ESCOLA DE GUERRA NAVAL

CMG MÁRCIO REBELLO DE OLIVEIRA

# AS INFRAESTRUTURAS CRÍTICAS NACIONAIS ANTE ÀS AMEAÇAS CIBERNÉTICAS: Análise Comparativa das Governanças Cibernéticas do Brasil e do Reino Unido, com foco nas Infraestruturas Críticas Marítimas

Rio de Janeiro

2022

CMG MÁRCIO REBELLO DE OLIVEIRA

# AS INFRAESTRUTURAS CRÍTICAS NACIONAIS ANTE ÀS AMEAÇAS CIBERNÉTICAS: Análise Comparativa das Governanças Cibernéticas do Brasil e do Reino Unido, com foco nas Infraestruturas Críticas Marítimas

Tese a ser apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Política e Estratégia Marítimas.

Orientador: CMG (FN-RM1) Alexandre Ricciardi dos Reis

Rio de Janeiro

Escola de Guerra Naval

2022

**AGRADECIMENTOS**

Ao meu orientador e instrutor, CMG (FN-RM1) Alexandre Ricciardi dos Reis, agradeço as orientações precisas e pertinentes que contribuíram para a conclusão deste trabalho.

Aos Oficiais do GSI/PR, e principalmente o Cel (EB) Marcelo Paiva Fontenele e o CMG Marcio Braga de Souza, agradeço as informações prestadas que ajudaram a entender as atribuições do GSI/PR na identificação e proteção das nossas IC/ICM.

Aos amigos e companheiros da Turma do Curso de Política e Estratégia Marítimas/2022, Turma do Bicentenário da Independência do Brasil, agradeço os momentos de convívio e descontração, além do compartilhamento de experiências, que ajudaram na elaboração desta tese.

Aos meus pais Ismael (*in memoriam*) e Rita, pelo exemplo de dedicação, educação e carinho, que forjaram quem eu sou hoje.

Ao meu filho José Rafael, pelo amor e compreensão da importância deste trabalho.

A minha amada esposa Érica, pelo apoio e incentivo diários na consecução deste projeto acadêmico.

Por fim, agradeço a Escola de Guerra Naval e todos os seus instrutores e professores pela transmissão de valorosos ensinamentos que em muito contribuíram no meu enriquecimento profissional.

*“Mesmo com as melhores práticas de segurança cibernética em vigor, é quase impossível parar um atacante altamente determinado, com tempo e recursos suficientes para violar um sistema. Sem dúvida, a violação é simplesmente uma questão de tempo.”*

*(CHUBB; FINN; NG, 2022, p.25. Tradução própria. Original em inglês.)*

**RESUMO**

A indústria 4.0 revolucionou a maneira como pessoas e empresas trocam informações e dados através da internet e em nuvem. A cada dia mais pessoas e sistemas estão se conectando e se interligando em redes e à internet, e esse aumento de conectividade acaba provocando vulnerabilidades que poderão ser utilizadas para um ataque cibernético. O ambiente cibernético não possui fronteiras físicas claramente definidas, e por isso, a atribuição da responsabilidade de uma ação é difícil de ser totalmente confirmada. As perdas globais devidas aos crimes cibernéticos crescem a cada dia e, para se precaverem, os governos e empresas também tem aumentado seus investimentos na área de segurança cibernética. As infraestruturas críticas e infraestruturas críticas marítimas são instalações, serviços, bens e sistemas vitais para a sociedade, e se forem destruídas ou tiverem seu desempenho degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional de um país. Apesar de a maioria dessas infraestruturas críticas serem operadas pelo setor privado, os governos têm procurado adotar uma governança cibernética, quer seja por meio da publicação de normas e leis, quer seja por inciativas que visem aumentar a segurança e a resiliência cibernética dessas infraestruturas. Esse trabalho analisou e comparou as governanças cibernéticas do Brasil e do Reino Unido, a fim de identificar possíveis deficiências na governança cibernética brasileira referente à proteção dessas infraestruturas. Para essa comparação, foram utilizados 08 critérios. Durante a comparação, foi constatado que o Brasil, desde 2009, adotou várias iniciativas no campo cibernético, e a partir de 2018 implementou ações que visam aumentar a segurança das infraestruturas críticas do país, mas ainda carece da concretização de diversas orientações que constam em normas e publicações, bem como da publicação de algumas normas que estão previstas. O Brasil não dispõe de uma governança cibernética específica que vise a proteção das infraestruturas críticas marítimas, e para sanar esta deficiência, necessita que seja elaborada uma Estratégia de Segurança Marítima ou documento similar que divulgue orientações e diretrizes cibernéticas para o setor marítimo. Já o Reino Unido, considera as ameaças cibernéticas como a mais alta prioridade para o país, e desta forma, tem realizado grandes investimentos em pesquisa e desenvolvimento, e em soluções que aumentam a segurança cibernética e a resiliência dos setores críticos, inclusive das infraestruturas críticas. Em relação às infraestruturas críticas marítimas, esse país realizou diversas ações, tais como a publicação de estratégias e normas, código de prática e guia de boas práticas que orientam o setor marítimo a se proteger das ameaças cibernéticas.

**Palavras-chave**: Ambiente Cibernético; Ameaças Cibernéticas; Infraestruturas Críticas; Infraestruturas Críticas Marítimas; Governança Cibernética.

***ABSTTRACT***

Industry 4.0 has revolutionized the way people and companies exchange information and data over the internet and in the cloud. Every day more people and systems are connecting and interconnecting in networks and the internet, and this increase in connectivity ends up causing vulnerabilities that could be used for a cyber-attack. The cyber environment does not have clearly defined physical boundaries, so the attribution of responsibility for an action that is difficult to be fully confirmed. Global losses due to cybercrime are growing every day and, to be on guard, governments and companies have also increased their investments in cybersecurity. Critical maritime infrastructures and critical maritime infrastructures are facilities, services, goods and systems that are vital to society, and if they are destroyed or have their performance degraded, they will have a serious social, economic, political, international or national security impact on a country. Although most of these critical infrastructures are operated by the private sector, governments have sought to adopt cyber governance, whether through the publication of regulations and laws, or through initiatives aimed at increasing the cyber security and resilience of these infrastructures. This work analyzed and compared the cyber governances of Brazil and the United Kingdom, in order to identify possible deficiencies in Brazilian cyber governance regarding the protection of these infrastructures. For this comparison, 08 criteria were used. During the comparison, it was found that Brazil, since 2009, has adopted several initiatives in the cybernetic field, and from 2018 onwards it has implemented actions aimed at increasing the security of the country's critical infrastructures, but it still lacks the implementation of several guidelines contained in standards. and publications, as well as the publication of some norms that are foreseen. Brazil does not have a specific cyber governance aimed at protecting critical maritime infrastructures, and to remedy this deficiency, a Maritime Security Strategy or similar document must be prepared that discloses cyber guidelines and guidelines for the maritime sector. The United Kingdom, on the other hand, considers cyber threats as the highest priority for the country, and thus has made large investments in research and development, and in solutions that increase cyber security and the resilience of critical sectors, including critical infrastructure. Regarding critical maritime infrastructure, this country has taken several actions, such as the publication of strategies and standards, code of practice and guide to good practices that guide the maritime sector to protect itself from cyber threats.

**Keywords**: Cybernetic Environment; Cyber Threats; Critical Infrastructures; Critical Maritime Infrastructures; Cyber Governance.

**LISTA DE ILUSTRAÇÕES**

**LISTA DE TABELAS**

**LISTA DE ABREVIATURAS E SIGLAS**

| | |
|---|---|
| AED – | Ações Estratégicas de Defesa |
| AMB – | Autoridade Marítima Brasileira |
| ANATEL – | Agência Nacional de Telecomunicações |
| ANAC – | Agência Nacional de Aviação Civil |
| ANEEL – | Agência Nacional de Energia Elétrica |
| ANP – | Agência Nacional do Petróleo |
| ANTAQ – | Agência Nacional de Transportes Aquaviários |
| ANTT – | Agência Nacional de Transportes Terrestres |
| DSI – | Departamento de Segurança da Informação do GSI |
| APF – | Administração Pública Federal |
| CAF – | *Cyber Assessment Framework* (Estrutura de Avaliação Cibernética) |
| CCDCOE – | Centro de Excelência em Defesa Cibernética Cooperativo |
| CDCiber – | Centro de Defesa Cibernética |
| CERT – | *Computer Emergency Response Team* |
| Código ISPS – | Código Internacional de Segurança de Embarcações e Instalações Portuárias |
| ComDCiber – | Comando de Defesa Cibernética |
| CMM – | *Cybersecurity Capacity Maturity Model for Nations* |
| CPNI – | Centre for the Protection of National Infrastructure (Centro de Proteção da Infraestrutura Nacional) |
| CREDEN – | Câmara de Relações Exteriores e Defesa Nacional |
| CSA – | Avaliação de Segurança Cibernética |
| CSP – | Plano de Segurança Cibernética |
| CTIR – | Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos |
| CTIR Gov – | Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo |
| DPC – | Diretoria de Portos e Costas |
| DSIC – | Departamento de Segurança da Informação e Comunicações |
| DSI – | Departamento de Segurança da Informação |

| | |
|---|---|
| EB – | Exército Brasileiro |
| ED – | Estratégia de Defesa |
| E-Digital – | Estratégia Brasileira para a Transformação Digital |
| E-Ciber – | Estratégia Nacional de Segurança Cibernética do Brasil |
| EGC – | Exercício Guardião Cibernético |
| EGDI – | *E-Government Development Index* |
| END – | Estratégia Nacional de Defesa |
| ENINT – | Estratégia Nacional de Inteligência |
| ENISA – | *European Union Agency for Cybersecurity* |
| ENSI – | Estratégia Nacional de Segurança da Informação |
| ENSIC – | Estratégia Nacional de Segurança de Infraestruturas Críticas |
| ETIR – | Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos |
| ETIR Setorial – | Equipe de Coordenação Setorial |
| EUA – | Estados Unidos da América |
| FA – | Forças Armadas |
| GCHQ – | *Government Communications Headquarters* |
| GCI – | *Global Cybersecurity Index* |
| GDSDI – | Glossário de Segurança da Informação do Departamento de Segurança da Informação do GSI/PR |
| GPS – | Sistema de Posicionamento Global |
| GTI – | Grupo de Trabalho Interministerial |
| GT SEG CIBER – | Grupo Técnico de Segurança Cibernética |
| IA – | Inteligência Artificial |
| IC – | Infraestruturas Críticas |
| ICM – | Infraestruturas Críticas Marítimas |
| IoT – | Internet das Coisas |
| ITU – | *International Telecommunication Union* |
| GSI/PR – | Gabinete de Segurança Institucional da Presidência da República |
| LBDN – | Livro Branco da Defesa Nacional |
| LGPD – | Lei Geral de Proteção de Dados |
| LVSC – | Livro Verde: Segurança Cibernética |

| | |
|---|---|
| MB – | Marinha do Brasil |
| MD – | Ministério da Defesa |
| NCF – | *National Cyber Force* (Força Cibernética Nacional do RU) |
| NCSS – | Estratégia Nacional de Cibersegurança |
| NCSC – | Centro Nacional de Segurança Cibernética do RU |
| NORMAM – | Normas da Autoridade Marítima |
| NSMS – | *National Strategy for Maritime Security* (Estratégia Nacional para a Segurança Marítima) |
| OMI – | Organização Marítima Internacional |
| ONU – | Organização das Nações Unidas |
| ONS – | Operador Nacional do Sistema |
| OTAN – | Organização do Tratado do Atlântico Norte |
| PCD – | Política Cibernética de Defesa |
| PFSP – | Plano de Segurança de Instalação Portuária |
| PIB – | Produto Interno Bruto |
| PLANSIC – | Plano Nacional de Segurança de Infraestruturas Críticas |
| PMN – | Política Marítima Nacional |
| PND – | Política Nacional de Defesa |
| PNSI – | Política Nacional de Segurança da Informação |
| PNSIC – | Política Nacional de Segurança de Infraestruturas Críticas |
| PSP – | Plano de Segurança Portuária |
| PTD – | Processo e Tomada de Decisão (PTD) |
| REGIC – | Rede Federal de Gestão de Incidentes Cibernéticos |
| Regulamentos NIS – | *Network and Information Systems Regulations* (Regulamentos de Rede e Sistemas de Informação) |
| RU – | Reino Unido |
| SegCiber – | Segurança Cibernética |
| SIC – | Segurança da Informação e Comunicações |
| SIDSIC – | Sistema Integrado de Dados de Segurança de Infraestruturas Críticas |
| SGS – | Sistema de Gerenciamento de Segurança |
| SMDC – | Sistema Militar de Defesa Cibernética |
| SSA – | Avaliação de Proteção do Navio |

| | |
|---|---|
| SSP – | Plano de Proteção do Navio |
| STJ – | Superior Tribunal de Justiça |
| TI – | Tecnologia da Informação |
| TIC – | Tecnologia da Informação e Comunicações |
| UEP – | Unidades de Exploração e Produção Marítimas |
| UK GDPR – | Lei de Proteção de Dados do RU |

**SUMÁRIO**

## 1 INTRODUÇÃO

Nas duas últimas décadas, bilhões de pessoas tiveram suas vidas melhoradas com o crescimento exponencial de acesso à internet, das oportunidades sociais e econômicas, do aumento acelerado da adoção de recursos de tecnologia da informação e comunicações (TIC), e oriundas do ambiente digital (BRASIL, 2020a).

Após a Indústria 4.0, conhecida também como a 4ª Revolução Industrial, houve uma proliferação do uso de TIC, que engloba um sistema amplo de tecnologias avançadas como a Inteligência Artificial (IA), a robótica, a computação em nuvem e a Internet das Coisas (IoT), e que alteraram de forma significativa os métodos da produção e os modelos de negócios no mundo e no Brasil (ABREME, 2021).

A cada dia mais e mais pessoas se conectam com a internet. A tecnologia tem evoluído e ficado mais complexa, além de facilitar a conexão entre as pessoas. De acordo com dados da pesquisa *Global Digital Report* 2022, 4,95 bilhões de pessoas têm acesso à internet e 92,1% desse total acessam a internet via aparelho celular, sendo que 4,62 bilhões de pessoas tem alguma rede social ativa[1]. Essa revolução digital tem transformado sobremaneira várias áreas da nossa sociedade.

Os avanços rápidos na área de TIC resultam em um uso acentuado do espaço cibernético para as atividades mais diversas, inclusive na oferta de vários serviços oferecidos pelo Governo Federal. Entretanto, surgem, na mesma proporção, novas e crescentes ameaças cibernéticas, que podem colocar em risco a sociedade brasileira e a administração pública do país (BRASIL, 2020a).

O *World Economic Forum* estimou que o mundo digital atingiria, em 2020, cerca de 44 zettabytes de dados. Para exemplificar e tentar demonstrar o quão conectado o mundo atual se encontra no momento, seguem alguns exemplos numéricos de feitos diários[2]:

– 294 bilhões de e-mails são transmitidos; 4 terabytes de dados são criados a partir de cada carro conectado; e 65 bilhões de mensagens são trocadas no WhatsApp;

---

[1] Global Digital Report, 2022. Disponível em: <https://www.hootsuite.com/pt/recursos/digital-trends>. Acesso em: 27 fev. 2022.

[2] *World Economic Forum*, 2019. *How much data is generated each day?*. Disponível em: <https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/>. Acesso em: 27 fev. 2022.

– Até 2025, estima-se que 463 exabytes de dados serão criados todos os dias globalmente (equivalente a 212.765.957 DVDs por dia).

A pandemia COVID-19, que afetou a humanidade em 2020, fez com que muitos trabalhadores passassem a trabalhar a partir de casa, em teletrabalho, acessando e compartilhando muitos dados remotamente, por meio de programas em nuvem; somado a exposição pessoal nas redes sociais, fazendo com que o número de pontos vulneráveis aumentasse, e, como resultado desse novo método de trabalho, houve um aumento exponencial dos casos de vazamentos de informações e ataques cibernéticos contra empresas, pessoas e instituições governamentais (BRASIL, 2021d).

A Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) define as infraestruturas críticas (IC) como: “instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade”; e a segurança de infraestruturas críticas como: “conjunto de medidas, de caráter preventivo e reativo, destinadas a preservar ou restabelecer a prestação dos serviços relacionados às infraestruturas críticas” (BRASIL, 2018b).

No século 21, governos, empresas e indivíduos dependem cada vez mais das TIC para grandes transações e para dar suporte às infraestruturas críticas nacionais (NGUYEN, 2015).

O Brasil não possui uma definição para as Infraestruturas Críticas Marítimas (ICM), mas o tema 2 do trabalho de Processo e Tomada de Decisão (PTD) do Curso de Política e Estratégia Marítimas da Escola de Guerra Naval/2021, definiu as ICM como: “Instalações, serviços, bens e sistemas marítimos cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade” (BRASIL, 2021e).

No espaço cibernético, inexistem fronteiras físicas, seus limites permeiam todos os setores (marítimo, terrestre, aéreo e espacial), sendo um ambiente em que a imputação de responsabilidades de qualquer ato é extremamente difícil de ser totalmente confirmada. Nesse contexto conturbado e difuso, destaca-se a possibilidade da ocorrência de ataques cibernéticos às ICM, sendo capazes até de tornar essas instalações indisponíveis temporariamente.

O uso elevado do espaço cibernético para diversas e variadas atividades faz com que surjam, na mesma proporção, novas e crescentes ameaças cibernéticas, que colocam em risco a sociedade, empresas e governos, e as IC dos países.

Apesar dessa tecnologia ter tornado a vida cotidiana mais conveniente, ela aumentou significamente o risco associado a esses sistemas, principalmente porque grupos e indivíduos, assim como os próprios estados, encontraram maneiras de manipular ou 'hackear' esses sistemas para promover seus objetivos próprios (NGUYEN, 2015).

As perdas globais devido aos crimes cibernéticos foram de US$ 3 trilhões em 2015, estimadas em US$ 6 trilhões em 2021, podendo chegar até US$ 10,5 trilhões em 2025. Esses custos incluem a perda de produtividade, desfalque, danos e destruição de dados, roubo de propriedade intelectual, fraude, roubo de dados pessoais e financeiros, exclusão e restauração de dados, sistemas hackeados e danos à reputação (MORGAN, 2020).

Segundo a Estratégia Nacional de Segurança Cibernética do Brasil (E-Ciber), a governança cibernética abrange as ações, as normas, os instrumentos e as medidas a serem executadas, a fim de obter uma simplificação e modernização do gerenciamento dos recursos humanos, financeiros e materiais, além do acompanhamento dos desempenhos e a avaliação dos resultados obtidos (BRASIL, 2020a).

Para o desenvolvimento deste trabalho, será feita a comparação da governança cibernética brasileira com a análoga de algum outro país, segundo os seguintes critérios:

a) Classificação no *Global Cybersecurity Index* (GCI) 2020 do *International Telecommunication Union* (ITU).

O país a ser comparado deverá ter participado e ter obtido classificação superior ao do Brasil no GCI 2020, o que teoricamente denotaria que está em uma fase mais avançada na conscientização dos perigos do ciberespaço, uma vez que foram analisadas 82 perguntas, 20 indicadores em 05 pilares distintos. Alguns países se recusaram a verificar dados coletados ou participar da edição do GCI, e, mesmo estando melhor classificados do que o Brasil, como é o caso do Canadá e dos Estados Unidos da América (EUA), não serão considerados neste trabalho. Como o Brasil obteve 96,6 pontos e com isso ocupa a 18ª posição, sobrariam 20 países a serem analisados, em função de alguns países estarem empatados. A tabela 1 contém a relação dos países que participaram e estão melhor classificados do que o Brasil, com suas respectivas classificações.

b) Classificação do *United Nations E-Government Development Index* (EGDI) 2020 da Organização das Nações Unidas (ONU)

O país a ser analisado também deverá ter obtido classificação superior ao Brasil no índice, uma vez que ele fornece uma avaliação comparativa do desenvolvimento do governo eletrônico em três dimensões (prestação de serviços online, recursos humanos e conectividade de telecomunicações), em nível nacional de cada país em perspetivas regionais e globais dos Estados Membros da ONU. A tabela 2 contém a relação dos 20 países melhor classificados do que o Brasil no GCI 2020, com suas respectivas classificações no EGDI 2020.

A Índia e Ilhas Maurício serão desconsiderados por terem obtido classificação superior ao do Brasil. Restaram então 18 países.

c) Idioma

Serão desconsiderados os seguintes países da análise, pois, além de serem muito difíceis na obtenção de dados e documentos, aqueles que porventura foram encontrados estavam em seus idiomas nativos, o que inviabilizaria suas análises: Arábia Saudita, Federação Russa, Estônia, Emirados Árabes Unidos, Malásia, Lituânia, Turquia, Luxemburgo, República da Coreia, Cingapura e Letônia.

Para o desenvolvimento deste trabalho, dentre os 07 países restantes (RU, Espanha, França, Alemanha, Austrália, Japão e Portugal), este autor optou por selecionar o RU, pois considerando esses dois índices, esse país ficou mais bem classificado na média dos dois. Ele obteve, no GCI 2020, 99,54 pontos e com isso ficou na 2ª colocação, e no EGDI 2020, ele obteve 0,9358, ficando na 7ª colocação.

Nesse contexto, este trabalho tem o objetivo de analisar e comparar as governanças cibernéticas do Brasil e do RU a fim de identificar possíveis deficiências na governança cibernética brasileira referente à proteção das IC, principalmente as ICM, ante às ameaças cibernéticas, e caso necessário, propor aperfeiçoamentos.

O trabalho está dividido em seis capítulos, sendo que, no Capítulo 2, são apresentadas considerações acerca do espaço cibernético e suas ameaças. Logo após, no Capítulo 3, é analisada a governança cibernética do RU referente à proteção das ICM ante às ameaças cibernéticas. No Capítulo 4, é analisada a governança cibernética brasileira referente a proteção das ICM ante às ameaças cibernéticas. No Capítulo 5, será feita uma comparação e análise entre as governanças cibernéticas do Brasil e do RU. Como último capítulo, o capítulo

6 apresentará a conclusão deste trabalho, em que serão apontadas as possíveis deficiências na governança cibernética brasileira referente à proteção das ICM ante às ameaças cibernéticas, e caso necessário, serão propostos aperfeiçoamentos.

## 2 O ESPAÇO CIBERNÉTICO E SUAS AMEAÇAS

Este capítulo tem como propósito definir o espaço cibernético, identificar suas principais características, as ameaças que circundam esse espaço, os atores envolvidos com essas ameaças e as possíveis razões e motivos que levam esses atores a cometê-las.

### 2.1 Definição do Espaço Cibernético

Definir o espaço cibernético não é algo simples, pois é um ambiente extremamente complexo. O senador americano do Alasca Ted Stevens, durante uma sessão do Congresso em 2006, o definiu como: “Não é um caminhão. É um conjunto de tubos”. Tal definição simplista demonstra até certo ponto um desconhecimento total do que realmente é o ciberespaço (SINGER, 2017).

Em suas origens, o espaço cibernético é um ambiente de informação, feito de dados digitalizados, que são criados, armazenados e principalmente, compartilhados. Logo não é somente um local meramente físico, o que torna a sua mensuração desafiadora do ponto de vista da dimensão física. Ele não é puramente virtual, compreendendo também os computadores que armazenam os dados e suas respectivas infraestruturas, que permitem o fluxo de dados, incluindo ainda a internet, redes internas fechadas, tecnologias celulares, cabos de fibra ótica, e comunicações baseadas no espaço (SINGER, 2017).

> “A definição de espaço cibernético constante no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) é: “espaço virtual composto por um conjunto de canais de comunicação da Internet e outras redes de comunicação, que garantem a interconexão de dispositivos de tecnologia da informação. Engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo, além de todas as ações, humanas ou automatizadas, conduzidas por meio desse ambiente” (BRASIL, 2019).

A Organização do Tratado do Atlântico Norte (OTAN) define o espaço cibernético como sendo o domínio global que consiste em todas as comunicações interconectadas, tecnologia da informação e outros sistemas eletrônicos, redes e seus dados, incluindo aqueles separados ou independentes, que armazenam, processam ou transmitem dados (OTAN, 2019).

A Estratégia Nacional de Segurança Cibernética (2016) do RU define o espaço cibernético como a rede interdependente de infraestruturas de tecnologia da informação, que inclui a internet, as redes de telecomunicações, os sistemas informáticos, dispositivos ligados à internet e os processadores e controladores incorporados. Pode se referir também ao mundo ou domínio virtual enquanto experiência ou conceito abstrato (RU, 2016).

Como pode ser visto, existem diversas definições para o espaço cibernético, mas basicamente ele é composto pelos computadores, com seus hardwares e *softwares*, e suas interligações com a internet e as redes fechadas (intranet). Para este trabalho, este autor considerará o espaço cibernético como sendo um ambiente complexo, composto por redes conectadas, incluindo a internet e as de comunicações, e as suas infraestruturas de *software* e *hardware*, que processam, transmitem ou armazenam dados.

## 2.2 O 5º Domínio da Guerra

Alfred Thayer Mahan, em seu livro *The Influence of Sea Power Upon History,* de 1890, dizia que o território de alguém precisava ser defendido de apenas dois vetores de ataque, por terra ou por mar. Logo, o mundo de Mahan possuía apenas dois domínios (MAHAN, 2004).

Um pouco depois da Primeira Guerra Mundial, em 1920, o General italiano Giulio Douhet, em sua obra *Il domínio dell'aria*, ressaltou a importância do domínio aéreo, passando este então a compor os domínios da guerra, juntamente com a terra e o mar (DOUHET, 1932).

Em 1982, com a criação do Comando Espacial da Força Aérea dos EUA (*Air Force Space Command*), ficando responsável por preparar e normatizar as operações espaciais, surge então o domínio espacial, passando a ser o 4º domínio (THOMPSON, 2018).

O jornal britânico *The Economist*, em sua edição de 01 de julho de 2010, divulgou uma reportagem com o título "*War in the fifth domain*", incluindo pela primeira vez o espaço cibernético como o 5º domínio. O Departamento de Defesa dos EUA incorporou esse novo domínio em seus planejamentos, doutrina e operações, de maneira oficial, em 2011. A OTAN somente passou a reconhecer o ciberespaço como um domínio operacional em 2016 (SEEBECK, 2019).

O que faz deste 5º domínio ser tão diferente dos demais? Cada um dos outros quatro primeiros domínios (terra, mar, ar e espacial) está no mundo natural, são espaços físicos.

Alguns autores, como *Michael P. Kreuzer*[3], entendem que o espaço cibernético não é domínio como os demais, e sim uma construção operacional multi-domínio, semelhante as operações especiais ou operações de inteligência. Essas operações atuam em todas as camadas e domínios da guerra. Assim como na inteligência e nas operações especiais, as operações cibernéticas representam uma série de desafios não tradicionais para a organização e execução de operações (KREUZER, 2021).

## 2.3 Características do Espaço Cibernético

Segundo Ventre (2011), uma das características principais desse ambiente cibernéticos sistemas é sua transversalidade, em que o ciberespaço permeia todas as demais dimensões (terra, ar, mar e espaço), ou seja, uma ação cibernética em uma dimensão pode impactar uma ou todas as outras, e também pode ser impactada pelas ações em qualquer uma delas. A Figura 1 representa essa transversalidade do ambiente cibernético.

Na era da internet das coisas[4], o ciberespaço é cada vez mais "uma camada em cima da nossa realidade existente", que permeia os equipamentos em todos os domínios da guerra. Os meios remotamente pilotados dependem do espaço cibernético para executar suas ações, bem como o comando e controle globais. O controle espacial também é quase inteiramente dependente de operações cibernéticas. Até o soldado está cada vez mais conectado em rede, desde seu rastreador e outras ferramentas guiadas por sistema de posicionamento global (GPS), até o uso crescente de equipamentos automatizados (KREUZER, 2021).

Potências globais como os EUA, Reino Unido, Rússia, China e França têm maior capacidade do que outros estados e atores não estatais para controlar o mar, o ar ou o espaço, mas não faz sentido falar de domínio no ciberespaço. Em todo caso, a dependência de

[3] Michael P. Kreuzer é um oficial da Força Aérea dos EUA e professor assistente de segurança internacional na *Air University*.

[4] A Internet das Coisas (ou “Internet of Things” - IoT) consiste em uma revolução tecnológica que promete unir sistemas distintos, permitindo que produtos se conectem e possuam conhecimento um do outro e ainda se inter-relacionem. Disponível em: <https://canaltech.com.br/internet/A-era-da-Internet-das-Coisas/>. Acesso em 16 abr. 2022.

sistemas cibernéticos complexos para apoio a atividades militares e econômicas criam novas vulnerabilidades em potências globais que podem ser exploradas por atores não estatais (NYE, 2010).

A Doutrina Cibernética da Marinha descreve esse “novo espaço” como virtual e etéreo por não possuir fronteiras ou limites, mas real e concreto pelos impactos infligidos à vida das pessoas (BRASIL, 2021d) .

## 2.4 As Ameaças Cibernéticas

No mundo físico, os governos têm um quase monopólio do uso da força em larga escala, o defensor tem um conhecimento mais detalhado do terreno, e os ataques terminam por causa do desgaste ou da exaustão. Tanto os recursos despendidos quanto a mobilidade são caros. Por outro lado, no mundo cibernético, os atores são diversos (e às vezes anônimos), a distância física é imaterial, e algumas formas de ofensiva são muito baratas. Como a internet foi projetada para facilitar o seu uso em vez da segurança, atualmente, os atacantes têm a vantagem sobre os defensores (NYE, 2012).

As ameaças cibernéticas têm como objetivo básico, seja no nível estratégico, operacional ou tático, a informação. No nível estratégico, elas têm como objetivo os sistemas relacionados às IC de energia (eletricidade, petróleo e gás), do sistema financeiro e social (transportes, abastecimento e outros serviços públicos), contribuindo para a diminuição da capacidade de defesa e reação de um Estado (SILVA, 2014).

Segundo Latha (2016)*, a* quantidade de conhecimento necessário para que um intruso consiga efetuar um ataque cibernético mais sofisticado tem diminuído ao longo do tempo. A Figura 2 apresenta o gráfico com essa relação.

Dessa forma, a cada dia, o conhecimento necessário para a realização de um ataque cada vez mais sofisticado tem diminuído, e o volume dos ataques aumentado. Consequentemente, será necessária uma maior quantidade de recursos financeiros a serem gastos com a SegCiber, e uma mão de obra mais especializada e em maior número.

Segundo a Doutrina Militar de Defesa Cibernética, as ações cibernéticas são divididas em três tipos: o ataque cibernético; a exploração cibernética; e a proteção cibernética. O Ataque Cibernético compreende as ações para negar, interromper, degradar, corromper ou destruir informações e/ou sistemas computacionais do inimigo. A Exploração

Cibernética consiste nas ações de coleta ou busca, em Sistemas de TI de interesse, para que sejam obtidas informações sobre a consciência situacional daquele ambiente cibernético. As informações obtidas servirão para a produção de conhecimento ou a identificação de vulnerabilidades nesses sistemas. A Proteção Cibernética constitui as ações para neutralizar os ataques e a exploração cibernética contra os nossos próprios dispositivos e redes computacionais. Esta é a principal atividade quando se trata de uma ameaça cibernética, e ela deve ser executada em caráter permanente, ou seja, executada 24h, 07 dias por semana (BRASIL, 2014b). Este trabalho abordará somente a ação de Proteção Cibernética, pois é a atividade que está diretamente relacionada com o tema proposto, ou seja, proteger as IC/ICM contra ameaças cibernéticas.

A fim de exemplificar um ataque cibernético a um órgão do país, podemos citar o ocorrido no Superior Tribunal de Justiça (STJ), no dia 02 de novembro de 2020, em que foi criptografada toda a base de dados daquele tribunal, inclusive os backups, tornando-os completamente inacessíveis para os funcionários da Corte e os cidadãos. Até que o problema fosse solucionado, com a restauração de backups a partir de fitas, todas as sessões de julgamento foram canceladas. Este ataque foi considerado como um dos ataques mais graves do país, já ocorrido em uma instituição do Estado (MARIN, 2020).

Segundo o especialista em segurança cibernética (SegCiber) da TÜV Rheinland[5], Wolfgang Kiener, a tecnologia atualmente embarcada nos transportes marítimos inclui vários sistemas, tais como, sistemas de navegação e comunicações por satélite, cartas náuticas eletrônicas e até mesmo a própria logística portuária. Isso faz com que os navios possam se tornar vulneráveis a possíveis ataques cibernéticos, bem como os terminais portuários ou as empresas de navegação. Os navios porta-contêineres, que são o principal núcleo do tráfego econômico global, estão totalmente integrados ao mundo digital. Isso faz com que a cadeia de suprimentos funcione de forma adequada, mas também torna os sistemas vulneráveis aos possíveis cibercriminosos (KIENER, 2020).

Dados de um relatório elaborado pela empresa marítima de segurança cibernética *CyberOwl* e pelo escritório de advocacia global HFW, relataram que 3% dos ataques cibernéticos ocorridos na indústria marítima, resultaram em pagamentos de resgate por parte dos armadores, no valor de US$ 3,1 milhões aos cibercriminosos. O relatório revela ainda a

[5] TÜV Rheinland é uma das principais prestadoras de serviços de teste e de certificação do mundo, com mais de 20.600 funcionários e receita anual de cerca de 2 bilhões de euros.

existência de grandes lacunas na gestão de riscos cibernéticos existentes entre as organizações marítimas e a cadeia de suprimentos (CHUBB; FINN; NG, 2022).

Segundo a empresa de segurança de tecnologia da informação McAfee, há nove tipos diferentes de *hackers*, mas este autor selecionou os cinco principais[6]:

a) *Hackers* de chapéu preto – São os vilões, popularmente conhecidos apenas como *hackers*. Eles criam vírus informáticos ou ainda se infiltram em redes ou computadores, procurando encontrar o ponto de menor resistência, quer seja devido a um algum erro humano ou a um descuido. A principal motivação desse tipo de *hackers* é a financeira.
b) *Hackers* de chapéu branco – São os "*hackers* bons", os heróis. São peritos de segurança informática contratados por empresas e agências governamentais para verificar suas vulnerabilidades de segurança, e assim garantir que os sistemas de TI da empresa são seguros.
c) *Hackers* de chapéu cinzento – Estes *hackers* não usam as suas habilidades para obter ganho pessoal, mas eles também não operam com certa integridade. Um exemplo de uma ação deste tipo de *hacker* seria a infiltração em um sistema de uma empresa a fim de revelar as suas vulnerabilidades e depois publicá-las na Internet.
d) Hacktivistas – São *hackers* que operam por uma causa específica, quer seja social ou política.
e) Ciberterroristas – São *hackers*, normalmente motivados por crenças políticas ou religiosas, que tentam gerar algum caos prejudicando as IC de um país. Eles são os mais perigosos, e possuem uma ampla gama de habilidades e objetivos. A principal motivação deles é espalhar o medo e o terror.

Segundo o relatório *Radware's Global Application and Network Security Report* 2019-2020, os principais motivos dos ataques cibernéticos em 2019 foram: ganhos financeiros (33%), interrupção dos serviços (31%) e roubo de dados (22%)[7].

---

[6] 9 tipos de *hackers* e as suas motivações. Disponível em: <https://www.mcafee.com/blogs/pt-br/family-safety/9-tipos-de-hackers-e-as-suas-motivacoes/>. Acesso em 16 abr. 2022.

[7] *Global Application & Network Security Report* 2019-2020. Disponível em: <https://www.radware.com/ert-report-2020-lpc-64936/>. Acesso em 16 abr. 2022.

Grupos de *hackers*, em ataques cibernéticos recentes, têm focado como alvos rentáveis, os sistemas de governo, a fim de provocar diferentes impactos, como por exemplo: a descrença da população nos serviços públicos, com potenciais danos à imagem do Governo perante o próprio público interno e a comunidade internacional, bem como na desconfiança de investidores estrangeiros na capacidade da administração pública proteger os seus próprios sistemas, o descontentamento da população em relação à administração pública, e o receio da licitude dos processos eleitorais. Além da proteção dos próprios sistemas do Governo, outro ponto importante refere-se à proteção cibernética das empresas constantes das IC (BRASIL, 2020a).

Atualmente, todas as IC de transporte, produção, distribuição de energia, de telecomunicações, armazenagem e distribuição de água, logística de produtos, dentre várias outras, possuem seus dados de controle inseridos em plataformas cibernéticas. Para ocorrer um ataque, não é preciso o uso de força ou acesso físico, pois o Espaço Cibernético pode ser atacado de forma anônima, quer seja, por grupos, por países, ou até mesmo por um único indivíduo, desde que tenha um certo grau de conhecimento em sistemas de decifração de senhas e busca por portas de entrada. Ele será um invasor, que em silêncio atacará utilizando-se de *softwares* "malignos" que são inseridos nos sistemas de controle das infraestruturas, fábricas, empresas, escritórios, e qualquer outro lugar de onde podem obter alguma vantagem com o acesso das informações ou com a paralização do funcionamento daquele sistema (CORREA, 2020).

## 2.5 Conclusões Parciais

Conforme demonstrado nos parágrafos acima, o espaço cibernético não respeita fronteiras físicas, e os ataques podem acontecer em qualquer lugar e serem deflagradas de locais fisicamente afastados. A sua característica principal é a transversalidade, pois pode permear todas as dimensões, e por esse motivo é considerado como o 5º domínio.

Diferentemente de outras armas, seus alvos mais comuns são os civis, e principalmente estruturas críticas. Outra grande diferença, é que, ao contrário da dissuasão nuclear, por exemplo, em que os arsenais são conhecidos, na Guerra Cibernética isso não acontece, pois qualquer pessoa de qualquer lugar pode fazer parte de um grupo que poderá

realizar um ataque cibernético contra alvos de interesse, e ele é revestido de total sigilo e anonimato.

Quanto mais desenvolvido for o país, maior será a sua dependência do ciberespaço e, consequentemente, aumentará a sua vulnerabilidade.

Outra característica importante do meio cibernético é que o conhecimento necessário para a realização de um ataque cada vez mais sofisticado têm diminuído, e por um custo pequeno, o dano causado por um simples ataque cibernético poderá ser enorme. Como consequência será necessário, cada vez maiores investimentos em SegCiber e na capacitação de recursos humanos especializados.

A garantia de uma SegCiber eficaz depende do trabalho conjunto de vários atores envolvidos nesse tema, tais como: o governo, a sociedade, as Forças Armadas (FA), as empresas, a comunidade técnica e a academia.

As IC/ ICM têm sido um alvo rentável para os *hackers*, o que deverá causar um aumento desses ataques, logo elas deverão se preparar, a fim de mitigar os danos e os impactos para a sociedade.

A Proteção Cibernética das IC/ ICM deve ser mantida permanentemente ativa e atualizada, a fim de minimizar as possibilidades de uma possível ação de um hacker.

## 3 A GOVERNANÇA CIBERNÉTICA DO REINO UNIDO REFERENTE A PROTEÇÃO DAS INFRAESTRUTURAS CRÍTICAS NACIONAIS, PARTICULARMENTE AS INFRAESTRUTURAS CRÍTICAS MARÍTIMAS, ANTE ÀS AMEAÇAS CIBERNÉTICAS

Este capítulo têm como propósito identificar e analisar as ações de governança cibernética do Reino Unido, entre elas a legislação e normas deste país afetas ao ambiente cibernético, as IC e as ICM e a estrutura governamental relacionada a esse tema.

### 3.1 A Legislação do Reino Unido afeta ao Ambiente Cibernético

O RU incluiu a ameaça cibernética em seus documentos estratégicos a partir do ano de 2010, durante o governo de coalizão conservadora e liberal democrata de 2010 a 2015. Nesse ano foram publicados dois documentos de alto nível, a Revisão Estratégica de Defesa e Segurança (Protegendo a Grã-Bretanha na era de incerteza) e a Estratégia de Segurança Nacional (Uma Grã-Bretanha forte na era da incerteza).

Esses dois documentos marcam uma mudança na capacidade do Reino Unido em aumentar sua segurança e avançar com seus interesses internacionalmente, em uma era repleta de incertezas[8].

A Segurança Nacional do RU, bem como a prosperidade da economia, dependerá da sua capacidade de proteção no espaço cibernético. O uso da internet para a prestação de serviços e para o comércio oferece benefícios indiscutíveis para o Governo e para a indústria. Isso pode ser demonstrado pelo aumento contínuo dos gastos através da internet: em agosto de 2010, as compras online do RU somaram £ 4,4 bilhões (alta de 15% em 12 meses). Mas o RU também enfrenta uma ameaça contínua e persistente d e outros Estados, terroristas e criminosos que operam no ciberespaço e, por isso, precisa ser protegido. Por exemplo: a existencia de mais de 20.000 e-mails maliciosos nas redes do governo a cada mês, centenas de fóruns de *hackers*, e onde constam milhares de detalhes de cartões de crédito roubados do RU, e estão disponíveis para venda por apenas $ 2 (RU, 2010b).

[8] Disponível em: <https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty>. Acesso em: 12 jun. 2022.

A Revisão Estratégica de Defesa e Segurança cita que no período de 2000 a 2010, houve um aumento exponencial do número de ataques cibernéticos, e que esse crescimento têm tendência de perdurar ao longo das próximas décadas. Em face dessas ameaças, o Governo do RU estabeleceu um programa nacional transformador a fim de proteger seu espaço cibernético. Seriam investidos £ 650 milhões para implementação deste Programa Nacional de Segurança Cibernética, durante quatro anos (RU, 2010a).

Essa Revisão apresentou os três maiores riscos à Segurança Nacional, considerados como Riscos Nível Um (*Tier One*)[9], que são o terrorismo, as emergências civis (riscos naturais ou acidentes) e a SegCiber. Ela determina ainda a criação de um novo Grupo Cibernético de Operações de Defesa com as tarefas de integrar a SegCiber, abordar as deficiências na infraestrutura cibernética crítica, apoiar pesquisas de segurança cibernética de longo prazo e introduzir um programa de educação e habilidades em SegCiber, e construir novas acordos de cooperação na área de segurança cibernética (RU, 2010a).

O país percebeu que estava inserido em uma era repleta de incertezas, com o aumento exponencial do uso de TI, particularmente da internet, nos setores governamentais e de comércio, tendo os gastos com as compras online disparado. Como resultado da utilização de toda esse tecnologia, há um aumento das vulnerabilidades, ocasionando inúmeras tentativas de novos ataques. Diante desse cenário, o Governo considerou, pela primeira vez, a SegCiber como uma ameaça do mais alto nível para a Segurança Nacional. Para se proteger dessa nova ameaça, o Governo investirá grandes somas de recursos a fim de aumentar a sua SegCiber.

A Estratégia de Segurança Nacional relata em sua introdução que a Grã-Bretanha, naquele momento, era mais segura e mais vulnerável do que na maior parte de sua longa história, sendo mais vulnerável, por ser uma das sociedades mais abertas, em um mundo que está mais cada vez mais conectado. O país enfrenta uma gama diferente e mais complexa de ameaças oriundas de uma infinidade de fontes, tais como o terrorismo, ataque cibernético, ataques não convencionais usando produtos químicos, nucleares ou armas biológicas. Qualquer uma dessas ameaças poderá causar graves danos ao país. Em razão dessas novas

[9] Risco Nível Um, é o mais alto grau de um risco. Riscos com esse grau são considerados com maiores prioridades para a Segurança Nacional do RU, levando em conta a probabilidade de ocorrência e o impacto causado. Disponível em: <https://assets.publishing.service.gov.uk /government/uploads/system/uploads/attachment_data/file/62500/Factsheet18-Cyber-Security.pdf>. Acesso em: 12 jun. 2022.

ameaças e em evolução, é necessário que existam estruturas que permitam uma reação rápida e eficaz à elas, garantindo a segurança do país. Para atingir seus objetivos, a Estratégia cita que as empresas e governo deverão trabalhar muito mais juntos, a fim de robustecer a defesa contra ataques cibernéticos, e caso isso venha a ocorrer, a recuperação dos sistemas possa ser realizada rapidamente de modo a manter o país em funcionamento (RU, 2010c).

Ela relaciona também os quatro riscos com maior prioridade ao RU, para o período de 2010 a 2015, que são o terrorismo internacional, ataque cibernético, crises militares internacionais e os acidentes graves e/ou riscos naturais. Para se contrapor a essas ameaças, ela cita dois objetivos estratégicos complementares: sendo o primeiro a garantia de um RU seguro e resiliente (protegendo o povo, economia, infraestrutura, território e modo de vida de todos os principais riscos que podem afetá-los diretamente), e o segundo moldando um mundo estável (ações para reduzir a probabilidade de riscos que afetem o RU ou seus interesses no exterior) (RU, 2010c).

Em relação aos ataques cibernéticos, a Estratégia diz que esse tipo de ataque, assim como o terrorismo, não é simplesmente um risco para o futuro, pois o governo, o setor privado e os cidadãos comuns já estão sob ataque cibernético na atualidade, tanto de estados hostis quanto de criminosos (RU, 2010c).

A Estratégia de Segurança também elencou a SegCiber como uma ameaça de nível um para a Segurança Nacional, e para que exista uma proteção eficaz contra essa nova ameaça, que já estariam acontecendo, é imprescindível que haja uma estreita cooperação entre os setores público e privado, com troca de informações e experiências.

Em 2011 foi publicada a primeira Estratégia Nacional de Segurança Cibernética do RU (Proteger e promover o RU em um mundo digital). Essa Estratégia define como o país apoiará a prosperidade econômica, protegerá a Segurança Nacional e salvaguardará o modo de vida da sociedade, de modo a construir um ambiente digital mais confiável e resiliente (RU, 2011).

Por ocasião do lançamento dessa Estratégia, o então Primeiro-ministro do RU, David Cameron enfatizou a importância da internet para o crescimento da economia do país, mas que ela precisaria ser protegida dos criminosos cibernéticos que ameaçam a prosperidade britânica, bem como os cidadãos comuns. Por esses motivos, a SegCiber seria uma prioridade do Governo, que trabalharia conjuntamente com outros países, o setor privado e os órgãos

de segurança, a fim de manter o RU um país seguro para que sejam estabelecidas relações comerciais[10].

A Estratégia de Segurança Cibernética prevê uma nova fase de cooperação entre o Governo e o setor privado na área de SegCiber, ou seja, ambos trabalhando lado a lado para tornar o RU um dos lugares mais seguros do mundo para se fazer negócios. Essa cooperação visa a troca de informações sobre ameaças cibernéticas e a gerência das respostas aos ataques cibernéticos. Ela apresenta ainda, que cerca de 6% do Produto Interno Bruto (PIB) do país é gerado pela internet e que esse valor deve crescer, tornando a internet um setor maior do que os serviços públicos ou a agricultura (RU, 2011).

Nesse documento o Governo mais uma vez enfatiza a importância do trabalho colaborativo no campo da SegCiber, e que esta é uma prioridade governamental, ainda mais porque o comércio pela internet têm contribuído com uma parcela considerável do PIB nacional, com tendência a aumentar.

Em relação ao combate do crime cibernético, a Estratégia prevê a criação de uma unidade de crimes cibernéticos dentro da Agência Nacional de Crimes. Essa unidade seria a responsável pelos crimes cibernéticos de grande vulto em nível nacional, bem como das respostas a esses incidentes nacionais (RU, 2011). A Unidade foi efetivamente ativada em 2013, conforme previsto na Estratégia.

A principal lei do RU que tipifica os cibercrimes é a Lei de Uso Indevido de Computadores de 1990. Essa a lei rege a maneira como os indivíduos podem acessar legalmente dados em uma máquina, logo ela criminaliza qualquer acesso não autorizado aos dados sem a permissão do proprietário (RU, 1990). Segundo McCallion (2022), essa lei sofreu algumas mudanças ao longo dos anos, a fim de retratar algumas evoluções nas áreas de TI e SegCiber, mas, mesmo assim, não internalizou as inovações mais recentes da informática, e por isso, ela precisa ser atualizada.

Para o enfrentamento de ameaças cibernéticas de alta complexidade, como já citado acima na Revisão Estratégica de Defesa e Segurança, ela reitera a criação de um novo Grupo de Operações Cibernéticas de Defesa, que será o responsável pelo desenvolvimento de novas táticas, técnicas e planos para fornecer capacidades cibernéticas militares (RU, 2011).

[10] Disponível em: <https://www.gov.uk/government/news/protecting-and-promoting-the-uk-in-a-digital-world--3>. Acesso em: 14 jun. 2022.

Além das medidas de proteção do espaço cibernético, também há a necessidade do combate ao crime neste espaço, para que haja uma dissuasão aos propensos atacantes, e para isso foi criada uma unidade específica para atuar nessa área, além de um grupo de operações cibernéticas que desenvolverá as capacidades cibernéticas militares.

Uma inciativa interessante prevista nessa Estratégia, que visa conscientizar a população e as pequenas e médias empresas sobre as medidas de prevenção e segurança no espaço cibernético, é a criação do *site* Fique Seguro Online (*Get Safe Online*[11]), por meio de uma parceria público-privada. Esse *site* contém várias informações e orientações sobre boas práticas cibernéticas, que abordam dicas e conselhos sobre temas como proteção de seu computador pessoal, compras online, vírus, uso das redes sociais, roubo de dados, fraude de identidade, entre outras informações muito úteis, que de uma maneira simples fornecem conteúdo para que a população possa se proteger ao utilizar o espaço cibernético. Essa iniciativa possui, além do *site*, páginas nas principais mídias sociais, como o *Facebook* e *Instagram* (RU, 2011).

Uma das maiores vulnerabilidades cibernéticas é a falta de consciência da importância e do perigo desse assunto no dia a dia da população e das empresas menores, que possuem poucos recursos para investimento na proteção de seus interesses online. A iniciativa da criação do *site*

Fique Seguro Online tenta aumentar esse consciência, com a divulgação de informações e orientações de boas práticas cibernéticas, de forma gratuita, e com uma linguagem simples e objetiva.

Outra iniciativa que foi implementada no RU, em 2014, foi o Essenciais Cibernéticos (*Cyber Essentials*), que é um programa de certificação cibernética, apoiado pelo governo, que ajuda na proteção de empresas, independentemente do tamanho, contra os ataques cibernéticos mais comuns. Existem dois níveis de certificação, o básico e o *plus*. O nível básico é considerado como o padrão mínimo para a SegCiber no RU. Para incentivar as empresas a obterem essa certificação, algumas licitações com o governo, obrigam que as empresas participantes tenham essa certificação cibernética[12].

---

[11] Disponível em: <https://www.getsafeonline.org/>. Acesso em: 14 jun. 2022.

[12] *Cyber Essentials*. Disponível em: <https://www.ncsc.gov.uk/cyberessentials/overview>. Acesso em: 17 jun. 2022.

O Essenciais Cibernéticos foi uma inciativa que visa a certificação de empresas a atingir um nível mínimo de SegCiber, com um custo relativamente baixo[13], o que garantirá que as empresas certificadas estarão minimamente seguras, e ainda para forçar que uma maior número de empresas obtenham essa certificação, a participação de algumas licitações governamentais exigem essa certificação.

Em novembro de 2015, foram publicadas a Estratégia de Segurança Nacional e a Revisão da Estratégia de Defesa e Segurança para o período compreendido de 2016 a 2021, com a visão de um RU Seguro e Próspero, com alcance e influência global. Em relação às principais ameaças (classificadas como Risco Um) para os próximos cinco anos (2011-2016), permaneceram algumas dos documentos estratégicos de 2010 (Terrorismo, Ameaça Cibernética, Crises Militares Internacionais e Grandes Riscos Naturais), e foram incluídas duas novas ameaças, a Instabilidade no Exterior e a Saúde Pública (RU, 2015).

Em relação ao ambiente cibernético, ela cita que, desde 2011, foram investidos £ 860 milhões em novas tecnologias e capacidades, e que o RU se tronou um líder mundial em SegCiber. É citado também que foi estabelecido o Centro de Avaliação Cibernética e a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do RU (CERT-UK)[14], e que foi concretizada uma estreita parceria entre o Governo, o setor privado e a academia, visando o compartilhamento de pesquisas, e desta forma, impulsionando a inovação digital no país. Foram estabelecidas parcerias com os países aliados, com troca de conhecimentos especializados nessa área (RU, 2015).

Esses novos documentos estratégicos mantiveram a classificação da SegCiber com o maior nível de ameaça à Segurança Nacional, e citam o alto investimento realizado pelo país no desenvolvimento de novas tecnologias e capacidades, o que fizeram com que o RU se tornasse, segundo esses documentos, um líder mundial nessa área. Eles falam ainda da criação da primeira ETIR do país, órgão imprescindível para o tratamento de respostas a incidentes cibernéticos.

Esses documentos ressaltam que o volume e a complexidade dos ataques cibernéticos contra o RU têm aumentado bastante, assim como os custos de proteção para as

[13] Custo da certificação básica para empresas com: até 9 funcionarios: £ 300+impostos; 10 a 49 funcionarios: £ 400+impostos; 50 a 249 funcionarios: £ 450+impostos; mais de 250 funcionarios: £ 500+impostos. Disponível em: <https://www.ncsc.gov.uk/cyberessentials/faqs>. Acesso em: 17 jun. 2022.

[14] *Computer Emergency Response Team* (CERT) é conhecido, no Brasil, como Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

empresas. Para enfrentar esse aumento de ataques, o país iria investir £ 1,9 bilhão nesse período (2011-2016), para a proteção cibernética do RU, para o desenvolvimento de novas capacidades no espaço cibernético, como recursos para detecção e análise de ameaças, e o rastreamento dos responsáveis (RU, 2015).

Para a capacitação de recursos humanos na área cibernética, a Estratégia cita que será criado um programa nas escolas para identificar e incentivar novos talentos entre jovens de 11 a 17 anos em todo o país, que será o Programa Primeiro Ciber (*CyberFirst*[15]), que visa inspirar e encorajar estudantes de todas as origens a considerar uma carreira em SegCiber. Um outro programa que têm obtido algum exito, e existe desde 2010, é o Desafio de Cibersegurança (*Cyber Security Challenge*[16]), cujo objetivo é encontrar e nutrir talentos de SegCiber, além de atrair novas pessoas para o mercado, executando eventos, competições, feiras de carreiras, jogos, *networking* universitário, dias de treinamento organizacional e muitas outras atividades em todo o país. Dentro desse programa, o Centro Nacional de Segurança Cibernética do RU (*National Cyber Security Centre* (NCSC)) oferece o Cursos *CyberFirst*, que são alguns cursos com curta duração, desenvolvidos para apresentar aos jovens o mundo da SegCiber (RU, 2015).

Os Programas Primeiro Ciber e o Desafio de Cibersegurança têm o objetivo de identificar e atrair estudantes para o mercado de trabalho da segurança cibernético.

Em 2016 foi publicada a segunda Estratégia Nacional de Segurança Cibernética, sendo esta para o período de 2016 a 2021. A visão desta Estratégia é que o RU seja um país seguro e resiliente às ameaças cibernéticas, próspero e confiante no mundo digital. Ela possui três objetivos que são defender, desenvolver e dissuadir. Para cada um dos objetivos, a Estratégia prevê resultados estratégicos esperados e indicadores de sucesso associados, a serem integralmente cumpridos até 2021 (RU, 2016a).

Na apresentação do documento, o então *Chancellor of the Exchequer* (Ministro da Fazenda), Philip Hammond escreveu o seguinte:

> "Em última análise, a ameaça cibernética não pode ser completamente eliminada. A tecnologia digital somente funciona por ser aberta, e essa abertura traz consigo um risco inerente. O que podemos fazer é reduzir a ameaça a um nível que garanta a nossa permanência na vanguarda da revolução digital. Esta Estratégia traça o caminho nesse sentido". (RU, 2016a, p. 6. Tradução própria. Original em inglês).

[15] Programa *CyberFirst*. Disponível em: <https://www.ncsc.gov.uk/cyberfirst/overview>. Acesso em: 16 jun. 2022.

[16] Programa *Cyber Security Challenge.* Disponível em: < https://cybersecuritychallenge.org.uk/>. Acesso em: 16 jun. 2022.

Um fato importante na publicação é a criação do *NCSC* que é o centro de referência em SegCiber do país, onde são compartilhados conhecimentos, é realizado o tratamento de vulnerabilidades sistêmicas e é o órgão de liderança em questões da SegCiber nacional (RU, 2016a). A atuação do NCSC será tratada mais adiante neste trabalho.

Essa segunda Estratégia Nacional de Segurança Cibernética, assim como a primeira versão deste documento, prevê um investimento dispendioso na área de SegCiber do país, de forma a enfrentar a constante evolução das ameaças. O Ponto mais importante deste documento é a criação do NCSC, órgão que será o ponto central da segurança cibernética do RU, como veremos logo a seguir.

Inaugurado em 2016, o NCSC é o órgão central, a nível nacional, para a SegCiber. Ele está vinculado ao *Government Communications Headquarters* (GCHQ), que é a agência de inteligência, segurança e cibersegurança do RU, e que têm a missão de manter o país seguro. O NCSC é o responsável pela resposta a incidentes cibernéticos (CTIR Nacional) e serve como referência em SegCiber no país. O CTIR Nacional fornece suporte 24/7 para os órgãos essenciais em assuntos "cibernéticos", e ele têm um papel ativo em torno de incidentes de segurança. Eles monitoram possíveis incidentes, fornecem a devida resposta a eles e o suporte pós-incidente. O NCSC têm como objetivos ofertar uma estrutura de resposta a incidentes cibernéticos, de modo a tratar e reduzir os danos causados, desde os ataques contra organizações isoladas até os ataques de grande porte a nível nacional; divulgar informações sobre as atitudes que podem ser adotadas por organizações do setor público e privado para lidar com questões de SegCiber, facilitando assim o intercâmbio de informações sobre ameaças cibernéticas; e prestar consultoria setorial especializada ao governo e a setores das infraestruturas críticas, como os de energia, telecomunicações, finanças, e também divulgando diretrizes e orientações sobre a SegCiber. A esse Centro cabe ainda, a responsabilidade de formular orientações de segurança cibernética que acompanhem a evolução constante das ameaças e o desenvolvimento de novas tecnologias a fim de enfrentá-las (RU, 2016b).

Como vimos, podemos dizer que o NCSC é o coração da SegCiber do RU, que além de possuir uma estrutura para fornecer uma rápida resposta aos incidentes cibernéticos, ele ainda é responsável por divulgar e formular informações e orientações sobre as questões cibernéticas, e manter e operar o CTIR do país.

A campanha Ciber Consciente (*Cyber Aware*[17]), é uma outra inciativa citada nessa Estratégia, que são conselhos à população, com as diretrizes necessárias para se protegerem de cibercriminosos. São mensagens dirigidas, veiculadas por meio das redes sociais e campanhas publicitárias, com o apoio da iniciativa privada (RU, 2016a). O interessante dessa campanha é que as informações são transmitidas ao público, principalmente, por meio das redes sociais, facilitando e aumentando a referida difusão.

O RU, em 2018, lançou a sua Lei de Proteção de Dados (UK GDPR), que foi a internacionalização do Regulamento Geral sobre a Proteção de Dados (2016), da União Europeia. Ela se aplica a grande parte das empresas e organizações do país, e cita os princípios, direitos e obrigações de todos os atores na proteção de dados (RU, 2018a).

Em 2020 foi criada a Força Cibernética Nacional (*National Cyber Force* (NCF)), através de uma parceria entre a Defesa e a Inteligência do RU. Essa Força é responsável por operar dentro e através do ciberespaço para perturbar, negar, degradar e contestar aqueles que prejudicariam o RU e seus aliados, a fim de manter o país seguro e para proteger e promover os interesses internos do país e no exterior. A NCF pode atuar em favor da segurança nacional do país, operando desde o nível tático até o nível estratégico, contra atores estatais e não estatais. Seu trabalho se divide em três categorias principais: O combate às ameaças de terroristas, criminosos e estados que usam a internet para prejudicar o RU e outras sociedades democrática; o apoio à SegCiber do país e o trabalho desenvolvido pelo NCSC, de modo a combater as ameaças no ciberespaço; e a habilitação de operações de Defesa do RU e a ajuda no cumprimento da política externa (RU, 2020a).

Tal força foi criada em uma parceria do Ministério da Defesa e a GCHQ, e têm um foco militar, de caráter mais ofensivo e dissuasório, do que defensivo.

No ano passado, o governo britânico publicou a Revisão Integrada de Segurança, Defesa, Desenvolvimento e Política Externa (Uma Grã-Bretanha Global em uma Era Competitiva), para o período de 2021 a 2025. Ela cita que o país será reconhecido como uma superpotência na área de ciência e tecnologia, e que estará à frente dos demais em relação a regulamentação sobre as áreas de tecnologia, cibernética, digital e de dados, com uma previsão de gastos com defesa, de 2,2% do PIB, a fim de alavancar um programa de modernização que engloba os novos domínios do ciberespaço, e investimentos em ciência e

[17] Campanha Ciber Consciente (*Cyber Aware*). Disponível em: <https://www.ncsc.gov.uk/cyberaware/home>. Acesso em: 17 jun. 2022.

tecnologia, com ênfase no crescimento do poder cibernético. Um dos objetivos estratégicos dessa publicação é a construção de resiliência no país e no exterior, uma vez que não é possível prever ou se prevenir de todos os riscos, sejam eles, de origens naturais, como eventos climáticos extremos ou ameaças como os ataques cibernéticos. O país adotará uma postura de um poder cibernético responsável e democrático, mantendo a vantagem competitiva neste domínio em rápida evolução (RU, 2021).

Essa Revisão salienta que a SegCiber é a base do poder cibernético e ela têm sido o principal foco das últimas estratégias, mas para que o RU se consolide nessa área, será adotada uma estratégia cibernética abrangente, onde serão consideradas todas as capacidades do país no desenvolvimento de tecnologias cibernéticas críticas, bem como na cooperação internacional (RU, 2021).

Neste ano, foram publicados dois documentos estratégicos cibernéticos, a Estratégia de Segurança Cibernética do Governo: 2022 a 2030 e a Estratégia Cibernética Nacional 2022.

A Estratégia Cibernética Nacional 2022 (Pioneirismo em um futuro cibernético com todo o RU) têm como visão, que o país, em 2030, continuará a ser um líder no poder cibernético responsável e democrático, capaz de proteger e promover seus interesses dentro e através do ciberespaço em apoio aos objetivos nacionais (RU, 2022a).

Essa Estratégia estabeleceu cinco ações prioritárias, e que são consideradas como os pilares do quadro estratégico, e que servirão de orientação para que os resultados das ações específicas sejam atingidos até 2025. As ações são as seguintes: Robustecer o sistema cibernético do país, investindo em pessoal e habilidades, e aumentar a parceria entre governo, academia e indústria; Fazer do RU um país digital, resiliente e próspero, reduzindo os riscos cibernéticos para que as empresas possam maximizar os benefícios econômicos da tecnologia digital e os cidadãos estejam mais seguros online e confiantes de que seus dados estão protegidos; Fomentar sua capacidade industrial e desenvolver estruturas para sua proteção cibernética; Alavancar sua liderança global, influenciando uma ordem internacional mais segura, próspera e aberta; Detectar, interromper e dissuadir os adversários para aumentar a segurança do país no ciberespaço (RU, 2022a).

A terceira edição do país da Estratégia Cibernética Nacional revela a vontade do RU em se manter como uma potência cibernética mundial, capaz de influenciar outros países e manter o mundo mais seguro e próspero. Ela reitera a necessidade de o país continuar

investindo em novas tecnologias e na formação de recursos humanos, a fim de tornar o país mais resiliente e seguro.

Segundo Baker (2022), a Estratégia Cibernética Nacional insere uma nova expressão no ambiente cibernético, que é o poder cibernético, e o define como a capacidade de proteger e promover interesses nacionais dentro e através do ciberespaço. Essa expressão é amplamente utilizada em todo o documento, e enfatiza uma mudança significativa na forma como o governo enxerga o espaço cibernético. Haverá um novo foco na capacidade de um Estado de proteger e promover seus interesses dentro e através do espaço cibernético em vez de apenas garantir a sua segurança. O foco da Estratégia consiste na elevação do domínio cibernético de um nível básico de pura segurança, e inseri-lo como uma preocupação de toda a sociedade, com interesse proeminente em como aproveitar o poder cibernético para ganho econômico e social (BAKER, 2022).

Essa Estratégia cita que o RU deve solidificar a sua posição como um "poder cibernético" internacional, e tenta ainda, envolver toda a sociedade nas questões de SegCiber.

Em relação à capacitação de recursos humanos cibernéticos, a Estratégia cita que a força de trabalho do setor de SegCiber cresceu cerca de 50% nos últimos quatro anos, mas com uma demanda por habilidades muitas vezes superando a oferta. Ela fala ainda da criação de uma ampla gama de iniciativas extracurriculares para inspirar os jovens a seguir uma carreira em SegCiber. De 2019 a 2020, cerca de 57.000 jovens participaram do programa de aprendizagem Primeiro Ciber. Apesar dessas inciativas, ainda há um déficit de pessoas com habilidades mais específicas, pois das 1,32 milhões de empresas, cerca de 50% ainda revelam que possuem uma lacuna de habilidades técnicas de SegCiber (RU, 2022a).

Apesar de todas as ações implementadas pelo RU, a Estratégia relata ter evidências crescentes de lacunas na resiliência nacional, com um aumento dos crimes cibernéticos e violações, que afetam o governo, as empresas e os indivíduos. As vulnerabilidades da cadeia de suprimentos e a escassez de profissionais de SegCiber são áreas críticas crescentes de preocupação. Quase quatro em cada dez empresas (39%) relataram ter sofrido ataques ou violações de SegCiber no último ano, e muitas organizações (especialmente as pequenas e médias empresas) não têm a capacidade de se proteger e responder a incidentes (RU, 2022a).

A capacitação de recursos especializados em SegCiber é um problema que envolve diversos países, principalmente nas empresas de pequeno e médio porte, que possuem

recursos limitados para contratação e pagamento de salários mais elevados. Apesar das boas iniciativas adotadas pelo RU para a captação de pessoal, como o Primeiro Ciber e o Desafio de Cibersegurança, que contribuiram para um aumento de 50% da força de trabalho, ainda assim, metade das empresas britânicas alegam ter falta de pessoal especializado em seus quadros, fazendo com que o nível de segurança dessas empresas fique enfraquecido e elas fiquem mais vulneráveis.

A Estratégia Cibernética Nacional 2022 destina-se a ser um guia de ação, não apenas para os órgãos do Governo que têm alguma responsabilidade na área cibernética, mas também para cada pessoa e organização em toda a sociedade, que têm interesse e responsabilidade pelo esforço cibernético nacional. É também o início de uma troca de informações, para a garantia de que os objetivos e prioridades permaneçam relevantes nos próximos cinco a dez anos. Essa publicação será usada como uma plataforma para um maior engajamento entre os setores público e privado em todo o RU (RU, 2022a).

A outra publicação lançada este ano foi Estratégia de Segurança Cibernética do Governo: 2022 a 2030, onde estão definidos os planos mais detalhados para melhorar a segurança do governo e do setor público, em apoio a Estratégia Cibernética Nacional 2022. Em sua introdução ela cita que as organizações governamentais são rotineiras e incansavelmente visadas a ataques, e que dos 777 incidentes gerenciados pelo NCSC, entre setembro de 2020 e agosto de 2021, cerca de 40% foram destinados ao setor público, com uma tendência de aumento. Sua visão é garantir que as funções principais do governo, desde a prestação de serviços públicos até a operação do aparato de Segurança Nacional, sejam resilientes a ataques cibernéticos, fortalecendo o RU como uma nação soberana e consolidando sua autoridade como um poder cibernético democrático e responsável. O seu objetivo central é que as funções críticas do governo sejam significativamente robustecidas contra ataques cibernéticos até 2025, com todas as organizações governamentais sendo resilientes a vulnerabilidades conhecidas e métodos de ataque até 2030 (RU, 2022b).

Essa Estratégia do Governo indica mais detalhadamente as ações que devam ser executadas a fim de cumprir o previsto na Estratégia Cibernética Nacional 2022. Ela cita que os órgãos governamentais têm sido alvos de ataques cibernéticos, com uma média de 40% de todos os incidentes registrados, e com uma tendência de aumentar, e por isso seu principal objetivo é fortalecer a resiliência das funções críticas e os órgãos do governo contra ataques cibernéticos até 2025 e 2030, respectivamente.

A própria Estratégia considera que este objetivo é ousado e ambicioso. Para alcançá-lo, serão necessários que sejam estabelecidos amplos processos, mecanismos e parcerias, uma tarefa complicada em virtude dos diferentes níveis de maturidade cibernética de cada órgão. Porém, caso o país consiga alcançá-lo, isso permitirá que o governo proteja seus dados e opere sem interrupções indevidas, e garantirá que as organizações governamentais sejam estruturadas e organizadas para gerenciar, quando surgirem, as ameaças desconhecidas e mais sofisticadas. Ela possui dois pilares fundamentais, que são: 1 – A fortificação da resiliência de SegCiber do governo; e 2 – A defesa executada como se fosse um só (RU, 2022b).

O Pilar 1 será alcançado, basicamente, com a adoção por todos os órgãos da Estrutura de Avaliação Cibernética (*Cyber Assessment Framework* (CAF)). A adoção da CAF garante que o governo esteja avaliando sua resiliência cibernética de maneira consistente e comparável a outras organizações que operam os serviços essenciais do RU. A CAF será detalhada mais adiante neste trabalho. O Pilar 2 será alcançado com o compartilhamento de dados, conhecimentos e capacidades de SegCiber em todo o governo, de forma a garantir que todas as organizações governamentais tenham acesso oportuno a dados relevantes de SegCiber que possam melhorar sua capacidade de gerenciar riscos cibernéticos, além de trabalhar de modo colaborativo para coordenar e direcionar melhor os recursos e serviços governamentais compartilhados que abordam questões comuns de SegCiber em escala (RU, 2022b).

Como citado na própria Estratégia, seu objetivo principal é extremamente ousado e difícil de ser atingido, pois dependem de várias variáveis difíceis de se controlar, mas caso o país consiga atingi-lo, ele garantirá a segurança de suas informações e dados, e o fornecimento dos serviços públicos sem interrupções causadas por agentes cibernéticos externos. Os dois pilares básicos citados nela, serão cumpridos com a adoção basicamente da CAF para o Pilar 1 e do compartilhamento de informações e experiências, e trabalho coordenado para o Pilar 2.

Em 30 de março de 2022, o Governo publicou a Pesquisa de Violações de Segurança Cibernética 2022. Esta pesquisa é realizada anualmente, conforme estabelecido na Estratégia Cibernética Nacional, e visa obter dados sobre a resiliência cibernética do RU. Essa edição relata que nos últimos 12 meses, 39% das empresas britânicas sofreram algum ataque cibernético. O custo médio estimado de todos os ataques cibernéticos nos últimos 12 meses

foi de £ 4.200. Como conclusões da pesquisa, foram apontadas que houve uma aumento do número de empresas (82%) que classificam a SegCiber como de alta prioridade; que as empresas têm conseguido manter uma boa SegCiber, utilizando-se das regras, políticas e técnicas de mitigação de riscos permanecendo em percentuais estáveis nos últimos anos, apesar dos desafios contínuos; mais de 80 % das empresas de médio e grande porte adotaram medidas, conforme orientação do Governo, para melhorar a sua SegCiber em pelo menos 5 áreas; as organizações conseguiram implementar uma boa cultura de SegCiber entre seus funcionários, mas ainda há lacunas na SegCiber organizacional; apenas 20% das empresas têm um plano formal de gerenciamento de incidentes; algumas empresas relataram dificuldades em realizar investimentos em SegCiber, em função do orçamento limitado e de outras prioridades organizacionais concorrentes; algumas organizações têm optado em terceirizar suas soluções SegCiber para um fornecedor terceirizado, de maneira que possam ter recursos de um especialista e com mais recursos (RU, 2022c).

A divulgação de uma pesquisa anual com as informações sobre as violações de SegCiber ocorridas, é uma excelente prática, de maneira que todos possam avaliar como está a SegCiber do país e orientar o próximos passos, a fim de corrigir alguma vulnerabilidade. A pesquisa desta ano, identificou lacunas que precisam ser corrigidas, principalmente na elaboração de planos formais de gerenciamento de incidentes por parte das empresas e um maior investimento em SegCiber nas empresas de pequeno e médios portes.

### 3.2 A Legislação do Reino Unido afeta as Infraestruturas Críticas

As IC do RU, incluem todos os serviços essenciais que mantêm o funcionamento do país, desde as funções centrais do governo até a garantia da disponibilidade de bens imprescindíveis, como alimentos e água, combustíveis e comunicações confiáveis. Grande parte das IC estão no setor privado. Desta forma o Governo deverá trabalhar em apoio aos proprietários e seus operadores, a fim de mitigar os riscos contra possíveis ameaças. O Governo deverá, ainda, lançar um marco regulatório apropriado, de modo a garantir a resiliência das IC às ameaças futuras (RU, 2015).

O RU possui um órgão denominado Centro de Proteção da Infraestrutura Nacional (*Centre for the Protection of National Infrastructure (*CPNI)), que foi criado em 2007. Esse Centro define que no RU, existem 13 setores de IC nacionais, que são: “Químico, Nuclear Civil,

Comunicações, Defesa, Serviços de Emergência, Energia, Finanças, Alimentos, Governo, Saúde, Espaço, Transporte e Águas". O CPNI é Autoridade Técnica Nacional do governo britânico para assuntos relativos à segurança física e de proteção pessoal da IC. As ameaças que são consideradas no *site* oficial do Centro, estão o Terrorismo, a Espionagem e as outras ameaças (Armas de Destruição em Massa e Crime Organizado). Em relação às ameaças cibernéticas, a responsabilidade pela proteção das redes de TI, dados e sistemas das IC é do NCSC, e para isso, ele, atuará em parceria com departamentos do governo e reguladores, aos quais caberá assegurar que os riscos cibernéticos sejam gerenciados em seus setores segundo os padrões exigidos por interesses nacionais (RU, 2007).

Assim como no Brasil, a maioria das IC no RU são operadas pelo setor privado. O CPNI é a autoridade responsável pelos assuntos inerentes a segurança delas, particularmente em relação às questões de segurança física e de proteção pessoal. Em relação às ameaças cibernéticas, a responsabilidade pela SegCiber das IC é do NCSC, em coordenação com os órgãos reguladores, os seus proprietários e operadores.

A Estratégia de Segurança Nacional, 2010, possui um dos objetivos complementares, que é garantir um RU resiliente e seguro, por meio da proteção de vários ativos nacionais, como a população, a economia, as IC, e o território, das principais ameaças, como o terrorismo e o ataque cibernético (RU, 2010c).

Quando a primeira Estratégia Nacional de Segurança Cibernética foi lançada, em 2011, foi incluída como uma das suas prioridades de ação, o contínuo melhoramento da detecção e análise das ameaças cibernéticas, principalmente focado nas IC, e outros sistemas de interesse nacional (RU, 2011).

A Estratégia de Segurança Nacional e a Revisão da Estratégia de Defesa e Segurança para o período compreendido de 2016 a 2021, cita que o Governo trabalhará junto com os proprietários e operadores a fim de fortalecer a SegCiber das IC, e que seria estabelecido um centro de treinamento cibernético e um laboratório de testes para apoiar o desenvolvimento de tecnologia mais moderna e segura para ser usada em todas as IC, aumentando assim, os padrões de segurança das IC (RU, 2015).

A Estratégia Nacional de Segurança Cibernética para o período de 2016 a 2021, estabelece que a garantia da segurança e resiliência das IC contra ataques cibernéticos é uma prioridade para o governo, e que nesses setores prioritários, ainda não há uma conscientização e controle adequado do risco cibernético, enquanto as ameaças continuam a

se diversificar e proliferar. Segundo essa Estratégia, o governo e os órgãos públicos não assumirão a responsabilidade de controlar os riscos das IC a favor do setor privado, cuja responsabilidade será da administração e dos operadores das respectivas empresas. Essas organizações devem identificar seus sistemas críticos e avaliar periodicamente sua vulnerabilidade diante da constante evolução tecnológica e das ameaças, além de investir em tecnologia para reduzir as vulnerabilidades nos sistemas, mantendo um nível de SegCiber proporcional ao risco. Deverão, ainda, atuar de forma colaborativa com órgãos governamentais e reguladores para assegurar que o risco cibernético seja adequadamente tratado. Caberá ao governo classificar o nível de SegCiber nas IC e adotar medidas para intervir, quando necessário, a fim de promover melhorias de interesse nacional (RU, 2016a).

Os documentos estratégicos citados acima, que compreendem o período de 2010 a 2021, ressaltam a importância do aumento da resiliência das IC contra ataques cibernéticos, que seria uma prioridade do Governo, principalmente em relação a conscientização do risco cibernético. Esses documentos afirmam ainda, que a responsabilidade da proteção das IC será dos administradores e operadores delas, porém eles deverão trabalhar de maneira cooperativa com os órgãos governamentais. O Governo poderá intervir caso ameace a Segurança Nacional.

Como ação decorrente dessa Estratégia Nacional de Segurança Cibernética, em que o Governo se comprometeu em garantir a adoção de uma estrutura regulatória correta a fim de garantir que o risco cibernético fosse gerenciado adequadamente por todas as organizações que fornecem serviços essenciais, como as IC, e os provedores de serviços digitais relevantes, foi laçado em 10 de maio de 2018, os Regulamentos de Rede e Sistemas de Informação *(Network and Information Systems Regulations* (NIS *Regulations*)). O objetivo geral desses Regulamentos é melhorar a segurança das redes e sistemas de informação que são críticos para a prestação de serviços essenciais que, se interrompidos, podem causar sérios danos aos cidadãos, empresas e a infraestrutura crítica nacional. São medidas técnicas e organizacionais para proteger a rede e sistemas de informação. Os regulamentos foram projetados para elevar os padrões de segurança dos setores críticos por meio de regulamentação baseada em resultados, que permite que a abordagem se adapte consistentemente em um ambiente em rápida evolução (RU, 2018b).

Os Regulamentos NIS se aplicam as IC dos setores de transporte, energia, água, saúde e infraestrutura digital. Essas organizações devem adotar medidas adequadas e

proporcionais para garantir a segurança da rede e dos sistemas de informação usados para fornecer seus serviços essenciais, tanto gerenciando riscos quanto minimizando impactos de qualquer perturbação; e notificar a sua Autoridade Competente sobre qualquer incidente que afete negativamente a segurança da rede e dos sistemas de informação utilizados para prestar os seus serviços essenciais, de acordo com os critérios estabelecidos sobre a comunicação de incidentes. Ao notificar um incidente ao CTIR Nacional, este pode intervir diretamente para apoiar o órgão afetado em sua resposta ao incidente, bem como prover suporte pós-incidente. A implementação e aplicação dos Regulamentos NIS são de responsabilidade das Autoridades Competentes designadas. A autoridade designada responsável pelo setor de transportes marítimos, incluindo as empresas de navegação e os terminais portuários, é o Secretário de Estado para Transporte (RU, 2018b).

Esses Regulamentos NIS foram a principal medida adotada pelo Governo do RU para a proteção das IC, pois visam aumentar os seus níveis de SegCiber, e com isso a resiliência. As IC são obrigadas a adotar medidas de segurança adequadas e proporcionais para gerenciar os riscos as suas redes e sistemas de informação, e a notificar incidentes graves ao CTIR Nacional. O NCSC atuará fornecendo conselhos e orientações de SegCiber, e como uma assessoria técnica especializada. Outra característica desses regulamentos é que eles listam as autoridades responsáveis por cada setor das IC.

Em complemento aos Regulamentos NIS, o NCSC desenvolveu, em 2018, a CAF, que consiste em um conjunto de 14 princípios de SegCiber e resiliência, juntamente com orientações sobre o uso e aplicação destes princípios, e destina-se a ser usada por organizações responsáveis por serviços essenciais (IC), com o objetivo de ajudar a organização a alcançar e demonstrar um nível adequado de resiliência cibernética em relação a certas funções essenciais especificadas e desempenhadas por essa organização. Ela também serve para fornecer aos órgãos reguladores das IC (Autoridades Competentes), uma avaliação da SegCiber das IC de seu setor. A CAF possui quatro objetivos de segurança, tendo cada um deles vários questionamentos específicos, totalizando 39 questões. Os objetivos são: Objetivo A – Gerenciar os riscos de segurança; Objetivo B – Proteção contra ataques cibernéticos; Objetivo C – Detecção de eventos de SegCiber; e Objetivo D – Minimização do impacto de incidentes de SegCiber (RU, 2018c).

A CAF fornece uma abordagem sistemática e abrangente para avaliar até que ponto os riscos cibernéticos estão sendo gerenciados pela organização responsável. Destina-

se a ser usado pela própria organização responsável (autoavaliação) ou por uma entidade externa independente, possivelmente um regulador ou uma organização devidamente qualificada atuando em nome de um regulador. Os 39 questionamentos poderão ser respondidos da seguinte forma: "alcançados", "parcialmente alcançados", ou "não alcançados". Ela foi projetada de tal forma, que um resultado no qual todas as 39 respostas sejam avaliadas como "alcançados", indicaria um nível de SegCiber além do nível mínimo exigido (RU, 2018c).

A CAF foi desenvolvida pelo NCSC para complementar os Regulamentos NIS, a fim de melhorar a segurança dos sistemas de rede e de informação no Reino Unido, com um foco particular nas IC, que se comprometidas, poderiam causar danos significativos à economia, à sociedade e ao meio ambiente. Se o conjunto de regras prescritivas da CAF forem totalmente alcançados, resultarão na obtenção do estado final desejável, ou seja, uma boa SegCiber para organizações.

### 3.3 A Legislação do Reino Unido afeta as Infraestruturas Críticas Marítimas

Como o RU é um país insular, e por possuir uma forte história marítima, a maioria de suas conexões com o restante do mundo são realizados pelo mar. A prosperidade e a segurança do país são dependentes do mar. A indústria marítima do RU contribui diretamente com até £ 13,8 bilhões para a economia e indiretamente contribui com mais £ 17,9 bilhões (RU, 2014).

Para que uma Infraestrutura Crítica no RU seja considerada como Marítima, ela deverá estar enquadrada em alguns requisitos, de acordo com o previsto no anexo 2 dos Regulamentos NIS, podendo ser uma Empresa de Navegação, uma Autoridade Portuária, um Operador de uma Instalação Portuária ou um Operador de Serviços de Tráfego de Embarcações de um porto. Por exemplo, uma Empresa de Navegação será considerada como uma ICM, se ela lidar com mais de 5 milhões de toneladas de frete anual total nos portos do RU ou ainda, se ela tiver mais de 30% do frete em qualquer porto individual do RU. Uma Autoridade Portuária, um Operador de uma Instalação Portuária ou um Operador de Serviços de Tráfego de Embarcações de porto, para serem considerados como uma ICM, esse porto ou instalação portuária deverá ter um fluxo anual de passageiros superior a 10 milhões, ou um

volume de carga de mais de quinze por cento do tráfego total de cargas do tipo roll-on roll-off ou lift-on lift-off do RU (RU, 2018b).

As ICM são essenciais para muitos países, mas particularmente para o RU, elas são de vital importância, por ser um país insular. Os Regulamentos NIS especificam claramente quais são os requisitos necessários para que uma organização seja considerada como uma ICM. Tais requisitos são basicamente atrelados a uma geração mínima de receita, quer seja por volume de carga ou passageiros.

Em 2014, o Governo do RU lançou a sua primeira Estratégia Nacional para a Segurança Marítima (*National Strategy for Maritime Security* (NSMS)).

Essa Estratégia foi a primeira tentativa do RU de lidar com uma agenda de segurança marítima, que concebe o domínio marítimo como um sistema complexo de segurança interligado e transnacional. Ela foi um documento marcante na política marítima do país, pois foi o primeiro a incluir as questões de segurança não tradicionais, tais como os crimes azuis (pirataria, contrabando e pesca), a proteção das ICM (portos, navios e rotas comerciais marítimas), o meio ambiente marinho e sustentabilidade. Ela também inaugurou uma nova abordagem de governo e instalou novos mecanismos de governança para lidar com esses desafios (BUEGER; EDMUNDS; EDWARDS, 2021).

Ela incluiu o ataque cibernético à ICM do RU como um dos principais riscos de segurança marítima para o biênio 2014-2015, juntamente com o terrorismo, a interrupção de rotas comerciais marítimas vitais, o transporte de itens ilegais por mar, e o contrabando de pessoas e tráfico humano (RU, 2014).

A NSMS de 2014 do RU foi o primeiro documento estratégico que procurou expor o modo como deveriam ser organizadas as capacidades nacionais para identificar, classificar e enfrentar os desafios de segurança marítima. Ela apontou que um ataque cibernético seria um desses principais desafios.

Em 2017, foi lançada a publicação Código de Prática: Segurança Cibernética para Navios. O Código foi produzido pela Instituição de Engenharia e Tecnologia com apoio do Laboratório de Ciência e Tecnologia de Defesa, e patrocinado pelo Departamento de Transportes. Ele considera os requisitos de SegCiber para navios navegando, atracados ou fundeados, e destina-se a complementar as normas de segurança dos navios e respectivos requisitos, fornecendo orientações adicionais sobre os aspectos de proteção cibernética, fazendo-se uso de princípios em vez de uma legislação nacional para ajudar a promover boas

práticas. Essas medidas devem considerar o tipo do navio, da sua utilização e da natureza das cargas movimentadas. Em função do aumento das vulnerabilidades cibernéticas em razão de avanços na automação e integração de vários sistemas eletrônicos, é de suma importância que os armadores, operadores e comandantes compreendam essas vulnerabilidades e implementem as medidas de segurança apropriadas, a fim de aumentar a resiliência cibernética (RU, 2017).

Essa publicação descreve que um navio é um sistema complexo de engenharia ciberfísica que engloba atividades, sistemas e elementos remotos, como sinais de navegação. O navio possui, basicamente, cinco sistemas principais (instalações de máquinas, sistemas operacionais, sistemas de tecnologia da informação, rádio comunicações e sistemas de navegação) que são usados para fornecer um gama de serviços operacionais e onde a tecnologia exerce um papel cada vez mais importante. Um ataque cibernético em um navio pode resultar em um número de situações indesejáveis, tais como: exposição acidental ou inadvertida de sistemas, aplicativos ou dados sensíveis a usuários não autorizados; a perda de resiliência ou redundância de sistemas; e falhas em sistemas ou processos. Em qualquer situação dessas, elas podem trazer significativas consequências econômicas e da reputação da empresa (RU, 2017). A Figura 4 representa os cinco sistemas básicos de um navio.

A resiliência dos sistemas do navio está intimamente ligada à segurança e quanto maior o risco potencial de segurança, maior o nível de redundância e disponibilidade de sistemas críticos. Esses sistemas são monitorados para fornecer consciência situacional constante com base nos dados do sensor recebidos de vários tipos de sensores. A integridade e disponibilidade de tais dados são, portanto, críticas para a operação segura do navio e seus sistemas, especialmente quando os sistemas são integrados em um sistema de sistemas, cada um interdependente dos outros para aquisição de dados, análise computacional ou atuação física. A compreensão das ligações entre sistemas em nível de dados ou informações é essencial para manter a integridade do sistema geral desses sistemas.

O Código de Prática fornece orientações sobre como desenvolver uma Avaliação de Segurança Cibernética (CSA) e um Plano de Segurança Cibernética (CSP), e como executar o gerenciamento da SegCiber nos navios. A CSA têm como objetivo adotar uma de gestão de riscos para avaliar e mitigar os riscos associados as ameaças que são relevantes para os navios que estão sendo avaliados. Os benefícios de adotar essa avaliação é que os riscos de SegCiber podem ser priorizados, e desta forma, os investimentos podem ser direcionados para os

setores mais deficientes, ou seja, com maiores riscos e impactos. O CSP se baseia no SSP existente, e pode ser um anexo a ele. Os CSP devem abranger as pessoas, processos, aspectos físicos e tecnológicos do navio (RU, 2017).

Esse Código foi publicado especificamente para melhorar a SegCiber a bordo dos navios. Em função da maior utilização de sistemas conectados, os navios estão ficando cada vez mais vulneráveis a um ataque cibernético. Ao se desenvolver a CSA e o CSP, os armadores poderão priorizar seus investimentos nos setores mais críticos de cada navio, e aumentar assim a sua segurança e resiliência cibernética.

Como citado no capítulo anterior, o Código ISPS exige que todos os navios devem ser submetidos a uma Avaliação de Proteção do Navio (SSA), e depois elaborado um Plano de Proteção do Navio (SSP). A relação do CSA e CSP com o Código ISPS, a SSA e o SSP estão ilustrados na Figura 5.

Em 2020 houve a revisão da publicação Código de Prática: Segurança Cibernética para Portos e Terminais 2016, sendo lançado então, o Guia de Boas Práticas: Segurança Cibernética para Portos e Instalações Portuárias. Assim como o Código de Prática: Segurança Cibernética para Navios, o Guia também foi produzido pela Instituição de Engenharia e Tecnologia com apoio do Laboratório de Ciência e Tecnologia de Defesa, e patrocinado pelo Departamento de Transportes. O Guia considera o requisito de SegCiber em portos e instalações portuárias, e destina-se a complementar padrões de segurança dos portos e seus respectivos requisitos, fornecendo orientações complementares sobre os aspectos das medidas de SegCiber estabelecidas, fazendo o uso de princípios, em vez de uma legislação nacional. Essas medidas de SegCiber devem considerar o perfil do porto e suas instalações, seu uso e a natureza das cargas movimentadas. O Guia destina-se a ser utilizado por todos que têm a responsabilidade de proteger um porto/instalação portuária, pessoas, carga, unidades de transporte de carga e armazéns dos riscos de um incidente de segurança cibernético (RU, 2020b).

O Guia de Boas Práticas cita que um porto é um ambiente cibernético complexo que engloba atividades e sistemas terrestres e marítimos, e normalmente, possuem quatro principais tipos de ativos (edifícios, infraestrutura linear, plantas e maquinário, e sistemas de informação e comunicação) que são usados para fornecer uma diversidade de serviços operacionais, onde a tecnologia é amplamente utilizada. Assim como o Código de Prática: Segurança Cibernética para Navios, o Guia também fornece orientações sobre como

desenvolver uma CSA e um CSP, e como executar o gerenciamento da SegCiber só que nos portos e instalações portuárias. As avaliações de segurança formam a base dos planos de segurança para os portos e instalações, que devem abordar os problemas identificados na avaliação e o correto estabelecimento de medidas de segurança de modo a minimizar a probabilidade de uma violação de segurança. É desejável que o CSP se baseie no Plano de Segurança Portuária (PSP) ou Plano de Segurança de Instalação Portuária (PFSP) (RU, 2020b).

De maneira análoga ao Código de Prática: Segurança Cibernética para Navios, foi publicado o Guia de Boas Práticas: Segurança Cibernética para Portos e Instalações Portuárias, só que este está focado na melhoria da segurança e resiliência cibernética dos portos e instalações portuárias. Assim como os navios, os portos e suas instalações são sistemas complexos e altamente interligados e conectados à internet, proporcionando vulnerabilidades.

O Departamento de Transportes do RU, publicou em janeiro de 2019 a publicação Marítimo 2050: Navegando o Futuro. Ela cita que a segurança marítima é, sem dúvida, essencial para a política nacional do Reino Unido. Sem a segurança dos navios, portos e serviços, ou seja, as ICM, a prosperidade e a resiliência do país estará em risco, logo o setor exige, portanto, policiamento e regulamentação nos níveis nacional e internacional. A publicação cita que a evolução da tecnologia têm tornado as ICM cada vez mais vulneráveis e, com isso, mais suscetíveis à ataques cibernéticos. O RU têm se comprometido em liderar o desenvolvimento de normas e regulamentos apropriados e orientação nestes domínios. As empresas responsáveis pelas ICM têm o ônus de proteger e garantir a resiliência contra às ameaças cibernéticas. No entanto, isso estará em sintonia com o governo, que fornece avaliações de ameaças e riscos, regulamentação e orientação para assegurar que, coletivamente, o RU seja um centro de excelência para o fornecimento de soluções de cibersegurança marítima (RU, 2019).

As tecnologias digitais são cada vez mais a espinha dorsal das operações marítimas, pois os proprietários buscam criar eficiência, redução de custos e aumentar a sua SegCiber. O setor de tecnologia de transporte do RU emprega cerca de £ 4 bilhões, por ano, e têm uma estimativa de aumentar esse valor para £ 13 bilhões por ano até 2030. As cadeias de suprimentos e serviços de suporte são sustentados por sistemas de dados e sistemas conectados na internet. As operações portuárias e marítimas podem funcionar independentemente de sistemas conectados (em rede), mas cada vez mais estão

dependentes deles, para operações seguras e eficientes. As vulnerabilidades a esses sistemas podem ser exploradas a partir de uma variedade de Estados e atores não estatais para fins financeiros, disruptivos e violentos (RU, 2019).

A Marítimo 2050 cita o ataque ocorrido em junho de 2017, na empresa A.P. *Moller-Maersk,* maior transportadora de contêineres mundial, que foi vítima de um ataque cibernético causado por um ransomware[18], sendo obrigada a interromper as operações em 76 terminais portuários em todo o mundo, causando perdas estimadas de US$ 200 a 300 milhões e, dessa maneira, demonstrou as vulnerabilidades dos sistemas marítimos conectados ao ataque cibernético. Desta forma, e de modo a permanecer seguro, protegido e resiliente diante das ameaças cibernéticas o Setor de Transportes do RU necessita alcançar alguns objetivos que foram estipulados, tais como a compreensão da ameaça cibernética e as suas vulnerabilidades no setor de transportes marítimos; ser capaz de mitigar os riscos cibernéticos e tomar as medidas apropriadas para proteger os ativos marítimos; poder responder aos incidentes cibernéticos de forma eficaz e garantir que as lições sejam aprendidas; e promover uma mudança cultural, conscientizando o setor marítimo acerca da importância da mentalidade de SegCiber. Para pôr em prática esses objetivos, o Departamento de Transportes criou uma equipe de SegCiber dedicada que tem como missão considerar os aspectos de SegCiber no setor de transporte do RU, além de trabalhar também em estreita colaboração com o NCSC. Este Centro desempenhará um papel de apoio na prestação de aconselhamento e orientação contra um ataque cibernético aos operadores das ICM (RU, 2019).

Como já explicado, os navios e os portos estão cada vez mais conectados e dependentes das tecnologias de informação e da internet, para melhoria e agilidade de processos, bem como para sua eficiência. O incidente com a empresa A.P. Moller-Maersk é um exemplo do que pode acontecer em caso de um ataque cibernético, com a paralização e atraso de toda cadeia de transportes da empresa, ocasionando um prejuízo milionário.

O Setor de Transportes do RU têm buscado melhorar a resiliência cibernética das ICM, com o lançamento de publicações, a orientação e conscientização da necessidade do

[18] *Ransomware,* de acordo com o GDSDI é um tipo de malware, que, por meio de criptografia, impede o acesso a dados computacionais. Para recuperar o acesso, exige-se pagamento de um valor de resgate. Caso o pagamento do resgate não seja realizado, pode-se perder definitivamente o acesso aos dados sequestrados.

aumento da SegCiber das ICM, bem como com a criação da equipe de SegCiber, que trabalhará coordenada com o NCSC, a fim de proteger as ICM do RU de um incidente cibernético.

### 3.4 A Conferência CYBERUK

A *CYBERUK*, conduzido pelo NSCC, é considerada o principal evento de SegCiber do governo britânico. Ela consiste em uma conferência, com palestras e painéis para discussões e debates dos temas cibernéticos da atualidade. A primeira *CYBERUK* ocorreu em 2017, a segunda em 2018, e a terceira em 2019. Em 2020 não houve a conferência em função da pandemia, e em 2021 ela ocorreu de forma virtual. A sua quinta edição, a *CYBERUK* 2022, ocorreu no mês de maio deste ano, na cidade de Newport. Durante os dois dias de evento, participaram mais de 1.500 delegados, entre líderes de SegCiber e profissionais técnicos, dessa forma, fortalecendo a comunidade de SegCiber do Reino Unido[19].

### 3.5 Conclusões Parciais

A partir do ano de 2010, o RU mudou de maneira expressiva a forma como a SegCiber é vista pelo Governo, pela Sociedade e pelas empresas. Eles perceberam a importância da internet na prestação de serviços, no comércio e para as indústrias, com gastos expressivos da população através da internet.

Como decorrência do aumento da conectividade e do uso cada vez maior da internet, houve um aumento do número de casos de ataques cibernéticos, com tendências a aumentar ao longo dos anos. A SegCiber passou a ser considerada como uma ameaça de Risco Um à Segurança Nacional, o nível mais alto. Para enfrentar esse fenômeno, o Governo lançou investimentos elevados para a implantação do Programa Nacional de Segurança Cibernética.

A primeira Estratégia de Segurança Cibernética do país foi publicada em 2011, e elencou a SegCiber como uma prioridade para o Governo, e uma necessidade de estreita cooperação deste com o setor privado para uma correta troca de informações e a gerência das respostas aos ataques cibernéticos.

[19] Conferência Cibernética CYBERUK. Disponível em: <https://www.cyberuk.uk/website/7174/>. Acesso em: 21 jun. 2022.

Com a criação do NCSC, o órgão se tornou o centro de liderança e referência para as questões da SegCiber, além de ser o responsável pela resposta a incidentes cibernéticos através do CTIR Nacional.

A expressão poder cibernético, é muito difundida a partir do lançamento da Estratégia Cibernética Nacional 2022, e marca uma significativa mudança na forma como o Governo utiliza o espaço cibernético, não apenas garantindo a sua segurança nele, mas também poderá ser usado para promover os interesses do país dentro e através desse espaço.

Uma preocupação constante no ambiente cibernético é a escassez de recursos humanos qualificados, onde normalmente, a demanda por habilidades supera a oferta disponível. Para tentar minimizar esse problema, o Governo do RU lançou alguns programas, como o Primeiro Ciber e o Desafio de Cibersegurança, para identificar e inspirar os jovens a seguir uma carreira em SegCiber.

A Estratégia de Segurança Cibernética do Governo: 2022 a 2030 é ousada e ambiciosa, pois seu objetivo central consiste em robustecer as funções críticas do Governo para se contrapor aos ataques cibernéticos até 2025, e garantir a resiliência de todas as organizações governamentais contra métodos de ataque e das vulnerabilidades conhecidas até 2030.

O Governo do RU implementou dois programas que visam conscientizar a população e empresas sobre os perigos cibernéticos, que são o *site* Fique Seguro Online que disponibiliza várias informações e orientações sobre boas práticas cibernéticas e o outro é a campanha Ciber Consciente, que consiste na divulgação por meio das redes sociais e campanhas publicitárias de conselhos a sociedade.

Já a inciativa Essenciais Cibernéticos, é um programa apoiado pelo governo para certificação cibernética de empresas, de modo a garantir o padrão mínimo do país em SegCiber.

O RU criou em 2020 a sua NCF, para agir em prol da Segurança Nacional, mantendo o país seguro e promovendo seus interesses no exterior.

A Conferência *CYBERUK* é realizada anualmente, e é o maior evento de SegCiber, onde são discutidos e debatidos os temas cibernéticos atuais.

O país possui o CPNI, mas que trata de assuntos relativos à segurança física e de proteção pessoal da IC, cabendo ao NCSC a responsabilidade pela proteção das redes de TI das IC, em coordenação com os operadores das IC.

Para auxiliar na proteção de suas IC, há dois programas principais, que são os Regulamentos NIS e a CAF. Os Regulamentos são medidas técnicas e organizacionais que visam elevar os níveis de segurança dos setores críticos. A CAF consiste em um conjunto de princípios de SegCiber e resiliência, que se destinam a ajudar as organizações a alcançar um nível adequado de resiliência cibernética.

As ICM no RU podem ser uma Empresa de Navegação, uma Autoridade Portuária, um Operador de uma Instalação Portuária ou um Operador de Serviços de Tráfego de Embarcações de um porto, dependendo de alguns critérios estabelecidos, tais como volume de carga ou números de passageiros. Um ataque cibernético as ICM foi considerado pela NSMS como um dos principais riscos de segurança marítima do país.

Como decorrência do aumento das vulnerabilidades cibernéticas nos navios, em função de uma maior automação e integração dos vários sistemas eletrônicos, foi lançada a publicação Código de Prática: Segurança Cibernética para Navios, que enumeram os requisitos de SegCiber a serem adotados pelos navios, de modo a complementar as normas de segurança e respectivos requisitos, e consequentemente, aumentar a sua resiliência cibernética.

Em relação aos portos e terminais portuários, a publicação Guia de Boas Práticas: Segurança Cibernética para Portos e Instalações Portuárias fornece os requisitos de SegCiber a serem adotados por eles, de modo a minimizar os riscos de um incidente de segurança cibernético.

O RU por ser um país insular, é totalmente dependente da navegação marítima para realizar seu comércio. A publicação Marítimo 2050: Navegando o Futuro enfatiza que sem a segurança das ICM, a prosperidade e a resiliência do país estará em risco. Ela cita ainda que a crescente evolução tecnológica têm tornado as ICM mais vulneráveis e consequentemente mais propensas a sofrerem ataques cibernéticos.

Como vimos, o Governo do RU têm considerado as ameaças cibernéticas como a mais alta prioridade, e por conta disso, têm buscado aumentar a resiliência de suas IC, inclusive as ICM. Para enfrentá-las, têm investido grandes volumes de recursos, publicado vários documentos normativos, e lançados programas para elevar o nível da SegCiber e para captar recursos humanos necessários a proteção do seu ciberespaço.

# 4 A GOVERNANÇA CIBERNÉTICA BRASILEIRA REFERENTE A PROTEÇÃO DAS INFRAESTRUTURAS CRÍTICAS NACIONAIS, PARTICULARMENTE AS INFRAESTRUTURAS CRÍTICAS MARÍTIMAS, ANTE ÀS AMEAÇAS CIBERNÉTICAS

Este capítulo têm como propósito identificar e analisar as ações de governança cibernética do país, entre elas a legislação e normas brasileira afetas ao ambiente cibernético, as IC e as ICM, e o Exercício Guardião Cibernético (EGC).

## 4.1 A Legislação Brasileira afeta ao Ambiente Cibernético

O Governo Brasileiro começou a se preocupar com a segurança da informação, em 2006, quando foi criado o então Departamento de Segurança da Informação e Comunicações (DSIC), dentro da estrutura do GSI/PR (BRASIL, 2006).

Em 2008, foi aprovada a primeira Estratégia Nacional de Defesa (END) do Brasil, e que instituiu três setores estratégicos e decisivos para a Defesa Nacional, e que deveriam ser fortalecidos, sendo um deles o cibernético. Ela ressalta ainda, que todas as instâncias do Estado deverão contribuir para o incremento do nível de Segurança Nacional, com particular ênfase a várias áreas, e, na área cibernética, destaca-se o aperfeiçoamento dos procedimentos e dispositivos de segurança que contribuam para a redução da vulnerabilidade dos sistemas afetos à Defesa Nacional contra ataques cibernéticos e, caso atacados, que sejam prontamente restabelecidos (BRASIL, 2008b).

Como visto, desde 2008, o Brasil considera o ambiente cibernético como uma possível ameaça para a Defesa Nacional, e por isso foi considerado como um setor estratégico para o país.

No ano seguinte, foi expedida a Portaria nº 45/2009 do GSI/PR, que instituiu o Grupo Técnico de Segurança Cibernética (GT SEG CIBER) com o objetivo de propor diretrizes e estratégias para a SegCiber, no âmbito da Administração Pública Federal (APF). Em seu preâmbulo, a portaria já considerava a crescente utilização de recursos de TIC na prestação dos serviços públicos, o que aumentaria a vulnerabilidade e as tentativas de possíveis ataques cibernéticos às redes governamentais e aos bancos de dados, podendo afetar a APF; a necessidade de assegurar, dentro do espaço cibernético, as ações de segurança da informação como fundamentais para garantir a integridade, a autenticidade, a disponibilidade e a

confidencialidade das informações e comunicações que circulam no âmbito da APF; e a possibilidade real do uso de recursos computacionais visando ações ofensivas contra as redes de computadores de instituições estratégicas dentro do Governo Brasileiro (BRASIL, 2009b). Podemos dizer que a criação do Grupo Técnico foi a primeira ação concreta do país visando a SegCiber, principalmente no âmbito da APF.

Em 9 de novembro de 2009, o Ministério da Defesa (MD) expediu a Diretriz Ministerial nº 0014, que tratava da integração e coordenação dos setores estratégicos da defesa, em que foram definidas as responsabilidades para cada FA. Ao Comando do Exército, coube a responsabilidade pela integração e coordenação do setor cibernético. A portaria citava algumas orientações específicas em relação ao setor cibernético, como a possibilidade de criação de um centro para o desenvolvimento de quaisquer tipos de ações e a concentração de militares das três Forças em um mesmo ambiente de atuação (BRASIL, 2009c). Como ação decorrente dessas orientações específicas, foi ativado em 4 de agosto de 2010, o Núcleo do futuro Centro de Defesa Cibernética, por meio da Portaria Nº 666, de 4 de agosto de 2010, do Comandante do Exército.

O Governo Federal atribuiu a responsabilidade de cada um dos três setores estratégicos para cada uma das FA, ficando o cibernético de responsabilidade do Exército Brasileiro (EB). Para que o EB pudesse desempenhar essa atribuição, ele criou uma nova Organização Militar, incialmente um núcleo de implantação, do futuro Centro de Defesa Cibernética (CDCiber).

Ainda em 2009, foram incluídos como temas dos assuntos a serem tratados na Câmara de Relações Exteriores e Defesa Nacional[20] (CREDEN) do Conselho de Governo, a SegCiber e a segurança para as IC (BRASIL, 2009a).

Como resultado dos trabalhos do GT SEG CIBER, foi lançado em 2010, o Livro Verde: Segurança Cibernética no Brasil (LVSC). O livro tinha como objetivo expressar potenciais diretrizes estratégicas para o estabelecimento de uma futura Política Nacional de Segurança Cibernética, articulando visões de curto (2 - 3 anos), médio (5 - 7 anos), e longo (10 - 15 anos) prazos ao tema, abrangendo, como ponto de partida, os seguintes vetores: Político

[20] Câmara de Relações Exteriores e Defesa Nacional (CREDEN) do Conselho de Governo é órgão de assessoramento com a finalidade de: "I - formular políticas públicas e diretrizes para a área das relações exteriores e defesa nacional; II - aprovar, promover a articulação e acompanhar a implementação dos programas e ações cujas competências ultrapassem o escopo de apenas um Ministério" (Decreto nº 9.819, de 03 de junho de 2019).

e Estratégico, Social, CT&I, Econômico, Ambiental, Legal, Educação, Cooperação Internacional, e a Segurança das Infraestruturas Críticas (MANDARINO; CANONGIA, 2010).

O GT SEG CIBER fez um bom trabalho em prol da SegCiber no país, e consolidou todo esse material no LVSC. A ideia era que as considerações constantes nesse livro, especialmente as diretrizes estratégicas, fossem incorporadas em uma Política Nacional de Segurança Cibernética, mas infelizmente isso não aconteceu, pois, essa publicação nunca foi lançada.

O Decreto nº 7.411/2010, alterou as competências e atribuições do DSIC do GSI/PR, incluindo o planejamento e a coordenação das atividades de SegCiber e Segurança da Informação e Comunicações (SIC) pelos órgãos e entidades da APF; e a operação e manutenção de um Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (CTIR) dos eventos ocorridos nas redes de computadores da APF (BRASIL, 2010a). Com esse Decreto, o DSIC passa a ser o responsável pela SegCiber dos órgãos da APF, e pela implementação de CTIR.

O CDCiber foi ativado em 20 de setembro de 2012, sendo criado dentro da estrutura regimental do Comando do Exército, por meio do Decreto nº 7.809/2012 (BRASIL, 2012b). A sua responsabilidade foi estabelecida através da portaria nº 3.405/MD, que consistia na coordenação e integração das atividades de defesa cibernética, no âmbito do MD (BRASIL, 2012g).

A END sofreu uma revisão e atualização em 2012, em que são destacados os seguintes pontos prioritários para o setor cibernético: o redimensionamento do CDCiber, de maneira a poder evoluir para o Comando de Defesa Cibernética (ComDCiber) das FA; o fomento de pesquisas pesquisa científicas direcionadas para o Setor Cibernético, com o envolvimento das comunidades acadêmicas nacionais e estrangeiras, com vistas à criação da Escola Nacional de Defesa Cibernética; o desenvolvimento da capacitação, o preparo e o emprego dos poderes cibernéticos nos níveis operacional e estratégico, em prol da proteção das infraestruturas estratégicas e das operações conjuntas (BRASIL, 2012c). Já a revisão e atualização no mesmo ano da Política Nacional de Defesa (PND), estabeleceu que para se alcançar o desenvolvimento e a autonomia nacionais, seria essencial o domínio de tecnologias sensíveis, principalmente nos setores estratégicos: espacial, cibernético e nuclear (BRASIL, 2012d).

A END e a PND estabelecem a importância da cooperação nacional e internacional, com participação da academia para desenvolver a pesquisa de novas tecnologias que serão empregadas na SegCiber e na criação de uma escola nacional para o ensino das capacidades cibernéticas, que capacitará os recursos humanos que vão proteger as IC do país. Além disso, elas citam a evolução do CDCiber para o ComDCiber.

O Livro Branco de Defesa Nacional (LBDN), foi lançado pela primeira vez em 2012, e ele também abordou a questão cibernética, e entre as suas premissas sobre o setor cibernético, aponta que a proteção do espaço cibernético engloba muitas áreas, tais como: capacitação, pesquisa científica, doutrina, inteligência, preparo e emprego operacional, e a gestão de pessoas. Compreende, também, a proteção dos seus próprios ativos e a sua capacidade de atuação em rede. O Livro constata ainda que a ameaça cibernética se tornou uma grande preocupação por ameaçar a integridade das IC, que são essenciais à condução e ao controle de diversos sistemas e órgãos relacionados diretamente à segurança nacional (BRASIL, 2012e).

O LBDN, corrobora as diretrizes previstas na END e na PND, e acrescenta a importância da proteção das IC, vitais para o país, das ameaças cibernéticas, que estão ficando cada vez mais complexas.

Em 2012 também, por intermédio da Lei nº 12.737, foram tipificados como crimes os delitos informáticos, principalmente, a invasão de um dispositivo informático alheio. Tal lei ficou conhecida como Lei Carolina Dieckmann, pois esta lei foi publicada logo após a referida atriz ter tido seu celular invadido e fotos íntimas suas expostas na internet (BRASIL, 2012a).

De nada adianta um país se preocupar com a sua SegCiber se não houver leis criminais que possam tipificar uma ataque cibernético como um crime. A Lei nº 12.737/2012 fez exatamente isso.

Ainda em 2012, por meio da Portaria Normativa nº 3.389/MD, foi aprovada e publicada a Política Cibernética de Defesa (PCD). Essa publicação têm o propósito de orientar as ações de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis tático e operacional, no âmbito do MD. São alguns dos objetivos da PCD: garantir o uso do espaço cibernético pelas FA e dificultar ou impedir a sua utilização contra os interesses da Defesa Nacional; capacitar recursos humanos necessários à condução das atividades cibernéticas; contribuir para a segurança das redes de computadores da APF, no tocante à SegCiber. Além disso, a PCD têm uma diretriz que determina que o MD faça a concepção e a implantação do

Sistema Militar de Defesa Cibernética (SMDC), que será guarnecido por militares das FA e civis. Há uma outra diretriz para que seja realizado o levantamento das infraestruturas críticas de informação associadas ao setor cibernético, de maneira que possa contribuir com a formação de uma consciência situacional visando às atividades de Defesa Cibernética. Essa diretriz determina ainda, o estabelecimento dos critérios de risco, inerentes a cada um dos ativos de informação, para que possa ser realizado o seu correto gerenciamento, reduzindo assim a possibilidade de riscos às IC de interesse da Defesa Nacional a níveis que sejam aceitáveis (BRASIL, 2012f).

O SMDC é um conjunto de instalações, doutrinas, equipamentos, tecnologias, procedimentos, pessoal e serviços essenciais para a realização das atividades de defesa no Espaço Cibernético, bem como dificultando ou impedindo a sua utilização contra os interesses da Defesa Nacional. Ao SMDC também cabe a coordenação e integração da proteção das IC de interesse da Defesa Nacional, definidas pelo MD. O órgão central do SMDC é o CDCiber. O CDCiber manterá um canal técnico para integração e coordenação com os órgãos envolvidos nas atividades de Defesa Cibernética (CERT.br, CTIR Gov, órgãos de Defesa/Guerra Cibernética das FA, Agências Governamentais, Ministérios, APF e outros) (BRASIL, 2014b). Com a evolução do CDCiber para o ComDCiber, este passou a ser o órgão central do SMDC.

A PCD e o SMDC têm um foco na Defesa e na Guerra Cibernética, no viés militar das ações da Defesa Nacional. Essas atividades serão executadas pelas FA, e pelo órgão central do SMDC. Essa estrutura também contribui com a SegCiber dos órgãos da APF e das IC.

A Lei nº 12.965/2014, que ficou conhecida como a Lei do Marco Civil da Internet, instituiu os princípios, garantias, direitos e deveres para o uso da Internet no Brasil (BRASIL, 2014a). Essa lei complementa a Lei nº 12.737/2012, pois enquanto aquela tipifica o crime cibernético, esta estabelece os direitos e deveres do uso da internet no país.

A Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF - 2015/2018, lançada em 2015, representa uma importante ferramenta a fim de melhorar a segurança e a resiliência das IC e dos serviços do país, e têm como finalidade expor as diretrizes estratégicas para o desenvolvimento da SIC e da SegCiber no âmbito da APF, otimizando os recursos dos diversos atores envolvidos, e, dessa forma, diminuindo a exposição aos riscos existentes (BRASIL, 2015).

Essa Estratégia foi o passo inicial do Governo Federal em termos de ações, metas e objetivos estratégicos a serem cumpridos pelos órgãos da APF em relação à SIC e à SegCiber, buscando o fortalecimento dos ativos de informações e das IC do país.

Em 2016, houve a revisão dos documentos estratégicos da PND e da END, sem mudanças significativas em relação ao ambiente cibernético. Destacam-se os seguintes pontos principais: esta versão da PND cita que a defesa e a segurança do espaço cibernético merecem uma atenção especial, e a necessidade da conclusão da estrutura do SMDC. Ela cita ainda a importância, em todas as instâncias do Estado, do aprimoramento da SegCiber, com ênfase na proteção das Estruturas Críticas Nacionais (BRASIL, 2016a, 2016b).

A Estratégia Nacional de Inteligência (ENINT) foi publicada em 2017. Dentre os seus Objetivos Estratégicos, há dois relacionados ao campo cibernético, sendo um relativo à ampliação da capacidade da Inteligência Cibernética do Estado, visando a obtenção de dados, e outro para a promoção da qualificação técnica de recursos humanos, de modo a ampliar a proteção e a exploração de dados no campo cibernético (BRASIL, 2017). A ENINT visa a exploração cibernética, com a qualificação de pessoal e a obtenção dos dados de inteligência cibernética.

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, estabeleceu os procedimentos acerca do tratamento dos dados pessoais, inclusive aqueles disponíveis nos meios digitais, de modo a garantir a proteção dos direitos fundamentais de liberdade e de privacidade. Ela destaca a segurança como um dos princípios mais importantes no tratamento dos dados pessoais e exige que organizações estipulem as medidas de segurança técnicas e administrativas necessárias para a proteção de tais dados contra quaisquer incidentes (BRASIL, 2018a).

A Política Nacional de Segurança da Informação (PNSI) foi publicada em 2018. De acordo com essa Política, a segurança da informação engloba assuntos relacionados à segurança e defesa cibernética, a proteção e segurança física dos dados das organizações, e as ações que assegurem, a confidencialidade, a disponibilidade, a integridade, e a autenticidade das informações. A PNSI prevê, além da elaboração da Estratégia Nacional de Segurança da Informação (ENSI), alguns Planos Nacionais, que servirão para nortear a implementação de ações para a cibersegurança no país. A ENSI, a ser elaborada pelo GSI/PR, será composta pelos seguintes cinco módulos: “1– segurança cibernética; 2– defesa cibernética; 3– segurança das infraestruturas críticas; 4– segurança da informação sigilosa; e

5– proteção contra o vazamento de dados". Entre os principais objetivos apresentados na PNSI, destacam-se: o incentivo da formação e da qualificação de recursos humanos afetos à área; a necessidade do contínuo aprimoramento do arcabouço legal e normativo; a orientação de ações ligadas à segurança das informações das IC; e o fortalecimento da mentalidade de segurança da informação dentro da sociedade brasileira. Esta Política determina que todos os órgãos e entidades inseridas na APF devam implementar dentro de suas estruturas uma equipe de prevenção, tratamento e resposta a incidentes cibernéticos (ETIR), em coordenação com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov). A PNSI designa o GSI/PR como sendo o responsável dos temas afetos à segurança da informação, e estabelece que a governança da segurança da informação compete à alta administração de cada órgão e entidade da APF (BRASIL, 2018c).

A PNSI foi fruto de um extenso trabalho do GSI/PR, que coordenou um Grupo de Trabalho Interministerial (GTI) para a sua elaboração, com amplo debate e participação de diversos ministérios e entidades. Após a finalização da proposta pelo GTI, ela ainda foi submetida a várias rodadas de reuniões bilaterais, a fim de permitir que ela fosse amplamente analisada e pudesse receber as contribuições de diversos especialistas de vários setores envolvidos e interessados nesse tema[21].

A PNSI também impulsionou a difusão e as discussões sobre o tema cibernético na sociedade e dentro do próprio Governo (BRASIL, 2020a).

Podemos dizer que a publicação da PNSI foi a primeira grande mudança em termos do arcabouço legal brasileiro em se tratando de segurança da informação, e consequentemente da defesa e da SegCiber. Como visto nos parágrafos anteriores, ela estabeleceu diretrizes e um modelo de governança para que fosse possível a coordenação nacional e a integração das atividades de segurança da informação, bem como evitar superposições e ou redundâncias das ações entre os órgãos envolvidos, em um ambiente que teve um aumento significativo do uso da Tecnologia da Informação (TI), e consequentemente, do aumento crescente de ataques cibernéticos.

Em 2018, foi publicada também a Estratégia Brasileira para a Transformação Digital (E-Digital), que consiste em ações de longo prazo, visando a economia digital. Ela cita que o Brasil têm realizado avanços na área de defesa cibernética nos últimos anos, como

[21] Disponível em: <https://www.gov.br/gsi/pt-br/assuntos/dsi/politica-nacional-de-seguranca-da-informacao-pnsi>. Acesso em: 24 mai. 2022.

exemplos a priorização do tema na END, e a criação do ComDCiber. Porém é ressaltada a necessidade contínua de investimentos na área de defesa e SegCiber, particularmente na formação de recursos humanos especializado e em pesquisa e desenvolvimento, de forma a garantir a autonomia tecnológica nacional nessa área. A E-Digital aponta como os maiores desafios o estabelecimento de uma estrutura institucional adequada, e a formulação de uma estratégia nacional abrangente, com um foco especial na proteção das IC. A cooperação internacional, é citada como essencial para a prevenção e as respostas aos crimes cibernéticos, seja por meio de acordos de cooperação, intercâmbios de recursos humanos ou a troca de informações estratégicas (BRASIL, 2018d). A E-Digital ressalta bastante a importância do trabalho cooperativo na área cibernética, principalmente na formação de mão de obra e na pesquisa científica, de modo a garantir que o Brasil possa ser autônomo e respeitado no cenário internacional.

Como previsto na PNSI, a futura ENSI será composta por cinco módulos, e o GSI/PR elegeu a SegCiber como o primeiro módulo a ser elaborado, pois essa área foi considerada a mais importante e crítica no momento. Desta forma, em 05 de fevereiro de 2020, foi lançada primeira E-Ciber (BRASIL, 2020a).

Nela estão contidas as principais ações pretendidas pelo Governo Federal, na área da SegCiber para o quadriênio 2020-2023. Ela foi elaborada da mesma forma que a PNSI, ou seja, foi amplamente discutida e debatida em um GTI, coordenado pelo GSI/PR, durante 07 meses de trabalhos, onde foram analisadas as estratégias de outros países e de um diagnóstico da SegCiber interna do país. A E-Ciber contém três Objetivos Estratégicos que serviram para que fossem estabelecidas as ações estratégicas do país visando a SegCiber, e são eles: “1– Tornar o Brasil mais próspero e confiável no ambiente digital; 2– Aumentar a resiliência brasileira às ameaças cibernéticas; e 3– Fortalecer a atuação brasileira em segurança cibernética no cenário internacional”. Em relação às Ações Estratégicas, foram estabelecidas dez ações, e são elas: “1– Fortalecer as ações de governança cibernética; 2– Estabelecer um modelo centralizado de governança no âmbito nacional; 3– Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade; 4– Elevar o nível de proteção do Governo; 5– Elevar o nível de proteção das Infraestruturas Críticas Nacionais; 6– Aprimorar o arcabouço legal sobre segurança cibernética; 7– Incentivar a concepção de soluções inovadoras em segurança cibernética; 8– Ampliar a cooperação internacional do Brasil em Segurança cibernética; 9– Ampliar a parceria,

em segurança cibernética, entre setor público, setor privado, academia e sociedade; e 10 – Elevar o nível de maturidade da sociedade em segurança cibernética" (BRASIL, 2020a).

A E-Ciber destaca a necessidade de redimensionamento da estrutura do GSI/PR de modo a possibilitar sua atuação em âmbito nacional, como o coordenador estratégico da SegCiber do país, e que para isso ocorra, é necessária a promulgação de uma lei específica que contenha atribuições e regule ações dessa área temática no país (BRASIL, 2020a).

De acordo com o *National Cybersecurity Strategies Repository* da ITU, mais de cem países do mundo já possuem suas Estratégias Nacionais de Segurança Cibernética, e dentre os países da América Latina e Caribe, o Brasil foi o 12º país a promulgar sua Estratégia (ITU, 2022).

Segundo a *European Union Agency for Cybersecurity* (ENISA), uma Estratégia Nacional de Cibersegurança (NCSS) é um documento que contém as ações que deverão ser executadas a fim de melhorar a segurança e a resiliência cibernética das infraestruturas e serviços nacionais. É um documento de alto nível, do tipo *top-down*, e que contém os objetivos e as prioridades nacionais que deverão ser alcançadas dentro de período estabelecido[22].

Conforme afirma Hurel (2021), a E-Ciber foi criticada por não possuir claramente as metas a serem alcançadas, nem tampouco prever formas de acompanhamento das ações estratégicas estipuladas, e nem indicadores, e com isso ela seria apenas "uma carta de boas intenções do governo brasileiro".

O Governo Federal considerou a área de SegCiber como sendo a mais importante no momento, e por isso ela foi priorizada. Como dito no parágrafo anterior, o Brasil foi o 12º país da América Latina e Caribe a promulgar a sua E-Ciber, mesmo tendo considerado a área cibernética como um setor estratégico desde 2008. Apesar de seu lançamento tardio, ela estava sendo muito esperada, pois as ameaças cibernéticas estão cada vez presentes no dia a dia das instituições, inclusive nos órgãos da APF, e por isso eles necessitavam de orientações acerca das ações pretendidas pelo Governo Federal, na área da SegCiber, de modo a tornar o país mais confiante e resiliente às ameaças cibernéticas. Porém a E-Ciber precisava ser mais clara em relação as metas a serem atingidas e estipular mecanismos de acompanhamento das ações. É necessário redimensionar a estrutura do GSI/PR para que ele possa atuar em nível nacional, como coordenador estratégico da SegCiber do país.

[22] Disponível em: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies>. Acesso em: 24 mai. 2022.

Segundo Fontenele, Diretor do Departamento de Segurança da Informação (DSI), o GSI/PR já concluiu a elaboração da minuta da Política Nacional de Segurança Cibernética do país, que será lançada por meio de um projeto de lei. Essa minuta foi enviada para apreciação da Subchefia de Assuntos Jurídicos da Casa Civil, em Novembro de 2021, e ainda tramitará por outros órgãos competentes, para depois então, ser enviada para tramitação no Legislativo[23].

Em maio de 2021, foi promulgada a Lei nº 14.155, que tornou maios rigorosas as penas para crimes cibernéticos, tais como crimes de violação de dispositivo informático, estelionato e furto cometidos de forma eletrônica ou pela internet (BRASIL, 2021b).

### 4.2 A Legislação Brasileira afeta às Infraestruturas Críticas

Em fevereiro de 2008, a segurança para as IC, incluindo serviços, foi incluída dentre as atribuições da CREDEN, do Conselho de Governo (BRASIL, 2008a).

A END de 2008 ressalta que todas as instâncias do Estado deverão contribuir para o incremento do nível de Segurança Nacional, com ênfase em várias áreas, entre elas as medidas para a segurança das áreas de IC, em especial no que se refere aos setores de transportes, de energia, de água e de telecomunicações. Ela cita ainda, que o GSI/PR será o responsável pelo trabalho de coordenação, avaliação, monitoramento e redução de riscos dessas medidas (BRASIL, 2008b).

Apesar das iniciativas anteriores, podemos dizer que o primeiro grande passo dado no país em relação a segurança das IC ocorreu com a publicação da Portaria nº 31/2010, do GSI/PR, na qual foi criado o Núcleo de Segurança de Infraestruturas Críticas, dentro da estrutura do próprio GSI/PR. Esse Núcleo tinha o objetivo de identificar as demandas necessárias para o efetivo desenvolvimento das atividades de segurança das IC do país, em cooperação com os órgãos e entidades dos setores público e privado (BRASIL, 2010b).

Segundo Capella (2022), há uma falta de nivelamento de SegCiber e gerenciamento de riscos entre as diversas IC brasileiras, enquanto algumas apresentam um elevado grau de preparação, outras estão totalmente despreparadas, além disso, muitas delas possuem sistemas e dispositivos industriais desatualizados. Ele acrescenta, ainda, que não existe um protocolo padrão de defesa cibernética que possa ser aplicado em todos os setores de maneira efetiva, mas poderiam ser implementadas imediatamente algumas importantes

[23] FONTENELE, Coronel Marcelo Paiva. Disponível em: <https://teletime.com.br/18/11/2021/gsi-envia-minuta-de-politica-nacional-de-seguranca-cibernetica-a-casa-civil/>. Acesso em: 23 jul. 2022.

recomendações, de modo a elevar o nível de SegCiber, tais como o estabelecimento de padrões básicos consagrados de higiene cibernética[24], a divulgação de dados transparentes e a responsabilização dos operadores das IC (CAPELLA, 2022).

A END (2016b) possui a Estratégia de Defesa nº 1 (ED-1), cujo título é o Fortalecimento do Poder Nacional, e dentre as suas Ações Estratégicas de Defesa (AED), a de número 2 (AED-2), estabelece que deverá haver contribuição para o aumento do nível de segurança das Estruturas Críticas, particularmente dos setores de água, energia elétrica, transporte, combustíveis, comunicações, entre outros (BRASIL, 2016b).

Entre os objetivos da PNSI, há um que estabelece que deverão ser orientadas ações para a segurança das informações das IC (BRASIL, 2018c).

A primeira PNSIC do país, foi lançada em 2018, e ela têm a finalidade de garantir a resiliência e a segurança das IC do País, bem como a continuidade da prestação de seus serviços. A PNSIC designa o GSI/PR como sendo o responsável por realizar o acompanhamento dos assuntos pertinentes às IC no âmbito da APF. Nesta Política constam seis objetivos, sendo os seguintes os que se destacam: a prevenção de quaisquer interrupções das atividades de IC ou, a redução de impactos em caso de sua ocorrência; a elaboração de diretrizes para a salvaguarda das IC, indispensáveis à Segurança Nacional; a integração dos dados referentes às ameaças e a gestão de riscos; o levantamento das possíveis relações de interdependência entre as IC; e o desenvolvimento de uma mentalidade sobre a necessidade da segurança das IC. Em relação as suas diretrizes, as principais são: a integração da PNSIC com as outras políticas de Estado; a cooperação entre todos os órgãos e entidades, de quaisquer esferas, nas ações necessárias à manutenção da segurança das IC; a identificação junto ao Sistema Brasileiro de Inteligência, de possíveis ameaças que possam comprometer o funcionamento das IC; a desejável cooperação e parcerias entre os setores privado e público, a fim de elevar o nível de segurança das IC; o incentivo à cooperação com organizações internacionais e nacionais, visando o aprimoramento da segurança das IC; e a contínua atualização dos meios de segurança das IC, em função da constante evolução tecnológica e doutrinária (BRASIL, 2018b).

[24] higiene cibernética refere-se às etapas que os usuários de computadores e outros dispositivos podem realizar para melhorar sua segurança on-line e manter a integridade do sistema. Disponível em: <https://www.kaspersky.com.br/resource-center/preemptive-safety/cyber-hygiene-habits>. Acesso em: 24 mai. 2022.

A PNSIC é composta de três instrumentos básicos, sendo eles a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC); o Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC); e o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas (SIDSIC) (BRASIL, 2018b). A ENSIC já foi publicada e será tratada mais adiante do trabalho. O PLANSIC ainda está em elaboração e o SIDSIC está em fase de desenvolvimento.

A PNSIC foi a primeira legislação específica para a proteção exclusiva das IC, de forma a garantir a sua resiliência e segurança. Essa Política é a primeira parte de um conjunto de normas afetas as IC, que são a ENSIC, o PLANSIC e o SIDSIC.

É de responsabilidade do GSI/PR, o acompanhamento de assuntos pertinentes às IC, principalmente aqueles relacionados à avaliação dos riscos, conforme previsto na Lei 13.844/2019 (BRASIL, 2019a). De acordo com subsídios recebidos do GSI/PR, este órgão está desenvolvendo o SIDSIC, que permitirá um melhor assessoramento ao Presidente da República e ao Ministro-Chefe, caso sejam instaurados gabinetes de crises. A previsão é que esse sistema esteja em operação ainda este ano.

A ENSIC foi lançada em 2020. Nela estão contidas as ações mais importantes a serem adotadas de modo a assegurar a continuidade da prestação de serviços, fundamentais para o funcionamento do país. A ENSIC estabelece os princípios básicos para a segurança das IC, e aponta os principais desafios a serem vencidos, bem como possui eixos estruturantes e objetivos e iniciativas estratégicas, que servirão de orientação para a elaboração do PLANSIC, que será a fase das ações da implementação da PNSIC. Ela possui quatro princípios, quatro eixos estruturantes, quatorze objetivos estratégicos e vinte e nove ações estratégicas. Para que os objetivos e as ações sejam cumpridas, diversos atores envolvidos com a segurança das IC deverão formular ações que serão inseridas no PLANSIC, ora em elaboração (BRASIL, 2020a).

Complementando a PNSIC, foi lançada a ENSIC na qual define claramente as principais ações que devem ser executadas para a correta implementação da PNSIC, bem como os resultados a serem alcançados. A ENSIC é a referência básica para a elaboração da futura PLANSIC.

O GSI/PR, a fim de facilitar a sua atribuição em relação às IC, instituiu, no âmbito da CREDEN do Conselho de Governo, Grupos Técnicos de Segurança de Infraestruturas Críticas nas seguintes áreas: energia, transporte, águas, comunicações e finanças. Cada um desses

Grupos Técnicos são compostos por representantes de diversos órgãos e entidades afetos a cada área, além de especialistas que poderão ser convidados. As atribuições de cada Grupo Técnico estão relacionadas ao contínuo aperfeiçoamento, identificação e classificação das IC, identificação das possíveis ameaças e vulnerabilidade e pela proposição de possíveis medidas de controle para a redução dos riscos (BRASIL, 2020a).

Após a publicação da ENSIC, duas novas áreas foram incluídas além das citadas no parágrafo anterior, que foram as áreas de Biossegurança/Bioproteção e a de Defesa, totalizando assim, 07 áreas prioritárias para o Governo.

Segundo informações recebidas do GSI/PR, estão sendo realizadas reuniões e estudos, afetos às sete áreas prioritárias, desenvolvidos pelos treze Grupos Técnicos multidisciplinares, com objetivos de identificar as IC de cada setor; identificar as ameaças, vulnerabilidades e medidas de contingência para cada IC; realizar a análise de riscos de cada IC; elaborar um Diagnóstico Nacional de cada Setor; e analisar as interdependências existentes entre as IC identificadas. A Figura 3 apresenta os Grupos Técnicos de Segurança de Infraestruturas Críticas das várias áreas criadas pelo governo.

Não há, ainda no país, um órgão dedicado à segurança das IC, porém alguns setores estão adotando medidas para o enfrentamento desse problema. Como exemplo disso, podemos citar a expedição de uma resolução normativa pela Agência Nacional de Energia Elétrica, em que são estabelecidas algumas diretrizes para a atuação em SegCiber e alguns itens mínimos que deverão ser incluídos nas políticas de segurança cibernética a serem adotadas pelo setor de energia elétrica (CAPELLA, 2022).

Para que seja analisado os possíveis riscos de uma IC, são necessários dois levantamentos prévios: das ameaças potenciais ou reais, com base em vários fatores; e das vulnerabilidades, que podem ser relacionadas aos sistemas de proteção, a estrutura física, aos processos e operações que possam ser alvos de eventos adversos. Dessa forma, será possível que seja realizada uma avaliação de como as possíveis ameaças podem explorar as vulnerabilidades e, assim determinar o nível do risco, sua frequência de ocorrência ou probabilidade, e os possíveis impactos ou consequências do evento (BRASIL, 2020a).

A maioria das IC do país são de propriedade ou operadas pelo setor privado. Desta forma, é necessária uma grande cooperação entre o Governo Federal e este setor, a fim de que haja uma união de esforços na proteção e resiliência das IC. Para que essa cooperação ocorra, é imprescindível o compartilhamento de informações entre eles, respeitando é claro,

a privacidade, a liberdade e a necessidade de sua salvaguarda. Esse compartilhamento de informações será útil na formulação de políticas relacionadas as questões de segurança e ao treinamento de recursos humanos especializados (BRASIL, 2020a).

As IC são importantíssimas para os governos, as economias, e as sociedades. Por este motivo, a sua segurança e sua resiliência determinam o grau em que os países podem ser afetados, quer sejam por desastres naturais, por acidentes e/ou por ataques deliberados. Outro fator importante das IC, é a sua capacidade de resposta e recuperação após a ocorrência de tais acontecimentos. Logo, deve haver um investimento preventivo em segurança das IC, visando a sua preservação ou restabelecimento de seus serviços. Os recursos públicos necessários para o reparo de uma IC, após a ocorrência de um desastre, serão expressivos. Dessa forma, o Governo possui um importante papel no grau de resiliência das IC, estimulando a implementação de medidas para a redução de riscos pelos proprietários e/ou operadores dessas IC, e o financiamento de atividades para fomentar o aumento da conscientização das pessoas envolvidas em relação aos riscos e a medidas de resiliência (BRASIL, 2020a).

A correta identificação das IC é de suma importância para que sejam definidos os possíveis riscos e os graus de ameaças associados a cada um dos riscos, bem como as vulnerabilidades de cada IC. O GSI/PR têm conduzido esse trabalho, mas ainda não foi completamente finalizado. A cooperação e troca de informações e experiências entre o governo e os operadores das IC, é de vital importância para aumentar a segurança e resiliência, e diminuir o tempo de respostas aos incidentes.

Em 2021, o Governo Federal promulgou a lei que institui a Rede Federal de Gestão de Incidentes Cibernéticos (REGIC), conforme estava prevista na PNSI. Esta rede têm a participação obrigatória dos órgãos e das entidades da APF, e é facultativa, através de adesão, das empresas públicas e das sociedades de economia mista federais e das suas subsidiárias. O DSI do GSI/PR é o coordenador da Rede, por meio do CTIR Gov. A finalidade desta rede é a melhoria da coordenação dos seus órgãos componentes, a fim de aumentar a resiliência em SegCiber de seus dados. Entre os seus objetivos, destacam-se o compartilhamento dos alertas, vulnerabilidades, ataques e medidas de prevenção, tratamento e resposta cibernéticos, e o incremento da cooperação entre todos os participantes da Rede (BRASIL, 2021c).

Esse Decreto institui ainda, alguns deveres para as agências reguladoras, de modo que elas passem a ter responsabilidade sobre as IC de seus setores regulados, e assim melhorar a SegCiber delas, tais como: a designação de uma equipe de coordenação setorial

(ETIR Setorial)[25]; a identificação das equipes principais[26] das áreas mais importantes de seu setor regulado; notificação ao CTIR Gov, por meio da equipe de coordenação setorial, sobre incidentes cibernéticos de maior impacto, das entidades sob a sua regulação; análise dos riscos cibernéticos que comporão os planos setoriais de gestão de incidentes cibernéticos de seu setor regulado; e realizar a identificação das IC de suas áreas reguladas que possam ser consideradas relevantes para a SegCiber nacional. Essas deverão ser implementadas até dezoito meses, a partir da data de publicação do Decreto, ou seja, até janeiro de 2023 (BRASIL, 2021c).

A REGIC foi uma iniciativa importante para a proteção das IC, pois além de dar responsabilidades as Agências Reguladoras dos setores, também obrigou que os órgãos e as entidades da APF participassem da referida rede, e os demais participam por meio de adesão. A criação das ETIR Setoriais, que nada mais são do que uma ETIR específica relacionada a cada um dos setores das IC, tiveram o propósito de elevar o nível de proteção das IC. A troca de informações afetas aos incidentes cibernéticos, entre as ETIR Setoriais e o CTIR Gov, torna-se obrigatória, e com isso há um aumento da cooperação entre todos os atores envolvidos, aumentando a segurança e diminuindo o respectivo tempo de resposta.

### 4.3 As Legislação afeta às Infraestruturas Críticas Marítimas

Como citado no capítulo 1, o país não possui uma definição clara para o que sejam ICM, mas o trabalho do PTD/2021 as definiu como: “Instalações, serviços, bens e sistemas marítimos cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade”. (Brasil, 2021e)

Acordo subsídios recebidos do GSI/PR, as ICM foram identificadas através dos trabalhos realizados por dois Grupos Técnicos de Segurança de Infraestruturas Críticas coordenados pelo GSI/PR: no Setor de Transportes Aquaviários (Portos e Terminais) e no Setor de Petróleo, Gás Natural e Biocombustíveis (Unidades de Exploração e Produção Marítimas -

[25] Equipe de Coordenação Setorial - ETIR das agências reguladoras que coordenará as tarefas de segurança cibernética e centralizará as notificações de incidentes do seu setor regulado, ou seja, é uma ETIR específica relacionada a cada setor das IC. Decreto nº 10.748, 16 de julho de 2021.

[26] equipes principais - ETIR de entidades, privadas ou públicas, que tem a responsabilidade sobre os ativos de informação, principalmente aqueles relativos aos serviços das IC. Decreto nº 10.748, 16 de julho de 2021.

UEP). Porém a relação dessas Infraestruturas é considerada de caráter sigilosa pelo GSI/PR, não podendo ser divulgada, mas em termos quantitativos, foram classificadas, como ICM, 29 Portos/Terminais (entre públicos e privados), de um total de 235 estudados, e 23 UEP Marítimas, de um total de 111 estudadas. Dessa maneira, o Brasil possui hoje 52 ICM, sendo 29 Portos/Terminais e 23 UEP Marítimas.

Como o Brasil é Estado Membro da Organização Marítima Internacional (OMI) e ratificou suas Convenções, ele passou a ter obrigações e compromissos com essa Organização, com os outros países membros e com a comunidade marítima internacional[27].

A OMI lançou, desde Julho de 2004, o Código Internacional de Proteção de Navios e Instalações Portuárias (Código ISPS). Esse Código estabelece a base de um regime de segurança obrigatório para o transporte internacional marítimo. Ele é dividido em duas seções, Parte A e Parte B. A Parte A descreve requisitos detalhados relacionados à proteção marítima e portuária, em que os Governos, Autoridades Portuárias e as empresas de navegação devem seguir. A parte B fornece uma série de orientações e recomendações sobre como atender aos requisitos e obrigações estabelecidos na Parte A (OMI, 2004).

O Código ISPS estabelece que alguns tipos de navios[28] devem ser submetidos a uma Avaliação de Proteção do Navio (SSA), a fim de verificar se eles estão cumprindo as disposições da Parte A do Código. A SSA identificará os aspectos específicos do navio e as ameaças e potenciais vulnerabilidades. Após isso, deverá ser elaborado um Plano de Proteção do Navio (SSP) (OMI, 2004).

A OMI, através do Comitê de Facilitação e do Comitê de Segurança Marítima, considerou, em 2017, que era necessário elevar a conscientização sobre as ameaças e vulnerabilidades cibernéticas, quando então, elaborou Diretrizes sobre a gestão do risco cibernético marítimo. Essas diretrizes fornecem recomendações de alto nível sobre gerenciamento de riscos cibernéticos marítimos, a fim de proteger o transporte marítimo contra ameaças e vulnerabilidades cibernéticas relacionadas à digitalização, integração e

[27] Brasil e a Organização Marítima Internacional. Disponível em: <https://www.marinha.mil.br/dhn/?q=pt-br/omi>. Acesso em: 28 jun. 2022.

[28] embarcações de passageiros, embarcações de carga (com arqueação bruta igual ou superior a 500), unidades móveis de perfuração marítimas, embarcações de Apoio Marítimo e conjuntos integrados de barcaças (com arqueação bruta igual ou superior a 500). Disponível em: <https://www.marinha.mil.br/dpc/sites/www.marinha.mil.br.dpc/files/NORMAM-01-DPC_Mod%2047.pdf>. Acesso em: 28 jun. 2022.

automação de processos e sistemas no transporte[29]. Ainda em 2017, durante a 98ª sessão, o Comitê de Segurança Marítima da OMI aprovou a Resolução MSC.428(98), que trata da Gestão de Riscos Cibernéticos Marítimos em Sistemas de Gestão de Segurança. Essa resolução incentiva que os riscos cibernéticos sejam adequadamente abordados nos sistemas de gerenciamento de segurança existentes, pelos administradores, até a primeira verificação anual do Documento de Conformidade da empresa, após 1 de janeiro de 2021 (OMI, 2017).

A Diretoria de Portos e Costas (DPC), como representante da Autoridade Marítima Brasileira (AMB), internalizou essa Resolução nas Normas da Autoridade Marítima (NORMAM), especificamente na NORMAM-01/DPC, em que prevê que o Sistema de Gerenciamento de Segurança (SGS) dos navios deverá constar, entre outros itens, de uma abordagem dos riscos cibernéticos, na primeira verificação anual do documento de conformidade da empresa, a partir de 1 de janeiro de 2021 (BRASIL, 2005).

O Brasil possui uma Política Marítima Nacional (PMN), publicada em 1994, e por ser muito antiga, não trata do ambiente cibernético (BRASIL, 1994). A PMN encontra-se em revisão, por meio de um GTI instituído pelo Presidente da República (BRASIL, 2021a). O país não possui uma Estratégia Marítima, em que pudessem constar orientações de SegCiber para o setor marítimo.

Em que pese o Brasil ser membro da OMI, e adotar suas convenções e resoluções, e as ter inserido nas NORMAM, não há nenhuma outra norma ou regra nacional a ser adotada especificamente pelas ICM operadas no país.

### 4.4 O Exercício Guardião Cibernético

O EGC é um exercício cibernético colaborativo, anual, conduzido pelo ComDCiber, com a participação de civis e militares, que envolve a proteção cibernética, e têm o propósito de contribuir com o aumento da resiliência cibernética dos principais setores estratégicos do país, principalmente, as IC. Ele é considerado o maior exercício de defesa cibernética do hemisfério sul, e consiste na criação de um ambiente realista para que as IC participantes possam efetivamente realizar a proteção de seus sistemas de TI de ataques cibernéticos, e, dessa forma, aperfeiçoar e aumentar sua resiliência cibernética. Durante o exercício são

[29]Disponível em: <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx>. Acesso em: 03 jun. 2022.

criados desafios cibernéticos simulados, que são apresentados aos participantes, que normalmente são pessoas das áreas de TI e jurídica. Esses desafios estão inseridos em diversas áreas de conhecimento, tais como: Redes, Programação, Exploração Web, Criptografia e Forense Computacional, e seguem uma escala crescente de dificuldade, desde o nível iniciante até o nível mais avançado. Então, diante do problema apresentado, eles devem tomar decisões considerando o ambiente simulado do exercício e a colaboração interagências na mitigação das possíveis consequências[30].

O primeiro EGC, o EGC 1.0, ocorreu em 2018, e contou com 26 organizações e 106 participantes, e abrangeu os setores da defesa, nuclear e do governo. O EGC 2.0 ocorreu em 2019, com 41 organizações e 215 participantes, e além dos setores do EGC 1.0, contou ainda com os setores de telecomunicações e elétrico. Em 2020, em função da pandemia, não houve exercício. Em 2021, ocorreu o EGC 3.0, já com 75 organizações e 350 participantes, e foram incluídos os setores de água e transportes, e um hub secundário na cidade de São Paulo, além do hub principal em Brasília[31].

A E-Ciber prevê dentro da Ação Estratégica nº 2.3.3, a realização de exercícios cibernéticos com a participação de vários atores, como é o caso do EGC (BRASIL, 2020a).

O EGC 4.0 têm previsão de ser realizado no mês de agosto deste ano, com a participação de 110 organizações e empresas, e 450 participantes civis e militares. Dentre os participantes, destacam-se os seguintes setores com suas respectivas Agências Reguladoras: de Energia (ANEEL, ONS e ANP), de Comunicações (ANATEL e Correios), e de Transportes (ANAC, ANTAQ e ANTT)[32].

> "A eficiência da resposta a um ataque cibernético depende antes de tudo do nível de treinamento dos profissionais, assim como da interação e colaboração das empresas dos vários setores, que deixam de se ver como competidores pois, quando o inimigo é comum, não deve existir competição. Esse é o grande legado dos Exercícios como o Guardião Cibernético" (SANTOS, 2021).

O Brasil, além de conduzir o seu próprio exercício cibernético, têm sido convidado a participar de exercícios similares no exterior, tais como o *Locked Shields* e o Ciber Perseu. O

[30] Edital de Chamamento Público para o EGC 4.0, 2022. Disponível em: <https://www.in.gov.br/en/web/dou/-/edital-de-chamamento-publico-376272001>. Acesso em: 10 jun. 2022.

[31] Disponível em: <https://www.marinha.mil.br/cepe/sites/www.marinha.mil.br.cepe/files/a_defesa_cibernetica_no_brasil.pdf>. Acesso em: 12 ago. 2022.

[32] Disponível em: <https://www.convergenciadigital.com.br/Seguranca/Guardiao-Cibernetico-4-tera-110-orgaos-e-empresas-em-guerra-virtual-61122.html>. Acesso em: 12 ago. 2022.

primeiro é organizado pelo Centro de Excelência em Defesa Cibernética Cooperativo (CCDCOE), organização ligada à OTAN, e é o exercício internacional que conta com o maior número de participantes e que possui os exercícios mais complexos de defesa cibernética de dupla ação (ataque contra defesa) do mundo. Na edição do ano de 2021, participaram mais de 2 mil especialistas cibernéticos oriundos de 32 países, e o Brasil foi o único representante da América Latina[33]. O segundo é organizado pelo exército de Portugal, e em sua edição de 2021, contou com a participação de 51 organizações portuguesas e 12 delegações militares estrangeiras, incluindo a delegação brasileira[34].

Segundo o Contra-Almirante Rudicley Cantarin, então Chefe do Estado-Maior Conjunto do ComDCiber, em 2021, esses exercícios possuem um alto nível de exigência técnica e são oportunidades únicas para que ocorra uma interação nas atividades de proteção de sistemas militares e civis, em um ambiente de cooperação mútua, contra adversários de altíssimo nível, possibilitando que os países participantes possam exercitar suas capacidades cibernéticas, em um ambiente seguro e controlado, permitindo a troca de experiências e consequentemente, contribuindo para o aumento da maturidade do setor cibernético e da capacidade militar de defesa cibernética do Brasil[35].

Podemos dizer que o EGC, nos dias de hoje, é o principal evento de segurança cibernético do país, além de ser considerado o maior exercício de defesa cibernética do hemisfério sul. Ele têm a participação das equipes cibernéticas dos principais setores das IC do país, além dos militares do ComDCiber e convidados, que podem trocar experiências e se aperfeiçoar através dos exercícios gerados, que simulam incidentes e situações de crises muito próximas da realidade.

### 4.5 Conclusões Parciais

Desde 2008 o Brasil incluiu a segurança da informação na agenda do país, com a criação do DSIC[36], no GSI/PR, e o assunto cibernético com a inclusão do setor estratégico

[33] Disponível em: <https://www.defesaemfoco.com.br/forcas-armadas-participam-de-maior-exercicio-de-defesa-cibernetica-do-mundo>. Acesso em: 10 jun. 2022.
[34] Disponível em: <https://www.afcea.pt/2021/12/13/afcea-portugal-parceiro-do-exercito-no-ciber-perseu/>. Acesso em: 10 jun. 2022.
[35] Disponível em: <https://www.defesaemfoco.com.br/forcas-armadas-participam-de-maior-exercicio-de-defesa-cibernetica-do-mundo>. Acesso em: 10 jun. 2022.
[36] O DSIC posteriormente, teve seu nome alterado para DSI.

cibernético como um dos três setores estratégicos decisivos para a Defesa Nacional, ficando este sob a responsabilidade do Exército Brasileiro.

A criação do GT SEG CIBER, que tinha como o objetivo a proposição de diretrizes e estratégias para a SegCiber, pode ser considerado o primeiro passo para o estabelecimento da segurança cibernética no âmbito da APF. O trabalho executado por esse grupo foi consolidado no LVSC, que seria um publicação pré-lançamento de uma Política Nacional de Segurança Cibernética, mas que infelizmente essa Política não foi concretizada.

O DSI do GSI/PR foi designado como o órgão responsável por planejar e coordenar a SegCiber e a SIC dentro da APF, e implementar e operar um CTIR, porém para ele possa desempenhar estas tarefas, e ser o coordenador estratégico da SegCiber do país, é necessário que haja um redimensionamento da sua atual estrutura. A Defesa Cibernética do país ficou a cargo do MD, especificamente com recém criado CDCiber, que depois evoluiu para o ComDCiber.

A importância da cooperação nacional e internacional, a inclusão da academia como partícipe no desenvolvimento de novas tecnologias, e a capacitação de recursos humanos que serão empregadas na SegCiber e na proteção das IC do país, são destacadas nos documentos estratégicos, particularmente na PND, END, LBDN e E-Digital.

Na questão jurídica, a tipificação como crime dos delitos cibernéticos foram incluídos, em 2012, com a Lei nº 12.737/2012, os direitos e deveres do uso da internet no país, pela Lei do Marco Civil da Internet, em 2014, e o tratamento de dados pessoais, na LGPD, de 2018. A Lei nº 14.155/2021, aumentou as penas para alguns crimes cibernéticos.

A Defesa Cibernética está explicitada na PCD e na implantação do SMDC, cuja responsabilidade ficou a cargo do MD, por meio do ComDCiber, que é o órgão central do SMDC. Esse Sistema também irá contribuir com a proteção das IC do país.

Em 2015, o Governo Federal lançou as primeiras ações concretas, em relação a SIC e a SegCiber na APF, pela Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018. Essas ações também impactam no fortalecimento da segurança e resiliência cibernética das IC.

As atividades de inteligência ligadas ao ambiente cibernético foram abordadas na ENINT, principalmente no objetivo estratégico de ampliação da capacidade da Inteligência Cibernética do Estado, particularmente em relação a exploração cibernética.

Uma grande guinada em relação a segurança da informação aconteceu com o lançamento da PNSI, que consolidou um longo trabalho de um GTI, coordenado pelo GSI/PR, e contou com a participação de especialistas de inúmeros setores. Além de ela ter alavancado a disseminação do tema na sociedade, ela estabeleceu diretrizes a fim de coordenar e integrar as atividades relacionadas com a segurança da informação no país. Ainda faltará ao país a elaboração da sua ENSI.

Em 2020, foi lançada a primeira E-Ciber do país. Ela contém as principais diretrizes do Governo Federal, na área da SegCiber, até o ano de 2023, mas carece de metas mais específicas e mecanismos de acompanhamento das ações. O Brasil foi o 12º país da América Latina e Caribe a promulgar a sua Estratégia Nacional de Segurança Cibernética. O país aguarda a publicação da Política Nacional de Segurança Cibernética, que está tramitando por alguns órgãos competentes.

A segurança das IC é primordial para o incremento do nível de Segurança Nacional, pois caso elas venham a sofrer danos ou paralisem seu funcionamento, poderão causar graves consequências para o país e a sociedade. O GSI/PR é o órgão responsável, dentro do Governo, pela coordenação, avaliação, monitoramento e redução de riscos das IC. Para aumentar a segurança e a resiliência das IC, foi editada a PNSIC, que contém orientações a serem seguidas visando o aumento da segurança. Em seguida, foi publicada a ENSIC, que define os resultados a serem alcançados pelo Governo na proteção das IC. Ainda está em elaboração o PLANSIC e em desenvolvimento o Sistema Integrado de Dados de Segurança das IC. O PLANSIC deverá conter algumas diretivas gerais para a implementação da segurança das IC, atribuição de responsabilidades dos atores envolvidos e orientações para a elaboração dos planos setoriais de segurança de IC. Já o SIDSIC armazenará os dados referente as condições de segurança das IC, contendo o cadastro e os níveis de risco de cada IC existente no país. Cabe ressaltar que não há no país, nenhuma norma ou regra nacional a ser adotada especificamente pelas ICM operadas no país.

Os Grupos Técnicos de Segurança de Infraestruturas Críticas estão trabalhando na identificação e classificação das IC, bem como no levantamento das vulnerabilidades e ameaças, a fim de propor ações para a minimização dos riscos. Como resultado desses grupos, já foram identificadas 52 ICM, sendo 29 Portos/Terminais e 23 UEP Marítimas.

O EGC é uma ferramenta importantíssima no aprimoramento das capacidades de segurança e defesa cibernética do país, pois seus os participantes trocam experiências e

conhecimentos, através dos exercícios gerados, que simulam incidentes e situações de crises de maneira muito realística.

# 5 COMPARAÇÃO ENTRE AS GOVERNANÇAS CIBERNÉTICAS DO BRASIL E A DO REINO UNIDO ANTE ÀS AMEAÇAS CIBERNÉTICAS NA PROTEÇÃO DAS INFRAESTRUTURAS CRÍTICAS NACIONAIS, PRINCIPALMENTE DAS INFRAESTRUTURAS CRÍTICAS MARÍTIMAS

Este capítulo têm como propósito comparar e analisar as governanças cibernéticas do Brasil e do RU ante às ameaças cibernéticas na proteção das IC, particularmente das ICM.

## 5.1 Definição dos Critérios de Comparação

O Centro Global de Capacidade em Segurança Cibernética, da Universidade de Oxford, a fim de analisar as capacidade de SegCiber dos países-membros da Organização dos Estados Americanos, desenvolveu uma metodologia de análise da maturidade em cibersegurança nacional (CMM). Esta metodologia compreende cinco áreas a serem analisadas, que são: (i) Política e Estratégia de cibersegurança; (ii) Cultura da sociedade em cibersegurança; (iii) Construção de capacidades e conhecimentos em cibersegurança; (iv) Marcos legais e regulatórios; e (v) Controle de riscos através de normas e tecnologias (UO, 2021).

Segundo Meyer e Montoya (2022), devem ser analisados cinco aspectos em relação a SegCiber de uma organização, que são: (i) Higiene cibernética; (ii) Cooperação; (iii) Educação; (iv) Tecnologia; e (v) Eficiência operacional (MEYER; MONTOYA, 2022).

Aproveitando os critérios de análise da CMM e de Meyer e Montoya, e a fim de comparar as governanças cibernéticas dos dois países, este autor estipulou 08 critérios, que estão diretamente envolvidos com a SegCiber das IC/ICM, de maneira que será verificado se dentre as ações executadas pelos dois governos, há a ocorrência de pelo ao menos uma ação afeta a cada um dos critérios. Os critérios selecionados foram os seguintes:

1 – Políticas e Estratégias afetas as IC – Se existe, dentro das Políticas e Estratégias publicadas, alguma citação sobre a necessidade de proteção das IC, principalmente contra as ameaças cibernéticas.

2 – Políticas e Estratégias afetas as ICM – Se existe, dentro das Políticas e Estratégias publicadas, alguma citação sobre a necessidade de uma proteção específica das ICM, principalmente contra ameaças cibernéticas.

3 – Cooperação Nacional – Interações cooperativas, principalmente com a troca de informações, entre os setores público e privado, academia e outros atores locais (indivíduos e organizações).

4 – Cooperação Internacional – Interações cooperativas entre os órgãos nacionais com órgãos de outros países, principalmente com a troca de informações.

5 – Conscientização da Sociedade – Ações ou diretrizes sobre a divulgação de orientações básicas sobre cibersegurança.

6 – Recrutamento/ Capacitação de Recursos Humanos na Área Cibernética– Ações ou diretrizes voltadas para atrair novas pessoas para essa área de trabalho, e/ou medidas que visem melhorar a capacitação da mão de obra existente hoje no mercado.

7 – Órgão responsável de Defesa e Segurança Cibernética das IC/ICM – Identificar a existência de órgãos responsáveis pela Defesa e Segurança Cibernética das IC/ICM.

8 – Arcabouço Legislativo sobre Crimes Cibernéticos – Verificar a existência de leis que tipifiquem os crimes cibernéticos.

Após definidos os critérios, foi realizada a comparação das ações realizadas pelos dois países, dentro de cada categoria. As tabelas com os dados preenchidos encontram-se no Apêndice A.

## 5.2 Análise dos Dados Comparativos

Em relação ao critério Políticas e Estratégias afetas as IC, podemos observar que no Brasil, a necessidade da proteção das IC aparece desde a publicação da END (2012), e continuou aparecendo nas publicações seguintes, como por exemplo, na END (2016) e na PNSIC. A LDBN foi a primeira publicação a correlacionar as ameaças cibernéticas com as IC e citar que as IC poderiam ter sua integridade comprometida por esse novo desafio. Mas somente com o lançamento da E-Ciber é que essa tema ganhou mais notoriedade, com a preocupação de elevar os níveis de segurança das IC e aumentar a SegCiber. E ENSIC, logo em seguida, complementa, estabelecendo princípios fundamentais para essa segurança e elenca os principais desafios. Em relação ao RU, como as ameaças cibernéticas foram classificadas com o maior grau de risco à Segurança Nacional, a partir de 2010, a Estratégia de Segurança Nacional daquele ano, já foi contemplada com um objetivo estratégico complementar, que elencava a proteção das IC contra as principais ameaças, entre elas, o ataque cibernético. A

primeira Estratégia Nacional de Segurança Cibernética (2011), incluiu como uma das ações prioritárias, o contínuo melhoramento da detecção e análise das ameaças cibernéticas, principalmente com foco nas IC. As outras publicações estratégicas mantém esse enfoque prioritário da necessidade da proteção das IC contra as ameaças cibernéticas. Uma outra ação criada no RU, especificamente focada nessa atividade, foi a criação dos Regulamentos NIS, a fim de elevar os padrões de segurança das IC do país.

No segundo critério, Políticas e Estratégias afetas as ICM, o Brasil não emitiu nenhum documento deste nível, com um foco especifico na proteção das ICM. Já o RU, além da Estratégia Nacional para a Segurança Marítima, que considera o ataque cibernético, como um dos maiores riscos de segurança marítima, o país também lançou duas publicações especialmente desenvolvidas visando aumentar a SegCiber das ICM, sendo uma para Navios e a outra para Portos e Instalações Portuárias. Visando o futuro, o RU publicou também, a Marítimo 2050: Navegando o Futuro, com um enfoque de que o setor marítimo precisa permanecer seguro, protegido e resiliente diante das ameaças cibernéticas, alcançando certos objetivos de segurança estabelecidos.

Em relação ao terceiro critério, a Cooperação Nacional, o Brasil cita em vários documentos, desde a PNSIC, a necessidade e a importância desta ação para elevar o nível de proteção e resiliência das IC. A criação da REGIC, foi uma ação voltada para aumentar e melhorar a cooperação e troca de informações, como alertas, vulnerabilidades, ataques e medidas de prevenção, entre os órgãos e das entidades da APF, além da criação das ETIR Setoriais que trocarão informações diretamente com o CTIR Gov. O RU também incluiu a necessidade da cooperação nacional dentro de vários documentos lançados, desde 2010.

Na Cooperação Internacional, quarto critério estabelecido, os dois países incluíram esse tema nas suas políticas e estratégias, ressaltando a importância dessa cooperação, principalmente para o desenvolvimento de novas tecnologias que serão usadas na SegCiber.

Sendo o ser humano o elo mais fraco da SegCiber, o quarto critério, a Conscientização da Sociedade, é de grande importância para minimizar a ocorrência de um ataque cibernético. O Brasil incluiu este assunto, principalmente, na E-Ciber, porém não se viu nenhuma ação concreta, por parte do Governo, para que a mentalidade de SegCiber fosse difundida na sociedade. O RU, como ação decorrente de algumas políticas e estratégias, desenvolveu duas ações que têm esse objetivo, que são o Fique Seguro Online e a Campanha

Ciber Consciente. São ações desenvolvidas em parceria com a iniciativa privada, que através de informações disponibilizadas em *sites* e através das principais mídias sociais, tais como *Facebook*, *Instagram*, *Twitter*. Dessa forma as principais informações relativas a SegCiber, podem atingir milhões de pessoas, com orientações e dicas simples de como se proteger de ameaças cibernéticas.

O sexto critério, o Recrutamento/ Capacitação de Recursos Humanos na Área Cibernética é outro ponto importante da SegCiber, uma vez que há uma demanda crescente por profissionais dessa área em todo o mundo, em função do aumento de incidentes e da constante evolução da ameaça cibernética. No Brasil, tal tema têm sido inserido em diversas publicações, tendo aparecido pela primeira vez na PCD, mas não foram encontradas ações concretas do Governo Federal sobre essa tema. Já no RU, fruto de orientações constantes em algumas políticas e estratégias, foram criados dois programas, que são o Programa Primeiro Ciber e o Desafio de Cibersegurança. Esse programas desenvolvem atividades dentro das escolas e universidades, divulgando e fomentando as atividades da SegCiber, de maneira a atrair jovens para trabalharem nesse ramo do mercado.

Em relação a existência de um Órgão responsável pela Defesa e Segurança Cibernética das IC/ICM, que é o sétimo critério, o Brasil possui essa responsabilidade dividida entre o MD e o GSI/PR, responsáveis pela Defesa e pela SegCiber, respectivamente. Essa decisão poderá dificultar a interação e a troca de informações entre os setores, pois passam a depender da afinidade e espírito colaborativo das pessoas e dos chefes desses órgãos. Já o RU, a responsabilidade por ambos é unicamente do NCSC.

Em relação ao oitavo e último critério, a existência de um Arcabouço Legislativo sobre Crimes Cibernéticos, ambos os países possuem leis que tipifiquem os crimes cibernéticos. No Brasil, a Lei nº 12.737/2012 tipificou pela primeira vez os crimes cibernéticos, e a Lei nº 14.155/2021, aumentou as penas de alguns desses crimes. A única lei desse tipo existente no RU é a Lei de Uso Indevido de Computadores, de 1990, que como citado no capítulo 4, carece de atualizações.

## 5.3 Conclusões Parciais

Existem vários critérios utilizados por diversas organizações nacionais e internacionais a fim de mensurar a capacidade cibernética de um país.

Para realizar a comparação das governanças cibernéticas entre o Brasil e o RU, este autor estipulou 08 critérios, onde todos eles poderão influenciar na proteção das IC/ICM ante às ameaças cibernéticas.

Foi constatado que ambos os países apresentaram dados satisfatórios no primeiro critério. Cabe destacar neste critério, a criação pelo RU dos Regulamentos NIS, uma ação concreta para aumentar a resiliência cibernética das suas IC/ICM.

Na divulgação de Políticas e Estratégias especialmente afetas as ICM, o Brasil deixa muito a desejar, pois ele não editou nenhuma publicação que pudesse orientar os operadores das ICM, acerca do aumento do nível de suas SegCiber. A PMN existente, por ser tão antiga, sequer menciona as ICM, e muito menos as ameaças cibernéticas. O país não possui uma Estratégia de Segurança Marítima. Já o RU, além de possuir uma NSMS, lançou guias de orientações cibernéticas para Navios, Portos e Instalações Portuárias, além de uma publicação com diretrizes para o futuro.

Na Cooperação Nacional, os dois países têm divulgado em seus documentos a importância deste tema na atualidade. Particularmente, o Brasil com a criação da REGIC deu um grande passo para incentivar a cooperação dentro dos órgãos e das entidades da APF, porém necessita criar um outro mecanismo para aumentar a cooperação com os atores de fora do governo, como a academia e o setor privado.

No quarto critério, ambos os países apresentaram resultados satisfatórios, com o tema da Cooperação Internacional presentes em seus documentos estratégicos.

Em relação a maior fragilidade de qualquer sistema de SegCiber, que é o ser humano, o Brasil, apesar de fazer constar em suas políticas e estratégias, não adotou nenhuma medida concreta para conscientizar a população da importância deste tema, tampouco com orientações e dicas que venham a minimizar incidentes cibernéticos nas residências e nas empresas. O RU por sua vez, possui dois programas que divulgam essas informações para a sociedade, por meio de *sites* e das redes sociais.

A oferta de empregos na área de SegCiber têm sido frequentemente inferior a demanda por esses profissionais, principalmente pelos mais especializados. Por esse motivo, o recrutamento de novos talentos é de vital importância para qualquer país. Mais uma vez, apesar do Brasil ter inserido essa tema em suas políticas e estratégias, não foram encontradas ações concretas por parte do governo. O RU possui dois programas que têm realizado ações

para as crianças e adolescentes, nas escolas e universidades, a fim de despertar o interesse deles por essa carreira, e com isso aumentar sua mão de obra nessa área.

Em relação às responsabilidades pela Defesa e Segurança Cibernética das IC/ICM, o Brasil adota um modelo diferente do RU, pois elas são divididas entre o MD e o GSI/PR, responsáveis pela Defesa e pela SegCiber, respectivamente. No RU, a responsabilidade por ambos é apenas do NCSC.

Na parte da tipificação dos crimes cibernéticos, o Brasil possui duas leis para tentar coibir esse tipo de crime e o RU somente uma, e bastante antiga, apesar de algumas atualizações.

Dessa forma, percebe-se que o Brasil têm tido um compromisso crescente para enfrentar e reduzir as ameaças cibernéticas e melhorar a sua SegCiber, sejam com ações ou a publicação de normas e diretrizes e, de certa forma, têm conseguido, pois tal fato pode ser constatado em sua ascensão na classificação em rankings internacionais de cibersegurança, como, por exemplo, no GCI da ITU, em que o Brasil avançou 53 posições, saindo da 71ª posição na edição de 2018, para a 18ª posição na edição de 2020. O país precisa realizar ações visando a conscientização da sociedade em relação a SegCiber e o recrutamento de talentos para trabalhar nessa área, e principalmente, em relação a proteção cibernética das ICM, o país precisa urgentemente da elaboração de uma Estratégia de Segurança Marítima ou documento similar que divulgue orientações e diretrizes sobre SegCiber para o setor marítimo.

O RU têm priorizado a área cibernética, e investido grandes somas de recursos na área de SegCiber, com ênfase na proteção de suas IC/ICM. No GCI da ITU, o país caiu da 1ª posição na edição de 2018, para a 2ª posição na edição de 2020, perdendo a posição para os EUA. Mesmo assim, continua sendo uma referência no assunto na comunidade internacional.

## 6 CONCLUSÃO

Este trabalho comparou e analisou as governanças cibernéticas do Brasil e do Reino Unido ante às ameaças cibernéticas na proteção das Infraestruturas Críticas (IC), particularmente das Infraestruturas Críticas Marítimas (ICM), a fim de identificar possíveis deficiências na governança cibernética brasileira e, caso necessário, seriam propostos aperfeiçoamentos.

O espaço cibernético é um ambiente extremamente complexo, cuja característica principal é sua transversalidade, pois pode permear todas as dimensões. Ele não respeita as fronteiras físicas e, por esse motivo é considerado como o 5º domínio da guerra.

As tecnologias e a internet têm sido cada vez mais usadas e estão presentes no dia a dia das sociedades, das empresas e dos governos. Essa revolução digital têm transformado várias áreas da nossa sociedade, e como consequência desse processo, surgem, na mesma proporção, novas e crescentes ameaças cibernéticas, que podem colocar em risco todos os sistemas conectados.

Estima-se que as perdas globais devido aos crimes cibernéticos podem chegar até US$ 10,5 trilhões em 2025[37]. Para enfrentarem essas ameaças, e aumentarem sua Segurança Cibernética, os setores públicos e privado desembolsam enormes montantes financeiros por ano.

As IC/ICM são essenciais para o desenvolvimento dos países, bem como para o bem estar das sociedades, e uma possível interrupção e/ou destruição de qualquer uma delas, poderá ocasionar sérios impactos à segurança do Estado e da própria sociedade. Por esse motivo, é extremamente necessário o desenvolvimento de ações por parte de seus operadores, a fim de protegê-las dessa nova ameaça, desenvolvendo sistemas de proteção adequados, atualizados e permanentemente ativos, a fim de aumentar a Segurança Cibernética e a resiliência delas.

Ataques a IC/ICM têm ocorrido com certa frequência, pois têm sido um alvo rentável para os *hackers*. Em função das características do ciberespaço, esses ataques podem ser originados de lugares distantes dos alvos, e por um custo pequeno para o atacante, o dano causado poderá ser enorme.

---

[37] Disponível em: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>. Acesso em: 01 ago. 2022.

Em 2008 o Brasil incluiu o setor cibernético como um dos três setores estratégicos mais importantes para a Defesa Nacional, ficando sob a responsabilidade do Exército Brasileiro. No mesmo ano foi criado o Departamento de Segurança da Informação e Comunicações, dentro da estrutura do GSI/PR, que ficou incumbido de tratar dos assuntos ligados a segurança da informação no país.

O Grupo Técnico de Segurança Cibernética propôs, ao final de seu trabalho, diretrizes e estratégias para a Segurança Cibernética no âmbito da Administração Pública Federal. Essas informações foram consolidadas e foram incluídas no Livro Verde: Segurança Cibernética, e posteriormente, serviriam de base para a elaboração da Política Nacional de Segurança Cibernética, mas infelizmente a elaboração dessa Política não foi concretizada. Pode-se afirmar que foi a primeira tentativa do governo brasileiro em se estabelecer orientações para a Segurança Cibernética na Administração Pública Federal.

Com o lançamento da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal, em 2015, o Governo Federal estabeleceu formalmente as diretrizes estratégicas para o desenvolvimento da Segurança da Informação e Comunicações e da Segurança Cibernética a serem adotadas somente no âmbito da Administração Pública Federal.

A Política Nacional de Segurança da Informação foi elaborada com a participação de vários especialistas de setores diversos, e estabeleceu as diretrizes de coordenação e integração das atividades relacionadas com a segurança da informação no país, além de ter difundido esse tema dentro da sociedade.

A primeira Estratégia Nacional de Segurança Cibernética do Brasil (E-Ciber) foi lançada em 2020. Ela estipulou as principais diretrizes de Segurança Cibernética do Governo Federal, para o quadriênio de 2020 a 2023. O país foi o 12º país da América Latina e Caribe a promulgar a sua Estratégia Nacional de Segurança Cibernética. Essa estratégia não contém metas muito específicas e claras, não estipula mecanismos para o acompanhamento das ações estratégicas propostas e nem indicadores para medir os resultados alcançados. A Política Nacional de Segurança Cibernética, ainda está em tramitação, sendo apreciada por alguns órgãos competentes, para depois então, ser lançada.

O Brasil avançou na questão jurídica em relação aos crimes cibernéticos, que foram tipificados com a Lei nº 12.737/2012, e posteriormente tiveram algumas penas aumentadas pela Lei nº 14.155/2021. A Lei do Marco Civil da Internet estabeleceu os direitos

e deveres do uso da internet no país, e a Lei Geral de Proteção de Dados o tratamento de dados pessoais.

O Governo designou o GSI/PR para ser o coordenador estratégico da área cibernética, que inclui a coordenação, avaliação, monitoramento e redução de riscos das IC, além de manter o CTIR Gov. Porém, como citado na E-Ciber, é necessário que a sua estrutura atual seja revisada e aumentada, de forma a propiciar sua atuação no nível nacional.

As IC/ICM ainda não estão totalmente identificadas e classificadas, pois os Grupos Técnicos de Segurança de IC ainda não concluíram esse trabalho. Esse levantamento também incluirá as vulnerabilidades e ameaças, bem como uma proposta de ações para minimizar os riscos. Até o momento, foram identificadas 52 ICM, sendo 29 Portos/Terminais e 23 UEP Marítimas.

Para orientar e aumentar o nível de proteção das IC, o Governo editou algumas normas. As orientações que visam elevar o nível de segurança e a resiliência foram divulgados na Política Nacional de Segurança de Infraestruturas Críticas, e os resultados a serem alcançados estão contidos na Estratégia Nacional de Segurança de Infraestruturas Críticas. O GSI/PR ainda está desenvolvendo o Plano Nacional de Segurança de Infraestruturas Críticas e o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas. O primeiro conterá as atribuições de responsabilidades dos órgãos envolvidos e diretrizes para a elaboração dos planos setoriais de segurança de IC. O Sistema Integrado de Dados de Segurança de Infraestruturas Críticas será o sistema que controlará os níveis de segurança e de risco de cada IC no país.

Um dos eventos mais importantes para o aprimoramento das capacidades de segurança e defesa cibernética do país e das IC/ICM é o Exercício Guardião Cibernético. A cada edição ele têm incluído mais setores das IC participantes, e durante o exercício são geradas situações de crises bem próximas da realidade, e as equipes de cada setor têm que atuar de maneira a se contrapor aos incidentes gerados e buscar o restabelecimento do sistema o quanto antes. Há uma grande troca de experiências e conhecimentos entre os participantes.

Para que a Segurança Cibernética seja eficiente, é necessário a atuação coordenada e cooperativa de diversos atores envolvidos no tema, dentre eles o governo, a sociedade, as FA, as empresas, a comunidade técnica e a academia.

Em relação ao Reino Unido, desde 2010, o país passou a considerar a Segurança Cibernética como uma ameaça de Risco Um à Segurança Nacional, o nível mais alto. Essa

atitude foi baseada no aumento do número de casos de ataques cibernéticos, em função do crescimento da conectividade e do uso da internet. O Governo também percebeu a importância da internet na prestação de serviços, no comércio e para as indústrias, com gastos expressivos da população por desse meio.

A fim de preparar o país para essa ameaça, o Governo implementou o Programa Nacional de Segurança Cibernética, com elevados investimentos na área cibernética. Em 2011, foi lançada a primeira Estratégia de Segurança Cibernética, que apresentou a SegCiber como uma prioridade para o Governo.

O Centro Nacional de Segurança Cibernética do RU (NCSC) foi criado para ser o órgão de liderança e referência nos assuntos ligados a Segurança Cibernética, além de ser o responsável pela resposta a incidentes cibernéticos por meio do CTIR Nacional. Já a NCF, foi criada para agir em favor da Segurança Nacional, a fim de manter o país seguro e promover seus interesses internacionalmente.

Com o lançamento da Estratégia Cibernética Nacional 2022, o Governo mudou a forma como enxerga o espaço cibernético, pois ele passou a perceber que poderia utilizar esse espaço para a promoção de seus interesses dentro e por meio dele, e não tendo apenas a obrigação de garantir a segurança do país nele. Nesse momento surge a expressão poder cibernético, que congrega essas ações nesse espaço.

A escassez de recursos humanos qualificados no ambiente cibernético é um desafio a ser enfrentado pelo setor público e privado, pois a demanda por profissionais supera a oferta disponível no mercado de trabalho. Para minimizar esse problema, o Governo do RU desenvolveu alguns programas para inspirar e atrair os jovens a seguirem uma carreira em SegCiber, como, por exemplo, o Primeiro Ciber e o Desafio de Cibersegurança.

O ambicioso e ousado objetivo central da Estratégia de Segurança Cibernética do Governo: 2022 a 2030 é robustecer, até 2025, as funções críticas governamentais para se contraporem aos ataques cibernéticos, e até 2030, garantir a resiliência dos órgãos do setor público contra ataques e vulnerabilidades conhecidas.

Para que seja garantido um padrão mínimo em Segurança Cibernética nas empresas do país, o Governo apoiou o desenvolvimento de um programa de certificação cibernética, que é o Essenciais Cibernéticos. Algumas licitações do Governo, exigem que as empresas participantes tenham essa certificação.

A proteção cibernética das IC/ICM no Reino Unido é de responsabilidade do NCSC, em coordenação com os operadores das IC/ICM. Dois programas foram desenvolvidos para auxiliarem os operadores de IC/ICM na Segurança Cibernética, que são os Regulamentos NIS e a Estrutura de Avaliação Cibernética. Os Regulamentos contêm medidas técnicas e organizacionais que visam elevar os níveis de segurança, e a Estrutura de Avaliação Cibernética oferece um conjunto de princípios de SegCiber e resiliência, para que as organizações consigam alcançar um nível adequado de resiliência cibernética.

No Reino Unido, as ICM podem ser uma Empresa de Navegação, uma Autoridade Portuária, um Operador de uma Instalação Portuária ou um Operador de Serviços de Tráfego de Embarcações de um porto, a depender do cumprimento de alguns critérios estabelecidos, tais como volume de carga ou números de passageiros. A Estratégia Nacional para a Segurança Marítima considerou um ataque cibernético as ICM como um dos principais riscos à segurança marítima do país.

O governo britânico lançou duas normas que visam aumentar a SegCiber e a resiliência das ICM, em função do aumento da automação e integração dos vários sistemas eletrônicos, que são o Código de Prática: Segurança Cibernética para Navios e o Guia de Boas Práticas: Segurança Cibernética para Portos e Instalações Portuárias. Como os próprios títulos das publicações sugerem, o primeiro aborda a questão cibernética nos Navios e o segundo nos portos e terminais portuários. Já a publicação Marítimo 2050: Navegando o Futuro, enfatiza os desafios para o setor marítimo no futuro, onde é citado, que sem a segurança das ICM, a prosperidade e a resiliência do país estará em risco.

Para a comparação das governanças cibernéticas entre o Brasil e o Reino Unido, foram utilizados 08 critérios, que poderão influenciar na proteção das IC/ICM ante às ameaças cibernéticas.

Durante a comparação, foi constatado que o Brasil realizou várias iniciativas no campo cibernético, desde 2009, e a partir de 2018 começou a agir no sentido de aumentar a segurança das IC do país, porém muitas das orientações constantes em suas normas e publicações não foram transformadas em ações concretas. Dentre as que se concretizaram, podemos destacar a criação da Rede Federal de Gestão de Incidentes Cibernéticos que incentivou a cooperação e troca de informações entre os integrantes da rede e as leis que tipificam os crimes cibernéticos, que podem dissuadir possíveis intenções de ataques cibernéticos.

Devido ao Brasil ter sido a sede de grandes eventos, no período compreendido entre 2012 e 2016 , houve uma preparação do país visando aumentar sua segurança contra alguns incidentes, entre eles o cibernético. Por este motivo podemos notar algumas ações neste período, como por exemplo a ativação do CDCiber, e a publicação da Política Cibernética de Defesa e da Lei do Marco Civil da Internet.

Ainda faltam a publicação de algumas normas que estão previstas, por parte do governo brasileiro, e fazem parte do normativo estabelecido, que são: no campo da segurança da informação, a Estratégia Nacional de Segurança da Informação, no campo da segurança das IC, o Plano Nacional de Segurança de Infraestruturas Críticas, e no campo cibernético a Política Nacional de Segurança Cibernética, além da finalização do desenvolvimento do Sistema Integrado de Dados de Segurança de Infraestruturas Críticas. Em relação as ICM, por enquanto, não está prevista a elaboração de nenhuma norma específica.

O Reino Unido por sua vez, desenvolveu inúmeras iniciativas concretas para auxiliar o país no combate as ameaças cibernéticas. Dentre elas, podemos destacar o Fique Seguro Online e a Campanha Ciber Consciente que transmitem orientações e dicas de SegCiber para a sociedade e as pequenas e médias empresas; os Programa Primeiro Ciber e o Desafio de Cibersegurança têm foco no recrutamento de jovens e talentos para o mercado de trabalho na área cibernética; a Estrutura de Avaliação Cibernética e o Regulamento NIS para aumentar a resiliência e elevar o nível de SegCiber das IC/ICM.

Especificamente em relação as ICM, o Reino Unido, bem diferente do Brasil, realizou diversas ações, com a publicação de estratégias e normas estritamente voltadas para o setor marítimo e a segurança das ICM. Podemos destacar a Estratégia Nacional para a Segurança Marítima, o Código de Prática: Segurança Cibernética para Navios, o Guia de Boas Práticas: Segurança Cibernética para Portos e Instalações Portuárias e a publicação Marítimo 2050: Navegando o Futuro.

O Governo do Reino Unido continua considerando as ameaças cibernéticas como a mais alta prioridade, e como consequência, continua investindo grandes montantes financeiros em pesquisa e desenvolvimento, e em soluções que aumentam a SegCiber e a resiliência dos setores críticos, inclusive das IC/ICM, além de incentivar a qualificação e o recrutamento de recursos humanos cibernéticos. Por conta dessas ações, o país têm se mantido bem classificado nas avaliações das capacidades cibernéticas de organizações internacionais, bem como continua sendo uma referência mundial no tema cibernético.

Em relação às responsabilidades pela Defesa e Segurança Cibernética das IC/ICM, o Brasil adota um modelo diferente do RU, pois elas são divididas entre o MD e o GSI/PR, responsáveis pela Defesa e pela SegCiber, respectivamente. Essa divisão de responsabilidades, poderá dificultar o trabalho cooperativo essencial entre os órgãos, dificultando a troca de informações, e em casos de crises, poderá ocasionar um retardo na devida e necessária pronta resposta. No Reino Unido, a responsabilidade por ambos é centralizada apenas do Centro Nacional de Segurança Cibernética.

O Brasil, apesar dos esforços e da sua melhoria na classificação nas avaliações das capacidades cibernéticas de organizações internacionais, ainda precisa aprimorar e investir mais recursos na área cibernética, principalmente em pesquisa e desenvolvimento, na capacitação de recursos humanos e na conscientização do tema cibernético na sociedade. Uma possível solução desses problemas, seria desenvolver programas similares aos executados pelo Reino Unido, e descritos anteriormente. Como as ameaças cibernéticas encontram-se em constante evolução, deverá haver um mecanismo que oriente as revisões periódicas nas normas afetas ao tema.

Em relação a governança do Brasil ante às ameaças cibernéticas na proteção das IC, podemos dizer que o Brasil está caminhando bem com ações no sentido de melhorar a SegCiber das IC, mas deverá concluir a identificação das IC, bem como de suas vulnerabilidades, a publicação do normativo pendente (Plano Nacional de Segurança de Infraestruturas Críticas e Política Nacional de Segurança Cibernética) e finalizar o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas. Deverá, também, serem estipulados indicadores que possam medir o grau de SegCiber de cada IC.

Para as ICM, a governança brasileira ante às ameaças cibernéticas, é praticamente inexistente. O Brasil precisa urgentemente elaborar uma Estratégia de Segurança Marítima ou documento similar que divulgue orientações e diretrizes cibernéticas para o setor marítimo. Poderá também expedir algum normativo específico para as ICM, como o Reino Unido fez, com os Código de Prática: Segurança Cibernética para Navios e o Guia de Boas Práticas: Segurança Cibernética para Portos e Instalações Portuárias. Não se pode esquecer que mais de 95% do comércio exterior brasileiro é transportado por via marítima[38], e como comentado

[38] Disponível em: https://www.marinha.mil.br/agenciadenoticias/e-navigation-traz-mais-seguranca-e-aprimora-navegacao. Acesso em: 03 ago. 2022.

anteriormente, as ICM possuem grande automação e integração dos vários sistemas eletrônicos que podem sofrer ataques cibernéticos, com tendências de crescimento.

Como estudos futuros, sugere-se que sejam incluídos outros países nesta comparação, a fim de que haja uma maior quantidade de dados acerca das melhores práticas adotadas internacionalmente, que visem a proteção cibernética das IC/ICM.

## REFERÊNCIAS

ABREME blog, 2021. Os impactos da Indústria 4.0. Disponível em: <https://abreme.com.br/os-impactos-da-industria-4-0/>. Acesso em: 27 fev. 2022.

ALCARAZ, Cristina; ZEADALLY, She rali. Critical infrastructure protection: Requirements and challenges for the 21st century, 2015.

BAKER, Carla. Demystifying the UK's National Cyber Strategy 2022, 2022. Disponível em: <https://www.information-age.com/demystifying-uks-national-cyber-strategy-2022-123498763/>. Acesso em: 23 jul. 2022.

BALDONI, R. Critical Infrastructure Protection: Threats, Attacks and Countermeasures. In: TENACE Project, 2014.

BRASIL. Decreto nº 1.265 de 11 de outubro de 1994. Aprova a Política Marítima Nacional (PMN). *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 13 out. 2010. Seção 1. p. 15.443. Disponível em: <http://www.planalto.gov.br/CcIVIL_03/decreto/1990-1994/D1265.htm>. Acesso em 15 mai. 2022.

_____. Marinha do Brasil, Diretoria de Portos e Costas. NORMAM 01/DPC – Normas da Autoridade Marítima para Embarcações Empregadas na Navegação em Mar Aberto. 2005. Mod. 46. Rio de Janeiro, 2005.

_____. Decreto nº 5.772 de 08 de maio de 2006. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República, e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 09 mai. 2006. Seção 1. p. 3. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/decreto/d5772.htm>. Acesso em 15 mai. 2022.

_____. Decreto nº 6.371 de 12 de fevereiro de 2008a. Dá nova redação ao art. 1o do Decreto no 4.801, de 6 de agosto de 2003, que cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 13 fev. 2008. Seção 1. p. 1. Disponível em: <https://presrepublica.jusbrasil.com.br/legislacao/94031/decreto-6371-08>. Acesso em 15 mai. 2022.

_____. Decreto nº 6.703 de 18 de dezembro de 2008b. Aprova a Estratégia Nacional de Defesa, e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 19 dez. 2008. Seção 1. p. 4. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm>. Acesso em 15 mai. 2022.

_____. Decreto nº 7.009 de 12 de novembro de 2009a. Dá nova redação aos arts. 1º, 2º e 3º do Decreto nº 4.801, de 6 de agosto de 2003, que cria a Câmara de Relações Exteriores e

Defesa Nacional, do Conselho de Governo. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 13 nov. 2009. Seção 1. p. 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Decreto/D7009.htm>. Acesso em 24 mai. 2022.

_____. Gabinete de Segurança Institucional da Presidência da República (GSI/PR). Portaria nº 45 de 08 de setembro de 2009b. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 09 set. 2009. Seção 1. p. 2. Disponível em: <https://www.legisweb.com.br/legislacao/?id=213726>. Acesso em 15 mai. 2022.

_____. Ministério da Defesa. Diretriz Ministerial nº 0014 de 9 de novembro de 2009c. Integração e Coordenação dos Setores Estratégicos de Defesa. Brasília. 2009. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/File/legislacao/emcfa/portarias/0014a_2009.pdf>. Acesso em 24 mai. 2022.

_____. Decreto nº 7.411 de 29 de dezembro de 2010a. Dispõe sobre remanejamento de cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS, aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República; altera o Anexo II do Decreto nº 7.063, de 13 de janeiro de 2010, e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 30 dez. 2010. Seção 1. p. 44. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/decreto/D7411.htm>. Acesso em 24 mai. 2022.

_____.Gabinete de Segurança Institucional da Presidência da República (GSI/PR). Portaria nº 31 de 27 de abril de 2010b. Cria, no âmbito do Gabinete de Segurança Institucional da Presidência da República - GSIPR, o Núcleo de Segurança de Infraestruturas Críticas e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 28 abr. 2010. Seção 1. p. 164. Disponível em: <https://www.diariodasleis.com.br/legislacao/federal/214065-nucleo-de-seguranua-de-infraestruturas-cruticas-cria-no-umbito-do-gabinete-de-seguranua-institucional-da-presiduncia-da-republica-gsipr-o-nucleo-de-seguranua-de-infraestrutu.html>. Acesso em 24 mai. 2022.

_____. Lei nº 12.737 de 30 de novembro de 2012a. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 03 dez. 2012. Seção 1. p. 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 06 jun. 2022.

_____. Decreto nº 7.809 de 20 de setembro de 2012b. Altera os Decretos nº 5.417, de 13 de abril de 2005, nº 5.751, de 12 de abril de 2006, e nº 6.834, de 30 de abril de 2009, que aprovam as estruturas regimentais e os quadros demonstrativos dos cargos em comissão e das funções gratificadas dos Comandos da Marinha, do Exército e da Aeronáutica, do Ministério da Defesa. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 21 set. 2012.

Seção 1. p. 5. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7809.htm>. Acesso em 24 mai. 2022.

_____. Ministério da Defesa. Estratégia Nacional de Defesa (END). Brasília. 2012c. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/END-PNDa_Optimized.pdf>. Acesso em: 24 mai. 2022.

_____. _____. Política Nacional de Defesa (PND). Brasília. 2012d. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/END-PNDa_Optimized.pdf>. Acesso em: 24 mai. 2022.

_____. _____. Livro Branco de Defesa Nacional (LBDN). Brasília. 2012e. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/2012/mes07/lbdn.pdf>. Acesso em: 24 mai. 2022.

_____. _____. Política Cibernética de Defesa (PCD). Brasília. 2012f. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/doutrina_militar/MD31P02PoliticaCiberneticadeDefesa1Ed2012.pdf>. Acesso em: 24 mai. 2022.

_____. _____. Portaria nº 3.405 de 21 de dezembro de 2012g. Atribuir ao Centro de Defesa Cibernética (CDCiber), do Comando do Exército, a responsabilidade pela coordenação e integração das atividades de defesa cibernética, no âmbito do Ministério da Defesa (MD), consoante o disposto no Decreto nº 6.703, de 18 de dezembro de 2008, que aprova a Estratégia Nacional de Defesa (END). *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 24 dez. 2012. Seção 2. p. 247. Disponível em: < https://mdlegis.defesa.gov.br/norma_pdf/?NUM=3405&ANO=2012&SER=A>. Acesso em 24 mai. 2022.

_____. Lei nº 12.965 de 23 de abril de 2014a. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 24 abr. 2014. Seção 1. p. 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 06 jun. 2022.

_____. Ministério da Defesa. MD-31-M-07 - Doutrina Militar de Defesa Cibernética. Brasília, 2014b.

_____. Gabinete de Segurança Institucional da Presidência da República (GSI/PR). Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018. Brasília. 2015. Disponível em: <https://www.gov.br/gsi/pt-br/arquivos/4_estrategia_de_sic.pdf>. Acesso em: 17 jul. 2022.

_____. Ministério da Defesa. Política Nacional de Defesa (PND). Brasília. 2016a. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf>. Acesso em: 24 mai. 2022.

_____. _____. Estratégia Nacional de Defesa (END). Brasília. 2016b. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf>. Acesso em: 24 mai. 2022.

_____. _____. Livro Branco de Defesa Nacional (LBDN). Brasília. 2016c. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf>. Acesso em: 24 mai. 2022.

_____. Decreto de 15 de dezembro de 2017. Aprova a Estratégia Nacional de Inteligência. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 18 dez. 2017. Seção 1. p. 36. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/ENINT.pdf>. Acesso em 06 jun. 2022.

_____. Lei nº 13.709 de 14 de agosto de 2018a. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 15 ago. 2018. Seção 1. p. 59. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 06 jun. 2022.

_____. Decreto nº 9.573 de 22 de novembro de 2018b. Aprova a Política Nacional de Segurança de Infraestruturas Críticas Estratégia Nacional de Defesa, e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 22 nov. 2018. Seção 1. p. 40. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm>. Acesso em 04 mai. 2022.

_____. Decreto nº 9.637 de 26 de dezembro de 2018c. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 26 dez. 2018. Seção 1. p. 23. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm>. Acesso em 04 mai. 2022.

_____. Ministério da Ciência, Tecnologia e Inovações. Estratégia Brasileira para a Transformação Digital (E-Digital). Brasília, 2018d. Disponível em: <https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf>. Acesso em 24 mai. 2022.

_____. Lei nº 13.844 de 18 de junho de 2019a. Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios; altera as Leis nos 13.334, de 13 de setembro de 2016, 9.069, de 29 de junho de 1995, 11.457, de 16 de março de 2007, 9.984, de 17 de julho de 2000, 9.433, de 8 de janeiro de 1997, 8.001, de 13 de março de 1990, 11.952, de 25 de junho de 2009, 10.559, de 13 de novembro de 2002, 11.440, de 29 de dezembro de 2006, 9.613, de 3 de março de 1998, 11.473, de 10 de maio de 2007, e 13.346, de 10 de outubro de 2016; e revoga dispositivos das Leis nos 10.233, de 5 de junho de 2001, e 11.284, de 2 de março de 2006, e a Lei nº 13.502, de 1º de novembro de 2017. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 18 jun. 2019. Seção 1. p. 4. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13844.htm>. Acesso em 03 jun. 2022.

_____. Gabinete de Segurança Institucional da Presidência da República (GSI/PR). Departamento de Segurança da Informação. Glossário de Segurança da Informação, 2019b. Disponível em: <https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1>. Acesso em 09 abr. 2022.

_____. Decreto n. 10.222 de 05 de fevereiro de 2020a. Aprova a Estratégia Nacional de Segurança Cibernética. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 05 fev. 2020. Seção 1. p. 6. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419>. Acesso em 04 mai. 2022.

_____. Decreto nº 10.569 de 09 de dezembro de 2020b. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 10 dez. 2020. Seção 1. p. 8. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm>. Acesso em 03 jun. 2022.

_____. Decreto nº 10.607 de 22 de janeiro de 2021a. Institui o Grupo de Trabalho Interministerial para reformular a Política Marítima Nacional. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 25 jan. 2021. Seção 1. p. 3. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.607-de-22-de-janeiro-de-2021-300386191>. Acesso em 03 jun. 2022.

_____. Lei nº 14.155 de 27 de maio de 2021b. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 28 mai. 2021. Seção 1. p. 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/Lei/L14155.htm>. Acesso em 15 mai. 2022.

_____. Decreto nº 10.748 de 16 de julho de 2021c. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, 19 jul. 2021. Seção 1. p. 2. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.748-de-16-de-julho-de-2021-332610022>. Acesso em 28 jun. 2022.

_____. Marinha do Brasil, Estado Maior da Armada. EMA-419 - Doutrina Cibernética da Marinha. Brasília, 2021d.

_____. Marinha do Brasil, Escola de Guerra Naval. Tema 2 do Trabalho de Processo de Tomada de Decisão do Curso de Política e Estratégia Marítimas (C-PEM/2021). Rio de Janeiro, 2021e.

BUEGER, Christian; EDMUNDS, Timothy; EDWARDS, Scott. Innovation and New Strategic Choices. Refreshing the UK's National Strategy for Maritime Security. *The RUSI Journal, Londres*, v. 166, p. 66-75, 2021. Disponível em: <https://www.academia.edu/73592006/Innovation_and_New_Strategic_Choices_Refreshing_the_UK_s_National_Strategy_for_Maritime_Security_>. Acesso em 09 jul. 2022.

CAPELLA, Arthur. Infraestrutura no alvo dos ciberataques: é preciso blindar as vias conectadas, 2022. Disponível em: <https://canaltech.com.br/seguranca/infraestrutura-no-alvo-dos-ciberataques-e-preciso-blindar-as-vias-conectadas/>. Acesso em: 23 jul. 2022.

CHUBB, Nick; FINN, Patrick; NG, Daniel. The Great Disconnect: The state of cyber risk management in the maritime industry, 2022. Disponível em: <https://sites-hfw.vuturevx.com/32/4322/uploads/thetius-hfw-cyberowl-great-disconnect-cyber-risk-management-report.pdf?intIaContactId=l%2fbVKGHhVFHleAyp2Pc5xw%3d%3d&intExternalSystemId=1>. Acesso em: 11 ago. 2022.

CLARKE, Richard A.; KNAKE, Robert K.; GUIMARÃES, Bruno Salgado; BOCCARDO, Davidson Rodrigo; FERREIRA, Rafael Soares; MACHADO, Raphael Carlos Santos; SALVATORE, Ricardo. Guerra cibernética: a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Brasnorte, 2015. 242 p. ISBN 9788574527116.

CORREA, J. A. Centro de Defesa e Segurança Nacional - CEDESEN. Defesa e Segurança Nacional no espaço cibernético, 2020. Disponível em: <https://cedesen.com.br/defesa-e-seguranca-nacional-no-espaco-cibernetico/>. Acesso em: 19 abr. 2022.

DOUHET, Giulio. Il dominio dell'aria: probabili aspetti della guerra futura e gli ultimi scritti. 2. ed. Verona: A. Mondadori, 1932. 430 p ISBN (enc.)

HUREL, Louise Marie. Cibersegurança no Brasil: uma análise da estratégia nacional, 2021. Disponível em: <https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf>. Acesso em: 18 mai. 2022.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. Global Cybersecurity Index, 2020. Disponível em: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx/>. Acesso em: 25 mar. 2022.

_____. National Cybersecurity Strategies Repository, 2022. Disponível em: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx>. Acesso em: 06 jun. 2022.

KIENER, Wolfgang. Crescem as ameaças cibernéticas no transporte marítimo, 2020. Disponível em: <https://cryptoid.com.br/identidade-digital-destaques/crescem-as-ameacas-ciberneticas-no-transporte-maritimo/>. Acesso em: 19 abr. 2022.

KREUZER, Michael P. Cyberspace is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age, 2021. Disponível em: <https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age#:~:text=A%20domain%20of%20warfare%20%20is,the%20conduct%20of%20military%20operations>. Acesso em 10 abr. 2022.

LATHA, Keerthi. Learn About Intrusion Detection and Prevention, 2016. Disponível em: <https://www.juniper.net/documentation/en_US/learn-about/LA_IntrusionDetectionandPrevention.pdf>. Acesso em: 16 jun. 2022.

MAHAN, A. T. The influence of sea power upon history, 1660-1783**.** New York: Barnes & Noble, 2004. 494 p. ISBN 2005284415.

MANDARINO, R. J.; CANONGIA, Claudia. Livro Verde Segurança Cibernética no Brasil. Brasília, DF, 2010. Disponível em: <.https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf>. Acesso em 15 mai. 2022

MARIN, Jorge. Ataque hacker ao STJ é o pior da história do Brasil, 2020. Disponível em: <https://www.tecmundo.com.br/seguranca/206233-ataque-hacker-ter-atingido-stj-pf-investiga.htm>. Acesso em: 29 mai. 2022.

MCCALLION, Jane. O que é a Lei de Uso Indevido de Computadores?, 2022. Disponível em: <https://www.itpro.co.uk/it-legislation/28174/what-is-the-computer-misuse-act#:~:text=The%20Computer%20Misuse%20Act%20(CMA,the%20permission%20of%20the%20owner.>. Acesso em: 14 jun. 2022.

MEYER, Eric; MONTOYA, Michael. Como proteger a infraestrutura crítica contra ataques cibernéticos, 2022. Disponível em: <https://infrafm.com.br/Textos/1/22240/Como-proteger-a-infraestrutura-crtica-contra-ataques-ciberneticos>. Acesso em: 27 jul. 2022.

MORGAN, Steve. Cybercrime To Cost The World $10.5 Trillion Annually By 2025, 2020. Disponível em: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>. Acesso em: 03 mar. 2022.

NGUYEN, Nam. Evolution of the battlefield: Strategic and legal challenges to developing an effective cyber warfare policy. Australian Defence Force Journal, no. 196, 2015. p. 60-69. Disponível em: <https://search.informit.org/doi/epdf/10.3316/informit.377936686445802>. Acesso em: 04 abr. 2022.

NYE JR, J. S. Cyber Power. Havard Kennedy School - Belfer Center for Science and International Affairs, mai. 2010. Disponível em: <https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf>. Acessado em: 16 abr. 2022.

ORGANIZAÇÃO MARÍTIMA INTERNACIONAL - OMI. The International Ship and Port Facility (ISPS) Code, 2004. Disponível em: <https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx>. Acesso em: 03 jun. 2022.

_____. Resolution MSC.428(98). Maritime Cyber Risk Management in Safety Management Systems, 2017. Disponível em: <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf>. Acesso em: 03 jun. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS - ONU. E-Government Development Index (EGDI), 2020. Disponível em: <https://publicadministration.un.org/egovkb/Data-Center>. Acesso em: 25 mar. 2022.

ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE - OTAN. NATO Terminology Database, 2019. Disponível em: <https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en>. Acesso em: 09 abr. 2022.

REINO UNIDO (RU). Computer Misuse Act 1990, 1990. Londres. Disponível em: <https://www.legislation.gov.uk/ukpga/1990/18/crossheading/computer-misuse-offences>. Acesso em: 14 jun. 2022.

_____. Centre for the Protection of National Infrastructure (CPNI), 2007. Londres. Disponível em: <https://www.cpni.gov.uk/>. Acesso em: 21 jun. 2022.

_____. The Strategic Defence and Security Review, 2010a. Londres. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf>. Acesso em: 12 jun. 2022.

_____. _____. Fact Sheet 18: Cyber Security, 2010b. Londres. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62500/Factsheet18-Cyber-Security.pdf>. Acesso em: 12 jun. 2022.

_____. The National Security Strategy, 2010c. Londres. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf>. Acesso em: 12 jun. 2022.

_____. The UK Cyber Security Strategy, 2011. Londres. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf >. Acesso em: 14 jun. 2022.

_____. The UK National Strategy for Maritime Security (NSMS), 2014. Londres. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/322813/20140623-40221_national-maritime-strat-Cm_8829_accessible.pdf>. Acesso em: 22 jun. 2022.

_____. National Security Strategy and Strategic Defence and Security Review, 2015. Londres. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf>. Acesso em: 15 jun. 2022.

_____. National Cyber Security Strategy 2016 to 2021, 2016a. Londres. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf>. Acesso em: 17 jun. 2022.

_____. The National Cyber Security Centre (NCSC), 2016b. Londres. Disponível em: <https://www.ncsc.gov.uk/>. Acesso em: 09 abr. 2022.

_____. Data Protection Act 2018 (UK GDPR), 2018a. Londres. Disponível em: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>. Acesso em: 17 jun. 2022.

_____. Code of Practice: Cyber Security for Ships, 2017. Londres. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf>. Acesso em: 24 jun. 2022.

_____. The Network and Information Systems Regulations 2018, 2018b. Londres. Disponível em: <https://www.legislation.gov.uk/uksi/2018/506/made>. Acesso em: 19 jun. 2022.

_____. The Cyber Assessment Framework (CAF), 2018c. Londres. Disponível em: <https://www.ncsc.gov.uk/collection/caf>. Acesso em: 19 jun. 2022.

_____. Maritime 2050 Navigating the Future, 2019. Londres. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872194/Maritime_2050_Report.pdf>. Acesso em: 22 jun. 2022.

_____. National Cyber Force (NCF), 2020a. Londres. Disponível em: <https://www.gov.uk/government/organisations/national-cyber-force>. Acesso em: 17 jun. 2022.

_____. Good Practice Guide Cyber Security for Ports and Port Systems, 2020b. Londres. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf>. Acesso em: 24 jun. 2022.

_____. The Integrated Review of Security, Defence, Development and Foreign Policy, 2021. Londres. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf>. Acesso em: 17 jun. 2022.

_____. National Cyber Strategy 2022, 2022a. Londres. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf>. Acesso em: 17 jun. 2022.

_____. Government Cyber Security Strategy, 2022b. Londres. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf>. Acesso em: 17 jun. 2022.

_____. Cyber Security Breaches Survey 2022, 2022c. Londres. Disponível em: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022#glossary>. Acesso em: 03 jul. 2022.

SANTOS, M. B. dos. Guardião Cibernético 3.0: maior exercício de defesa cibernética do hemisfério sul, 2021. Disponível em:

<https://gblogs.cisco.com/br/seguranca/marcelobezerra/guardiao-cibernetico-3-0/>. Acesso em: 23 jul. 2022.

SEEBECK, Lesley. Why the fifth domain is different, 2019. Disponível em: <https://www.aspistrategist.org.au/why-the-fifth-domain-is-different/>. Acesso em: 10 abr. 2022.

SILVA, Júlio Cezar Barreto Leite da. Guerra Cibernética: a guerra no quinto domínio, conceituação e princípios. Revista da Escola de Guerra Naval, Rio de Janeiro, v. 20, n. 1 , p. 193-210, jun. 2014.

SINGER, Peter W.; FRIEDMAN, Allan; PORTILHO JÚNIOR, Geraldo Alves. Segurança e guerra cibernéticas: o que todos precisam saber. Rio de Janeiro: Biblioteca do Exército, 2017. 357p. (Biblioteca do Exército; 952). ISBN 9788570115898.

THOMPSON, David; GAGNON, G. J.; MCLEOD, C. W. Space as a War-fighting Domain, 2018. Disponível em: <https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-32_Issue-2/SLP-Thompson.pdf>. Acesso em: 10 abr. 2022.

UNIVERSIDADE DE OXFORD - UO. The Cybersecurity Capacity Maturity Model for Nations (CMM), 2021. Disponível em: <https://gcscc.ox.ac.uk/the-cmm>. Acesso em: 27 jul. 2022.

VENTRE, Daniel. Ciberguerra, 2011. Academia General Militar. Seguridad global y potências emergentes em um mundo multipolar. XIX Curso Internacional de Defensa. Disponível em: <https://publicaciones.defensa.gob.es/media/downloadable/files/ links/P/D/PDF48.pdf>. Acesso em: 10 abr. 2022.

# ANEXO A – Figuras

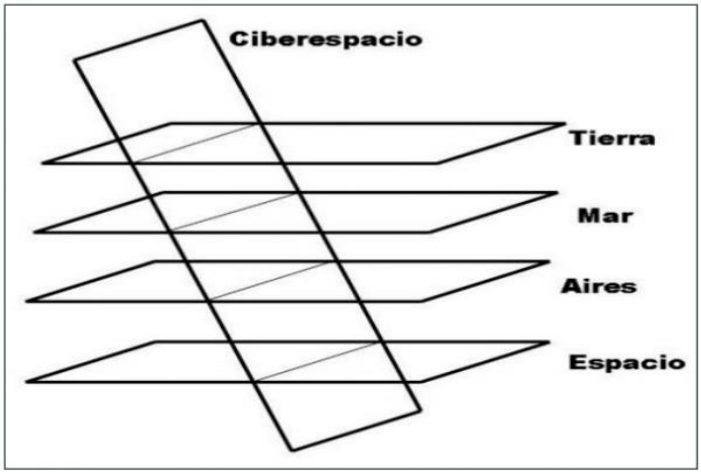



Figura 1 - Relação do Espaço Cibernético com os demais espaços geográficos
Fonte: Ventre (2011, p. 34)

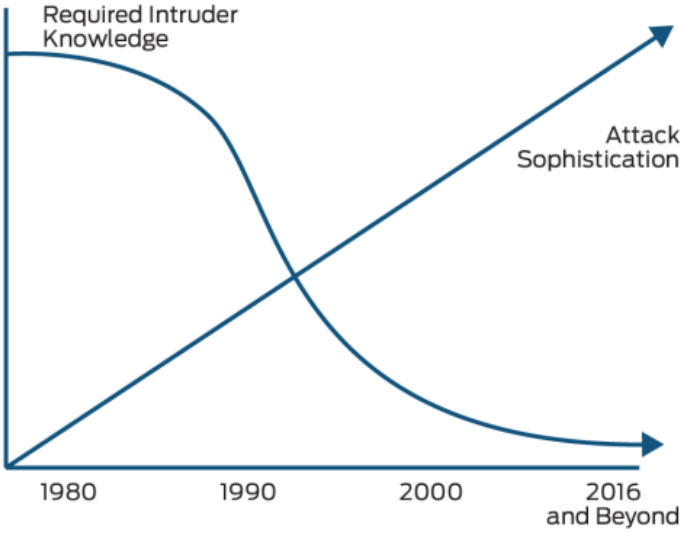



Figura 2 - Conhecimento necessário de um intruso versus a sofisticação do ataque
Fonte: Latha (2016, p. 2)


Figura 3 - Grupos Técnicos de Segurança de Infraestruturas Críticas do GSI/PR.
Obs.: Peganbio: Petróleo, Gás Natural e Biocombustíveis.
Fonte: GSI/PR (2022)

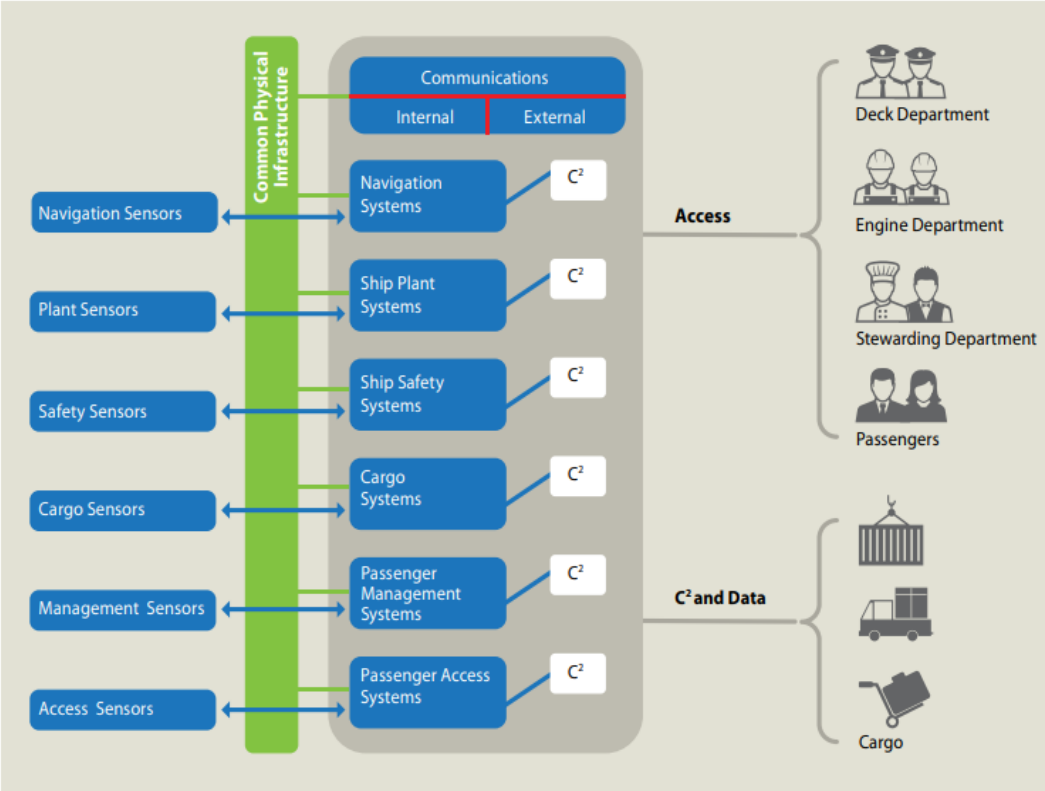



Figura 4 - Sistemas Básicos de um navio
Fonte: RU, 2017, p. 19

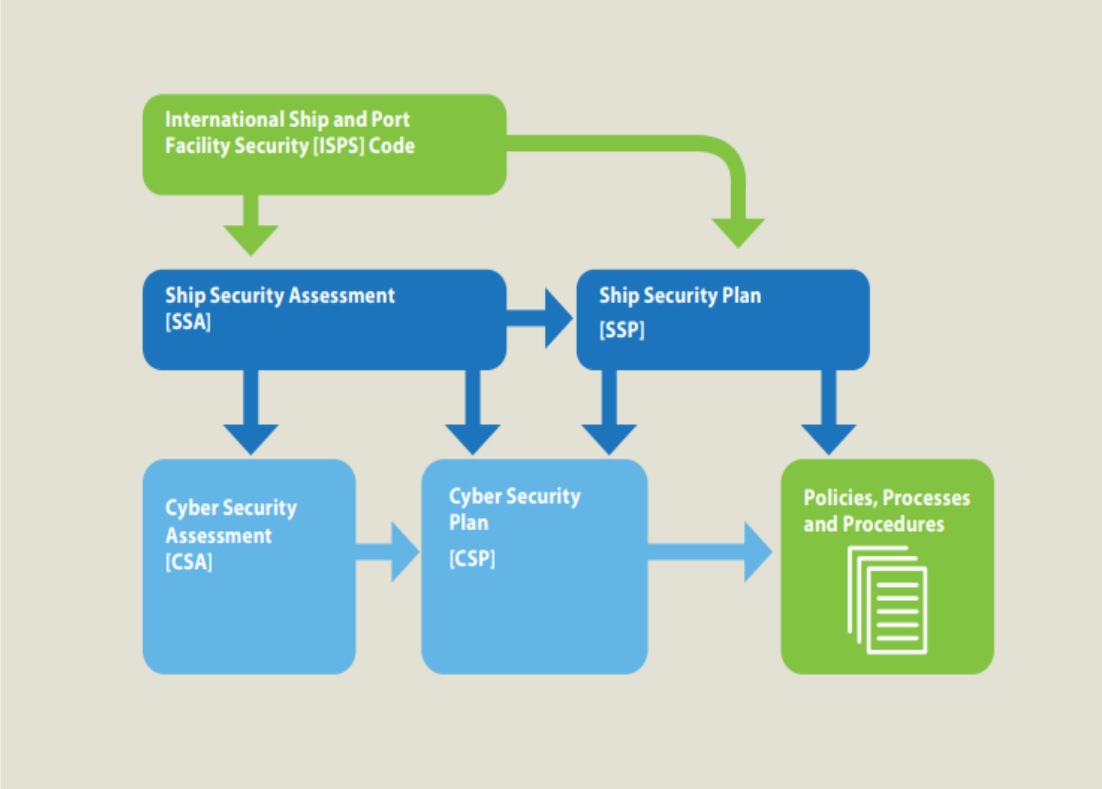



Figura 5 - relação do CSA e CSP com o Código ISPS, a SSA e o SSP
Fonte: RU, 2017, p. 21

**ANEXO B - E-mail do GSI/PR**

RES: Subsídios para Tese no C-PEM na EGN 11 de julho de 2022 17:30

De: "Marcio Braga" <xxxx@presidencia.gov.br>
Para: "Marcio Rebello" <yyyy@marinha.mil.br>

Boa tarde CMG Marcio Rebello!

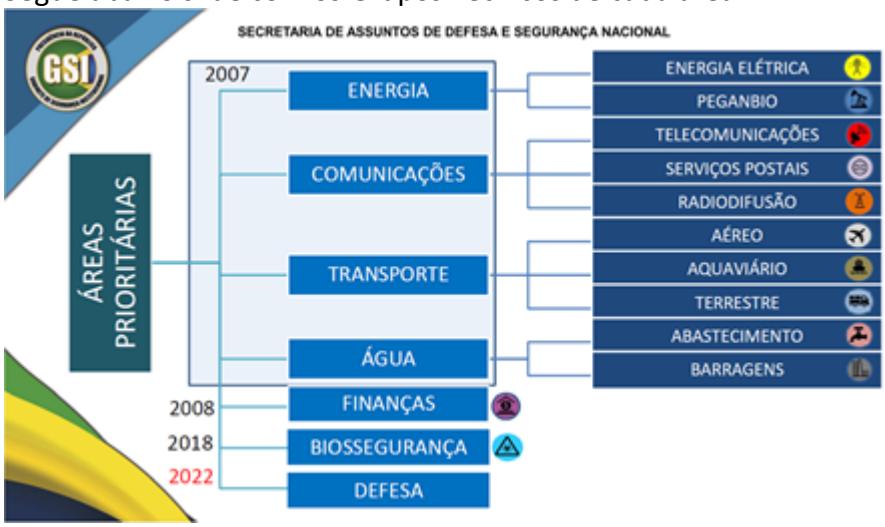
Vamos as respostas:
1 – As infraestruturas críticas, especialmente as relacionadas ao mar, já foram identificadas?? Se sim, quais são??
Sim, já foram. Elas foram identificadas ao longo dos estudos de dois Grupos Técnicos de Segurança de Infraestruturas Críticas coordenados pelo GSI/PR: no de Transportes Aquaviários (Portos e Terminais) e no de Petróleo, Gás Natural e Biocombustíveis (Unidades de Exploração e Produção Marítimas - UEP). A Lista dessas Infraestruturas é considerada sigilosa pelo GSI/PR, não podendo ser divulgada, exceto com a autorização do Ministro–Chefe. Contudo, podemos dizer que hoje consideramos 29 Portos/Terminais (entre públicos e privados) como Infraestruturas Críticas, de um total de 235 estudados. Em relação às UEP Marítimas foram identificadas 23 como Infraestruturas Críticas, de um total de 111 estudadas.
2 – Qual são os órgãos do governo responsáveis pela segurança delas, e suas atribuições?
A segurança patrimonial dessas Infraestruturas é de responsabilidade dos seus próprios administradores. No caso dos Portos Públicos ela é exercida pelas Guardas Portuárias, que podem manter efetivos para realizá-la ou, apenas, executar a supervisão de efetivos terceirizados. Nos Terminais Privados, a segurança patrimonial é exercida por funcionários da própria empresa, ou por empresas terceirizadas, ocorrendo o mesmo em relação às UEP Marítimas do Setor de petróleo e gás.
No entanto, a segurança pública nas áreas alfandegadas dos Portos/Terminais está sob responsabilidade da Polícia Federal, por meio de agentes que integram os NEPOM (Núcleos Especiais de Polícia Marítima) e/ou outras estruturas policiais, como as de controle imigratório e combate ao tráfico de drogas e armas, por exemplo. Nela também atuam outras entidades do Estado, cada qual com suas responsabilidades, como a RFB, Vigiagro, ANVISA, MB, dentre outros.
3 – Como o GSI tem trabalhado para realizar a segurança delas, especialmente contra uma ameaça cibernética??
De acordo com o inciso XI, do Art. 10, da Lei 13.844/2019, cabe ao GSI/PR “acompanhar assuntos pertinentes às infraestruturas críticas, com prioridade aos relacionados à avaliação de riscos.”

Assim sendo, o GSI/PR tem realizado as seguintes ações, visando cumprir o inciso acima mencionado:
a) Criação da Política Nacional de Segurança de Infraestruturas Críticas (Decreto nº 9.573/2018);

b) Criação da Estratégia Nacional de Segurança de Infraestruturas Críticas (Decreto n° 10.569/2020);
c) Realização de reuniões e estudos anuais, afetos à sete áreas prioritárias, desenvolvidos por treze Grupos Técnicos multidisciplinares, com objetivos:
- Identificar as Infraestruturas Críticas de cada setor;
– Identificar ameaças, vulnerabilidades e medidas de contingência para cada Infraestrutura Crítica selecionada;
– Realizar análise de riscos de cada Infraestrutura Crítica;
– Elaborar um Diagnóstico Nacional de cada Setor; e
– Analisar as interdependências existentes entre as Infraestruturas Críticas identificadas.
d) Criação de um Plano Nacional de Segurança de Infraestruturas Críticas (a ser publicado ainda neste ano);
e) Desenvolvimento de um Sistema Integrado de Dados de Infraestruturas Críticas (SIDSIC) que irá permitir o assessoramento do Ministro-Chefe e do Presidente, em caso de instauração de gabinetes de crises (em construção, com previsão de estar operacional ainda em 2022);
f) Divulgação dos trabalhos e desenvolvimento de mentalidade voltada para o tema, por meio de palestras e seminários realizados; e
g) Emissão de pareceres para subsidiar Notas Técnicas e Interditos Proibitórios junto à justiça, no caso de ameaças que possam provocar a paralisação das Infraestruturas Críticas identificadas.
Não cabe ao GSI/PR realizar a segurança física dos ativos existentes nas Infraestruturas Críticas. No entanto, no caso dos Portos/Terminais, o Art. 6º do Decreto nº 6.869/2009, atribui ao GSI/PR, as seguintes responsabilidades;
I – determinar a alteração para o nível três de proteção dos navios de bandeira brasileira e das instalações portuárias, quando julgar necessário;
II – comunicar ao Presidente da República, quando julgado conveniente, a ocorrência de incidente de proteção em navios na região de busca e salvamento marítimo brasileira ou nas bacias Amazônica e Paraguai/Paraná; e
III – monitorar os níveis de proteção vigentes nas instalações portuárias e nos navios de bandeira brasileira.
§ 1o O Gabinete de Segurança Institucional será o responsável pela coordenação das medidas de proteção para serem cumpridas nas instalações portuárias, quando estas estiverem operando no nível três de proteção, competindo ao comandante de cada navio a implementação das medidas correspondentes a bordo.
§ 2o Quando as instalações portuárias estiverem em nível três de proteção, será constituído colegiado formado por representantes dos Ministérios da Defesa, da Justiça, das Relações Exteriores, da Fazenda, dos Transportes, da Secretaria Especial de Portos, da Casa Civil da Presidência da República e do Gabinete de Segurança Institucional, sob a coordenação deste último, com as seguintes atribuições:
I – articular as ações de caráter político estratégico;
II – coordenar junto ao Ministério das Relações Exteriores solicitações relativas às medidas de proteção envolvendo países estrangeiros;
III – centralizar a comunicação social, de modo a divulgar adequadamente, antecipando-se a possível repercussão nacional e internacional;
IV – orientar as ações do comando operacional local na execução das medidas de proteção específicas correspondentes ao nível três de proteção, nas instalações portuárias;

V – fixar o período de vigência das medidas adicionais relativas ao nível três de proteção das instalações portuárias;
VI – prover apoio de informações à autoridade responsável pelo controle operacional na área portuária e meios adicionais, de acordo com a evolução do “incidente de proteção”; e
VII – comunicar ao Presidente da República a ocorrência de incidente de proteção do nível três, com manifestação fundamentada acerca da necessidade ou não de emprego das Forças Armadas na garantia da lei e da ordem, e se estão presentes os requisitos dispostos na Lei Complementar no 97, de 1999.
§ 3o  As medidas de proteção específicas para o nível três serão adotadas pelos órgãos representados na Comissão Estadual de Segurança Pública nos Portos, Terminais e Vias Navegáveis com atuação na área, conforme suas atribuições constitucionais e na forma estabelecida nos planos operacionais.
A maioria dessas ações poderá ser colocada em prática por meio de um Decreto Presidencial, autorizando ao MD o uso das Forças Armadas em ações de GLO, para intervenção em uma Instalação Portuária que estiver em nível III de proteção.

Segue abaixo slide com os Grupos Técnicos de cada área.




Obs.: Peganbio: Petróleo, Gás Natural e Biocombustíveis.

Qualquer dúvida, sigo à disposição.
Respeitoso abraço,

CF Marcio Braga

## APÊNDICE A – Tabelas

**TABELA 1**
**Relação dos países, em ordem crescente de suas respectivas classificações, que participaram e estão melhor classificados do que o Brasil no GCI 2020**

| PAÍS | CLASSIFICAÇÃO |
|---|---|
| Reino Unido | 2 |
| Arábia Saudita | 2 |
| Estônia | 3 |
| República da Coreia | 4 |
| Cingapura | 4 |
| Espanha | 4 |
| Federação Russa | 5 |
| Emirados Árabes Unidos | 5 |
| Malásia | 5 |
| Lituânia | 6 |
| Japão | 7 |
| França | 10 |
| Índia | 10 |
| Turquia | 11 |
| Austrália | 12 |
| Luxemburgo | 13 |
| Alemanha | 13 |
| Portugal | 14 |
| Letônia | 15 |
| Ilhas Maurício | 17 |
| Brasil | 18 |

Fonte: ITU, 2020

**TABELA 2**
**Relação dos 20 países melhor classificados do que o Brasil no GCI 2020, com suas respectivas classificações no EGDI 2020**

| PAÍS | CLASSIFICAÇÃO |
|---|---|
| República da Coreia | 2 |
| Estônia | 3 |
| Austrália | 5 |
| Reino Unido | 7 |
| Cingapura | 11 |
| Japão | 14 |
| Espanha | 17 |
| França | 19 |
| Lituânia | 20 |
| Emirados Árabes Unidos | 21 |
| Alemanha | 25 |
| Luxemburgo | 33 |
| Portugal | 35 |
| Federação Russa | 36 |
| Arábia Saudita | 43 |
| Malásia | 47 |
| Letônia | 49 |
| Turquia | 53 |
| Brasil | 54 |
| **Ilhas Maurício** | **63** |
| **Índia** | **100** |

Fonte: ONU, 2020

**TABELA 3**

**Políticas e Estratégias afetas as IC – Se existe, dentro das Políticas e Estratégias publicadas, alguma citação sobre a necessidade de proteção das IC, principalmente contra as ameaças cibernéticas.**

| | Brasil | Reino Unido |
|---|---|---|
| **Políticas e Estratégias afetas as IC** | **END (2012):** "o desenvolvimento da capacitação, o preparo e o emprego dos poderes cibernéticos nos níveis operacional e estratégico, em prol da proteção das infraestruturas estratégicas".<br>**LBDN:** "a ameaça cibernética se tornou uma grande preocupação por ameaçar a integridade das IC".<br>**END (2016):** "deverá haver contribuição para o aumento do nível de segurança das Estruturas Críticas".<br>**PNSIC:** "tem a finalidade de garantir a resiliência e a segurança das IC do País"<br>**ENSIC:** "estabelece os princípios básicos para a segurança das IC, e aponta os principais desafios a serem vencidos"; "Estimular o uso de recursos e de procedimentos visando elevar a segurança cibernética nas IC"<br>**E-DIGITAL:** "Elaborar planos nacional e subnacionais de prevenção, resposta a incidentes e mitigação de<br>ameaças cibernéticas, inclusive no âmbito de IC".<br>**E-CIBER**: "Elevar o nível de proteção das Infraestruturas Críticas Nacionais"; "Incentivar ações de segurança cibernética pelas IC". | **Estratégia de Segurança Nacional (2010):** "garantir um Reino Unido resiliente e seguro, através da proteção de vários ativos nacionais, como a população, a economia, as IC, e o território, das principais ameaças, como o terrorismo e o ataque cibernético".<br>**Estratégia Nacional de Segurança Cibernética (2011):** "contínuo melhoramento da detecção e análise das ameaças cibernéticas, principalmente focado nas IC, e outros sistemas de interesse nacional".<br>**Estratégia de Segurança Nacional e a Revisão da Estratégia de Defesa e Segurança (2015):** "a garantia da segurança e resiliência das IC contra ataques cibernéticos é uma prioridade para o governo"; "o Governo trabalhará junto com os proprietários e operadores a fim de fortalecer a segurança cibernética das IC".<br>**Regulamentos NIS:** "visam aumentar os níveis de segurança cibernética das IC". |

Fonte: Próprio autor, 2022

**TABELA 4**

**Políticas e Estratégias afetas as ICM – Políticas e Estratégias afetas as ICM – Se existe, dentro das Políticas e Estratégias publicadas, alguma citação sobre a necessidade de uma proteção específica das ICM, principalmente contra ameaças cibernéticas.**

| | Brasil | Reino Unido |
|---|---|---|
| **Políticas e Estratégias afetas as ICM** | XXX | **Estratégia Nacional para a Segurança Marítima:** "incluiu o ataque cibernético à ICM do Reino Unido como um dos principais riscos de segurança marítima"<br>**Código de Prática: Segurança Cibernética para Navios:** "destina-se a complementar as normas de segurança dos navios e respectivos requisitos, fornecendo orientações adicionais sobre os aspectos de proteção cibernética"<br>**Guia de Boas Práticas: Segurança Cibernética para Portos e Instalações Portuárias:** "destina-se a complementar padrões de segurança dos portos e seus respectivos requisitos, fornecendo orientações complementares sobre os aspectos das medidas de segurança cibernética"<br>**Marítimo 2050: Navegando o Futuro:** "As empresas responsáveis pelas ICM tem o ônus de proteger e garantir a resiliência às ameaças cibernéticas"; "de modo a permanecer seguro, protegido e resiliente diante das ameaças cibernéticas o Setor de Transportes do Reino Unido necessita alcançar alguns objetivos que foram estipulados" |

Fonte: Próprio autor, 2022

**TABELA 5**
**Cooperação Nacional – Interações cooperativas, principalmente com a troca de informações, entre os setores público e privado, academia e outros atores locais (indivíduos e organizações).**

| | Brasil | Reino Unido |
|---|---|---|
| **Cooperação Nacional** | **PNSIC:** "a desejável cooperação e parcerias entre os setores privado e público, a fim de elevar o nível de segurança das IC"; "o incentivo à cooperação com organizações internacionais e nacionais, visando o aprimoramento da segurança das IC"<br>**ENSIC:** "é necessária uma grande cooperação entre o Governo Federal e o setor privado, a fim de que haja uma união de esforços na proteção e resiliência das IC"<br>E-CIBER: "Ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e a sociedade**"**<br>**REGIC**: "e o incremento da cooperação entre todos os participantes da Rede"; "A troca de informações afetas aos incidentes cibernéticos, entre as ETIR Setoriais e o CTIR Gov, torna-se obrigatória" | **Revisão Estratégica de Defesa e Segurança (2010):** "e construir novas acordos de cooperação na área de segurança cibernética"<br>**Estratégia de Segurança Nacional (2010):** "as empresas e governo precisarão trabalhar muito mais juntos, a fim de robustecer a defesa contra ataques cibernéticos"<br>**Estratégia Nacional de Segurança Cibernética (2011):** "prevê uma nova fase de cooperação entre o Governo e o setor privado na área de segurança cibernética"<br>**Estratégia de Segurança Nacional (2015):** "é imprescindível que haja uma estreita cooperação entre os setores público e privado, com troca de informações e experiências"<br>**Estratégia Cibernética Nacional (2022):** "aumentar a parceria entre governo, academia e indústria" |

Fonte: Próprio autor, 2022

**TABELA 6**

**Cooperação Internacional – Interações cooperativas entre os órgãos nacionais com órgãos de outros países, principalmente com a troca de informações.**

| | Brasil | Reino Unido |
|---|---|---|
| **Cooperação Internacional** | **END / PND (2012):** "estabelecem a importância da cooperação nacional e internacional, com participação da academia para desenvolver a pesquisa de novas tecnologias que serão empregadas na segurança cibernética"<br>**PNSIC:** "o incentivo à cooperação com organizações internacionais e nacionais, visando o aprimoramento da segurança das IC"<br>**E-CIBER**: "Ampliar a cooperação internacional do Brasil em Segurança cibernética" | **Estratégia de Segurança Nacional (2015):** "Foram estabelecidas parcerias com os países aliados, com troca de conhecimentos especializados"<br>**Revisão Integrada de Segurança, Defesa, Desenvolvimento e Política Externa**: "onde serão consideradas todas as capacidades do país no desenvolvimento de tecnologias cibernéticas críticas, bem como na cooperação internacional" |

Fonte: Próprio autor, 2022

**TABELA 7**
**Conscientização da Sociedade – Ações ou diretrizes sobre a divulgação de orientações básicas sobre cibersegurança.**

| | Brasil | Reino Unido |
|---|---|---|
| **Conscientização da Sociedade** | **PNSI:** "o fortalecimento da mentalidade de segurança da informação dentro da sociedade brasileira"<br>**E-CIBER:** "Elevar o nível de maturidade da sociedade em segurança cibernética" | **Estratégia de Segurança Cibernética (2011):** "o Fique Seguro Online (*Get Safe Online*) visa conscientizar a população e as pequenas e médias empresas sobre as medidas de prevenção e segurança no espaço cibernético"<br>**Estratégia Nacional de Segurança Cibernética (2016):** "A Campanha Ciber Consciente (*Cyber Aware*) fornece conselhos à população, com as diretrizes necessárias para se protegerem de cibercriminosos, através de mensagens dirigidas, veiculadas por meio das redes sociais e campanhas publicitárias" |

Fonte: Próprio autor, 2022

**TABELA 8**

**Recrutamento/ Capacitação de Recursos Humanos na Área Cibernética– Ações ou diretrizes voltadas para atrair novas pessoas para essa área de trabalho, e/ou medidas que visem melhorar a capacitação da mão de obra existente hoje no mercado.**

| | Brasil | Reino Unido |
|---|---|---|
| **Recrutamento/ Capacitação de Recursos Humanos na Área Cibernética** | **PCD:** "capacitar recursos humanos necessários à condução das atividades cibernéticas"<br>**ENINT:** "promoção da qualificação técnica de recursos humanos"<br>**PNSI:** "destacam-se: o incentivo da formação e da qualificação de recursos humanos afetos à área"<br>**E-CIBER:** "estimular a criação de cursos de nível superior em segurança cibernética"; "propor a criação de programas de incentivo para graduação e pós-graduação no Brasil e no exterior em segurança cibernética"; "criar programas de capacitação continuada para profissionais do setor público e do setor privado"; "incentivar a formação de profissionais para atuar no combate aos crimes cibernéticos" | **Estratégia de Segurança Nacional (2015): "**Para a capacitação de recursos humanos na área cibernética, será criado um programa nas escolas para identificar e incentivar novos talentos entre jovens de 11 a 17 anos em todo o país, que será o Programa Primeiro Ciber (CyberFirst)"; "outro programa é o Desafio de Cibersegurança (*Cyber Security Challenge* ), cujo objetivo é encontrar e nutrir talentos de segurança cibernética, além de atrair novas pessoas para o mercado"<br>**Estratégia Cibernética Nacional (2022):** "Robustecer o sistema cibernético do país, investindo em pessoal e habilidades"; "criação de uma ampla gama de iniciativas extracurriculares para inspirar os jovens a seguir uma carreira em segurança cibernética" |

Fonte: Próprio autor, 2022

**TABELA 9**

**Órgão responsável de Defesa e Segurança Cibernética das IC/ICM – Identificar a existência de órgãos responsáveis pela Defesa e Segurança Cibernética das IC/ICM.**

| | Brasil | Reino Unido |
|---|---|---|
| **Órgão responsável de Defesa e Segurança Cibernética das IC/ICM** | **PNSIC: "**designa o GSI/PR como sendo o responsável por realizar o acompanhamento dos assuntos pertinentes às IC no âmbito da APF";<br>**E-CIBER:** "ficará a cargo do GSI/PR a coordenação da segurança cibernética em âmbito nacional, que possibilite a atuação de modo amplo, cooperativo, participativo, e alinhado com as ações de defesa cibernética, a cargo do Ministério da Defesa" | **Estratégia Nacional de Segurança Cibernética (2016):** "O NCSC é órgão central da segurança cibernética do Reino Unido" |

Fonte: Próprio autor, 2022

**TABELA 10**
**Arcabouço Legislativo sobre Crimes Cibernéticos – Identificar as leis que tipifiquem os crimes cibernéticos.**

| | Brasil | Reino Unido |
|---|---|---|
| **Arcabouço Legislativo sobre Crimes Cibernéticos** | **Lei nº 12.737/2012**<br>**Lei nº 14.155/2021** | **Lei de Uso Indevido de Computadores** |

Fonte: Próprio autor, 2022