utilização do espaço cibernético, desde o nível político até o nível do indivíduo usuário, surgiu após o aumento de ameaças virtuais que desafiavam o Estado, empresas e infraestruturas críticas. O combate a tais ameaças apontou para a necessidade de coordenação das ações.

2.1 DELIMITAÇÃO DO CONCEITO DE GOVERNANÇA CIBERNÉTICA

O termo governança possui diferentes empregos e definições, por ser utilizado em diferentes níveis organizacionais e áreas temáticas. Logo, faz-se necessário a delimitação da forma como o termo será utilizado e empregado.

Inicialmente, serão apresentadas as definições utilizadas por diferentes instituições, a nível nacional e mundial, conforme Tabela 1.

TABELA 1. Definições de governança

Instituição	Definição
Tribunal de Contas da União (BRASIL, 2014)	Pode ser definida como a habilidade e a capacidade governamental para formular e implementar, de forma efetiva, políticas públicas mediante o estabelecimento de relações e parcerias coordenadas entre organizações públicas e/ou privadas.
Organização para Cooperação e Desenvolvimento Econômico (2005, tradução do autor)	Refere-se aos arranjos formais e informais que determinam a tomada de decisões públicas e a condução de ações públicas, mantendo os valores comerciais de um país no enfrentamento a ambientes e problemas em constante mudança.

Instituto Brasileiro de Gestão Corporativa (2023)	É um sistema formado por princípios, regras, estruturas e processos pelo qual as organizações são dirigidas e monitoradas, com vistas à geração de valor sustentável para a organização, para seus sócios e para a sociedade em geral. Esse sistema baliza a atuação dos agentes de governança e demais indivíduos de uma organização na busca pelo equilíbrio entre os interesses de todas as partes, contribuindo positivamente para a sociedade e para o meio ambiente.
Programa das Nações Unidas para o Desenvolvimento (PNUD, tradução do autor)	É o sistema de valores, políticas e instituições pelas quais uma sociedade coordena seus assuntos econômicos, políticos e sociais, através de interações internas e entre os Estados, sociedade civil e setor privado. É o modo como a sociedade se organiza para tomar e implementar decisões - alcançando compreensão mútua, acordos e ações.
Banco Mundial (World Bank, 1992, tradução do autor)	É o modo como o poder é exercido no gerenciamento dos recursos econômicos e sociais em busca do desenvolvimento.

Fonte: elaborado pelo autor, baseado em Teixeira e Gomes (2019)

Diante de diferentes formas de emprego do termo, governança será utilizada no presente trabalho como definida por Rocha (2010): é a coordenação da ação e tomada de decisão entre sociedade, atores estatais e atores não estatais sobre determinado assunto. Tal definição sintetiza as ideias que se repetiram nos conceitos levantados.

Cibernética corresponde ao ambiente virtual no qual as pessoas se conectam para envio e recebimento de dados. Segundo o manual de Guerra Cibernética,

> É um domínio global dentro da dimensão informacional do ambiente operacional que consiste em uma rede interdependente de infraestruturas de Tecnologia da Informação e Comunicações (TIC) e de dados, incluindo a internet, redes de telecomunicações, sistemas de computador, processadores embarcados e controladores (BRASIL, 2017).

Essa característica global impede que sejam estabelecidos limites específicos geográficos e de responsabilidade, o que faz a governança essencial para coordenação das ações de segurança e de usos das redes de dados, principalmente a Internet, pelos diversos atores de uma sociedade.

Ao utilizarmos os dois termos acima analisados, podemos elaborar um conceito para o emprego do termos Governança Cibernética: é a coordenação das decisões e ações entre sociedade, atores estatais e atores não estatais sobre o uso do ambiente cibernético.

2.2 SELEÇÃO DOS PAÍSES

Os países foram selecionados segundo três critérios:

a. Os países devem ser de diferentes continentes.

b. Devem estar acima do Brasil no Índice Global de Cibersegurança (IGC), em inglês *Global Cybersecurity Index (*GCI), da União Internacional de Telecomunicações (UIT), em inglês *International Telecommunication Union (*ITU).

c. Estados Unidos da América (EUA) e China foram excluídos por terem um poder econômico muito superior ao do Brasil. São as duas maiores economias do mundo, com Produto Interno Bruto (PIB) de, respectivamente, cerca de US$ 25 trilhões e US$ 18 trilhões (somados, representam 42% do PIB global aproximadamente), enquanto o PIB brasileiro foi de US$ 2,17 trilhões em 2023.

A UIT é uma agência especializada da Organização das Nações Unidas (ONU) voltada para tecnologia digital (ITU, 2024, tradução do autor). Desde 2015, a UIT realiza estudos sobre o compromisso de países com a cibersegurança, em parceria com os próprios países participantes e especialistas, e elabora um relatório. Já foram elaboradas 04 edições nos anos de 2015, 2017, 2018 e 2020.

O site de divulgação do IGC traz a seguinte definição do índice:

> O Índice Global de Cibersegurança é uma referência confiável que mede o compromisso de países com segurança cibernética em um nível global – para elevar a consciência da importância e diferentes dimensões do assunto. Como segurança cibernética tem um amplo campo de aplicação, abrangendo muitas indústrias e vários setores, o nível de desenvolvimento ou engajamento de cada país é avaliado de acordo com cinco pilares: medidas legais, medidas organizacionais, capacidade de desenvolvimento e cooperação – que depois são agregados em uma pontuação geral (ITU, tradução do autor).

A seguir, serão definidos os cinco pilares avaliados para elaboração do IGC:

a. medidas legais: analisa as leis e regulamentações de crimes e segurança cibernéticos;

b. medidas técnicas: analisa a implementação de capacidades técnicas nas agências do Estado e de setores específicos;

c. medidas organizacionais: analisa as estratégias nacionais e organizações que implementam cibersegurança;

d. medidas de desenvolvimento: mede campanhas de conscientização, treinamento, educação e incentivos para o desenvolvimento de capacidades em segurança cibernética; e

e. cooperação: analisa parcerias entre agências, empresas e países.

Aplicados os fatores de seleção dos países para análise e comparação, chegamos à seleção de três países, os quais seguem com as respectivas posições no IGC: Reino Unido (2º), Japão (7º) e Canadá (8º). O Brasil ocupou a 18ª posição. Seguem as pontuações obtidas por tais países no IGC 2020:

TABELA 2. Pontuações IGC dos países selecionados

País	Pontuação geral	Medidas legais	Medidas técnicas	Medidas organizacionais	Capacidades	Cooperação
Reino Unido	99.54	20.00	19.54	20.00	20.00	20.00
Japão	97.82	20.00	19.08	18.74	20.00	20.00
Canadá	97.67	20.00	18,27	20.00	20.00	19.41
Brasil	96.60	20.00	18.73	18.98	19.48	19.41

Fonte: GLOBAL CYBERSECURITY INDEX, 2020.

As notas de cada pilar têm uma escala de 0 a 20 pontos, que podem totalizar a pontuação geral de 0 a 100 pontos por soma.

2.3 ESTABELECIMENTO DOS CRITÉRIOS PARA COMPARAÇÃO

Após a análise dos dados sobre a governança cibernética dos países selecionados, a comparação será realizada com os fatores levantados na pesquisa bibliográfica. Conforme a pesquisa se desenvolver, novos pontos poderão ser adicionados. Inicialmente, os fatores serão:

a. Quais legislações regulamentam as ações o espaço cibernético?

b. Quais estruturas participam da governança cibernética?

c. As legislações e estruturas de governo estão em sintonia?

d. As agências que atuam no setor cibernético da Defesa estão sob uma estrutura de governança própria?

3. METODOLOGIA

Neste capítulo, será apresentada a metodologia utilizada para atingir os objetivos propostos. Serão descritos o desenho e a estratégia da pesquisa, bem como detalhados o tratamento dos dados e o cronograma a ser seguido para cumprimento dos prazos estipulados.

Inicialmente, serão apresentados os métodos, procedimentos e técnicas que serão utilizados na pesquisa. Na sequência, abordaremos a estratégia para a coleta e o tratamento dos dados. Tudo isso para que sejam cumpridos os objetivos da pesquisa, formais e de conteúdo.

3.1 DESENHO DA PESQUISA

O desenho da pesquisa faz parte do rigor que separa a ciência do senso comum. Ele contém a descrição do que será realizado para alcançar o objetivo proposto, além dos aspectos formais e exigências técnicas que o trabalho deve apresentar. Como afirmaram Lakatos e Marconi, “não há ciência sem o emprego de métodos científicos” (2016, p. 65).

Quanto ao método de abordagem, a presente pesquisa aplicará o indutivo. Segundo Lakatos e Marconi, “o objetivo dos argumentos indutivos é levar a conclusões cujo conteúdo é muito mais amplo do que o das premissas nas quais se basearam” (2016, p. 68). Ao comparar a governança cibernética de diferentes países, a partir da análise de documentos, as conclusões serão mais amplas que as premissas, pois não estavam antes nelas, como afirmaram os mesmos autores sobre este método: “a conclusão encerra informação que não estava, nem implicitamente, nas premissas” (2016, p. 74).

Para atingir os objetivos da pesquisa, será utilizado o método de análise de conteúdo. Segundo Moraes:

> A análise de conteúdo constitui uma metodologia de pesquisa usada para descrever e interpretar o conteúdo de toda classe de documentos e textos. Essa análise, conduzindo a descrições sistemáticas, qualitativas ou quantitativas, ajuda a reinterpretar as mensagens e a atingir uma compreensão de seus significados num nível que vai além de uma leitura comum (1999, p. 2).

Em relação aos procedimentos, a presente pesquisa caracteriza-se como uma pesquisa documental. Uma vez que a fonte de informações sobre a assunto serão, majoritariamente, documentos produzidos por Estados e seus governos. Segundo Godoy (1995, p. 21-22), “os documentos normalmente são considerados importantes fontes de dados para outros tipos de estudos

qualitativos, merecendo portanto atenção especial", sendo que documento "deve ser entendido de uma forma ampla, incluindo os materiais escritos (como, por exemplo, jornais, revistas, diários, obras literárias, científicas e técnicas, cartas, memorandos, relatórios)" (Godoy, 1995, p. 21-22).

Do ponto de vista da natureza, o presente trabalho será uma pesquisa básica, pois busca apresentar novos conhecimentos a partir da análise dos dados coletados. Segundo Freitas e Prodanov, a pesquisa básica "objetiva gerar conhecimentos novos úteis para o avanço da ciência sem aplicação prática prevista" (2013, p. 51).

No que se refere aos seus objetivos, a pesquisa será exploratória, haja vista que busca levantar informações sobre a governança cibernética e estabelecerá uma base para aprofundamento em pesquisas futuras. Ainda, segundo os mesmos autores citados acima, "quando a pesquisa se encontra na fase preliminar, tem como finalidade proporcionar mais informações sobre o assunto que vamos investigar, possibilitando sua definição e seu delineamento, isto é, facilitar a delimitação do tema da pesquisa" (2013, p. 51-52).

Dessa forma, a partir do desenho descrito e para atingir o objetivo geral da pesquisa, seguiremos o seguinte plano:

QUADRO 2 – Desenho da Pesquisa

PROBLEMA	OBJETIVO GERAL	OBJETIVO ESPECÍFICO	PROCEDIMENTO	INSUMO	PRODUTO
A organização da governança cibernética no Brasil está adequada às necessidades estratégicas brasileiras, quando comparada a países do arco do conhecimento, especificamente, Canadá, Reino Unido e Japão?	**Comparar os modelos de governança cibernética adotados no Canadá, Reino Unido e Japão com o aplicado no Brasil**	**Explicar governança cibernética**	Pesquisa bibliográfica	Publicações científicas, publicações técnicas, jornais, revistas, livros, videos, manuais	- Texto com definições
		Explicar a seleção dos países para comparação	Pesquisa bibliográfica	Publicações científicas, publicações técnicas, jornais, revistas, livros, videos, manuais	- Texto com definições
		Descrever os modelos de governança dos países selecionados	Pesquisa bibliográfica	Publicações científicas, publicações técnicas, jornais, revistas, livros, videos, manuais	- Registro dos dados coletados
		Descrever o modelo de governança do Brasil	Pesquisa bibliográfica	Publicações científicas, publicações técnicas, jornais, revistas, livros, videos, manuais	- Registro dos dados coletados
		Comparar os modelos analisados	Análise de conteúdo	Dados levantados e tratados sobre os modelos de governança cibernética.	- Compilação e comparação dos dados

Fonte: elaborado pelo autor.

3.2 ESTRATÉGIA DE PESQUISA

O tópico anterior explicou a metodologia a ser utilizada para que o objetivo proposto seja alcançado, segundo o que nos apresentou Freitas e Prodanov:

> “A Metodologia, em um nível aplicado, examina, descreve e avalia métodos e técnicas de pesquisa que possibilitam a coleta e o processamento de informações, visando ao encaminhamento e à resolução de problemas e/ou questões de investigação” (2013, p. 14).

A investigação se concentra nos objetivos específicos e a análise de conteúdo será adotada como procedimento metodológico de revisão.

3.2.1 Coleta de dados

A coleta de dados pode ser entendida como a forma como uma amostra foi montada e como informações foram extraídas do material analisado. Segundo Freitas e Prodanov, a coleta de dados deve ser apresentada a fim de informar como foi selecionada e como foram extraídos elementos da amostra, a fim de garantir clareza em tal etapa (2013, p. 129).

O critério para seleção dos documentos a serem analisados foi a produção oficial dos Estados dos países selecionados, de todos os poderes, referentes à regulamentação do espaço cibernético. Já os dados a serem coletados foram os que tratavam da governança desse ambiente, ou seja, medidas legais, técnicas, organizacionais e de regulamentação.

Uma limitação encontrada foi a restrição de acesso a alguns dados, o que é compreensível pela sensibilidade do assunto Cibernética na atualidade. Alguns documentos possuíam informações que não eram claras ou citavam outros documentos que não estavam disponíveis em fontes abertas.

3.2.2 Tratamento de dados

Na presente pesquisa, será realizada uma codificação qualitativa baseada em ideias-chave selecionadas ao longo do trabalho. Como descreve Godoy (1995. p. 58) a pesquisa qualitativa “não procura enumerar e/ ou medir os eventos estudados, nem emprega instrumental estatístico na análise dos dados”. O objetivo será analisar documentações que os países produziram sobre governança do espaço cibernético e extrair informações sobre sua organização, para “compreender os fenômenos segundo a perspectiva dos sujeitos, ou seja, dos participantes da situação em estudo” (Godoy, 1995, p.58).

O tratamento dos dados deu-se, inicialmente, por meio da compreensão da organização da documentação dos Estados sobre o espaço cibernético. As informações foram selecionadas quando havia relato das organizações e instituições que têm responsabilidade sobre o setor. Outros dados extraídos foram as leis e regulamentações do uso desse ambiente. Os dados foram então compilados para verificar os padrões e se poderiam ser comparados entre os países.

A limitação dessa fase foi similar à da coleta de dados. Os detalhes de algumas estruturas e documentações não eram facilmente encontradas ou não estavam disponíveis em fontes abertas. Alguns dados coletados foram descartados pela falta de confirmação ou mais detalhes para sua exploração.

4. CRONOGRAMA

	FEV	MAR	ABR	MAIO	JUN	JUL	AGO	SET	OUT	NOV
Elaboração do Projeto de Pesquisa										
Pesquisa Bibliográfica										
Elaboração da Introdução e Referencial Teórico			26							
Elaboração da Metodologia					14					
Coleta de Dados										
Tratamento de Dados										
Elaboração da Análise e Discussão dos Resultados e Considerações Finais										
Revisão da Monografia										
Preparação de Documentação para Depósito										
Depósito								9		
Retificação das Observações da Banca Examinadora									4	
Preparação da Apresentação										
Apresentação dos Resultados										12

5. ANÁLISE E DISCUSSÃO DOS RESULTADOS

5.1 A GOVERNANÇA CIBERNÉTICA NO REINO UNIDO

No presente capítulo, analisaremos aspectos da governança cibernética do Reino Unido. Ela está organizada em diversos documentos, como estratégias e regulamentações, sendo que, como veremos, o setor público ocupa uma posição central nesse sistema. Isso leva a uma presença majoritária de publicações do governo britânico.

5.1.1 A visão de Governança Cibernética no Reino Unido

Como vimos na Introdução deste trabalho, o conceito de governança pode ter diferentes definições, pois pode ser aplicado em diferentes ambientes e diferentes níveis de liderança. Ao analisarmos diferentes países, tais diferenças são acentuadas, uma vez que o fator cultural apresenta-se como fator relevante.

O Código de Práticas de Governança Cibernética (*Cyber Governance Code of Practice*), de 2024, do Departamento de Ciência, Inovação e Tecnologia (Department for Science, Innovation and Technology - DSIT) do governo britânico, nos traz uma definição de governança aplicada ao ambiente cibernético:

> Governança Cibernética foca em uma abordagem *top-down* para gerir e mitigar os riscos associados à segurança no uso de tecnologias digitais por uma organização. Uma melhor governança do risco de segurança cibernética é fundamental para melhorar a resiliência cibernética das organizações e proteger melhor a economia e a sociedade do Reino Unido. Nossas evidências sugerem que o foco na melhoria da governança da segurança cibernética dentro de uma organização geralmente leva a melhorias mais rápidas na resiliência cibernética geral (REINO UNIDO, 2024, tradução do autor).

Podemos verificar que a abordagem de governança pelo governo do Reino Unido é prover um modelo no qual as organizações possam basear-se para fazer frente aos riscos do ambiente cibernético e, assim, toda a sociedade participa das ações de segurança. Isso relaciona-se ao fato de a Estratégia Cibernética Nacional 2022 (*National Cyber Strategy* 2022) tratar de poder cibernético (*cyber power)*, enquanto as anteriores enfatizavam em seguranca cibernética. A Estratégia caracteriza o poder cibernético como “distinto das formas mais tradicionais de poder. Envolve combinar perfeitamente capacidades coercitivas e dispositivos de influência mais suaves. É mais

distribuído e os governos devem trabalhar com parceiros para obtê-lo e exercê-lo” (REINO UNIDO, 2021, tradução do autor).

Dentro de tal contexto, o governo do Reino Unido definiu como um de seus objetivos, dentro da Estratégia Cibernética Nacional 2022, “agir como exemplo de melhores práticas em segurança cibernética” para incrementar a resiliência cibernética do reino. Isto terá de fazer parte de um esforço holístico de toda a sociedade, para ser plenamente eficaz (REINO UNIDO, 2021, tradução do autor).

Ou seja, o governo do Reino Unido visualiza a governança cibernética como um conjunto de ações a ser realizada por agentes distribuídos por toda a sociedade: governo, setores público e privado, infraestruturas nacionais críticas e cidadãos. Todos esses atores devem ser capazes de se defenderem das ameaças cibernéticas, enquanto o governo atua apoiando os que são menos capazes de agirem (REINO UNIDO, 2021, tradução do autor).

5.1.2 A estrutura para segurança cibernética no Reino Unido.

A governança cibernética distribui responsabilidades entre agentes que se organizam em uma estrutura distribuída nos setores político, estratégico e operacional. Estende-se desde o Chefe de Governo e seu Gabinete até líderes de organizações privadas, passando por Departamentos de Governo (Ministérios) e autoridades e agências públicas.

Baseado em um *briefing* redigido por Adam Clark para os Membros do Parlamento da Casa dos Comuns (House of Commons), de 2024, podemos resumir a estrutura na seguinte tabela de atores e funções e responsabilidades:

TABELA 3. Resumo das funções e responsabilidades no setor cibernético

Nível	Ator	Funções / responsabilidades
Departamentos de Governo	Gabinete (*Cabinet Office)*	Tem a função de definir a política de cibersegurança. É responsável por publicar a Estratégia Cibernética Nacional.
	Department for Science, Innovation and Technology (DSIT)	Tem a função de implementar políticas de segurança cibernética doméstica. É responsável pela implementação dos regulamentos do *Network and Information Systems* (NIS) 2018 e outros.
	Ministério do Interior (*Home*	Responsável pelas políticas de crime cibernético

	Office)	
	Ministério da Defesa (*Ministry of Defense - MoD*)	Responsável por detectar, interromper e dissuadir ações de adversários no espaço cibernético. Tem a função de coordenar a Força Cibernética Nacional (*National Cyber Force*)
	Ministérios das Relações Exteriores, Commonwealth e Desenvolvimento (*Foreign, Commonwealth and Development Office* - FCDO)	Tem responsabilidade pelas políticas de atividades internacionais de segurança cibernética .Também supervisiona O Centro de Segurança Cibernética Nacional (*National Cyber Security Centre* – NCSC) e a Força Cibernética Nacional junto ao MoD.
	Quartel-General de Comunicações do Governo (*Government Communications Headquarter* - GCHQ)	É a agência de inteligência, segurança e cibersegurança do Reino Unido.
	National Cyber Security Centre (NCSC)	É integrante do GCHQ e responsável, como “single point of contact (SPOC)”, pelas ligações com parceiros nacionais e internacionais. Tem a função de autoridade técnica, fornecendo assessoria técnica para Autoridades Competentes (*Competent Authorities*) e outras organizações. Atua como CSIRT (*Computer Security Incident Response Team*) do Reino Unido
Agências	Autoridades Competentes (*Competent Authorities*)	São departamentos do governo ou agências reguladoras responsáveis por orientar/regular a segurança cibernética em setores específicos. Trabalham com a NCSC .
	Gabinete do Comissionário de Informação (*Information Commissioner’s Office)*	Responsável pelas regras de Proteção de Dados e regula os Provedores de Serviços Digitais que estão sob o regulamento NIS
	Força Cibernética Nacional (*National Cyber Force*	Conduz operações para “combater, interromper, degradar e contestar” ameaças cibernéticas de atores terroristas, criminosos e estatais. Opera

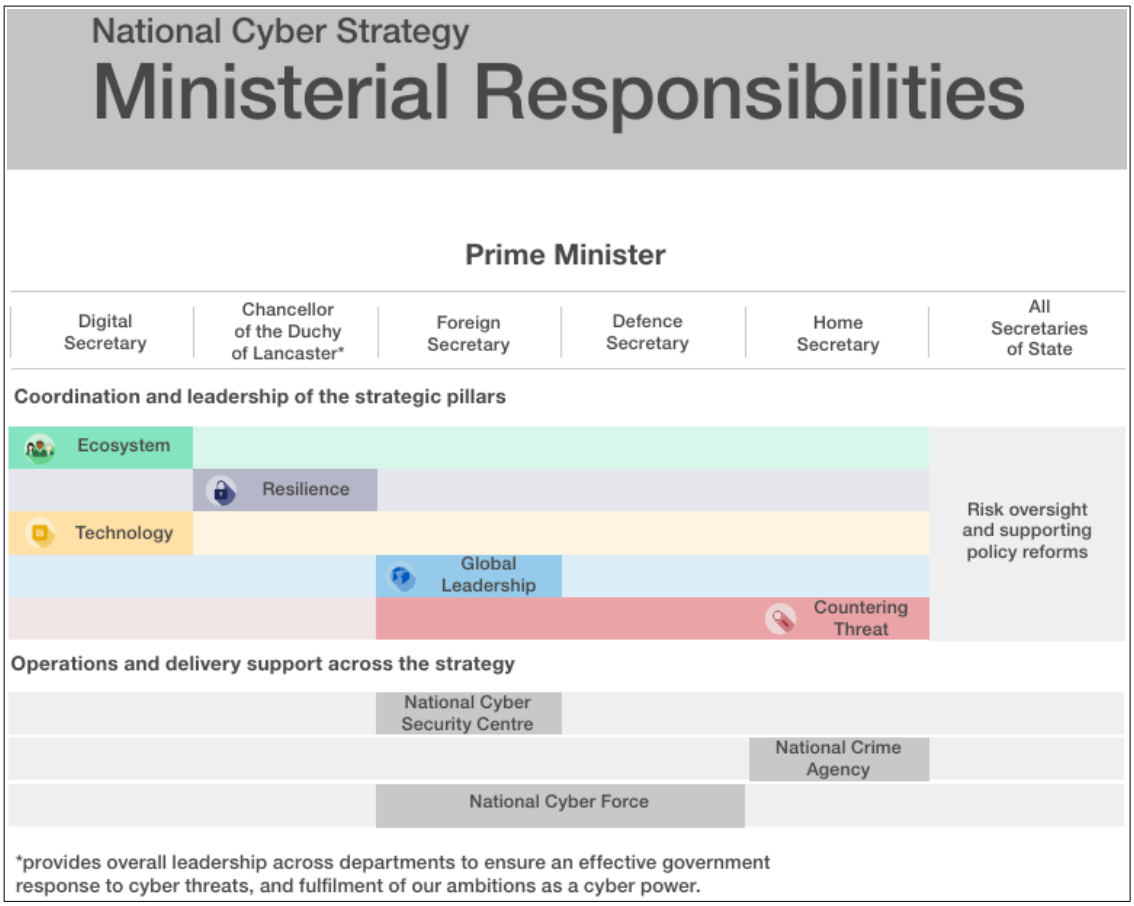
		sob uma parceria do MoD e do Quartel-General de Comunicações do Governo (*Government Communications Headquarter* - GCHQ)
	National Crime Agency	É uma autoridade legal responsável por combater o crime organizado. Possui uma unidade especializada em crimes cibernéticos, *National Cyber Crime Unit*.
	UK Cyber Security Council	É responsável por licenciar o exercício de profissão na área de segurança cibernética. É um órgão independente financiado pelo DSIT.
Outras Organizações	Infraestrutura Nacional Crítica	Têm responsabilidade de cibersegurança sob os regulamentos NIS. Podem ser operadores de serviços essenciais (serviços de saúde ou geração e fornecimento de água e energia elétrica, por exemplo) e provedores de serviços digitais essenciais (site de buscas, comércio eletrônico ou serviços de nuvem, por exemplo).
	Demais organizações e empresas	Atores não sujeitos aos regulamentos NIS, mas que possuem obrigações legais derivados de regras de proteção de dados e governança corporativa.

Fonte: elaborado pelo autor, baseado em Clark (2024, p. 25-27)

Como veremos à frente, a Estratégia Nacional Cibernética 2022, em vigor, traz responsabilidades para o Estado e para os cidadão em organizações privadas, considerando que a segurança cibernética deve ser holística e envolver toda a sociedade.

A seguir, veremos uma imagem que traz as responsabilidades dos Ministérios do Reino Unido dentro da NCS:

Figura 2: As responsabilidades ministeriais na NCS



Fonte: REINO UNIDO, 2021, p. 114.

5.1.3 A Estratégia Cibernética Nacional

A definição de uma estratégia nacional para o ambiente cibernético no Reino Unido teve início em 2010, quando a Estratégia de Segurança Nacional (*National Security Strategy*) identificou ataques cibernéticos realizados por atores estatais e crimes cibernéticos em grande escala como uma ameaça à segurança nacional na mais alta prioridade (“Nível 1”) (REINO UNIDO, 2011, p. 15).

Em 2011, o Gabinete publicou a primeira Estratégia de Segurança Cibernética (*Cyber Security Strategy*) do Reino Unido, com previsão de ações entre 2011 e 2016. Em 2016, foi assinada a segunda Estratégia de Segurança Cibernética, que esteve em vigor de 2016 a 2021. Em Dezembro de 2021, foi publicada a nova estratégia, a Estratégia Cibernética Nacional (*National Cyber Strategy* - NCS), modificando a abordagem.

Segundo Clark (2024, p. 28), com tradução do autor, “a estratégia de 2022 é mais abrangente que a anterior. A estratégia de 2016 colocava a

cibernética como uma questão de segurança, com ações voltadas para defesa de ataques cibernéticos.” A nova abordagem da NCS 2022 é mais abrangente e envolve toda a sociedade.

A NCS trouxe o conceito de “*cyber power”* (Poder Cibernético) e o definiu como “a habilidade de proteger e promover os interesses nacionais no espaço cibernético e através dele”. Esse conceito é mais amplo que e engloba segurança cibernética (REINO UNIDO, 2021, p. 11). Ainda, destaca a singularidade poder cibernético, com tradução do autor: “O poder cibernético distingue-se das formas tradicionais de poder. É mais distribuído e os governos devem trabalhar com parceiros em ordem para obter e exercê-lo”.

Em 2021, o governo britânico publicou o documento Revisão Integrada das Políticas de Segurança, Defesa, Desenvolvimento e Exterior 2021 (‘*Global Britain in a Competitive Age, the Integrated Review of Security, Defence, Development and Foreign Policy*’), que descreve a visão do governo para o papel do Reino Unido no mundo para a próxima década e as ações que o governo executará para 2025 (REINO UNIDO, 2021, p. 128, tradução do autor). Três conclusões desse documento influenciaram a NCS:

> Em primeiro lugar, que na era digital, o poder cibernético do Reino Unido será uma alavanca cada vez mais importante para atingir os nossos objetivos nacionais. Em segundo lugar, a sustentação do nosso poder cibernético requer uma estratégia mais abrangente e integrada, considerando toda a nossa gama de objetivos e capacidades cibernéticos. E terceiro, que esta deve ser uma abordagem de toda a sociedade – o que acontece na sala de reuniões ou na sala de aula é tão importante para o nosso poder cibernético nacional como as ações de especialistas técnicos e funcionários do governo, e trabalhar em parceria será essencial para o nosso sucesso (REINO UNIDO, 2021, p. 11, tradução do autor)

A Revisão Integrada 2021 definiu cinco ações prioritárias que foram utilizadas como pilares da estrutura da NCS. ou cinco objetivos estratégicos (REINO UNIDO, 2021, p. 13 e 33, tradução do autor):

a. Pilar 1: Fortalecer o ecossistema cibernético do Reino Unido, investindo no nas pessoas e competências, e aprofundando a parceria entre governo, academia e indústria.

b. Pilar 2: Construir um resiliente e próspero Reino Unido digital, reduzindo riscos cibernéticos para que os negócios possam maximizar os benefícios econômicos da tecnologia digital e os cidadãos estejam conectados de forma segura e confiantes na proteção de seus dados.

c. Pilar 3: Assumir a liderança nas tecnologias vitais para o poder cibernético, construindo capacidade industrial e desenvolvendo estruturas para proteger as tecnologias futuras.

d. Pilar 4: Promover a liderança e influência globais do Reino Unido para uma ordem internacional mais segura, próspera e aberta, trabalhando com parceiros governamentais e industriais e partilhando a experiência que sustenta o poder cibernético do Reino Unido.

e. Pilar 5: Detectar, impedir e dissuadir os adversários do Reino Unido para melhorar a segurança no espaço cibernético e através dele, utilizando de formar integrada, criativa e procedimental todo o espectro de dispositivos do Reino Unido.

Cada objetivo possui uma série de ações a serem realizadas para que sejam alcançados até 2025. Observando os pilares, podemos verificar que a estratégia é abrangente e envolve diversos atores da sociedade. Isto está alinhado ao Poder Cibernético, trazido anteriormente, que envolve todo o Reino Unido, Governo, setores público e privado e cidadãos.

Entretanto, a NCS considera que o governo e o setor público são essenciais para a resiliência cibernética do reino. Logo, uma estratégia específica foi desenhada para tal setor, a Estratégia de Segurança Cibernética do Governo 2022-203 (*Government Cyber Security Strategy 2022-2030* - GCSS), publicada em Janeiro de 2022 (REINO UNIDO, 2021, p. 120, tradução do autor). A visão definida para tal estratégia ajuda a compreendê-la:

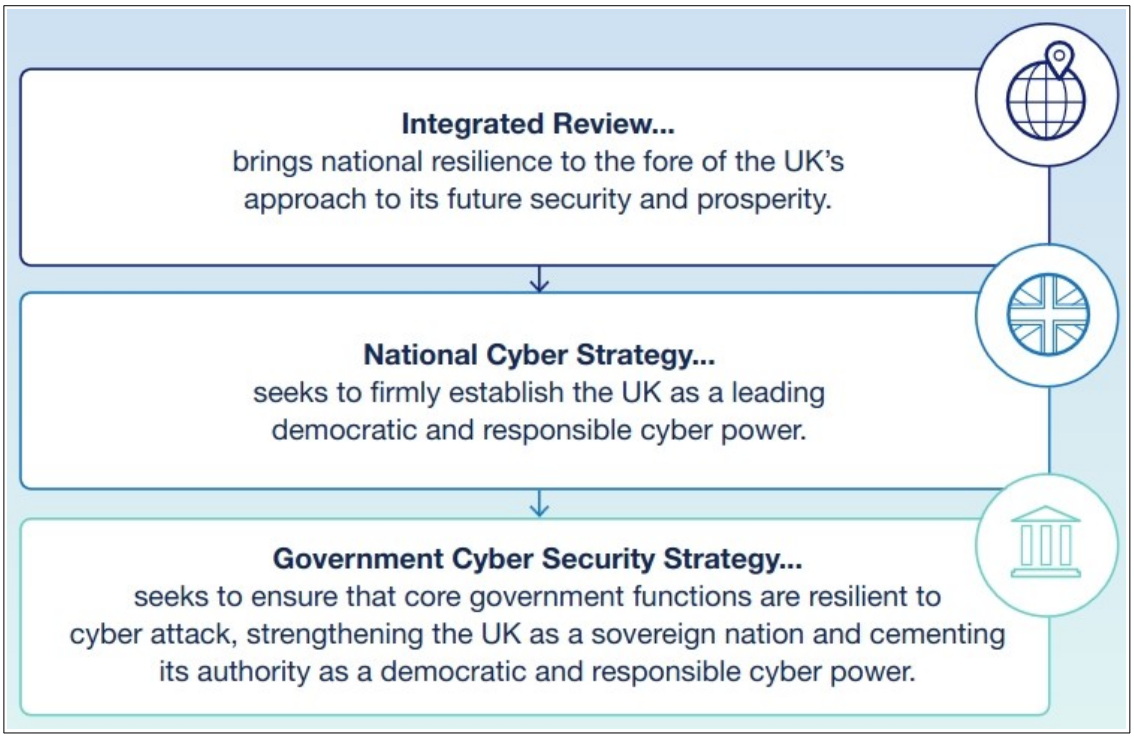
> A visão desta estratégia é, portanto, garantir que as funções centrais do governo - desde a prestação de serviços públicos até ao funcionamento do aparelho de Segurança Nacional - sejam resilientes a ataques cibernéticos, fortalecendo o Reino Unido como uma nação soberana e cimentando a sua autoridade como uma potência cibernética democrática e responsável (REINO UNIDO, 2021, p. 8).

Para viabilizar sua visão, a GCSS estabelece o seguinte objetivo:

> As funções críticas do governo significativamente reforçadas contra ataques cibernéticos até 2025, com todas as organizações governamentais em todo o sector público resilientes a vulnerabilidades conhecidas e métodos de ataque até 2030 (REINO UNIDO, 2021, p. 19).

Abaixo, podemos verificar um diagrama com a relação entre a Revisão Integrada 2021, a NCS e GCSS:

Figura 3: Relação entre Revisão Integrada, NCS e GCSS



Fonte: REINO UNIDO, 2022b, p. 13.

Dessa forma, podemos verificar que a governança cibernética está distribuída por toda a sociedade do Reino Unido, seguindo o conceito de Poder Cibernético. Apesar disso, o governo sabe que o setor público ocupa uma posição central nesse sistema, oferecendo serviços essenciais, definindo objetivos e provendo modelos que ajudam os demais atores a serem independentes na execução de própria segurança cibernética. Isso fortalece a resiliência cibernética, objetivo definido na estratégia nacional.

5.1.4 A cibernética na Defesa do Reino Unido

As atividades cibernéticas na Defesa, no meio militar, e o desenvolvimento de capacidades são liderado pelo Strategic Command (UKStratCom) (REINO UNIDO, 2022a, p. 61).

O UKStratCom é responsável pelas operações conjuntas (*joint capabilities)* e faz parte do Ministério da Defesa Britânico (*Ministry of Defence* – MOD) e uma de suas responsabilidades é a liderança no domínio cibernético para o MOD (REINO UNIDO, [s.d.]). Sobre a missão do UkStratCom, temos:

> Apoiamos o MOD ao garantir que capacidades conjuntas, como serviços médicos, treinamento e educação, inteligência e sistemas de informação, sejam desenvolvidas e gerenciadas em todos os 5 domínios: terrestre, marítimo, aéreo, espacial e cibernético. Também gerenciamos operações conjuntas no exterior (REINO UNIDO, [s.d.]).

Enquanto o UKStratCom lidera as atividades cibernéticas no âmbito da Defesa, “a atividade cibernética operacional é conduzida por comandos subordinados dentro do UKStratCom, parceiros em todo o governo e os Serviços Singulares [Forças Armadas]” (REINO UNIDO, 2022a, p. 61). A seguir, serão apresentados, resumidamente, tais atores e suas funções:

TABELA 4. Os atores operacionais do UKStratCom

Ator	Funções / responsabilidades
National Cyber Force	É uma joint venture entre Defesa e a comunidade de inteligência do Reino Unido, reúne pessoal uniformizado e civil. A missão da NCF é manter o país seguro e proteger e promover os interesses do Reino Unido em casa e no exterior. É responsável por operar dentro e através do ciberespaço para combater, interromper, degradar e contestar aqueles que prejudicariam o Reino Unido ou seus aliados (atividade comumente referida como operações cibernéticas ofensivas).
Defence Digital	É responsável pela segurança cibernética, resiliência e operações cibernéticas defensivas em toda a Defesa. A *Defence Digital* trabalha em estreita colaboração com parceiros da indústria de defesa para proteger os sistemas digitais da Defesa, tecnologia da informação corporativa e sistemas de comunicações militares. As operações cibernéticas defensivas são lideradas pelo Defence Digital Operations Headquarters e são conduzidas pela Cyber Security Operating Capability (CSOC), uma federação de equipes de defesa cibernética espalhadas pelos comandos da linha de frente e forças da Reserva. A Defesa Digital trabalha com o NCSC e o *Cabinet Office* para fornecer suporte em todo o governo e coopera rotineiramente com organizações cibernéticas aliadas.

MOD *Computer Emergency Response Team* (CERT)	Responsável por informar e alertar sobre vulnerabilidades e incidentes cibernéticos em redes fixas e de campanha. É uma organização subordinada ao *Cyber Security Operating Capability*.
Single Services (Forças Singulares)	A Marinha Real, o Exército Britânico e a Força Aérea Real operam centros de operações de segurança de informações cibernéticas que fornecem uma gama de capacidades defensivas para suas respectivas áreas de responsabilidade. Além disso, os *Single Services* também operam suas próprias equipes de proteção cibernética que têm a responsabilidade de proteger ativos de missão crítica.

Fonte: (REINO UNIDO, 2022a, p. 61 e 62)

Observamos que o setor de cibernética tem uma grande interação entre os militares e civis e entre o MOD e demais departamentos do governo britânico, sendo que muitas ações são conjuntas e alguns departamentos operam com uma combinação de diferentes departamentos, como a *National Cyber Force.*

5.2 A GOVERNANÇA CIBERNÉTICA NO CANADÁ

No presente capítulo, serão analisados os aspectos da governança do espaço cibernético no Canadá. Este país figura entre aqueles que possuem a maior proporção de internautas entre os habitantes. Segundo o estudo *Canadian Internet Use Survey* 2022 da *Statistics Canada* (2023)*:*

a. 94% dos canadenses tinham conexão à Internet em seus lares;

b. Dentre os que sabiam sua velocidade de conexão, 87% possúiam uma conexão com velocidade de download de, pelo menos, 50 Mbps;

c. 84% possuíam um plano de dados para seus aparelhos móveis.

Tais dados fazem que uma governança cibernética adequada seja essencial para o desenvolvimento da sociedade canadense. A seguir, analisaremos como ela está organizada.

5.2.1 A Segurança Cibernética do Canadá

Em 2010, o Governo do Canadá (GC) publicou sua primeira Estratégia de Cibersegurança, a *Canada's Cyber Security Strategy*: *For a stronger and more prosperous Canada* (CCSS 2010). A CCSS 2010 foi estruturada sobre três pilares:

a. proteger sistemas governamentais;

b. estabelecer parcerias para proteger sistemas cibernéticos vitais fora do governo federal; e

c. apoiar a segurança *online* dos canadenses

Após o estabelecimento da CCSS 2010, o GC publicou o plano para implementá-la, o *Action Plan 2010-2015 for Canada's Cyber Security Strategy* (Plano de Ação). Este documento descreve o plano do governo para implementar a CCSS 2010 e atingir nossa meta final de proteger o ciberespaço canadense para o benefício do povo e economia canadenses (CANADA, 2013, p. 1).

No Plano de Ação, uma das linhas de atuação foi o aperfeiçoamento da governança cibernética. Segundo o documento:

> muitos departamentos e agências realizaram um trabalho conjunto para desenvolver a Estratégia. Como o Governo trabalha com parceiros essenciais para implementar a Estratégia, precisa garantir que tais departamentos e agências trabalhem juntos eficaz e eficientemente para aprimorar a cibersegurança no Canada" (CANADA, 2013, p. 3 e 4).

A seguir, observaremos uma imagem extraída do Plano de Ação que apresenta as ações planejadas e executadas relativas ao aprimoramento da governança:

Figura 4: Ações para aprimoramento da governança cibernética

Action	Timeline	Deliverable	Status	Lead
Improve Governance				
Provide leadership and coordination across Government in order to focus cyber security programs and resources.	Start: 2010	Introduce Canada's *Cyber Security Strategy*.	Completed	Public Safety Canada
		Implement Canada's *Cyber Security Strategy*.	Ongoing	Public Safety Canada
Develop better governance within Government on cyber security.	Start: 2010	Establish interdepartmental governance mechanisms on Cyber Security.	Completed	Public Safety Canada
		Support these interdepartmental governance mechanisms.	Ongoing	Public Safety Canada
	Start: 2011	Establish a Government of Canada Security Governance Structure, consisting of a Lead Security Agency Steering Committee and a variety of working groups.	Completed	Treasury Board Secretariat
		Support the Government of Canada Security Governance Structure.	Ongoing	Treasury Board Secretariat
Improve collaboration within federal legal community on cyber security.	Start: 2011	Establish and operate a Justice Practice Group on Cyber Security.	Ongoing	Justice Canada
Provide the Government with timely and relevant metrics to measure the effectiveness of the efforts under *Canada's Cyber Security Strategy*.	Start: 2012	Develop a Horizontal Performance Measurement Strategy.	Completed	Public Safety Canada
		Evaluate *Canada's Cyber Security Strategy*.	On track to begin in 2015	Public Safety Canada

Fonte: Action Plan 2010-2015 (CANADA, 2013, p. 3 e 4)

Em 2017, o GC publicou uma revisão sobre o espaço cibernético (C*yber Review Consultations Report*), realizada a partir de consultas, conduzidas em 2016, a diversos segmentos da sociedade canadense, como setores público, privado, acadêmico e de infraestruturas críticas:

> "O ambiente de cibersegurança canadense está evoluindo. As rápidas mudanças na tecnologia digital têm abrangentes impactos de segurança, econômicos e sociais. Reconhecendo que a tecnologia digital possui um papel central na rotina dos canadenses, o Governo do Canadá quis ouvir as opiniões dos canadenses sobre essa questão" (CANADA, 2017, p. 1, com tradução do autor).

Dentro da consulta pública, algumas respostas, com recomendações de ações para o ciberespaço, foram direcionadas à área de governança. No seu Apêndice B – *Stakeholders Insight,* foram compiladas respostas que resumiam as ideias apresentadas, entre as quais encontramos a ideia de que era necessário incrementar a governança com a criação de uma agência central que funcionaria como um *hub* de inteligência (CANADA, 2017, p.33, com tradução do autor):

> "Dentro do cenário atual de segurança cibernética, há muitas agências do governo federal com objetivos semelhantes. Existe uma oportunidade de simplificar todos os setores críticos em uma única agência governamental."

> “A criação de um centro nacional de inovação em segurança cibernética permitiria que o governo, a indústria e a academia desenvolvessem em conjunto a educação, o talento, as políticas e os veículos de financiamento necessários.”

Tal revisão, influenciou a nova estratégia de segurança cibernética do Canadá a *National Cyber Security Strategy: Canada’s Vision for Security and Prosperity in the Digital Age*. (NCSS 2018), publicada em 2018. “Essa nova Estratégia de Cibersegurança reflete as perspectivas da revisão cibernética (*Cyber Review)”* (CANADA, 2018, p. 9, com tradução do autor).

Semelhante à primeira estratégia cibernética de 2010, que definiu três pilares de ação, a nova NCSS 2018 definiu três objetivos A seguir, tais fundamentos serão apresentados simultaneamente para fins de comparação:

TABELA 5: Comparação entre os pilares e objetivos das estratégias cibernéticas canadenses de 2010 e 1018.

Pilar	Pilares CCSS 2010	Objetivos da NCSS 2018
1	Proteção aos sistemas governamentais	Sistemas canadenses seguros e resilientes
2	Estabelecimento de parcerias para proteger sistemas cibernéticos vitais fora do governo federal	Um ecossistema cibernético inovador e adaptável
3	Apoio à segurança *online* dos canadenses	Liderança e colaboração eficazes

Fonte: elaborado pelo autor, baseado na CCSS 2010 e NCSS 2018

Da comparação acima, podemos observar que a NCSS 2018 mudou sua abordagem sobre a cibersegurança, migrando de uma centralização no governo para uma postura mais inclusiva dos demais atores da sociedade. Observemos o seguinte trecho extraído da NCSS 2018, no qual tal apreensão está presente:

> Uma segurança cibernética forte é elemento essencial da inovação e prosperidade canadenses. Indivíduos, governos e empresas querem confiar nos sistemas cibernéticos que sustentam suas vidas diárias. O Governo do Canadá prevê um futuro no qual todos os canadenses desempenham um papel ativo na formação e sustentação da resiliência cibernética de nossa nação (NCSS, 2018, p. 2 com tradução do autor).

Para implementar a NCSS 2018, em 2019, o GC estabeleceu o *National Cyber Security Action Plan* (NCSAP 2019 - Plano de Ação Nacional de Segurança Cibernética). Segundo tal documento:

> Este Plano de Ação apresenta o projeto para a implementação da Estratégia [NCSS 2018]. A segurança cibernética é uma responsabilidade compartilhada, e estamos comprometidos em

> trabalhar em estreita colaboração com outros níveis de governo, o setor privado, parceiros internacionais e cidadãos canadenses para nos adaptarmos ao cenário cibernético em mudança (CANADÁ, 2019, p.21, com tradução do autor).

O NCSAP 2019 está alinhado com a NCSS 2018 na medida em que suas ações estão orientadas para atingir os três objetivos desta. “Ele define as iniciativas e os marcos que dão suporte a cada um dos nossos três objetivos e apresenta um roteiro de como alcançaremos e manteremos nossa visão de segurança e prosperidade na era digital” (CANADÁ, 2019, p. 4, com tradução do autor).

Observemos, na tabela abaixo, duas iniciativas que levam ao objetivo de “liderança e colaboração eficazes”. As informações “Data Final” e “Status” estão conforme o documento e não foram atualizadas.

TABELA 6 – Iniciativas do NCSAP 2019

Goal 3 Liderança e colaboração eficazes			
Capacidade de Política Estratégica em Segurança Cibernética e Cibercrime			
Departamento	**Ação/Marco**	**Data final**	**Status**
Public Safety Canada (PS)	Recrutar equipe de política estratégica	2022	Em progresso
	Realizar revisão anual de progresso	2021-2024	Planejado
	Realizar revisão de governança	2021	Planejado
Canadian Centre for Cyber Security			
Departamento	**Ação/Marco**	**Data final**	**Status**
Communications Security Establishment (CSE)	Lançamento virtual do *Canadian Centre for Cyber Security*	2018	Completo
	Alcançar capacidade operacional básica	2022	Em progresso
	Alcançar capacidade operacional plena	2023	Em progresso

Fonte: elaborado pelo autor, baseado em Canada, 2019, p. 19

Em 2021, a NCSS 2018 passou por uma avaliação, a *Report on the Mid-term Review.* Seus objetivos eram avaliar o desempenho e a relevância contínua da Estratégia e revisar o progresso feito em direção aos resultados esperados e lições aprendidas (CANADA, 2021b). Sobre tal avaliação:

> Trabalhando junto com parceiros federais, o *Public Safety Canada* iniciou a Revisão em 2021 para avaliar o desempenho da Estratégia e identificar oportunidades de refinamento. Este relatório descreve as

> conquistas de desempenho, marcos alcançados e desafios e lições aprendidas na entrega da Estratégia. Ele pretende atuar como um primeiro passo em uma conversa nacional maior e contínua sobre segurança cibernética (National Cyber Security Strategy 2019-2024: Report on the Mid-term Review, 2021b).

.Ainda, associados à NCSS 2018, o GC publicou outros documentos, como o Federal Cyber Incident Response Plan (Plano Federal de Resposta a Incidentes Cibernéticos) e está associado a outras estratégias como a National Strategy for Critical Infrastructure (Estratégia Nacional para Infraestrutura Crítica).

A seguir, baseado nos documentos apresentados, analisaremos a organização, com as funções e responsabilidades, da governança do setor cibernético no Canadá.

5.2.2 Organização do Setor Cibernético

A publicação da CCSS 2010 marca o início da iniciativa do GC para estabelecer responsabilidades sobre a segurança do espaço cibernético, conforme está afirmado nesta: “Com um assunto tão crítico quanto a segurança cibernética, não há espaço para ambiguidade em relação a quem faz o quê. Esta Estratégia define a clareza necessária” (CANADA, 2010, p.9, com tradução do autor).

A seguir, serão apresentadas as responsabilidades e funções sobre a segurança cibernética definidas na CCSS 2010:

TABELA 7. Resumo das funções e responsabilidades no setor cibernético na Canadá

Departamento do Governo/ Instituição	Funções / Responsabilidades
Public Safety Canada	Responsável pela implementação da CCSS 2010. Coordenará a avaliação de ameaças complexas emergentes, desenvolverá e promoverá abordagens abrangentes e coordenadas para lidar com riscos dentro do Governo e em todo o Canadá.
Canadian Cyber Incident Response Centre	Subordinado ao *Public Safety Canada,* continuará sendo o ponto focal de monitoramento e aconselhamento sobre mitigação de ameaças cibernéticas, e direção da resposta nacional para

	qualquer incidente de segurança cibernética.
Communications Security Establishment Canada	Incrementar sua capacidade de detectar ameaças, fornecer serviços de inteligência estrangeira e segurança cibernética, além de responder a ameaças e ataques cibernéticos contra redes governamentais e sistemas de tecnologia da informação.
Canadian Security Intelligence Service	Analisará e investigará ameaças domésticas e internacionais à segurança do Canadá.
Royal Canadian Mounted Police	Investigará suspeitos, domésticos e internacionais, de atos criminosos contra redes de dados e infraestruturas críticas de informação canadenses.
Treasury Board Secretariat	Dar suporte e fortalecer as capacidades de gerenciamento de incidentes cibernéticos de todo o governo, por meio do desenvolvimento de políticas, padrões e ferramentas de avaliação. Também é responsável pela segurança da tecnologia da informação no GC
Foreign Affairs and International Trade Canada (Global Affairs Canada)	Aconselhará sobre a dimensão internacional da segurança cibernética e trabalhará para desenvolver uma política externa de segurança cibernética que ajudará a fortalecer a coerência no envolvimento do Governo no exterior quanto à segurança cibernética.
Department of National Defence and the Canadian Forces	Fortalecer suas capacidades de defender suas próprias redes de dados, trabalhar com outros departamentos do GC para identificar ameaças e possíveis respostas e continuar compartilhando com aliados informações sobre melhores práticas em cibernéticas. Também, trabalhar com aliados para desenvolver políticas e dispositivos legais sobre os aspectos militares de cibersegurança, complementando os esforços do *Foreign Affairs and International Trade Canada*

Fonte: elaborado pelo autor, baseado na CCSS 2010 (CANADA, 2010, p. 9-10)

As funções e responsabilidades enumeradas na Tabela 5 não foram alteradas pela nova estratégia. Entretanto, o novo *Centre for Cyber Security*

*(*Centro de Segurança Cibernética) foi criado em 2018 e seu financiamento foi introduzido na NCSS 2018 como nova medida:

> Financiamento para o novo Centro Canadense de Segurança Cibernética para apoiar a liderança e a colaboração entre diferentes níveis de governo e parceiros internacionais, ao mesmo tempo que fornece um recurso claro e confiável para cidadãos e empresas canadenses (CANADA, 2017, p. III, com tradução do autor).

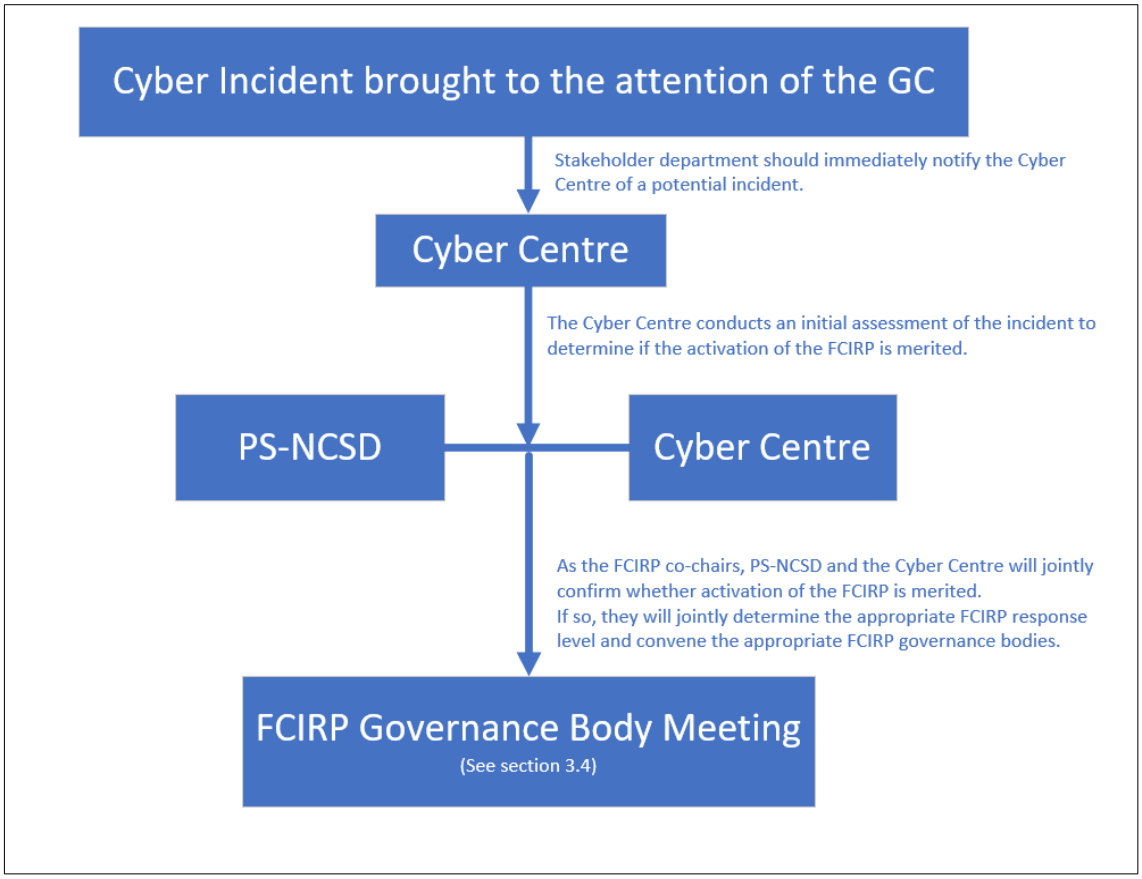
O Centro de Segurança Cibernética foi criado em 2018 sob a autoridade do *Communications Security Establishment Canada* (CSE). Foi uma resposta às consultas de 2016 do *Cyber Review,* com o papel de ser o único ponto de contato para orientações, serviços e suporte relacionados a segurança cibernética no Canadá (CSE, 2022). Além disso, lidera a resposta a incidentes cibernéticos do CG, atuando como CSIRT (Computer Security Incident Response Team) nacional, e CIRT (Computer Incident Response Team) do Governo (CANADIAN CENTRE FOR CYBER SECURITY, 2023). Resumindo, é o ponto focal no Canadá para segurança cibernética.

Essa função e organização podem ser observados no *Federal Cyber Incident Response Plan (*Plano de Respostas a Incidentes Cibernéticos Federal):

> Independentemente de como o GC toma conhecimento, os incidentes de segurança cibernética devem ser reportados ao Centro Cibernético do CSE o mais cedo possível, através dos canais de denúncia regulares (2023).

Na figura abaixo, é apresentado um fluxograma extraído do *Federal Cyber Incident Response Plan,* no qual podemos observar que todos os incidentes informados ao GC devem ser encaminhados ao *Canadian Centre for Cyber Security (Cyber Centre).* Embora as outras entidades não sejam alvo do presente trabalho, podemos observar o papel central do *Cyber Centre.*

Figura 5: Processo de notificação de incidente cibernético



Fonte: Federal Cyber Incident Response Plan, 2023

O NCSAP 2019 também define esse papel central do *Cyber Centre:*

> É uma equipe única e unificada de especialistas técnicos em segurança cibernética do governo que será a fonte definitiva de aconselhamento técnico exclusivo, orientação, serviços, mensagens e suporte em questões operacionais de segurança cibernética para o governo, proprietários e operadores de infraestruturas críticas, setor privado e público canadense. Os canadenses terão um lugar claro e confiável onde recorrer para todas as questões de operações de segurança cibernética.

5.2.3 A Defesa Cibernética no Canadá

A primeira estratégia de segurança cibernética do Canadá, a CCSS 2010, identificou que a cibernética estava modificando aspectos da estratégia militar:

> Alguns estados estrangeiros declararam publicamente que os ataques cibernéticos são um elemento central de sua estratégia militar. Alguns estados foram amplamente acusados de usar ataques cibernéticos para coincidir com – e ampliar os efeitos de – operações militares tradicionais. Esses programas de ataque cibernético são normalmente projetados para sabotar a infraestrutura e as comunicações de um adversário. Eles também podem apoiar ataques eletrônicos ao equipamento militar e às operações de um adversário (CANADA, 2010, p. 5, com tradução do autor).

Ainda, tal estratégia afirmou que as Forças Armadas Canadenses (*Canadian Armed Force* – CAF) não ficariam inertes a tais mudanças: “como os militares dos nossos aliados mais próximos, o *Department of National Defence* (DND - Departamento de Defesa Nacional) e as Forças Canadenses estão examinando como o Canadá pode responder melhor a futuros ataques cibernéticos” (CANADA, 2010, p. 5, com tradução do autor).

No que se refere às responsabilidades do DND e das CAF para o espaço cibernético definida pela CCSS 2010, não foi definida, de forma explícita, a possibilidade de execução ações ofensivas no espaço cibernético (ataque cibernético). Por outro lado, foi definida a obrigação de defender suas redes de dados:

> O Departamento de Defesa Nacional e as Forças Canadenses fortalecerão suas capacidades de defenderem suas próprias redes, trabalharão com outros departamentos do Governo para identificar ameaças e possíveis respostas e continuarão a trocar informações sobre as melhores práticas cibernéticas com os militares aliados. O Departamento de Defesa Nacional e as Forças Canadenses também trabalharão com os aliados para desenvolver a política e a estrutura legal para os aspectos militares da segurança cibernética (CANADA, 2010, p. 10, com tradução do autor).

Por sua vez, a Política de Defesa do Canadá de 2017, nomeada *Strong, Secure Engaged* (SSE – Forte, Seguro, Comprometido), afirmou a necessidade de desenvolvimento da capacidade ofensiva cibernética:

> Uma postura cibernética puramente defensiva não é mais suficiente. Consequentemente, desenvolveremos a capacidade de conduzir operações cibernéticas ativas focadas em ameaças externas ao Canadá no contexto de missões militares autorizadas pelo governo. O emprego dessa capacidade será aprovado pelo Governo missão a missão, consistente com o emprego de outros ativos militares, e estará sujeito ao mesmo rigor que outros usos de força militar. As operações cibernéticas estarão sujeitas a todas as leis nacionais e internacionais aplicáveis e a verificações e limites, como regras de engajamento, segmentação e avaliações de danos colaterais (CANADÁ, 2017, p. 72, com tradução do autor).

A SSE apresentou iniciativas visando preparar as CAF para as possibilidades de emprego, uma vez que “a qualquer momento, o Governo do Canadá pode convocar as Forças Armadas Canadenses para realizar missões de proteção do Canadá e dos canadenses, além de manutenção da paz e estabilidade internacionais” (CANADÁ, 2017, p. 106, com tradução do autor). Dentre essas, encontramos quatro voltadas para a capacidade cibernética:

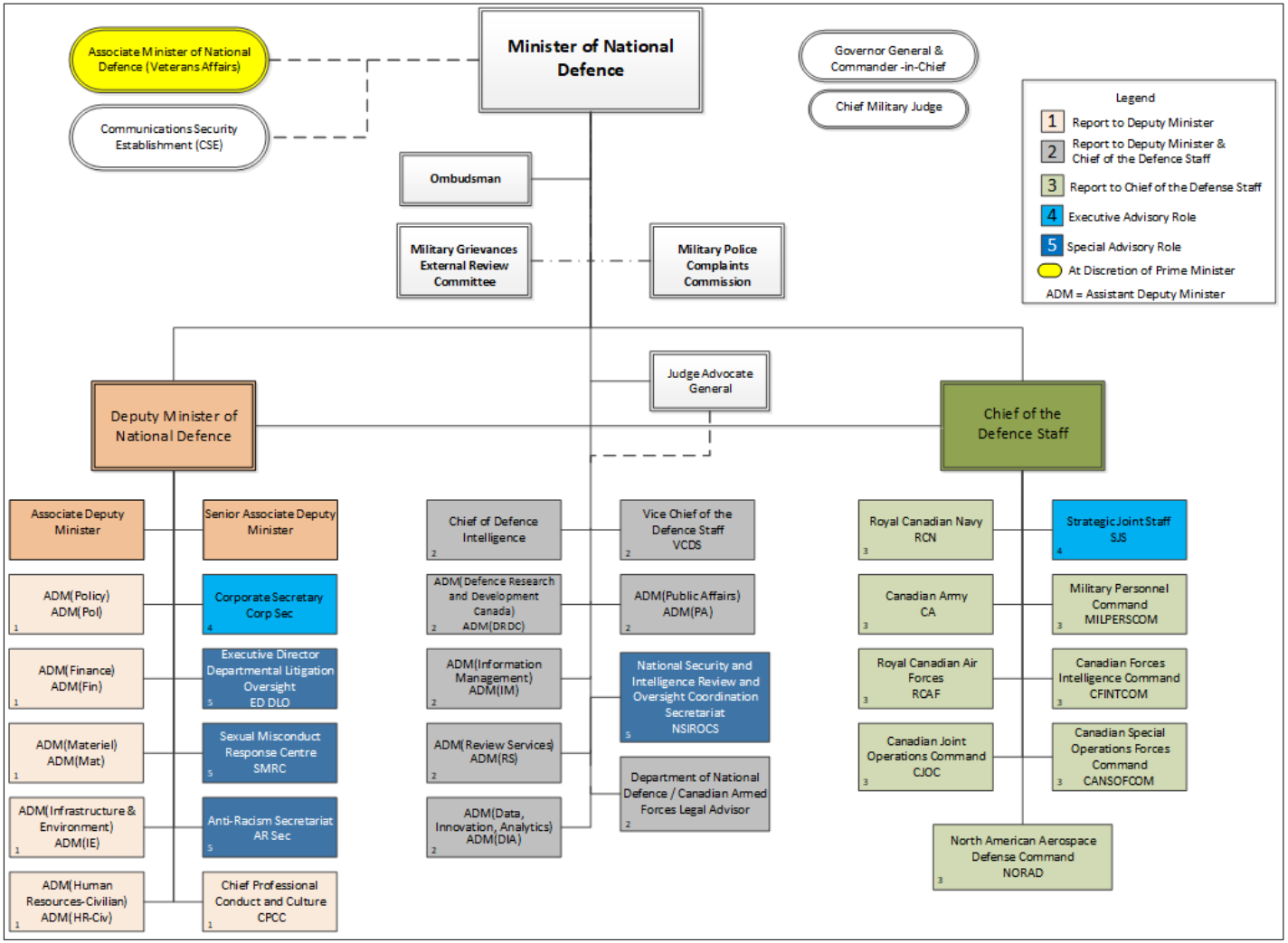
TABELA 8. Iniciativas da SSE para o setor cibernético.

Para melhor alavancar as capacidades cibernéticas em apoio às operações militares, a Defesa irá		
Nr	**Texto original**	**Tradução do autor**
87	Protect critical military networks and equipment from cyber attack by establishing a new Cyber Mission Assurance Program that will incorporate cyber security requirements into the procurement process.	Proteger redes e equipamentos militares críticos contra ataques cibernéticos estabelecendo um novo *Cyber Mission Assurance Program* que incorporará requisitos de segurança cibernética aos processos de aquisição.
88	Develop active cyber capabilities and employ them against potential adversaries in support of government-authorized military missions.	Desenvolver capacidades cibernéticas ativas e empregá-las contra potenciais adversários em apoio a missões militares autorizadas pelo governo.
89	Grow and enhance the cyber force by creating a new Canadian Armed Forces Cyber Operator occupation to attract Canada's best and brightest talent and significantly increasing the number of military personnel dedicated to cyber functions.	Aumentar e aprimorar a força cibernética criando uma nova função de Operador Cibernético das Forças Armadas Canadenses para atrair os melhores e mais brilhantes talentos do Canadá e aumentar significativamente o número de militares dedicados às funções cibernéticas.
90	Use Reservists with specialized skill-sets to fill elements of the Canadian Armed Forces cyber force.	Usar reservistas com habilidades especializadas para preencher cargos da força cibernética das Forças Armadas Canadenses.

Fonte: elaborado pelo autor, baseado em Canada, 2017, p. 111

Quando a estrutura de cibernética cresceu dentro do DND, foi inserida sob a autoridade do Assistant Deputy Minister (Information Management) (ADM(IM)). O ADM (IM) "fornece suporte direto às operações militares, incluindo a proteção e a gestão do ambiente cibernético da Defesa Nacional e das Forças Armadas Canadenses" (CANADÁ, 2018). A Figura 6 apresenta a organização do DND, onde podemos observar o ADM (IM).

FIGURA 6: Estrutura organizacional do DND



Fonte: CANADA, 2018.

A junção de todos os elementos que atuam no setor cibernético compõe as *Cyber Forces* (Força Cibernética), que “são aqueles militares e civis que geram, empregam e desenvolvem Operações Cibernéticas, Operações de Rede e *Cyber Mission Assurance*” (CANADÁ, 2021).

As *Cyber Forces* estão sob a autoridade do ADM (IM), por meio do *Director General Information Management Operations* (DGIMO) e *Director General Cyberspace* (DG Cyber) (CANADÁ, 2021). Como organizações militares se reportam ao *Chief of Staff (Information Management)*, DG Cyber também é o *Cyber Force Commander* (CFC) e o *DGIMO* também é o *Commander Cyberspace Division* (CCD) e o *Joint Forces Cyber Component Commander* (JFCCC) (SIEBRING, 2021).

Além de tal estrutura, o Canadá possui o *Canadian Forces Network Operations Centre* (CFNOC), que possui a missão de proteger as redes de dados do DND e CAF. Porém, este não tem a missão de conduzir operações no espaço cibernético (RUDOLPH, 2021).

A relevância do setor cibernético fez surgir a necessidade de uma estrutura distinta para coordenação das operações no setor cibernético. Tal iniciativa foi afirmada na nova política de defesa publicada em 2021, a O*ur North, Strong and Free: A Renewed Vision for Canada’s Defence (*ONSF - Nosso Norte, Forte e Livre: Uma Visão Renovada para a Defesa Do Canadá). Observemos o seguinte trecho de tal política:

> Para melhorar a capacidade das Forças Armadas Canadenses de conduzir operações cibernéticas, estabeleceremos o *Canadian Armed Forces Cyber Command* (Comando Cibernético das Forças Armadas Canadenses). Também criaremos uma capacidade conjunta de operações cibernéticas canadenses com o *Communications Security Establishment*, integrando os pontos fortes exclusivos de cada organização em uma equipe unificada que conduzirá operações cibernéticas ativas em apoio aos interesses canadenses. Isso permitirá que os militares gerem e empreguem forças cibernéticas e outras capacidades especializadas em curto prazo e contribuam para o avanço dos interesses canadenses e a proteção dos militares canadenses, aliados e parceiros domésticos e no exterior. As operações cibernéticas militares das Forças Armadas Canadenses são aprovadas pelo Governo missão a missão, em linha com o uso de todos os outros ativos militares.

A forma de operação conjunta entre um órgão de inteligência do governo (o CSE, no caso canadense) e os militares é um modelo utilizado em outros países membros da Organização do Tratado do Atlântico Norte (OTAN), da qual o Canadá é membro. É o modelo também adotado nos Estados Unidos da

América. Isso deve-se ao fato de as agências de inteligência, muitas vezes, já dominarem a capacidade de operar no espaço cibernético defensiva e ofensivamente. Segundo Rudolph, 2021:

> essa colaboração não é ruim, em teoria, mas é o modo comum de desenvolver estruturas de força cibernética entre os países da OTAN, devido ao seu conhecimento de nicho e conjunto de habilidades necessárias. O exemplo mais conhecido disso é o *United States Cyber Command*, que é uma colaboração entre a *National Security Agency*, a organização de inteligência de sinais dos Estados Unidos, e o Departamento de Defesa dos Estados Unidos.

Dessa forma, podemos analisar que o Canadá está aperfeiçoando suas capacidades de atuação no domínio cibernético. A crescente dependência de redes de dados e tecnologias conectadas levou ao crescimento da força cibernética que, agora, necessita de uma estrutura com governança própria, à semelhança de outros países.

5.3 A GOVERNANÇA CIBERNÉTICA NO JAPÃO

O Japão é um país que destaca-se por sua capacidade de gerar tecnologia e, consequentemente, de sua dependência dela. Isso explica o fato de o país ter tomado ações para garantir sua segurança do espaço cibernético já no ano 2000, com a publicação do documento "*Guidelines for the Formulation of Information Security Policie*s" e o estabelecimento do "*IT Security Office*". Como veremos, o país continua dando muita importância para o setor, face à rápida evolução das tecnologias de informação.

5.3.1 A estratégia de segurança cibernética japonesa

Nos parágrafos que se seguirão, serão apresentados aspectos básicos da política de Defesa do Japão, com foco nas questões que relacionam-se ao espaço cibernético. Em seguida, serão apresentadas as características da estratégia de segurança cibernética.

O princípio básico da organização da politica de Defesa do Japão é a Constituição da nação, já que seu artigo 9º prevê a renúncia à guerra e ao direito de beligerância do estado:

> Artigo 9. Aspirando, sinceramente, a uma paz internacional baseada na justiça e na ordem, o povo japonês renuncia, para sempre, à guerra como um direito soberano da nação e à ameaça ou uso da força como meio de resolver disputas internacionais.
>
> Para atingir o objetivo do parágrafo anterior, forças terrestres, marítimas e aéreas, bem como outros potenciais de guerra, nunca serão mantidas. O direito de beligerância do estado não será reconhecido. (JAPÃO, 1947, com tradução do autor)

A interpretação de tal dispositivo leva o governo japonês a manter apenas as forças de autodefesa e uma política de emprego de tais meios apenas para defesa:

> Portanto, o Japão, sob a Constituição, mantém as Forças de Autodefesa (SDF) como uma organização armada, mantendo sua política de emprego voltada exclusivamente para a defesa como sua estratégia básica de Defesa, e continua a mantê-las equipadas e prontas para operações. (Japão, 2023, p. 212, com tradução do autor)

Os principais documentos que normatizam a política de Defesa japonesa são o *National Security Strategy* (NSS), a *National Defense Strategy* (NDS) e o *Defense Buildup Program* (DBP). A seguir, serão apresentadas suas definições e objetivos:

TABELA 9: Principais documentos de Segurança e Defesa do Japão

Documento	Definição e objetivos
NSS	Documento supremo de política de segurança nacional. Fornece orientação estratégica para as áreas de política de segurança nacional do Japão, além de diplomacia e defesa, incluindo segurança econômica, tecnologia, cibernética, inteligência etc. Executado em um período de aproximadamente 10 anos.
NDS	Define objetivos de defesa e demonstra abordagens e meios pelos quais o Japão atinge esses objetivos. Reforça as capacidades fundamentais de defesa e a arquitetura de defesa de todo o país. Define a política de cooperação com seus aliados, países com ideais semelhantes e outros. Executado em um período de aproximadamente 10 anos.
DBP	Define o nível da capacidade de defesa que o Japão deve possuir e define um programa de desenvolvimento de médio a longo prazo para atingí-lo, que inclui o seguinte: - Organização das Forças de Autodefesa, em aproximadamente dez anos a partir da publicação. - Despesas totais para os próximos cinco anos e planejamento para grandes aquisições (programas de pesquisa e desenvolvimento e equipamentos de defesa)

Fonte: elaborado pelo autor baseado em Japão, 2023, p. 216

A atual conjuntura geopolítica influenciou a atualização desses documentos em 2022. A nova versão da NSS passou a abordar mais áreas além da Defesa e política externa japonesa:

> Diante do ambiente de segurança mais severo e complexo desde o fim da Segunda Guerra Mundial, uma nova *National Security Strategy* [Estratégia de Segurança Nacional] foi formulada em dezembro de 2022 para fornecer orientação estratégica para políticas em uma ampla gama de áreas, incluindo não apenas as áreas tradicionais de Diplomacia e Defesa, mas também segurança econômica, tecnológica e de inteligência (JAPÃO, 2023, p. 215 e 216, com tradução do autor).

Quanto à área da cibersegurança, a organização da estratégia teve início com a publicação do *Basic Act on Cybersecurity.* Em seu artigo 1º, lemos o objetivo dessa lei:

> O objetivo desta Lei é definir uma política básica para as iniciativas de segurança cibernética do Japão, esclarecer aspectos como as responsabilidades dos governos nacionais e locais, prever a formulação de uma estratégia de segurança cibernética, além de outros aspectos que se tornarão a base das iniciativas de segurança cibernética (JAPÃO, 2014).

Tal Ato criou duas instituições importantes para coordenação do setor cibernético japonês e sua segurança: o *Cybersecurity Strategic Headquarters* e o *National Center of Incident readiness and Strategy for Cybersecurity* (NISC).

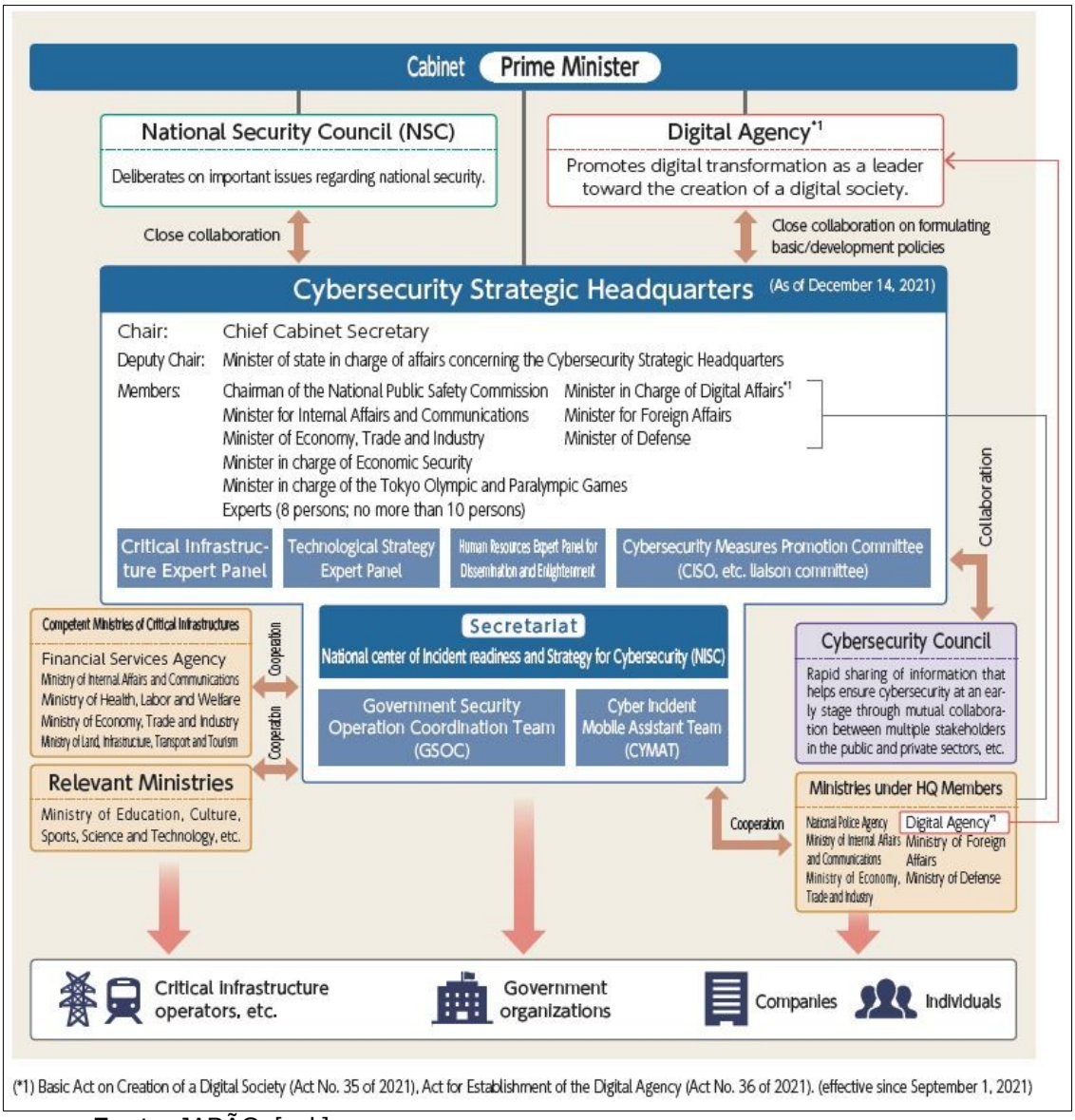
TABELA 10: Cybersecurity Strategic Headquarters e NISC

Cybersecurity Strategic Headquarters	O *Cybersecurity Strategic Headquarters* foi estabelecido sob o Gabinete em novembro de 2014 com o propósito de promover de forma eficaz e abrangente as políticas de segurança cibernética. É chefiado pelo Secretário-Chefe do Gabinete, com seu vice - o Ministro responsável pela Segurança Cibernética - e composta pelo Presidente da Comissão Nacional de Segurança Pública, os outros Ministros relevantes e especialistas experientes dos setores acadêmico e empresarial.
National Center of Incident readiness and Strategy for	O NISC foi estabelecido em 2015 e era anteriormente chamado de National Information Security Center desde 2005, sob a mesma abreviação “NISC”. É uma secretaria do *Cybersecurity Strategy Headquarters*, trabalhando

Cybersecurity	em conjunto com os setores público e privado em uma variedade de atividades para criar um ciberespaço livre, justo e seguros. O NISC desempenha seu papel de liderança como um ponto focal na coordenação da colaboração intragovernamental e na promoção de parcerias entre a indústria, a academia e os setores público e privado.

Fonte: JAPÃO, [s.d.]b, com tradução do autor

FIGURA 7. Estrutura criada pelo Basic Act on Cybersecurity



Fonte: JAPÃO, [s.d.]a

Outra norma criada pelo *Basic Act on Cybersecurity* foi o estabelecimento de uma estratégia para segurança cibernética, a *Cybersecurity*

Strategy (Estratégia de Segurança Cibernética). Sua primeira versão foi publicada em 2015 e cada edição tem a vigência de 03 (três) anos, sendo a segunda lançada em 2018 e a terceira em 2021, que está em vigor. Tal previsão está prevista no Artigo 12:

> O governo nacional deve estabelecer um plano básico de segurança cibernética (doravante denominado "cybersecurity strategy") com o objetivo de promover de forma abrangente e eficaz a política de segurança cibernética (JAPÃO, [s.d.]a, com tradução do autor).

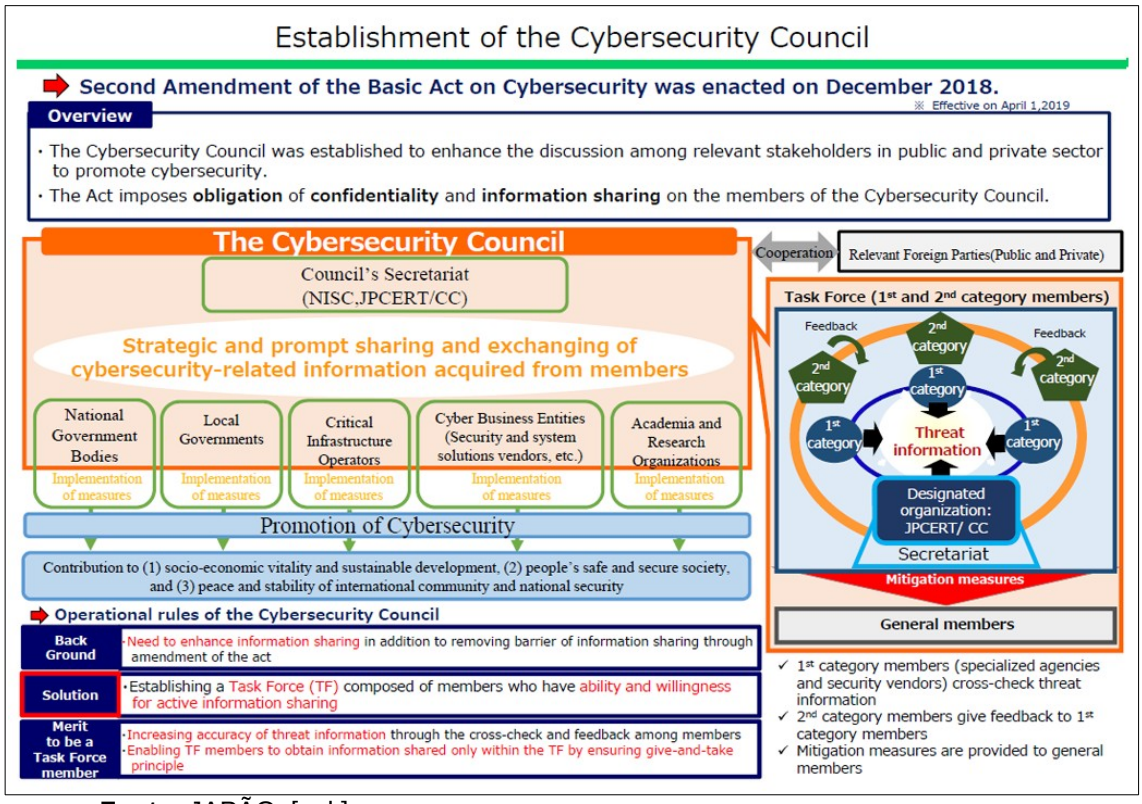
As medidas previstas pela Estratégia de Segurança Cibernética seguiram a mesma direção em suas três versões, para garantir um ciberespaço livre, justo e seguro (JAPÃO, 2022, p. 266, com tradução do autor):

1. promover a transformação digital e a segurança cibernética simultaneamente;
2. garantir a segurança geral do ciberespaço à medida que se torna público, interconectado e inter-relacionado; e
3. melhorar as iniciativas da perspectiva da segurança nacional.

Outra estrutura estabelecida pelo *Basic Act on Cybersecurity,* especificamente por uma emenda a este em 2018, *Cybersecurity Council* (Conselho de Cibersegurança):

> Para aprimorar o compartilhamento de informações entre as partes interessadas relevantes nos setores público e privado, com a emenda do *Basic Act on Cybersecurity*, o Conselho de Segurança Cibernética foi recentemente estabelecido em abril de 2019, composto por órgãos governamentais nacionais, operadores de infraestrutura crítica, fornecedores de segurança e outras organizações relacionadas (JAPÃO, [s.d.]a).

FIGURA 8. O Cybersecurity Council



Fonte: JAPÃO, [s.d.]a

5.3.2 A Defesa Cibernética japonesa

O primeiro ponto que deve ser considerado na análise das capacidades de Defesa Cibernética do Japão é o Artigo 9º da Constituição do Japão, apresentado no tópico anterior. A interpretação desse Artigo limita ações ofensivas no espaço cibernético, o que estimulou o desenvolvimento de capacidades defensivas. Segundo Soesanto, as atuais interpretações, pelo governo, do artigo citado "permite a aplicação da força para fins de autodefesa. Ou seja, operações cibernéticas ofensivas só são permitidas para "bloquear e eliminar" uma operação adversária em andamento que preencha os critérios legais de um ataque armado" (2021, p. 2, com tradução do autor).

A fim de facilitar o entendimento do presente subcapítulo, a seguir, serão apresentados os nomes e definições dos entes associados à Defesa no Japão que serão amplamente utilizados:

TABELA 11: Nomes e Siglas de órgãos associados à Defesa no Japão

Nome	Sigla	Tradução
Japan Ministry of Defense	JMOD/MOD	Ministério da Defesa
Japan Self-Defense Forces	JSDF/SDF	Força de Autodefesa do

		Japão
Japan Ground Self-Defense Force	JGSDF/GSDF	Força Terrestre de Autodefesa do Japão
Japan Maritime Self-Defense Force	JMSDF/MSDF	Força Marítima de Autodefesa do Japão
Japan Air Self-Defense Force	JASDF/ASDF	Força Aérea de Autodefesa do Japão

Fonte: elaborado pelo autor.

Outra importante definição é a relação entre o MOD e as SDF. Segundo o MOD:

> O MOD e o SDF formam uma única organização. Enquanto o termo “Ministério da Defesa” se refere aos aspectos administrativos da organização, que gerencia e opera o GSDF, MSDF e ASDF, o termo “SDF” se refere aos aspectos operacionais das organizações cuja missão é a defesa do Japão (JAPÃO, 2022, com tradução do autor).

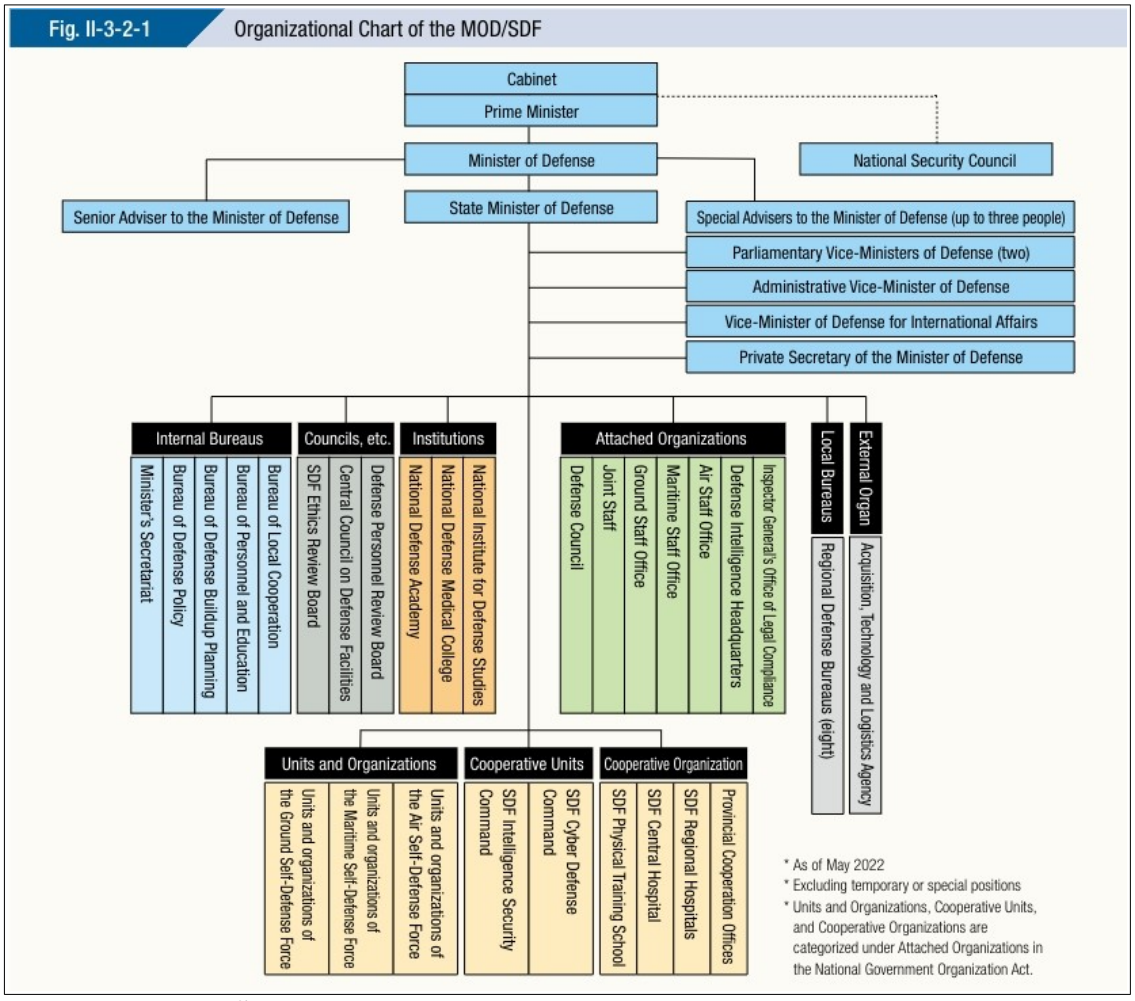
Podemos observar na Figura 9, abaixo, uma imagem que apresenta a estrutura organizacional do JMOD:

Analisando a estrutura organizacional acima, encontramos o SDF *Cyber Defense Command* subordinado diretamente ao MOD. O JSDF *Cyber Defense Command* é uma unidade conjunta (*Joint Unit*) que lida com ataques cibernéticos. Ele também fornece suporte para treinamento de unidades especializadas em cibernética das Forças de Autodefesa (GSDF, MSDF e ASDF), além de manter e operar a *Defense Information Infrastructure (DII)*, a infraestrutura de comunicações e rede de dados do MOD e SDF.

O JSDF Cyber Defense Command foi criado em 2022 a partir de uma reestruturação das unidades que atuavam na espaço cibernético: o *SDF C4 (Command, Control, Communication & Computers) Systems Command* e, subordinado a este, o *Cyber Defense Group*. Tal Comando Cibernético foi estabelecido a partir da expansão das funções do Cyber Defense Group e extinção do C4 Systems Command (JAPÃO, 2024, p. 9)

O *Cyber Defense Group* foi uma unidade conjunta especializada em cibernética, criada em 2014, subordinada ao SDF C4 *Systems Command*. Era responsável por monitorar redes de dados e pela resposta a ataques cibernéticos. (JAPÃO, [s.d.]b). Essas funções foram absorvidas pelo Cyber Defense Command.

FIGURA 9: Estrutura Organizacional do JMOD



Fonte: Japão, 2022, p. 209

Além do JSDF Cyber Defense Command (Joint Unit), as Forças de Autodefesa japonesa possuem unidades de proteção cibernética próprias: *Cyber Protection Unit* (GSDF), *Communication Security Group* (MSDF), and *Computer Security Evaluation Squadron* (ASDF) (JAPÃO, 2022, p. 266). Estas unidades são responsáveis por monitorar e proteger os sistemas de informação de suas Forças (JAPÃO, [s.d.]b).

À iniciativa japonesa de criação de um Comando de Defesa Cibernética, somam-se outras, como as seguintes medidas abrangentes:

TABELA 12: Os seis pilares de medidas defensivas abrangentes contra ataques cibernéticos

Pilar	Medidas
1) Garantir a segurança dos sistemas de informação	a) Introdução de firewall e software de detecção de vírus. b) Separação da rede em sistemas privados e

	públicos de Infraestrutura de Informação de Defesa (DII).
	c) Implementação de auditoria de sistema, etc.
2) Respostas de unidades especializadas a ataques cibernéticos	- Monitoramento 24 horas de redes e sistemas de informação, bem como medidas avançadas contra ataques cibernéticos (análise de malware) pelo JSDF Cyber Defense Command (Joint Unit), Cyber Protection Unit (GSDF), Communication Security Group (MSDF) e Computer Security Evaluation Squadron (ASDF)
3) Manutenção e desenvolvimento de uma postura de resposta a ataques cibernéticos	a) Implementação de exercícios de defesa cibernética b) Respostas aos riscos na cadeia de suprimentos c) Desenvolvimento de postura de resposta imediata à ocorrência de ataque cibernético
4) Pesquisa em tecnologia de ponta	- Pesquisa relacionada à utilização de Inteligência Artificial (IA).
5)Desenvolvimento de recursos humanos	a) Com o propósito de desenvolvimento de recursos humanos, implementando programas de estudo no exterior em organizações afiliadas à Carnegie Mellon University, programas de estudo em escolas de pós-graduação no Japão, bem como educação em cursos profissionais nas SDF.
	b) Com o propósito de promover a conscientização sobre segurança, oferecer educação nos locais de trabalho e educação profissional na National Defense Academy.
	c) Treinamento terceirizado.
	d) Educação cibernética para a geração mais jovem no “Curso especializado em sistemas/cibernéticos” na Escola Técnica Superior da JGSDF.
6) Coordenação com outras organizações e agências	a) Compartilhamento de informações com o *National Center of Incident Readiness and Strategy for Cybersecurity* (NISC), as Forças Armadas dos EUA e outras nações relevantes.
	b) Envio de pessoal do MOD ao NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE).
	c) Envio de oficiais de ligação para a instituição educacional cibernética do Exército dos EUA.
	d) Intercâmbio de pessoal público-privado.

Fonte: JAPÂO, 2022, p.266, com tradução do autor

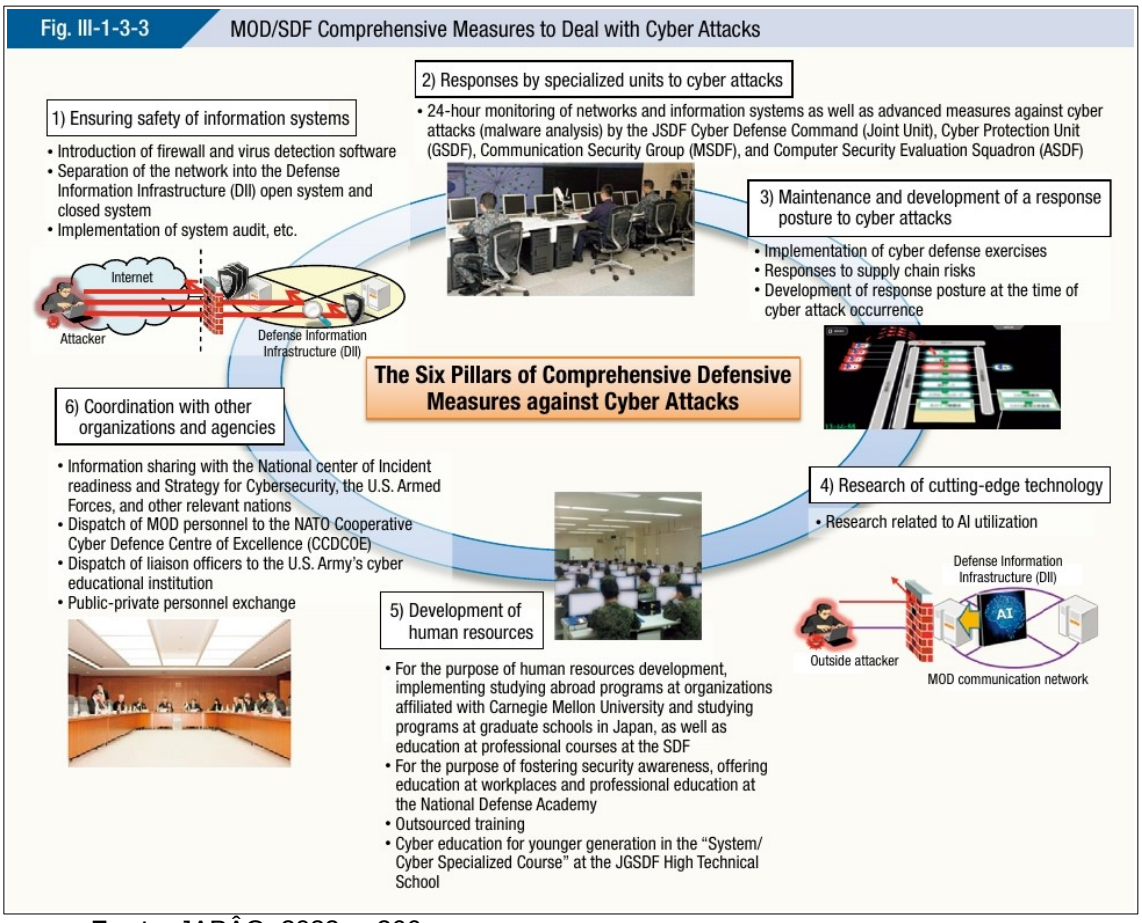
Cabe ressaltar que, como parte do pilar de coordenação com outras organizações e agências, o Japão tem estabelecido parcerias com outros países e suas agências centrais de Defesa Cibernética.

Em outubro de 2013, os governos japonês e americano criaram o *Cyber Defense Policy Working Group* (CDPWG) como uma estrutura para consultas políticas entre as autoridades de defesa dos dois países. As Diretrizes e a Declaração Conjunta do CDPWG foram publicadas em 2015 e envolveram o compartilhamento de informação, proteção de infraestruturas críticas para ambos os países, proteção de suas próprias redes de dados, intercâmbio e exercícios conjuntos (JAPÃO, 2023, p. 332, com tradução do autor).

O Japão estabeleceu acordos com o Organização do Tratado do Atlântico Norte (OTAN), e, desde 2019, envia pessoal para participar de atividades do Cooperative Cyber Defence Centre of Excellence (CCDCOE) da OTAN, além de participar do exercício de defesa cibernética "*Locked Shields* 2022" deste centro. (JAPÃO, 2023, p. 333, com tradução do autor).

Além disso, o Japão mantém conversas sobre o setor cibernético com Austrália, Reino Unido, Alemanha, França e Estônia. Em 2023, o GSDF realizou o Cyber KONGO 2023, uma competição multilateral de proteção cibernética com vários países, incluindo Estados Unidos, Austrália, Holanda, Alemanha, França, Romênia, Indonésia, Vietnã e outros (JAPÃO, 2023, p. 333, com tradução do autor).

Figura 10: Medidas abrangentes para lidar com ataques cibernéticos



Fonte: JAPÂO, 2022, p.266

Todas as medidas elucidadas demonstram como o Japão vem buscando preservar sua liberdade de ação no setor cibernético, investindo na organização e no preparo de suas capacidades de Defesa Cibernética, a fim de garantir um emprego eficaz se for necessário.

5.4 A GOVERNANÇA CIBERNÉTICA NO BRASIL

A utilização de redes de dados e a conexão à Internet tornaram-se essenciais no dia-a-dia do povo brasileiro. Segundo o Instituto Brasileiro de Geografia e Estatísticas (IBGE), em 2023, a Internet era utilizada em 92,5% dos domicílios do país, nas áreas urbanas, o percentual era de 94,1% e nas áreas rurais, de 81,0% (IBGE, 2024). Tais estatísticas demonstram que o espaço cibernético deve ser protegido a fim de garantir o pleno desenvolvimento da sociedade brasileira.

Nos tópicos a seguir, apresentaremos aspectos da governança desse espaço virtual em seus aspectos legais e organizacionais.

5.4.1 A Segurança Cibernética no Brasil

O entendimento dos termos Segurança e Defesa Cibernética é essencial para a compreensão dos ideias e conceitos que serão apresentados nos parágrafos abaixo. Segundo o Glossário das Forças Armadas:

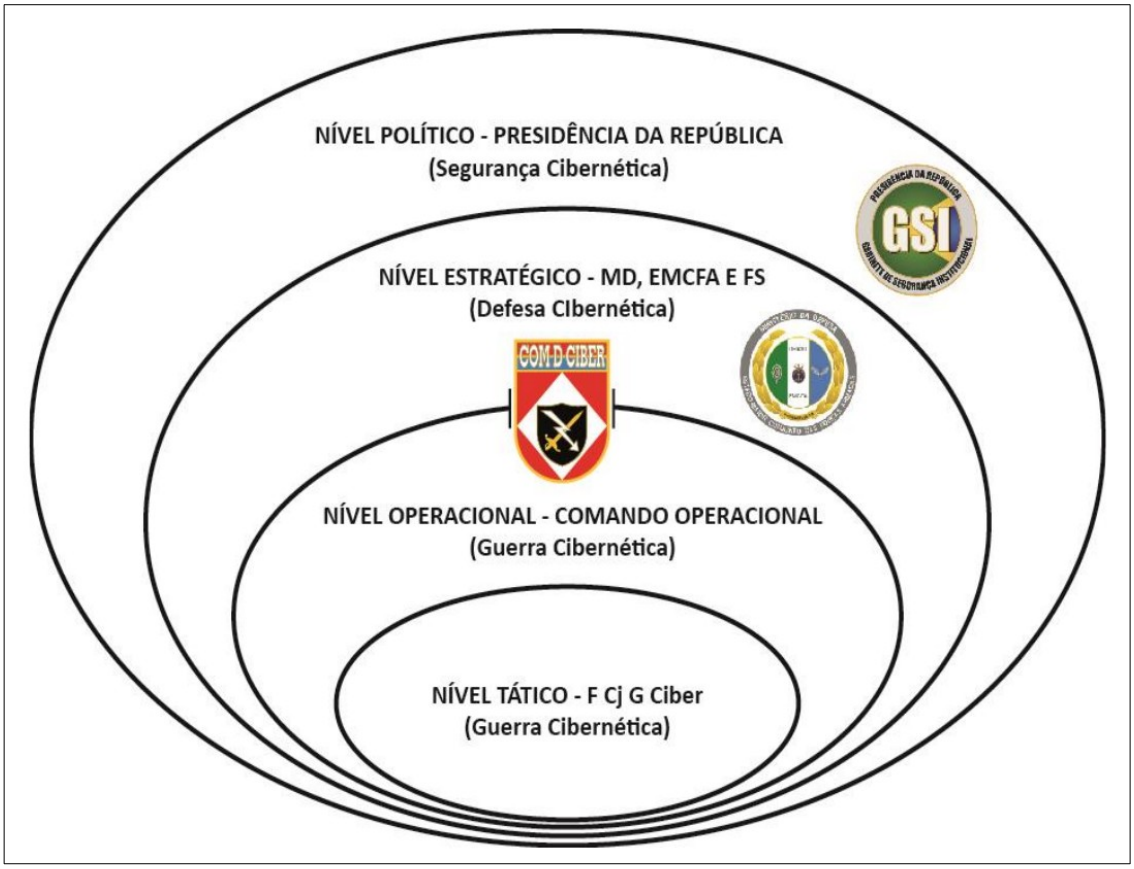
> SEGURANÇA CIBERNÉTICA - Arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas (2015).
>
> DEFESA CIBERNÉTICA - Conjunto de ações ofensivas, defensivas e exploratórias 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 produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (2015).

Das definições acima, podemos apreender que, no âmbito da Defesa, A Segurança Cibernética refere-se a garantia da liberdade de uso do ciberespaço por toda a nação. Já o termo Defesa Cibernética engloba as ações executadas no âmbito do Ministério da Defesa (MD).

A Doutrina Militar de Defesa Cibernética do MD - MD35-G-01 (2023) divide o espaço cibernético em níveis de decisão:

> a) Nível Político: Segurança Cibernética, coordenado pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), abrangendo a Administração Pública Federal (APF) e as Infraestruturas Críticas (IC);
>
> b) Nível Estratégico: Defesa Cibernética, a cargo do Ministério da Defesa (MD), do Estado-Maior Conjunto das Forças Armadas (EMCFA) e dos Comandos das Forças Armadas (FA), interagindo com o GSI/PR, APF, agências e IC de interesse para a Defesa Nacional; e
>
> c) Níveis Operacional e Tático: Guerra Cibernética, a cargo dos Comandos Operacionais ativados e das Forças Componentes (BRASIL, 2023a, p. 15)

FIGURA 11: Os níveis de decisão do setor cibernético



Fonte: BRASIL, 2023a, P. 15

No que se refere à regulamentação da da segurança cibernética, podemos considerar a Política Nacional de Segurança da Informação (PNSI) como seu marco inicial. Foi instituída pelo Decreto Nº 9.637, de 26 de Dezembro de 2018 do Presidente da República. Segundo seu Artigo 1º abrange a "administração pública federal, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional" (BRASIL, 2018).

o Artigo 6º da PNSI previu que "a Estratégia Nacional de Segurança da Informação conterá as ações estratégicas e os objetivos relacionados à segurança da informação" (BRASIL, 2018) e que tal estratégia seria divida em módulos, dentre os quais um específico para a cibernética. O Gabinete de Segurança Institucional (GSI) da Presidência da República, elaborou a Estratégia Nacional de Segurança Cibernética (E-Ciber) em 2019, com vigência 2020-2023:

> Em cumprimento ao estabelecido na Política Nacional de Segurança da Informação, e considerada a Segurança Cibernética - Seg Ciber como a área mais crítica e atual a ser abordada, o Gabinete de

> Segurança Institucional da Presidência da República elegeu, em janeiro de 2019, a Estratégia Nacional de Segurança Cibernética - E-Ciber como primeiro módulo da Estratégia Nacional de Segurança da Informação, a seu cargo, a ser elaborada (BRASIL, 2020b)

A E-Ciber definiu os seguintes objetivos estratégicos para que o “setor público, o setor produtivo e a sociedade possam usufruir de um espaço cibernético resiliente, confiável, inclusivo e seguro” (BRASIL, 2020b):

1. tornar o Brasil mais próspero e confiável no ambiente digital;

2. aumentar a resiliência brasileira às ameaças cibernéticas; enética no cenário internacional.

3. fortalecer a atuação brasileira em segurança ciber

Em 2023, a Presidência da República publicou o Decreto nº 11.856, de 26 de dezembro de 2023, por meio do qual institui a Política Nacional de Cibersegurança (PNCiber) e o Comitê Nacional de Cibersegurança (CNCiber). A PNCiber tem a finalidade de orientar a atividade de segurança cibernética no País, enquanto p CNCiber tem finalidade de acompanhar a implementação e a evolução da desta.

A PNCiber passou a definir a Estratégia Nacional de Cibersegurança, retirando esse instrumento da PNSI. O Artigo 4º da PNCiber prevê que sãos seus instrumentos: a Estratégia Nacional de Cibersegurança e o o Plano Nacional de Cibersegurança.

O Artigo 6º do da PNCiber define as missões do CNCiber.

> Art. 6º Ao CNCiber compete:
>
> I - propor atualizações para a PNCiber, a Estratégia Nacional de Cibersegurança e o Plano Nacional de Cibersegurança;
>
> II - avaliar e propor medidas para incremento da segurança cibernética no País;
>
> III - formular propostas para o aperfeiçoamento da prevenção, da detecção, da análise e da resposta a incidentes cibernéticos;
>
> IV - propor medidas para o desenvolvimento da educação em segurança cibernética;
>
> V - promover a interlocução com os entes federativos e a sociedade em matéria de segurança cibernética;
>
> VI - propor estratégias de colaboração para o desenvolvimento da cooperação técnica internacional em segurança cibernética; e
>
> VII - manifestar-se, por solicitação do Presidente da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, sobre assuntos relacionados à segurança cibernética (2023).

Além disso, o Artigo 7º da PNCiber, definiu os integrantes do CNCiber. A diversidade de instituições está relacionada à abrangência do espaço cibernético:

> Art. 7º O CNCiber será composto por representantes dos seguintes órgãos e entidades:
> I - um do Gabinete de Segurança Institucional da Presidência da República, que o presidirá;
> II - um da Casa Civil da Presidência da República;
> III - um da Controladoria-Geral da União;
> IV - um do Ministério da Ciência, Tecnologia e Inovação;
> V - um do Ministério das Comunicações;
> VI - um do Ministério da Defesa;
> VII - um do Ministério do Desenvolvimento, Indústria, Comércio e Serviços;
> VIII - um do Ministério da Educação;
> IX - um do Ministério da Fazenda;
> X - um do Ministério da Gestão e da Inovação em Serviços Públicos;
> XI - um do Ministério da Justiça e Segurança Pública;
> XII - um do Ministério de Minas e Energia;
> XIII - um do Ministério das Relações Exteriores;
> XIV - um do Banco Central do Brasil;
> XV - um da Agência Nacional de Telecomunicações - Anatel;
> XVI - um do Comitê Gestor da Internet no Brasil;
> XVII - três de entidades da sociedade civil com atuação relacionada à segurança cibernética ou à garantia de direitos fundamentais no ambiente digital;
> XVIII - três de instituições científicas, tecnológicas e de inovação relacionadas à área de segurança cibernética; e
> XIX - três de entidades representativas do setor empresarial relacionado à área de segurança cibernética (2023).

Pudemos observar que a legislação que busca regular a segurança do espaço cibernético brasileiro é recente, sendo a PNCiber de 2023. No *Global Cybersecurity Index* 2017, o Brasil ocupou a 70ª posição no ranking mundial (ITU, 2017). Em 2020, no entanto, passou a ocupar a 18ª posição (ITU, 2020). Isso é um sinal que o país está evoluindo nas questões de segurança cibernética.

5.4.2 A Defesa Cibernética no Brasil

Como vimos acima, a governança do setor cibernético foi organizado em níveis de decisão. Ainda, conforme apresentado na Figura 9, a Defesa Cibernética é coordenada pelo Ministério da Defesa e está no nível estratégico. “Embora medidas de segurança sejam implementadas em todos os níveis, a defesa implica que, além da proteção, a exploração e o ataque são executados neste nível, em cumprimento às demandas das autoridades competentes” (BRASIL, 2023a, p.28).

Segundo a Doutrina Militar de Defesa Cibernética, Defesa Cibernética compreende:

> ações 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 ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente (BRASIL, 2023a, p. 17).

A Defesa Cibernética faz parte da Defesa Nacional e, logo, faz parte da missão das Forças Armadas. No âmbito, as atividades de Defesa Cibernética são orientadas para atender às necessidades da Defesa Nacional. Entretanto, a liberdade de uso do espaço cibernético é essencial para a dinâmica de toda a sociedade brasileira e da comunidade internacional, sendo, por isso, envolvimento dos os setores público, privado, acadêmico, e base industrial de defesa, além do setor da Defesa (BRASIL, 2023a).

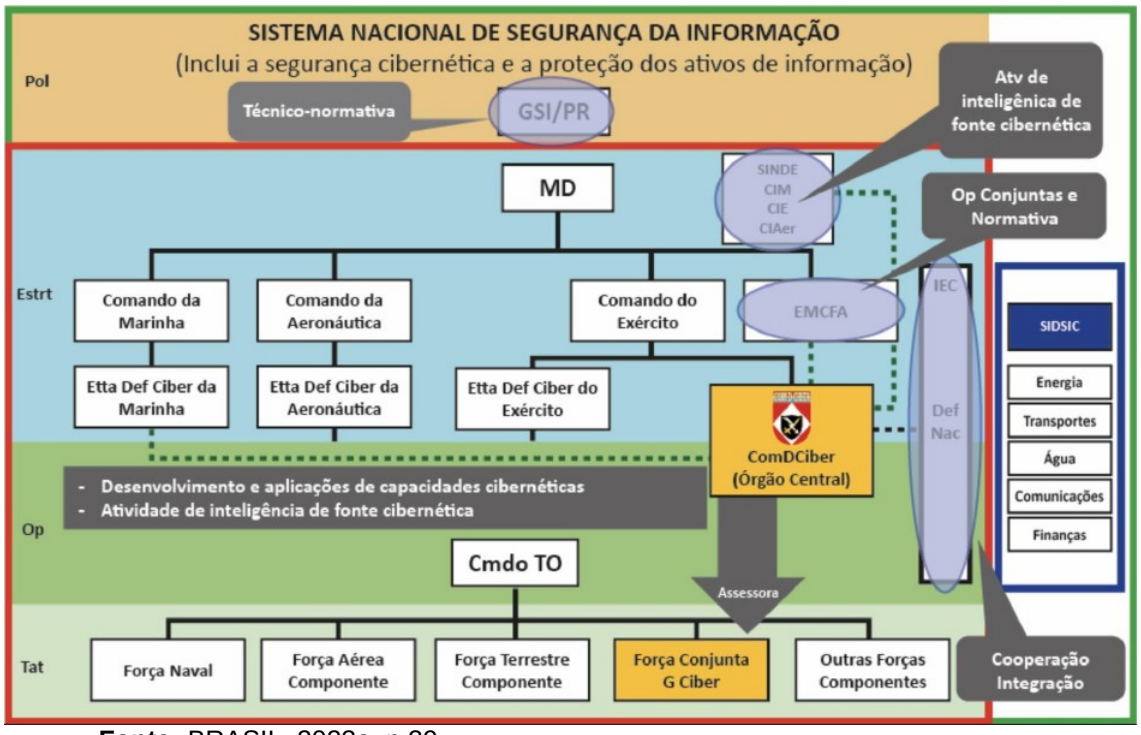
A fim de sistematizar as ações da Defesa no espaço cibernético, o MD estabeleceu o Sistema Militar de Defesa Cibernética (SMDC), por meio da Portaria nº 3.781/GM-MD, de 17 de novembro de 2020. A definição do SMDC consta no seu Artigo 2º:

> Art. 2º O SMDC é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar ações voltadas para assegurar o uso efetivo do espaço cibernético pela Defesa Nacional, bem como impedir ou dificultar ações hostis contra seus interesses.

Já o Artigo 4º de tal Portaria definiu os órgãos que constituem o SMDC, os quais são:

1. Comando de Defesa Cibernética (ComDCiber), como órgão central;
2. estruturas de Defesa Cibernética das Forças Singulares;
3. estruturas de Guerra Cibernética dos Comandos Operacionais ativados;
4. outras estruturas inseridas no Sistema, incluindo setores da administração central e organizações ligadas ao Ministério da Defesa.

FIGURA 12: Estrutura do SMDC



Fonte: BRASIL, 2023a, p.29

O ComDCiber é o órgão central do SMDC. É um Comando Operacional Conjunto, ou seja, com integrantes das três Forças Singulares, permanentemente ativado e está sob a estrutura regimental do Exército Brasileiro. Ainda O ComDCiber representa a Defesa na articulação com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, como equipe de coordenação setorial. (BRASIL, 2023a, p. 27 a 29)

Além disso,

> o ComDCiber é o órgão responsável por assessorar o Ministro de Estado da Defesa na implantação e na gestão do SMDC, com a finalidade de garantir, no âmbito da Defesa Nacional, a capacidade de atuação em rede, a interoperabilidade dos sistemas e a obtenção dos níveis de segurança necessários (BRASIL, 2023a, p. 28).

As operações cibernéticas, dentro do ComDCiber, são executadas pelo Centro de Defesa Cibernética (CDCiber). Segundo a Doutrina Militar de Defesa Cibernética, o CDCiber executa a função de Centro de Ações Cibernéticas (CAC) do ComDCiber e “tem como tarefas executar as operaçõees de Defesa e Guerra Cibernéticas, observando as técnicas, táticas e procedimentos específicos” (BRASIL, 2023a, p. 35).

As Estruturas de Defesa Cibernética da Marinha, Exército e Aeronáutica executam as atividades de Defesa Cibernética no âmbito das Forças, como parte do SMDC, e nas suas esferas de responsabilidade:

> Cabe também ao SMDC assegurar a proteção cibernética do Sistema Militar de Comando e Controle (SISMC²), possibilitando a capacidade de atuar em rede com segurança, bem como de maneira integrada e colaborativa na gestão de riscos que envolvam a proteção de infraestruturas críticas, conforme previsto no Plano Nacional de Segurança de Infraestruturas Críticas (BRASIL, 2023a, p. 27).

Na Política para o Sistema Militar de Comando e Controle, temos a definição do SISMC²,

> Sistema Militar de Comando e Controle (SISMC²) é o conjunto de instalações, equipamentos, sistemas de informação, comunicações, doutrinas, procedimentos e pessoal essenciais ao Comando e Controle, visando atender ao Preparo e ao Emprego das FA. Abrange os Sistemas Militares de C² das FA, bem como outros sob a responsabilidade do Ministério da Defesa (MD). Permite ao decisor planejar, dirigir e controlar as ações da sua organização. Esse conceito abrange os três componentes do C2 citados anteriormente (BRASIL, 2015, p.14).

A atividade de cibernética no âmbito das Forças Componentes é denominada Guerra Cibernética e está inserida no nível de decisão tático:

> Nível Tático – nível denominado de Guerra Cibernética e que fica a cargo das Forças Componentes. O nível tático é caracterizado pela ação da Força Conjunta de Guerra Cibernética (F Cj G Ciber) ou de um Destacamento Conjunto de Guerra Cibernética (Dst Cj G Ciber), além das estruturas de Guerra Cibernética das Forças Componentes. Neste nível ocorre a execução do planejamento tático, onde uma Força Conjunta de Guerra Cibernética atua no cumprimento ao que foi planejado no nível operacional (BRASIL, 2023a, p.28).

Dessa forma, no Brasil, as atividades de Defesa Cibernética ocorrem nos níveis estratégico, operacional e tático, sob coordenação do MD e das Forças Singulares. As atividades foram sistematizadas no SMDC, cujo órgão central é o ComDCiber.

6. CONSIDERAÇÕES FINAIS

Após analisarmos os aspectos da governança do setor cibernético do Reino Unido, Canadá, Japão e Brasil, podemos concluir que a organização básica de tal setor é similar nos quatro países.

O termo governança tem um uso difuso, conforme analisamos na Introdução. Nenhum dos países possuíam publicações específicas para tratar de governança cibernética. Foram analisados diversos documentos publicados pelos países que tratavam de áreas do setor cibernético.

Quanto ao arcabouço jurídico, todos os países possuem regulamentações emanadas do nível político, as estratégias nacionais de segurança cibernética. O Japão e o Brasil possuem, também, uma política, além da estratégia. O Japão publicou o *Basic Act on Cybersecurity* em 2014 e o Brasil a PNCiber em 2023.

Todos os países possuem agências que operam como referência para a segurança cibernética, as quais atuam como ponto de contato para toda a sociedade sobre questões de cibernética, incluindo tratamento de incidentes de rede.

Uma ideia presente nas estratégias de todos os países é a abordagem do setor cibernético como interesse de toda a sociedade. Por isso as políticas e estratégias estimulam o envolvimento dos governos, setores público, privado e academia na segurança cibernética, em uma atuação coordenada.

Quanto à Defesa Cibernética, todos os países consideram o espaço cibernético como um domínio e que seus interesses devem ser preservados. Nos quatro países, há separação entre a segurança cibernética nacional e a área da Defesa, embora a atuação seja coordenada e com apoio mútuo entre Ministérios da Defesa e agências do governo em todos eles.

Para melhor coordenação do espaço cibernético, Reino Unido, Japão e Brasil criaram estruturas centrais para coordenação das ações da Defesa no setor cibernético. O Canadá ainda não estabeleceu tal estrutura, mas já reportou a necessidade de estabelecimento de um comando específico para o setor cibernético em sua última política de defesa. No Canadá, como vimos, as *Cyber Forces* (união de todos os operadores do setor cibernético da Defesa) estão sob a estrutura administrativa do ADM (IM) atualmente.

As Forças de Defesa (ou Autodefesa, no caso do Japão) também possuem suas estruturas para operar no setor cibernético e para proteger suas próprias estruturas de Comando e Controle.

Quanto à organização do setor cibernético dentro da Defesa, Reino Unido, Japão e Brasil possuem uma estrutura de governança própria, com um Comando próprio. O Canadá, porém, já anuncio a criação de um Comando de Cibernética (C*anadian Armed Forces Cyber Command)* na última versão de sua política de defesa publicada em 2024.

Outro aspecto observado foi a proximidade entre a estrutura de Defesa Cibernética e as agências de inteligência dos governos. No Reino Unido, a *National Cyber Force* opera em uma parceria entre o MoD e GCHQ. No Canadá, o Comando Cibernético que será criado aturará conjuntamente com o *Communications Security Establishment*. Os documentos analisados sobre Japão e Brasil não deixaram explícito se utilizavam essa forma de operação conjunta.

Dessa forma, podemos concluir que, de maneira geral, os modelos de governança cibernética adotados no Reino Unido, Canadá e Japão são similares quanto à legislação e estrutura organizacional. Abaixo, será apresentada uma tabela comparativa que resume os dados levantados e analisados neste trabalho.

TABELA 13: resumo dos aspectos analisados

Fator analisado	REINO UNIDO	CANADÁ	JAPÃO	BRASIL
Legislação de nível político	*National Cyber Strategy*	National Cyber Security Strategy	*Basic Act on Cybersecurity* e *National Cyber Security Strategy*	Política Nacional de Cibersegurança (PNCiber) e Estratégia Nacional de Segurança Cibernética (E-Ciber)
Edições e versões das legislações	03 (três) versões: - 2011 - 2016 - 2021	02 (duas) versões: - 2010 - 2018	03 (três) versões: - 2015 - 2018 - 2021	01 (uma) versão: - E-Ciber, 2019 - PNCiber, 2023
Coordenação da segurança cibernética (nível nacional)	Department for Science, Innovation and Technology (DSIT)	Public Safety Canada	*Cybersecurity Strategic Headquarters*	Gabinete de Segurança Institucional / Presidência da República
Agência de referência para segurança cibernética	*National Cyber Security Centre* (NCSC)	*Centre for Cyber Security*	*National Center of Incident readiness and Strategy for Cybersecurity*	Secretaria de Segurança da Informação e Cibernética / GSI
Órgão Central de Defesa Cibernética	UKStratCom	Em criação (*Canadian Armed Forces Cyber*	SDF *Cyber Defense Command*	ComDCiber

		Command)		
Órgão operacional de Defesa Cibernética de referência	*National Cyber Force*	Ainda não estabelecido. Atividades são dispersas em agências atualmente.	Cyber Defense Group	CDCiber

Fonte: elaborado pelo autor, baseado na bibliografia de referência.

REFERÊNCIAS

ACHARYA, Amitav. The periphery as the core: the third world and security studies. In: KRAUSE, Keith; WILLIAMS, Michael (eds.). **Critical Security Studies**: concepts and cases, p. 299-328. London, UK: UCL Press, 1997

BRASIL. **Estratégia Nacional de Defesa**. Brasília: Presidência da República, 2020a.

BRASIL. **Estratégia Nacional de Segurança Cibernética.** Decreto nº 10.222, de 5 de fevereiro de 2020. Brasília: Presidência da República, 2020b.

BRASIL. **Guerra Cibernética**. Brasília: Exército Brasileiro, 2017.

BRASIL. **MD31-M-07: Doutrina Militar de Defesa Cibernética**. Brasília: Ministério da Defesa, 2023a.

BRASIL. **Política Nacional de Cibersegurança.** Decreto nº 11.856, de 26 de dezembro de 2023. Brasília: Presidência da República, 2023b.

BRASIL. **Política Nacional de Defesa.** Brasília: Presidência da República, 2020.

BRASIL. **Política para o Sistema Militar de Comando e Controle.** Brasília: Ministério da Defesa, 2015.

BRASIL. **Política Nacional de Segurança da Informação.** Decreto Nº 9.637, de 26 de Dezembro de 2018**.** Brasília: Presidência da República, 2018.

BRASIL. **Referencial básico de governança aplicável a órgãos e entidades da administração pública e ações indutoras de melhoria.** Brasília: Tribunal de Contas da União, 2014.

CANADÁ. **Action Plan 2010-2015 for Canada's Cyber Security Strategy.** Her Majesty the Queen in Right of Canada. 2013. Disponível em <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf>. Acesso em 07 Ago 24.

CANADÁ. **Evaluation of the Cyber Forces.** 2021. Disponível em <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/audit-evaluation/eval-cyber-forces.html>. Acesso em 23 Ago 24

CANADÁ. **National Cyber Security Action Plan (2019-2024).** Her Majesty the Queen in Right of Canada. 2019. Disponível em <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx>. Acesso em 21 Ago 24.

CANADÁ. **National Cyber Security Strategy: Canada's vision for security and prosperity in the digital age.** Her Majesty the Queen in Right of Canada. 2018. Disponível em <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf>. Acesso em 29 Fev 24.

CANADÁ. **National Cyber Security Strategy 2019-2024: Report on the Mid-term Review.** 2021b. Disponível em <https://www.publicsafety.gc.ca /cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019-md-trm/index-en.aspx>. Acesso em 21 Ago 24.

CANADÁ. **Organizational structure of the Department of National Defence and the Canadian Armed Forces.** 2018. Disponível em <https://www.canada.ca/en/department-national-defence/corporate/organizational-structure.html>. Acesso em 23 Ago 24.

CANADÁ. **Canada's Cyber Security Strategy: For a stronger and more prosperous Canada.** *Her Majesty the Queen in Right of Canada.* 2010. Disponível em: <https://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf>. Acesso em 07 Ago 24.

CANADÁ. **Cyber Review Consultations Report.** 2017. Disponível em <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnslttns-rprt/2017-cybr-rvw-cnslttns-rprt-en.pdf>. Acesso em 19 Ago 24.

CANADÁ. **National Defence**. Disponível em <https://www.canada.ca/en/department-national-defence.html> Acesso em 23 Ago 24.

CANADIAN CENTRE FOR CYBER SECURITY. **About the Cyber Centre.** 2023. Disponível em <https://www.cyber.gc.ca/en/about-cyber-centre>. Acesso em 19 Ago 24.

CLARK, Adam. **Cybersecurity in the UK, Research Briefing.** Londres: House of Commons Library, 2024. Disponível em <https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf>. Acesso em 17 Jul 24.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito**. Rio de Janeiro-RJ: Brasport, 2015.

CLARKE, Richard A. O *Worm* Nuclear. 2012. In: CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética:** a próxima ameaça à segurança e o que fazer a respeito, Apêndice. Rio de Janeiro-RJ: Brasport, 2015.

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA (CSE). **Our story.** 2022. Disponível em <https://www.cse-cst.gc.ca/en/culture-and-community/history/our-story>. Acesso em 19 Ago 24.

FREITAS, Ernani Cesar de; PRODANOV, Cleber Cristiano. **Metodologia do trabalho científico** [recurso eletrônico] : métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo-RS: Feevale, 2013.

GODOY, A. S. Introdução à pesquisa qualitativa e suas possibilidades. **RAE - Revista de Administracao de Empresas**, *[S. l.]*, v. 35, n. 2, p. 57–63, 1995. Disponível em: https://periodicos.fgv.br/rae/article/view/38183. Acesso em: 7 jun. 2024.

GODOY, A. S. Pesquisa qualitativa: tipos fundamentais. **RAE - Revista de Administracao de Empresas** , *[S. l.]*, v. 35, n. 3, p. 20–29, 1995. Disponível em: https://periodicos.fgv.br/rae/article/view/38200. Acesso em: 7 jun. 2024.

GUIMARÃES, Flávio de Queiroz. **Análise comparativa da estruturação do setor cibernético nacional em função das doutrinas cibernéticas internacionais** (Trabalho de Conclusão de Curso). Curso de Guerra Cibernética do Centro de Instrução de Guerra Eletrônica, Brasília-DF, 2017.

INSTITUTO BRASILEIRO DE GESTÃO CORPORATIVA (IBGC). **Código de Melhores Práticas de Gestão Corporativa**. 6.ed. São Paulo, SP : IBGC, 2023.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICAS (IBGE). **Internet foi acessada em 72,5 milhões de domicílios do país em 2023.** 2024. Disponível em <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41024-internet-foi-acessada-em-72-5-milhoes-de-domicilios-do-pais-em-2023>. Acessado em 20 Ago 2024.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **About International Telecommunication Union (ITU).** Disponível em: <https://www.itu.int/en/about/Pages/default.aspx>. Acesso em 23 Abr 24.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). Development Sector. **Global Cybersecurity Index 2020.** Geneva, Suíça: ITU Publications, 2020. Disponível em: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf>. Acesso em 24 Abr 24.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Global Cybersecurity Index.** Disponível em: <https://www.itu.int/pub/D-STR-GCI.01-2017>. Acesso em 24 Abr 24.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Statistics.** 2024. Disponível em <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>. Acesso em 25 Abr 24.

JAPÃO. **Defense of Japan White Paper 2022.** Ministério da Defesa, 2022. Disponível em <https://www.mod.go.jp/en/publ/w_paper/wp2022/DOJ2022_EN_Reference.pdf>. Acesso em 26 Ago 24.

JAPÃO. **Defense of Japan White Paper 2023.** Ministério da Defesa, 2023. Disponível em <https://www.mod.go.jp/en/publ/w_paper/wp_2023.html>. Acesso em 27 Ago 24.

JAPÃO. **Defense of Japan White Paper 2024 (digest).** Ministério da Defesa, 2024. Disponível em <https://www.mod.go.jp/j/press/wp/wp2024/pdf/DOJ2024_Digest_EN.pdf>. Acesso em 26 Ago 24

JAPÃO. Gabinete do Primeiro Ministro do Japão. **The Constitution of Japan.** 1947. Disponível em <https://japan.kantei.go.jp/constitution_and_government_of_ japan/constitution_e.html>. Acesso em 26 Ago 24.

JAPÃO. **National center of Incident Readiness and Strategy for Cybersecurity.** [s.d.]a. Disponível em <https://www.nisc.go.jp/eng/index.html>. Acesso e 28 Ago 24.

JAPÃO. O Governo do Japão. **Cybesecurity Strategy**. Disponível em <https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf>. Acesso em 29 Fev 2024

JAPÃO. Regarding response to a Cyber Attack. **Ministry of Defense.** [s.d.]b. Disponível em <https://www.mod.go.jp/en/publ/answers/cyber/index.html#a2>. Acesso em 27 Ago 24.

JAPÃO. **The Basic Act on Cybersecurity (Act Nº 104 of 2014).** 2014. Disponível em <https://www.japaneselawtranslation.go.jp/en/laws/view/3677 #je_ch1>. Acesso em 28 Ago 24.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 7. ed. São Paulo-SP: Atlas, 2016.

MORAES, R. Análise de conteúdo. **Revista Educação**. Porto Alegre-RS, v. 22, n. 37, p. 7-32, 1999.

Organização para Cooperação e Desenvolvimento Econômico (OCDE). **Modernising Government: The Way Forward.** Paris: OECD Publishing, 2005. https://doi.org/10.1787/9789264010505-en.

PROGRAMA DAS NAÇÕES UNIDAS PARA O DESENVOLVIMENTO (PNUD). **Responsible and Accountable Institutions.** Disponível em: https://www.undp.org/eurasia/our-focus/governance-and-peacebuilding/responsi ble -and-accountable-institutions. Acesso em 22 Abr 24.

REINO UNIDO. **Government Cyber Security Strategy: 2022 to 2030.** Cabinet Office. 2022. Disponível em <https://www.gov.uk/government/publications/ government-cyber-security-strategy-2022-to-2030>. Acesso em 29 Fev 24.

REINO UNIDO. **Cyber Primer.** Ministry of Defense. 2022. Disponível em <https://assets.publishing.service.gov.uk/media/63623df5d3bf7f04e12196d0/Cy ber_Primer_Edition_3.pdf>. Acesso em 02 Set 24.

REINO UNIDO. **National Cyber Strategy 2022b.** Cabinet Office. 2021. Disponível em <https://www.gov.uk/government/publications/national-cyber-strategy-2022>. Acesso em 29 Fev 24.

REINO UNIDO. **The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.** Cabinet Office. 2011. Disponível em <https://assets.publishing.service.gov.uk/media/5a78a991ed915d04220645e2/u k -cyber-security-strategy-final.pdf>. Acesso em 16 Jul 24.

REINO UNIDO. Department for Science, Innovation & Technology. **Cyber Governance Code of Practice: call for views.** 2024. Dispponível em <https://www.gov.uk/government/calls-for-evidence/cyber-governance-code-of-

practice-call-for-views/cyber-governance-code-of-practice-call-for-views>. Acesso em 15 Jul 24.

REINO UNIDO. **Strategic Commando Blog: About this blog.** Strategic Command. [s.d.]. Disponível em <https://stratcommand.blog.gov.uk/about/>. Acesso em 02 Set 24.

ROCHA, Henrique Ribeiro da. **Governança Securitária do Ciberespaço : questões sobre Segurança e Defesa** (Dissertação de Mestrado). Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, RJ, 2019.

RUDOLPH, Alexander. **Canada's Active Cyber Defence is Anything But Active.** Canadian Global Affairs Institute. 2021. Disponível em <https://www.cgai.ca/canadas_active_cyber_defence_is_anything_but_active>. Acesso em 23 Ago 24.

SIEBRING, James, Lt Col. **Operationalization of cyber defence: the next step** (Servive Paper)**.** Canadian Forces College, Toronto, Canadá, 2021.

SOESANTO, Stefan. **Comparing the Cyber Defense Postures of Japan, the Netherlands and the United States in Peace Time.** Konrad-Adenauer-Stiftung e. V, 2021, Berlin.

STATISTICS CANADA, The Daily. **Canadian Internet Use Survey, 2022.** 2023. Disponível em: <https://www150.statcan.gc.ca/n1/daily-quotidien/230720/dq230720b-eng.htm>. Acesso em 07 Ago 24.

TEIXEIRA, A. F.; GOMES, R. C. **Governança pública: uma revisão conceitual.** Revista do Serviço Público, *[S. l.]*, v. 70, n. 4, p. 519-550, 2019. DOI: 10.21874/rsp.v70i4.3089. Disponível em: https://revista.enap.gov.br/index.php/RSP/article/view/3089. Acesso em: 21 abr. 2024.

THE WORLD BANK. **Governance and Development.** Washington, D.C.: 1992. Disponível em: https://documents1.worldbank.org/curated/en/604951468739447676/pdf/multi-page.pdf. Acesso em 22 Abr 23.