ÁLVARO LOBO COSTA
ANDRÉ LUIZ ALVES FERREIRA
VICTOR JOSÉ QUEIROZ CABRAL

A CRIAÇÃO DE UMA AGÊNCIA BRASILEIRA DE SEGURANÇA CIBERNÉTICA COMO ESTRATÉGIA DE DEFESA NACIONAL

Trabalho de Conclusão de Curso apresentado à Escola Superior de Defesa, como exigência parcial para obtenção do título de Especialista em Altos Estudos em Defesa.

Orientador: Prof. Maj QCO R1 Carlos Maurício de Borges Mello

Brasília
2022

ÁLVARO LOBO COSTA
Idt 864094 SSP/DF

ANDRÉ LUIZ ALVES FERREIRA
Idt 472765 MD/FAB

VICTOR JOSÉ QUEIROZ CABRAL
Idt 011102464-2 MD/EB

ÁLVARO LOBO COSTA
ANDRÉ LUIZ ALVES FERREIRA
VICTOR JOSÉ QUEIROZ CABRAL

A CRIAÇÃO DE UMAAGÊNCIA BRASILEIRA DE SEGURANÇA CIBERNÉTICA COMO ESTRATÉGIA DE DEFESA NACIONAL

Trabalho de Conclusão de Curso apresentado à Escola Superior de Defesa, como exigência parcial para obtenção do título de Especialista em Altos Estudos em Defesa.

Trabalho de Conclusão de Curso **APROVADO**:

Brasília, DF, 21 de outubro de 2022

CARLOS MAURÍCIO DE BORGES MELLO – Maj R1 EB (ESD)
Orientador

IVAN CARLOS SOARES DE OLIVEIRA - Cel R1 EB (ESD)
Membro 1

MARCO AURÉLIO CARVALHO LEANDRO – CF RM1 (ESD)
Membro 2

A criação de uma agência brasileira de segurança cibernética como estratégia de defesa nacional

Álvaro Lobo Costa[1]
André Luiz Alves Ferreira[2]
Victor José Queiroz Cabral[3]

RESUMO

A segurança cibernética dos ativos de informação é um tema de interesse para a Defesa Nacional. Este trabalho, realizado de forma pioneira por alunos da Escola Superior de Defesa (ESD), trata-se de uma reflexão dos riscos decorrentes das ameaças que trafegam no espaço cibernético. O objetivo geral foi propor a solução do problema identificado, que é a vulnerabilidade do Estado brasileiro diante de tais ameaças. Inicialmente, foram apresentadas as lacunas no arcabouço normativo de governança que resultam em conflitos de competência entre os órgãos da administração pública. Para tanto, fez-se necessário também observar como foi construída a governança no mundo da internet. Em um segundo momento, buscou-se apresentar os desafios de normatização da homologação e certificação de produtos de Tecnologia da Informação e Comunicação (TIC). O texto apresenta alertas sobre as vulnerabilidades da existência de produtos não certificados em segurança cibernética, mesmo com os avanços regulatórios da Agência Brasileira de Telecomunicações (Anatel). Por fim, os autores realizam uma sugestão, propondo a criação de uma agência regulatória específica, a partir da inspiração de uma matriz consagrada, a Agência Brasileira de Inteligência (ABIN). A conclusão do trabalho mostrou que esta Agência Brasileira de Segurança Cibernética pode mitigar a vulnerabilidade estatal constatada, que coloca em risco a Defesa Nacional.

Palavras-chave: governança no ciberespaço; segurança cibernética; infraestruturas críticas.

The creation of a brazilian cyber security agency as a national defense strategy

ABSTRACT

The cyber security of information assets is a topic of interest for National Defense. This work, carried out in a pioneering way by students from the Escola Superior de Defesa (ESD), *is a reflection of the risks arising from the threats that travel in cyberspace. The general objective was to propose a solution to the identified problem, which is the vulnerability of the Brazilian State in the face of such threats. Initially, the gaps in the normative framework of governance that result in conflicts of competence between the bodies of the public administration were presented. Therefore, it was also necessary to observe how governance was built in the internet world. In a second moment, we sought to present the challenges of standardizing the approval and certification of Information and Communication Technology (ICT) products. The text presents alerts about the vulnerabilities of the existence of uncertified products in cyber security, even with the regulatory advances of the Brazilian Telecommunications Agency* (Anatel). *Finally, the authors make a suggestion, proposing the creation of a specific regulatory agency, based on the inspiration of an established matrix, the Brazilian Intelligence Agency* (ABIN). *The conclusion of the work showed that this Brazilian Cyber Security Agency can mitigate the verified state vulnerability, which puts National Defense at risk.*

Keywords*: governance in cyberspace; cyber security; critical infrastructures.*

[1] Especialista em Gestão de Telecomunicações da TELEBRAS S.A.
[2] Coronel Aviador da Força Aérea Brasileira
[3] Coronel de Comunicações do Exército Brasileiro

1 INTRODUÇÃO

A Estratégia Nacional de Defesa (END), desde a sua primeira edição, escrita em 2008, define a área Cibernética como um dos três setores estratégicos para o fortalecimento da Defesa Nacional (BRASIL, 2018c). A motivação surgiu a partir dos ataques cibernéticos ocorridos na Estônia, no ano anterior, evento este que inviabilizou quase a totalidade dos serviços públicos daquele país e que foram atribuídos a *hackers* russos.

Ao longo das últimas décadas, novas ferramentas e mecanismos de Tecnologia da Informação e Comunicação (TIC) passaram a integrar o cotidiano e revolucionaram a "Era do Conhecimento". O evento ocorrido na Estônia confirmou a crescente dependência dos estados ao espaço cibernético e, consequentemente, à maior percepção de ameaças que exploram suas vulnerabilidades. O espaço no qual circulam ativos de informação também pode ser usado como arma de guerra. Assim, a proteção de infraestruturas críticas faz-se mister para a Defesa Nacional.

A revolução tecnológica acelerou a estruturação do setor cibernético no Brasil, trazendo o assunto para a pauta de discussão dos setores público e privado. No Brasil, o primeiro marco legal foi a Política Nacional de Informática, de 1984, enquanto que o primeiro órgão afeto ao setor, o Departamento de Segurança da Informação e Comunicações (DSIC), posteriormente renomeado Departamento de Segurança da Informação (DSI), foi criado apenas em 2006, dentro da estrutura organizacional do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

O Decreto nº 3.505 instituiu a Política de Segurança da Informação no ano 2000, porém não foram realizadas considerações específicas sobre o espaço cibernético, ainda sem muito destaque naquela época. Este cenário mudou em 2018, após a edição do Decreto nº 9.637, Política Nacional de Segurança da Informação (PNSI), principal marco regulatório do setor na atualidade.

O termo "cibernética" se refere à comunicação e controle, relacionado ao uso de sistemas computacionais, redes de comunicação e suas interações. "No campo da Defesa Nacional, inclui os recursos estratégicos de TIC e os sistemas administrativos que possam afetar as atividades em geral" (BRASIL, 2020b). No Brasil, antes da consolidação do termo, as políticas públicas relacionadas ao setor eram chamadas apenas como Segurança da Informação (NETO, 2020, p. 57).

Segundo Fontenele (2022), atual Diretor do DSI, existe uma distinção entre segurança da informação e segurança cibernética. Para ele, o espaço físico no qual circulam informações

fora do espaço cibernético, via de regra exclusivamente em documentos físicos, é cada vez menor, devido à crescente revolução digital que ocorre nos dias atuais. Por outro lado, também existem tecnologias que se utilizam do espaço cibernético, mas que não necessariamente trafegam informações, tais como dados de telefonia celular ou sistemas de tecnologia de automação industrial.

Cabe salientar que não existem barreiras físicas no espaço cibernético e os ativos de informação trafegam livremente. O Comitê Gestor da Internet no Brasil (CGI.br)[4] foi o modelo de governança híbrido adotado entre governo, sociedade civil e academia, para uma solução compartilhada. Tal solução tornou-se única, haja vista a estabilidade e a regulamentação da internet serem concentradas por instrumentos privados, tais como a *Internet Corporation for Assigned Names and Numbers* (ICANN)[5] que gerencia os protocolos "IPs" e sistemas de nomes e domínios (DNS) a nível mundial.

Além do aspecto legal, novas tecnologias estão em constante evolução e surgem a todo o momento. O uso de tecnologias disruptivas, como a Inteligência Artificial (IA), podem auxiliar na proteção e segurança das redes governamentais e de infraestruturas críticas nacionais. O ataque ao Ministério da Saúde, ocorrido em dezembro de 2021, em que *hackers* conseguiram apagar dados sobre vacinas e registros de casos e óbitos relacionados à pandemia da COVID-19, poderia ser evitado através do uso de IA. As aplicações de segurança proporcionam a autoaprendizagem aos usuários, trabalhando com dados históricos de ataques para prever a próxima ameaça. Esta é uma nova tendência no mercado de soluções de segurança cibernética, que, aliada a estratégias como a arquitetura *zero trust*, podem melhorar a proteção de sistemas críticos.

As infraestruturas críticas nacionais, os órgãos da administração pública em suas diversas esferas e a sociedade civil possuem níveis variados de exigências de segurança cibernética. Sem uma normatização perfeita e a imposição de requisitos adequados por um órgão superior, cada ente busca se autoadministrar sem, contudo, resultar num processo contínuo de aperfeiçoamento. De outra sorte, as atribuições e competências para regulamentar, gerir e impor normas, padrões, políticas e estratégias, encontram-se dispersas por diversos

4 Comitê Gestor da Internet no Brasil (CGI.br) - possui a atribuição de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil e diretrizes para a execução do registro de Nomes de Domínio, alocação de Endereço IP (*Internet Protocol*) e administração pertinente ao Domínio de Primeiro Nível ".br". Também promove estudos e recomenda procedimentos para a segurança da Internet e propõe programas de pesquisa e desenvolvimento que permitam inovação no uso da internet. Disponível em: https://www.cgi.br/sobre/. Acesso em: 10 de junho de 2022.

5 *Internet Corporation for Assigned Names and Numbers* (ICANN) - é uma parceria mundial, sem fins lucrativos, de pessoas dedicadas a manter a Internet segura, estável, interoperacional e com o uso de identificadores únicos. Disponível em: https://www.icann.org/resources/pages/what-2012-02-25-pt. Acesso em: 9 de junho de 2022.

órgãos, o que dificulta a coordenação de esforços e uma governança adequada acerca dos assuntos relacionados à segurança cibernética.

Diante de tudo o que foi já explanado, identifica-se o problema que baliza o presente trabalho, que é a vulnerabilidade do Estado brasileiro diante de ameaças cibernéticas, que a cada dia exigem que os países estejam institucionalmente mais preparados para contrapô-las.

Nesse sentido, a criação de uma agência central regulatória teria a intenção de normatizar o setor, coordenar as ações, realizar a governança nos diversos níveis da sociedade e ser o principal instrumento de impulsão para fortalecer a segurança cibernética nacional.

A relevância do tema e a justificativa para a realização do presente estudo advém de sua importância para o país. Desde a primeira edição da Estratégia Nacional de Defesa, a segurança cibernética é definida como um dos três setores tecnológicos essenciais à Defesa Nacional.

No âmbito acadêmico, uma agência regulatória para o setor já vem sendo discutida, inclusive em estudos anteriores a este, como o trabalho apresentado na Escola Superior de Defesa, no ano de 2021, pelos Coronéis do Exército Nonato e Pinho (2021, p. 21), no qual, entre outras conclusões, sugeriram a criação de um órgão estatal.

O presente trabalho tem por objetivo geral de pesquisa buscar o incremento da segurança cibernética em nível nacional, que finde lacunas de gestão, normatizando o setor por meio de um órgão central que exerça a governança e as atividades de certificação. Diante do atual cenário mundial já descrito, no qual a ameaça cibernética é cada vez mais concreta e usada por indivíduos, grupos e países, o tema é relevante para as áreas de segurança, desenvolvimento e defesa do Brasil.

Em linhas gerais, o conteúdo em tela buscou alcançar três objetivos específicos como passos intermediários para melhor analisar o problema identificado. Dessa forma, o primeiro objetivo específico foi estudar o arcabouço normativo a fim de identificar as lacunas de governança no setor. O segundo foi estudar a necessidade de certificar e homologar produtos em segurança cibernética e o modelo adotado por agências que já executam atividades correlatas, a fim de salvaguardar as redes de dados e as informações que trafegam por elas. Por fim, o terceiro objetivo específico foi apresentar uma proposta de agência que reúna competências de órgão superior de caráter normativo e certificador. Como inspiração, estudou-se o modelo da Agência Brasileira de Inteligência (ABIN), vinculada ao GSI/PR.

Além de melhor gerir a segurança cibernética, uma agência minimizará os efeitos quando o país estiver sob ataque cibernético. Uma ação dessa natureza tem por objetivo espionar, gravar, alterar, manipular, interferir, roubar, sabotar e desestabilizar um estado e é

uma ferramenta para exercer poder por outros estados (BUCHANAN, 2020). No conflito na Ucrânia, muito se comenta sobre o emprego da "guerra cibernética". Além dos ataques convencionais, com blindados, mísseis e soldados, a Rússia tem empregado armas virtuais, que degradam o poder de defesa de seu oponente e afetam infraestruturas críticas, tanto militares quanto civis.

A metodologia adotada no presente trabalho se constituiu de numa abordagem do tipo qualitativa, com o uso de técnicas de pesquisa bibliográfica e documental, visando buscar referenciais e modelos comparativos. O principal meio utilizado foram sítios acadêmicos de busca e plataformas de bibliotecas indexadas da Rede BIE do Exército, além de outros de interesse, tais como do GSI/PR, Ministério da Defesa (MD), Comando de Defesa Cibernético (ComDCiber), CGI.br, *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE), ICANN, entre outros.

2 O SETOR CIBERNÉTICO

Nos primeiros anos do Século XXI, já com grande parte das conectividades mundiais estabelecidas, a internet consolidada e os ativos de informação circulando mundo afora, o Brasil encontrava-se em uma verdadeira escuridão normativa para o espaço cibernético. Os marcos jurídicos eram pontuais e discretos. O país tinha pela frente o desafio de organizar e disciplinar as ações de interesse do Estado sem, contudo, produzir limites e barreiras que prejudicasse a pujança e dinamismo dos setores privados. A estratégia seria mostrar ao mundo solidez e credibilidade de um país moderno que facilitasse a entrada de investimentos externos.

2.1 A GOVERNANÇA DA INTERNET NO MUNDO SEM FRONTEIRAS

A internet foi uma iniciativa do Departamento de Defesa dos Estados Unidos denominada *Defense Advanced Research Project Agency Network* (DARPA *Net*), nos anos de 1970, com recursos de comunicações eficientes para uma rede de pesquisas avançadas, que se expandiu depois da invenção e popularização a nível mundial de seu principal protocolo de transmissão, o "*Transmission Control Protocol/Internet Protocol"* (TCP/IP). Contudo, em 1994, a *US National Science Foundation* passou a terceirizar o Sistema de Nomes de Domínio (DNS) a uma empresa privada norte-americana denominada *Network Solutions Inc.* (NSI), que evoluiu posteriormente para a ICANN. Desde então, encontra-se com a governança privada, porém com uma forte e crescente influência estatal, fato que culminou com a Resolução nº 56, de 21 de dezembro de 2001, da ONU, na qual aprovou a realização de Cúpulas Mundiais sobre

a Sociedade da Informação (CMSI), coordenadas pela União Internacional de Telecomunicações (UIT), em Genebra (Suíça), em 2013, e em Túnis (Tunísia), em 2005. Nesses fóruns ficou estabelecido que a governança da rede seria compartilhada pelos governos, setor privado e sociedade civil (KURBALIJA, 2016).

A arquitetura inicial da internet foi concebida para ser uma rede de troca de informações entre pesquisadores, ou seja, com informações de livre trânsito, sem limitações de alcance e preocupações com segurança. Partindo dessa primícia, muito se questiona a respeito dos servidores-raiz estarem concentrados nos Estados Unidos. Tal influência poderia conduzir à retirada de nomes de domínios de um determinado país, levando a um apagão total de seu acesso à rede. Contudo, a adoção de tal procedimento não se mostra vantajosa para os próprios estadunidenses, haja vista que viria a provocar uma verdadeira instabilidade e a busca pelos excluídos de suas próprias redes, além do risco de se perder a primazia do uso do idioma inglês e prejuízos financeiros das grandes empresas americanas do gênero.

Soluções alternativas já foram idealizadas tais como o estabelecimento de servidores-raiz alternativos. Entretanto, esta solução nunca prosperou sob o argumento de poder levar a uma fragmentação total da rede, sendo contrário a todo o princípio de integração.

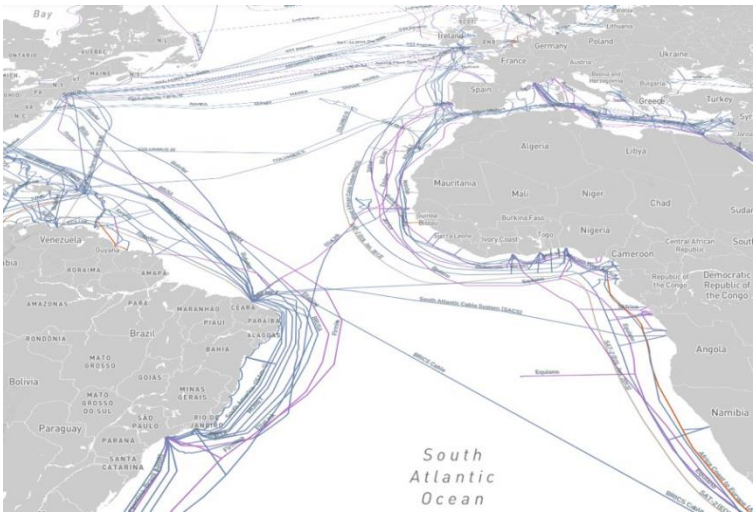
Com o avanço tecnológico, a comunicação em nuvem passou a ser a tendência do tráfego e armazenamento de dados. Empresas como Google, Microsoft, Apple, Amazon e Facebook, planejam desenvolver grandes parques de servidores para este fim. Essa realidade fez aumentar o questionamento sobre a privacidade e proteção dos dados em rede. (KURBALIJA, 2016).

Após as reuniões da CMSI citadas, as discussões têm oscilado entre uma política de governança da internet intergovernamental e uma política multissetorial. O Brasil, assim como muitos países, organizou-se a partir de estruturas que já se ligavam por afinidade com a UTI, porém, ao longo do tempo, essa modelagem se tornou cada vez mais horizontal, abordando o setor privado e a academia. Desde então, a infraestrutura lógica da internet no Brasil passou a ser montada com servidores para administração do domínio ".br", sediados em São Paulo, Rio de Janeiro e Brasília.

As discussões sobre soberania na rede não se limitam ao território geográfico onde se encontram os servidores de internet. A governança das conexões é outra questão preocupante em muitos países, principalmente pela conectividade proporcionada pelos cabos submarinos. Atualmente existem mais de 430 desses cabos responsáveis por 95% do tráfego de voz e dados da internet. São de origem variadas, como estados, grandes corporações, indivíduos e emprego militar.

A maioria dos cabos concentra-se no Atlântico Norte, na ligação entre os Estados Unidos e a Europa e são de propriedade americana. Desse modo, a informação trafega pelo território americano nesta camada física da rede, antes de chegar ao seu destino final. É o caso brasileiro, onde quase a totalidade do acesso à internet passa pelos Estados Unidos, sendo este país, em teoria, capaz de bloquear ou mesmo interceptar os ativos de informação dos servidores brasileiros.

Figura 1 - Cabos Submarinos no Atlântico (recorte). Infrapedia.



Fonte: Medeiros e Pinto (2022, p. 7)

Ao observar a figura 1 acima, apresentada no trabalho de Medeiros e Pinto (2022, p. 7), pode-se verificar as dependências de conectividade da América do Sul em relação à América do Norte. Todavia, as autoras ressaltam a importância estratégica da rede de cabos submarinos *South Atlantic Cable Systems* (SACS) que liga Fortaleza (Brasil) a Sangano (Angola) e da rede *South Atlantic Inter Link* (SAIL), entre Fortaleza (Brasil) e Kribi (Camarões), para a autonomia da América do Sul, no tocante à segurança, confiabilidade e flexibilidade das informações.

Os cabos submarinos possuem proteção por convenção internacional assinada em 1884 e em vigor nos dias atuais. Contudo, suas dimensões os tornam vulneráveis a qualquer ação externa de atores, estatais ou não, que tenham a intenção declarada de impedir, dificultar ou tirar proveitos da transmissão de ativos de informação circulantes de interesse de um determinado país. Em teoria, uma ação militar hostil sobre um desses cabos impede sua utilização como meio de comunicação.

2.2 A PROTEÇÃO DAS INFRAESTRUTURAS CRÍTICAS BRASILEIRAS

O Estado brasileiro definiu e normatizou o conceito de infraestruturas críticas por meio do Decreto nº 9.573, de 22 de novembro de 2018, Política Nacional de Segurança de

Infraestruturas Críticas (PNSIC), com abrangência para toda a administração pública. Assim redigido no art. 1º, inciso I: "infraestruturas críticas - 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" (BRASIL, 2018a).

A política acima não definiu quais áreas são prioritárias para a proteção cibernética, deixando esta tarefa para a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), Decreto nº 10.569, de 9 de dezembro de 2020, Anexo, na qual estabeleceu grupos técnicos nas áreas de energia, transporte, águas, comunicações e finanças sob a coordenação da Câmara de Relações Exteriores e Defesa Nacional (CREDEN). Todavia, apesar de estabelecer estes setores como prioritários, esta estratégia deixa espaço para estabelecimento de outras áreas julgadas de interesse para a Defesa Nacional (BRASIL, 2020e).

As ameaças no ciberespaço são motivos de preocupação dos países na proteção de suas infraestruturas críticas em um mundo cada vez mais digital. Em uma matriz de riscos promovida por qualquer especialista, seja qual for a metodologia empregada, certamente apontará um risco elevado para ataques cibernéticos. Estes podem ocorrer em qualquer parte do mundo, muitas vezes de origem desconhecida, podendo ser iminente e sem aviso prévio, e com grande capacidade de provocar prejuízos de todas as ordens à nação. Neste contexto, a principal "palavra de ordem" é resiliência, ou seja, a capacidade de se melhor resistir e manter as infraestruturas críticas nacionais em funcionamento, mesmo sob um ataque cibernético, seja por eventos de redes isoladas ou ataques massivos.

Para Hosang (2011), o panorama atual do espaço cibernético brasileiro é o seguinte:

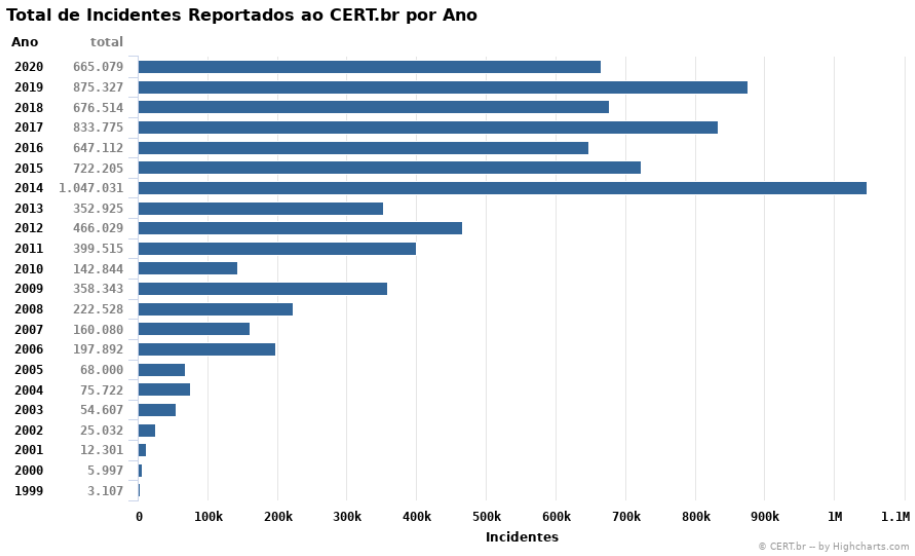
> […] - dos três parâmetros da informação – armazenagem, processamento e trânsito – os dois primeiros são em grande parte **hospedados fora do país** e, quanto ao terceiro, a banda não pode ser externalizada;
> - a infraestrutura é dominada em sua essência por **empresas multinacionais estrangeiras**;
> - existem **talentos** em todas as áreas, mas **em número insuficiente** perante o tamanho do espaço brasileiro, sendo que muitos estão fora do país; e
> - normalmente os profissionais da área são formados em dois compartimentos que não se comunicam de forma eficaz, quais sejam: o da Academia e o ambiente muito especializado do autodidatismo e/ou das certificações; esse último foi criado basicamente pelas empresas para a geração de recursos humanos especializados em seus produtos. […] ***(grifo nosso)***

Ao analisar a margem histórica de incidentes de rede reportados ao CERT.br[6], verificou-se um gradual aumento e um pico histórico no espaço cibernético brasileiro no ano em que o

6 O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de Responsabilidade Nacional, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. O NIC.br é uma organização privada sem fins lucrativos criada para implementar as

país sediou a Copa do Mundo FIFA 2014, conforme exposto na figura 2. Apesar de os dados estatísticos se manterem elevados nos anos seguintes, é possível constatar que as infraestruturas críticas, gradativamente, têm ampliado seu grau de maturidade em segurança cibernética, haja vista, poucos são os casos de interrupção na prestação de serviços.

Figura 2 - Estatísticas dos Incidentes Reportados ao CERT.br



Fonte: CERT.br, 2022. Disponível em: https://www.cert.br/stats/incidentes/

Deve-se ter em mente que ameaças decorrentes dos avanços tecnológicos estão cada vez mais prováveis, seja no campo internacional, seja no nacional. Dessa maneira, as formas de atuação que indivíduos, grupos ou Estados se utilizam do espaço cibernético para alcançar seus objetivos aparecem como uma das ameaças mais letais para qualquer nação.

Para Corrêa Filho (2016, p.19), uma ação pode ser considerada hostil de duas formas: ou pela obtenção de acesso privilegiado aos sistemas (*root access*), obtidos normalmente por falhas humanas associadas à fragilidade de segurança ou a trabalhos de engenharia social; ou por ataques de negação de serviço, executados por máquinas especializadas ou com a técnica DDoS (do inglês *Distributed Denial-of-Service*), normalmente com "furtividade" e uso de máquinas "zumbi" (*Botnet*) para gerar um fluxo de solicitações que não possa ser atendida pelo servidor.

Segundo apresentação da especialista Lucimara Desiderá, do CERT.Br, durante o 12º Colóquio do CTIR.Gov, em 2022, as causas mais comuns de invasões e vazamentos de dados reportados e mais observados em sensores do CERT.br são:

decisões e os projetos do CGI.br, que é o responsável por coordenar e integrar as iniciativas e serviços da Internet no país. Disponível em: https://cert.br/sobre/ Acesso em: 22 de julho de 2022.

- Tentativas de fraudes financeiras e de comércio eletrônico, via mensagens de correio eletrônico falsas (*phishings*), ou por via de infecção de roteadores de banda larga para DNS *hijacking*, ou via infecção de computadores e de celulares;

- Invasão por meio de senhas comprometidas, vazadas ou fracas, via *phishing*[7], ou tentativa de ataque de força bruta, ou senhas expostas pelos próprios donos/desenvolvedores dos sistemas; e

- Exploração de vulnerabilidades para invasão e/ou movimentação lateral, via falta de aplicação de correções, erros de configuração, e falta ou falha de processos.

Ressalta a especialista que mais de 80% dos incidentes de rede poderiam ser evitados se todas as correções de sistemas fossem aplicadas, ou mesmo se houvesse mais atenção a erros e configurações. Para uma melhor proteção, o CERT.br defende a adoção de procedimentos modernos de segurança e proteção de dados, tais como autenticação com múltiplos fatores, criptografia forte, segurança de DNS e de roteadores (DESIDERÁ, 2022).

Em linhas gerais, a ENSIC visa mitigar os riscos de ataques cibernéticos e desenvolver uma integração das diversas esferas do poder público, bem como estimular a participação de cooperativas do setor privado no desenvolvimento de processos comuns de segurança que aumentem a resiliência de serviços e sistemas. Esta estratégia abarca toda a administração pública e logicamente sem qualquer poder regulatório ao setor privado. Todavia, caberá ao próprio gestor corporativo realizar as ações de contenção aos incidentes em suas redes, mantendo a integridade lógica, ou mesmo de credibilidade de cada instituição. Apesar de ser incentivado, o compartilhamento de informações é apenas entre os respectivos operadores.

A realização de uma análise de riscos constante e tempestiva e o compartilhamento de informações nas ações e/ou reações das equipes de técnicas de tratamento de incidentes de rede são o *core* de uma boa atuação integrada.

Cada política para o setor cibernético induz uma estratégia equivalente. À semelhança da PNSIC que se derivou a ENSIC, a PNSI motivou a criação da Estratégia Nacional de Segurança Cibernética (E-Ciber). Tais estratégias visam, de forma matricial, desenvolver a capacidade de integração e compartilhamento de soluções que melhorem a capacidade de proteção cibernética das infraestruturas críticas do país e de interesse para a Segurança, Desenvolvimento e Defesa Nacional.

Neste contexto, em coordenação com o GSI/PR, o ComDCiber passou a desenvolver um exercício de integração, chamado “Exercício Guardião Cibernético”, que aproximasse estes

7 *Phishing* - é uma técnica de crime cibernético que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais. Disponível em: https://www.avast.com/pt-br/c-phishing

setores estratégicos. O modelo adotado teve sua inspiração no exercício *Locked Shields*[8], patrocinado pelo CCDCOE (*Cooperative Cyber Defence Centre of Excellence*) da OTAN, este último tratando-se do maior exercício anual de defesa cibernética da coalizão, que congregou mais de 30 países e cerca de 2.000 especialistas apenas na edição de 2021 (NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, 2022).

O exercício se desenvolve com o estabelecimento de grupos especializados nas áreas dos setores prioritários de energia, financeiro, nuclear, transporte, água e de telecomunicações/Internet para solucionar problemas cibernéticos simulados (PCS) por meio de técnicas de simulação construtiva e virtual.

A simulação construtiva emprega as metodologias de gabinetes de crise das áreas de TI. As decisões decorrentes demandam ações de respostas aos incidentes apresentados. A simulação virtual utiliza como ferramenta um simulador de operações cibernéticas de tecnologia nacional desenvolvido para este fim. Neste ambiente são reproduzidos a arquitetura de sistemas utilizados pelos especialistas dos órgãos e empresas participantes.

O ComDCiber contabilizou a participação de 135 organizações e empresas e 1.248 representantes na edição de 2022, além de 30 observadores estrangeiros. O principal objetivo do exercício foi o de incentivar o intercâmbio de conhecimentos, tomando por base de estudo o repositório de ameaças existentes na plataforma MISP (*Malware Information Sharing Platform*)[9], além da troca de experiências em tecnologias disruptivas tais como IA, telefonia móvel 5G, redes de cabos submarinos, computação quântica, internet das coisas (IoT), dentre outros.

2.3 LACUNAS NO ARCABOUÇO NORMATIVO DA GOVERNANÇA NO BRASIL

A normatização do setor cibernético teve rápida evolução nas últimas duas décadas. Inicialmente o tema começou a ser trabalhado depois da criação e estabelecimento de competências do GSI/PR, por meio da Medida Provisória (MP) nº 2.216-37, de 31 de agosto de 2001, ainda sob o conjunto da segurança da informação. Posteriormente, esta MP foi

8 Exercício *Locked Shields* - Exercício anual, organizado pelo CCDCOE desde 2010, que permite que especialistas em segurança cibernética aprimorem suas habilidades na defesa de sistemas nacionais de TI e infraestrutura crítica sob ataques em tempo real. O foco está em cenários realistas, tecnologias de ponta e simulando toda a complexidade de um incidente cibernético massivo, incluindo tomadas de decisão estratégicas, aspectos jurídicos e de comunicação. Disponível em: https://ccdcoe.org/locked-shields/. Acesso em: 28 de julho de 2022.

9 *Open Source Threat Intelligence Platform* (MISP) - é uma plataforma de software livre para compartilhamento de dados de inteligência de ameaças, quanto um conjunto de padrões abertos para compartilhamento destas informações.

consolidada pela Lei Federal nº 13.844, de 18 de junho de 2019, que destaca, dentre outras, as seguintes competências:

> Art. 10. Ao Gabinete de Segurança Institucional da Presidência da República compete:[...]
> IV - coordenar as atividades de segurança da informação e das comunicações no âmbito da administração pública federal;
> V- planejar, coordenar e supervisionar a atividade de segurança da informação no âmbito da administração pública federal, nela incluídos a **segurança cibernética**, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas; [...]
> XI - acompanhar assuntos pertinentes às infraestruturas críticas, com prioridade aos relacionados à avaliação de riscos. ***(grifo nosso)***

Para melhor cumprir as missões destacadas acima de planejar e coordenar a execução das atividades de segurança da informação na administração pública foi criado o DSIC na estrutura do GSI/PR, por meio do Decreto nº 5.772, de 8 de maio de 2006. Conforme já citado, posteriormente esse departamento passou a se chamar DSI, segundo o Decreto nº 10.363, de 21 de maio de 2020.

> Art. 16-A. Ao Departamento de Segurança da Informação compete:
> I - planejar, coordenar e supervisionar a atividade nacional de segurança da informação, incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas; [...]
> III - elaborar normativos e requisitos metodológicos relativos à atividade nacional de segurança da informação, no âmbito da administração pública federal, nela incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas;
> IV - manter o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, de responsabilidade nacional, para a proteção cibernética;
> V - coordenar e realizar ações destinadas à gestão de incidentes computacionais, no que se refere à prevenção, ao monitoramento, ao tratamento e à resposta a incidentes computacionais de responsabilidade nacional;
> VI - coordenar a rede de equipes de tratamento e resposta a incidentes computacionais formada por órgãos e entidades públicos; [...]
> XI - articular, para o estabelecimento de diretrizes para as políticas públicas de segurança da informação, com os Governos dos Estados, do Distrito Federal e dos Municípios, com a sociedade civil e com órgãos e entidades públicos federais; (BRASIL, 2020c).

As instruções normativas e normas complementares do DSI vinculam todos os órgãos da administração pública, conforme definido no Acórdão nº 1.233/2012 do Tribunal de Contas da União (TCU), no que se refere aos instrumentos de controle de segurança da informação e segurança cibernética (FONTENELE, 2022).

Após a END de 2008, o MD expediu a Diretriz nº 0014, de 9 de novembro de 2009, incutindo ao Exército Brasileiro a responsabilidade pela coordenação e integração do setor cibernético. Foi ativado, em 2010, o Centro de Defesa Cibernética (CDCiber) (BRASIL, 2014b).

Em 2012, o MD expediu duas portarias que impulsionaram o setor cibernético. A primeira foi a Portaria Normativa nº 3.405/MD, de 21 de dezembro, na qual atribuiu ao CDCiber responsabilidade pela coordenação e integração das atividades de defesa cibernética no âmbito do MD. A segunda foi a Portaria Normativa nº 3.389/MD, que aprovou a Política Cibernética de Defesa, cuja finalidade é orientar, no âmbito do MD, as atividades de defesa cibernética, no nível estratégico, e de guerra cibernética, nos níveis operacional e tático (BRASIL, 2012),

Em 2014, a fim de atender às demandas de proteção cibernética dos grandes eventos que o Brasil sediou, o MD publicou a Portaria Normativa nº 3.010, de 18 de novembro, Doutrina Militar de Defesa Cibernética. Nesta publicação, foi possível organizar, conforme os níveis decisórios, as responsabilidades de cada um dos atores incumbidos das atividades de proteção cibernética e estabelecer fundamentos, proporcionando unidade de pensamento sobre o assunto, no âmbito do MD, e contribuindo para a atuação conjunta das Forças Armadas. (BRASIL, 2014b)

A Doutrina Militar de Defesa Cibernética estabelece que a segurança da informação e a cibernética são coordenadas pelo GSI/PR no nível político, enquanto que a defesa cibernética será executada pelo MD, no nível estratégico. Por fim, define que a guerra cibernética se desenvolve nos níveis operacional e tático pelos Comandos Operacionais e Forças Componentes (BRASIL, 2014b).

A Portaria nº 3.781/GM-MD, de 17 de novembro de 2020, criou o Sistema Militar de Defesa Cibernética, definindo como órgão central o ComDCiber, comando operacional conjunto, permanentemente ativado e com capacidade interagências (BRASIL, 2020f).

Em nível nacional, a PNSI editada pelo Decreto nº 9.637, de 26 dezembro de 2018, e alterada pelo Decreto nº 10.641, de 2 março de 2021, encontra-se em fase de tramitação no Congresso Nacional com um objetivo de ser elevada a lei federal e, consequentemente, ampliar sua abrangência. A PNSI possui a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional. Ela abrange a segurança e a defesa cibernética e a segurança física e proteção de dados organizacionais (BRASIL, 2018b).

O art. 6º da PNSI definiu sua estratégia correspondente, a Estratégica Nacional de Segurança da Informação, que compreende um compêndio de dois diplomas normativos:

Decreto nº 10.222, de 05 de fevereiro de 2020, Estratégia Nacional de Segurança Cibernética (E-Ciber); e Decreto nº 10.569, de 09 de dezembro de 2020, Estratégia Nacional de Segurança das Infraestruturas Críticas (ENSIC) (BRASIL, 2020b). Além desses, outros dois diplomas ainda se encontram em fase de elaboração e deverão integrar-se ao conjunto de estratégias afins: Estratégia Nacional de Defesa Cibernética e a Estratégia para Segurança das Informações Sigilosas (BRASIL, 2020c; FONTENELE, 2022).

Recentemente, no dia 15 de setembro de 2022, foi promulgado, por meio do Decreto nº 11.200, o Plano Nacional de Segurança das Infraestruturas Críticas, no qual foi criado o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas. Esse sistema será a estrutura operacional de acompanhamento e monitoramento permanente a cargo do GSI/PR, de forma a integrar os diversos setores (BRASIL, 2022a).

Todavia, todos os marcos normativos acima não apresentam aplicações de caráter prático para a administração pública. A liberdade de se autoadministrar leva a que cada órgão estabeleça seus próprios critérios para segurança cibernética. Em outras palavras, cada órgão pode administrar suas redes corporativas com liberdade de procedimentos, além de comprar ou desenvolver produtos de origem diversa, sem comprovação de segurança, certificação ou nível mínimo de proteção. Entre órgãos, o compartilhamento de informações ocorre apenas em nível colaborativo.

A falta de uma agência reguladora se torna mais evidente com anúncio, pelo Ministério da Economia, no portal do governo, no dia 14 de setembro de 2022, da criação do Centro Integrado de Segurança Cibernética (CSIRT.gov.br), com apoio do Banco Interamericano de Desenvolvimento (BID) e da Rede Nacional de Ensino e Pesquisa (RNP), em uma invasão clara às competências do GSI/PR. A proposta desse novo centro é fortalecer a prevenção, o tratamento e a resposta a incidentes cibernéticos, como parte das ações de segurança cibernética no setor público.

O Ministério da Economia estabeleceu objetivos ousados para este novo centro, pois serão formadas equipes para tratamento de incidentes cibernéticos e para análises não invasivas e contínuas de ameaças e vulnerabilidades aos sistemas de governo. Tais competências deveriam ser estabelecidas pelo DSI, mesmo que não possua vocação para regulações de nível técnico, própria de uma agência normativa (BRASIL, 2022b).

3 CERTIFICAÇÃO E HOMOLOGAÇÃO DE SEGURANÇA CIBERNÉTICA

As previsões de estudiosos que, em uma guerra cibernética, ataques dessa natureza teriam a possibilidade de devastar países, sendo uma poderosa ferramenta de desestabilização da segurança nacional, é um entendimento que vem sendo corroborado por instituições importantes, como, por exemplo, o Departamento de Estado dos Estados Unidos da América. Em 2014, este órgão observou que países altamente industrializados, com um alto grau de dependência da infraestrutura cibernética, enfrentam riscos elevados de existência (UNITED STATES, 2014).

Num estudo de 2012, verificou-se que ao menos 114 países estavam desenvolvendo estratégias nacionais para poderem lidar com as ameaças cibernéticas (RID, 2013).

Apesar de o espaço cibernético ser aberto e acessível a todos os atores, inclusive a pequenos países e com pouca relevância, o que se tem observado nos incidentes relacionados a ataques cibernéticos é que, com exceção da Coreia do Norte, essas ações têm sido orquestradas por países com grande capacidade de recursos (RID, 2013).

Quando se fala em ataques cibernéticos, a primeira imagem que pode vir à mente é de países atacando outros países que possuem interesses conflitantes e não países que são tradicionalmente aliados. Entretanto, como revelou, em 2013, o famoso caso do ex-funcionário da Agência de Segurança Americana (NSA), Edward Snowden, ataques cibernéticos foram realizados pelos Estados Unidos da América contra vários países aliados, incluindo o Brasil. Em artigos no *The Washington Post* (GELLMAN, 2010), *The Guardian* (GREENWALD; MACASKILL; POITRAS, 2013) e no livro "Sem lugar para se Esconder" do jornalista investigativo norte-americano Glenn Greenwald, Snowden detalha as práticas de espionagem cibernética através de vários programas desenvolvidos pelo governo norte-americano (GREENWALD, 2014).

Os documentos divulgados por Snowden e mencionados no livro descrevem que países como França, Brasil, Índia e Alemanha, entre outros, foram alvos da vigilância cibernética dos Estados Unidos.

No caso do Brasil, os documentos revelaram que os atos de espionagem cibernética tiveram como alvo, àquela época, a Presidente da República, vários funcionários de alto escalão do Ministério da Fazenda, o Ministro da Casa Civil, os Embaixadores do Brasil na França, Alemanha e Suíça, vários assessores da Presidente, além do avião presidencial (GUROVITZ, 2015).

A vigilância se deu não apenas sobre assuntos de Estado, mas também sobre assuntos econômicos, com a interceptação de ligações e mensagens eletrônicas da Petrobras e do Ministério das Minas e Energia.

A reação de enfrentamento do Governo Brasileiro à época se deu em duas frentes. A primeira foi a publicação do Decreto 8.135 de 4 de novembro de 2013 (BRASIL, 2013). Este documento ficou conhecido como o "Decreto Antiespionagem" e estabelecia as condições das comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que pudessem comprometer a segurança nacional.

O decreto retirava da iniciativa privada e passava para órgãos ou entidades da administração pública, empresas públicas ou de economia mista da União e subsidiárias, a responsabilidade pelo tráfego das comunicações de dados da administração direta, autárquica e fundacional. Previa também que o serviço de correio eletrônico e o armazenamento e recuperação de dados deveriam ser realizados em centros de processamento de dados e fornecido pelos órgãos e entidades da administração pública, além da previsão de dispensa de licitação, com o objetivo de preservação da segurança nacional, para a contratação de serviços de telecomunicações e de TI.

A segunda frente de reação foi a solicitação da tramitação de urgência do Projeto de Lei nº 2126/2011 no Congresso Nacional, que posteriormente viria a ser aprovado como Lei n° 12.965, de 23 de abril de 2014, que ficou conhecida como "Marco Civil da Internet".

Essa Lei definiu os princípios, entre eles a neutralidade das redes, a liberdade de expressão, a privacidade dos usuários na rede, preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais, os direitos e garantias dos usuários, em especial no que se refere à privacidade das informações e a proteção aos registros, aos dados pessoais e às comunicações privadas (BRASIL, 2014a).

Em 2017, o Brasil deu mais um passo importante para a segurança de suas comunicações, especialmente no segmento de Defesa, com o lançamento do primeiro Satélite Geoestacionário de Defesa e Comunicações Avançadas, o SGDC-1. Desde a privatização da Embratel, em 1998, as comunicações em banda X, de uso exclusivo militar no Brasil e utilizadas pelas Forças Armadas, eram realizadas através de transponders satelitais alugados de empresas privadas.

O Brasil passou a contar, a partir de então, com um satélite geoestacionário, projetado e capacitado para atender a todo o território nacional, controlado pelas Forças Armadas em parceria com a Telebras, destinado ao transporte e o controle das comunicações estratégicas, em apoio às comunicações do Sistema Integrado de Monitoramento das Fronteiras (SISFRON), Sistema de Gerenciamento da Amazônia Azul (SisGAAz) e Sistema de Defesa Aeroespacial

Brasileiro (SISDABRA), dentre outras, além de operar também na banda Ka, que permite ao governo brasileiro levar internet a todos os pontos do Brasil (DEMENICIS, 2019).

Outro importante avanço em relação à segurança e defesa cibernéticas por parte do Brasil foi a publicação do já comentado Decreto 9.637, de 26 de dezembro de 2018, que veio substituir o de nº 8.135 e instituiu a PNSI, no âmbito da administração pública.

A contínua preocupação do governo brasileiro em relação à segurança cibernética foi demonstrada com a publicação do Edital nº 1/2021 do Ministério das Comunicações, em 27 de setembro de 2021, que tratou do leilão de faixas de frequências destinadas ao serviço de comunicações 5G (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, 2021b).

Apesar de o objeto do leilão ser a expedição de autorização para uso de radiofrequências em caráter primário para funcionamento das redes 5G no Brasil, o edital trouxe embutido o compromisso de os vencedores de determinados lotes custearem a implantação de uma Rede Privada de Comunicação da Administração Pública, nos termos do art. 2ª, Inciso VIII e § 10 da Portaria nº 1.924 - MCOM/2021, de 29 de janeiro 2021, do Ministério das Comunicações, composta por:

- Rede móvel, limitada ao território do Distrito Federal, para atendimento a atividades de segurança pública, defesa, serviços de socorro e emergência, resposta a desastres e outras atribuições críticas de Estado, incluindo as realizadas por entes federados, bem como para atendimento aos órgãos públicos federais;

- Rede fixa para atendimento aos órgãos públicos federais a ser instalada nos municípios de capitais estaduais e no Distrito Federal, complementar à rede de governo existente; e

- Funcionalidade de criptografia, baseada em algoritmos criptográficos definidos por órgãos de segurança da administração pública federal.

De acordo com o Ministro das Comunicações, o objetivo da implantação destas redes foi evitar vazamentos de informação e proteger dados. Entretanto, como ele à época reconheceu, não há como garantir que os equipamentos de rede de qualquer fornecedor não sejam entregues com *backdoors*, ou seja, com vulnerabilidades que permitam a espionagem. Para dar mais segurança às informações do governo, equipamentos de apenas um fornecedor seriam usados para a rede privativa, para que seja mais fácil identificar eventuais invasões ou vazamentos (WARTH, 2021).

A fala do Ministro apenas reforça uma realidade que ameaça a segurança dos sistemas, infraestruturas e informações sensíveis ou estratégicas dos Estados, a presença de vulnerabilidades intencionais, ou não, nos equipamentos que compõem as redes de

comunicações ou servidores que armazenam dados ou aplicações. Estas vulnerabilidades podem ser exploradas por agentes maliciosos para obterem acesso a dados sigilosos ou controle de serviços ou infraestruturas críticas.

Desde o início da implantação das novas redes de tecnologia 5G, o governo dos Estados Unidos tem pressionado parceiros e aliados para que não utilizem equipamentos do fornecedor chinês *Huawei* (SOUSA; ABRÃO; SANTOS, 2021), em função das alegações de potencial emprego destes equipamentos para espionagem cibernética, via vulnerabilidades intencionais ou *backdoors* implantados deliberadamente para esta atividades.

Contudo, a prática de utilização de vulnerabilidades ou *backdoors* para acesso não autorizado a informações privilegiadas é uma arma de ataque cibernético utilizada pelo próprio governo dos Estados Unidos, como divulgou Snowden (GREENWALD, 2014). No relato, a NSA interceptava carregamentos da Cisco, um dos maiores fornecedores de equipamentos de rede, servidores, roteadores, destinados aos alvos dos ataques e os encaminhava para um local secreto em que eram implantadas as ferramentas de espionagem cibernética. Posteriormente os equipamentos eram novamente embalados e recolocados em trânsito rumo ao destino original.

Isto demonstra que a aquisição de equipamentos, redes, aplicações e serviços sempre estarão vulneráveis a atores mal-intencionados que pretendam se utilizar de vulnerabilidades presentes para realizar ataques cibernéticos contra o Estado brasileiro.

Em relação à contratação de soluções de Tecnologia da Informação e Comunicação pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal, os instrumentos normativos (BRASIL, 2020a), deixam livres que os órgãos façam suas especificações técnicas, com base nas necessidades de cada um. Entretanto, não há, além da previsão dos requisitos técnicos, que as soluções e os equipamentos adquiridos sejam certificados e homologados quanto à segurança cibernética.

Conforme observado no anexo da E-Ciber, entende-se que a certificação de produtos e de soluções em segurança cibernética é um objetivo a ser perseguido, devido à complexidade dos equipamentos e dos sistemas aplicados, que exigem elevado grau de especialização das equipes e de recursos tecnológicos, sendo necessários organismos estruturados e equipados para conduzi-la (BRASIL, 2020b).

O processo de certificação e homologação de equipamentos e soluções de TIC para a administração pública e para a sociedade civil, especialmente para os órgãos que compõe o Sistema Brasileiro de Inteligência (SISBIN), poderia se espelhar nas atividades feitas hoje pela

Agência Nacional de Telecomunicações (Anatel) ou, de forma mais abrangente, na Agência da União Europeia para Segurança Cibernética (ENISA).

A Anatel foi criada em 1997 pela Lei 9.472, conhecida como Lei Geral de Telecomunicações. Vinculada ao governo federal, a Anatel foi a primeira agência reguladora a ser instalada no Brasil em 5 de novembro de 1997. Uma de suas atribuições é expedir ou reconhecer a certificação de produtos, observados os padrões e as normas por ela estabelecidos. Apenas produtos de telecomunicação certificados e homologados podem ser comercializados no Brasil (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, 2020).

O regulamento de avaliação da conformidade e de homologação de produtos para telecomunicações foi aprovado pela Resolução nº 715, de 23 de outubro de 2019 e estabelece os princípios e regras gerais relativos à avaliação da conformidade e à homologação de produtos para telecomunicações (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, 2019).

O processo de certificação é realizado por Organismos de Certificação Designados – OCD e por laboratórios de ensaio tecnicamente capacitados e devidamente habilitados pela agência. A certificação é baseada em processos operacionais e requisitos técnicos, definidos também pela Anatel, para cada item a ser certificado. Após a certificação do produto, a Anatel emite o termo de homologação, que é o pré-requisito obrigatório para o uso e comercialização do mesmo no Brasil.

Voltado especificamente para o tema certificação e homologação referente à segurança cibernética, a Anatel emitiu o Ato nº 77, de 05 de janeiro de 2021, que definiu os requisitos de segurança cibernética mínimos a serem observados na certificação e homologação dos produtos que executem a função de equipamento terminal com conexão à internet ou de equipamento de infraestrutura de redes de telecomunicações. A certificação quanto a estes requisitos de segurança não é mandatória e cabe ao solicitante emitir uma declaração informando quais as justificativas. A Anatel pode, posteriormente, realizar uma fiscalização de mercado para comprovar, através de ensaios, se as informações e os requisitos presentes na declaração são efetivamente atendidos. Caso contrário, pode impedir a comercialização e impor a remoção do mercado (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, 2021a).

Esta iniciativa da Anatel, relacionada à segurança cibernética, é importante, mas ainda incipiente e voltada apenas para o segmento de telecomunicações. A questão da homologação, da definição das certificações obrigatórias e da padronização de requisitos de segurança cibernética para a aquisição equipamentos e serviços de TIC, poderiam ser tratadas de forma mais objetiva, através de uma agência, nos moldes da ENISA.

Esta agência da União Europeia, criada em 2004, é voltada para segurança cibernética dos estados membros e seus cidadãos, visando aumentar a confiança na economia digital e reforçar a resiliência das infraestruturas de tecnologia da informação e comunicação (EUROPEAN UNION AGENCY FOR CYBERSECURITY, 2019). Suas principais atribuições são:

- Segurança de serviços de *Cloud e Big Data*
- Segurança de Infraestruturas Críticas
- Serviços de CSIRT
- Gerenciamento de Crises Cibernéticas
- Exercícios Cibernéticos
- Educação em Segurança Cibernética
- Proteção de Dados
- Divulgação de incidentes cibernéticos
- Proteção para equipamentos IoT e redes inteligentes
- Desenvolvimento de estratégias nacionais de Segurança Cibernética
- Regulamentação de Diretrizes de segurança
- Padronização de Processos e Certificação de Equipamentos
- Gerenciamento de ameaças e riscos
- Treinamento e Certificação de Especialistas em Segurança Cibernética

Por entender que a segurança das redes e dos sistemas de informação é um objetivo primário da agência, foi publicado, em 2019, o Regulamento 881, que ficou conhecido como o "Ato da Segurança Cibernética". Por meio dele, foi criada uma estrutura de certificação cibernética, visando estabelecer e manter a confiança de produtos, serviços e processos de TIC e garantir os requisitos especificados a fim de proteger a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados, transmitidos ou tratados.

A avaliação da conformidade definida por esta agência é um procedimento que se destina a avaliar se foram cumpridos os requisitos previamente especificados e definidos para um determinado produto, serviço ou processo. Esse procedimento deverá ser executado por um terceiro independente, que não seja o fabricante do produto, o prestador do serviço, nem o fornecedor do processo alvo da avaliação, assim como no caso da Anatel.

A ENISA entende que a avaliação e a certificação da conformidade não podem garantir por si só a segurança cibernética. As certificações, que compreendem procedimentos e metodologias técnicas, atestam que os produtos, serviços e processos foram ensaiados e que

cumprem requisitos estabelecidos em normas técnicas pré-estabelecidas, com o objetivo de reduzir o impacto ou prevenir incidentes relacionados à segurança cibernética

O sistema europeu de certificação definido pela ENISA, ao contrário do utilizado pela Anatel, especifica níveis de garantia, que correspondem ao rigor e a complexidade da avaliação e do emprego do produto, serviço ou processo a ser avaliado. É dividido em três níveis de garantia: básico, substancial e elevado, onde cada nível deve ser coerente com o emprego dos equipamentos e soluções e os requisitos de segurança a serem alcançados.

No nível básico, a certificação é realizada através, no mínimo, da análise de documentação do fornecedor, assim como faz a Anatel, e objetiva a garantia da redução ao mínimo dos riscos básicos conhecidos de incidentes e ataques cibernéticos.

Para o nível substancial, a certificação visa a redução ao mínimo dos riscos de incidentes e ataques que podem ser executados por autores com competências técnicas e recursos limitados. As atividades de avaliação compreendem testes para demonstrar a inexistência de vulnerabilidades que sejam do conhecimento público e a realização de ensaios para demonstrar que os produtos, serviços ou processos aplicam corretamente as funcionalidades de segurança necessárias.

O nível elevado deverá garantir que os produtos, serviços e processos, objeto dessa certificação, possuam um risco mínimo de impacto de ataques sofisticados executados por autores com competências e recursos significativos. Para tanto, os ensaios de certificação devem garantir a inexistência de vulnerabilidades que sejam do conhecimento público, demonstrem que os produtos, serviços ou processos apliquem corretamente as funcionalidades de segurança necessárias ao nível tecnológico mais avançado, além da avaliação da sua resiliência a ataques competentes através de ensaios de penetração.

A falta de padronização de requisitos e a ausência de certificações mandatórias de segurança cibernética, para a aquisição de equipamentos e soluções de TIC, aumentam a possibilidade de presença de vulnerabilidades e *backdoors*, que podem vir a comprometer a segurança e a defesa nacionais.

A obrigatoriedade de uso somente de equipamentos e soluções certificadas e homologadas por uma agência voltada para a segurança cibernética do Estado brasileiro contribuiria significativamente para que estes riscos fossem reduzidos. A Anatel, apesar de já ter iniciado um esforço ainda incipiente neste sentido, está voltada apenas para o segmento de telecomunicações e não conta com os recursos necessários para abranger o estabelecimento dos requisitos, nem os processos de certificação e homologação de equipamentos e soluções voltadas para o mercado mais abrangente de TIC.

No mundo, vários países já adotaram este modelo de agência voltada especificamente para a segurança cibernética. Podemos destacar como exemplos de agências nacionais: CISA - *Cybersecurity Infrastructure Security Agency* e NSA - *National Security Agency* dos Estados Unidos, *Agence Nationale de la Sécurité des Systèmes d'Information* da França, *National Cybersecurity Centre* do Reino Unido, *Australian Cybersecurity Centre* da Austrália, *Singapore Cybersecurity Agency* de Singapura, *National Cyber Coordination Centre* da Índia, *National Center of Incident readiness and Strategy for Cybersecurity* do Japão e a BSI - *Bundesamt für Sicherheit in der Informationstechnik* da Alemanha, agência que já possui experiência em certificação voltada para a segurança cibernética e que teve sua origem em um órgão análogo à nossa Agência Brasileira de Inteligência (ABIN).

4 PROPOSTA DE CRIAÇÃO DE AGÊNCIA BRASILEIRA DE SEGURANÇA CIBERNÉTICA

A percepção de que o Estado não está institucionalmente preparado para se sobrepor a ameaças na área cibernética leva à busca de uma solução organizacional. Para isso, a existência de um órgão estatal com preponderância sobre os demais da administração pública é indispensável para a segurança cibernética e para a Defesa Nacional.

4.1 O EXEMPLO DA AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN)

Mas qual o conceito e como deve ser estruturada essa entidade reguladora que aglutine esforços, de forma a normatizar as atividades dos diferentes órgãos governamentais, tanto civis quanto militares, a fim de fortalecer o país em termos de segurança cibernética?

A solução vislumbrada foi buscar um paralelismo, analisando a matriz de referência de uma agência relevante e consolidada em nível nacional e de temática similar. Nesse sentido, verificou-se a formação e estruturação do setor de inteligência, cujo estabelecimento de uma entidade reguladora, a Agência Brasileira de Inteligência (ABIN), como órgão central do SISBIN**,** fortaleceu o setor de defesa brasileiro, assegurando ao executivo federal o acesso a informações relativas à segurança do Estado e da sociedade brasileira.

Num primeiro momento, a análise focou os pormenores da história da criação da ABIN, de forma a esboçar um conceito sobre a estrutura de uma Agência Brasileira de Segurança Cibernética.

Segundo descreve Corrêa, 2009, quando da extinção do Serviço Nacional de Informações (SNI), ocorrida ainda no governo Collor, os trabalhos no setor de informação

ficaram a cargo da Secretaria de Assuntos Estratégicos (SAE). O objetivo era passar uma imagem de desmilitarização da atividade, propício ao período, anos após o fim da denominada "ditadura militar".

Seguindo essa linha, o clássico termo "informação" foi trocado por "inteligência", pois o primeiro passava uma pesada imagem de busca, coleta e aquisição a qualquer custo, enquanto o segundo levava ao viés de intuição e análise, com observância dos direitos e garantias individuais.

Posteriormente, decidiu-se pela criação de uma agência, como órgão central de um Sistema, o SISBIN. Surgiu então a ABIN, com a função de "planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência" (BRASIL, 1999). Um importante detalhe que norteia sua concepção está no papel de integração dos trabalhos dos demais órgãos do gênero em todo o país para a correta execução da Política Nacional de Inteligência em mais alto nível. Não há ainda, a nível nacional, estrutura similar a esta descrita em termos de segurança cibernética.

Ainda no reforço dessa concepção, Corrêa, 2009 cita que o Presidente Fernando Henrique Cardoso idealizou a criação de um órgão de inteligência do Estado e não do Governo, de forma que as informações coletadas pela ABIN fossem empregadas como assessoramento para a condução das políticas governamentais do país como um todo.

Com a sucessão dos governos desde 1999, alguns ajustes foram implementados e hoje, segundo o sítio eletrônico do governo, a ABIN está definida como "órgão da Presidência da República, vinculado ao Gabinete de Segurança Institucional, responsável por fornecer ao Presidente da República e a seus Ministros informações e análises estratégicas, oportunas e confiáveis, necessárias ao processo de decisão." O SISBIN é composto por 42 integrantes.

No exercício de suas funções, os profissionais de inteligência da ABIN produzem conhecimentos, em nível estratégico, através da análise de fatos e situações julgadas como ameaças ou mesmo oportunidades, de forma a contribuir com a segurança da sociedade e do Estado.

Outro ponto importante é que a ABIN, como centro do sistema, é o único órgão nacional que planeja e executa a chamada "Inteligência de Estado". Os demais elos atuam com inteligência para subsidiar suas próprias atribuições legais.

A sede da ABIN é em Brasília/DF e todas as capitais de unidades da federação possuem superintendências estaduais. Existem subunidades em localidades fronteiriças de interesse, como em Foz do Iguaçu/PR e Tabatinga/AM.

No exterior há 19 escritórios em países das Américas do Sul e do Norte, África, Europa e Oceania. Neles, oficiais de inteligência atuam como adidos civis, de forma a produzir conhecimentos ao Brasil. A estrutura atual da ABIN foi regulamentada por Decreto (BRASIL, 2020d). Nele estão descritas as nomenclaturas e as funções de cada setor.

Em linhas gerais, os órgãos de assistência direta e imediata ao Diretor-Geral são: Gabinete, Assessoria de Governança e Conformidade, Assessoria de Relações Internacionais, Assessoria Jurídica, Corregedoria-Geral e Secretaria de Planejamento e Gestão.

A Secretaria de Planejamento e Gestão, que é a espinha dorsal da instituição, elabora e propõe ao Diretor-Geral políticas, estratégias, planos orientadores, diretrizes, indicadores e metodologias de planejamento e gestão, de segurança orgânica e de pesquisa e desenvolvimento para a segurança das comunicações.

Essa secretaria é constituída das seguintes divisões: Coordenação-Geral de Segurança Orgânica, Coordenação-Geral de Planejamento e Gestão Estratégica, Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações, Departamento de Administração e Logística, Departamento de Gestão de Pessoal e Escola de Inteligência.

4.2 A AGÊNCIA BRASILEIRA DE SEGURANÇA CIBERNÉTICA

Cabe, nessa etapa do presente estudo, descrever, em linhas gerais, como devem ser desenvolvidas as atividades que a Agência Brasileira de Segurança Cibernética pode realizar com escopo regulatório e de governança, com vistas a buscar a solução do problema identificado, que é a vulnerabilidade do Estado brasileiro diante de ameaças cibernéticas.

Com vistas a alcançar seus objetivos e atuar de forma eficiente e eficaz junto a diversos órgãos da administração federal, tanto da área militar quanto da não-militar, a Agência Brasileira de Segurança Cibernética deve funcionar numa estrutura sistêmica radial, permitindo que as normas elaboradas por ela, como elo central, permeiem os demais pertencentes ao sistema, de forma a interligar os componentes e alcançar a operacionalidade da atividade.

Dentre as principais lacunas a serem mitigadas, em nível normativo, podemos destacar a implementação de diversas legislações, como a Política e a Estratégia Nacionais de Segurança Cibernética; a Política e a Estratégia Nacionais de Segurança para Infraestruturas críticas; e o Plano Nacional de Resiliência Cibernética.

Assim, esses vazios normativos que hoje não permitem a junção de esforços, a padronização de ações e a governança em nível estatal na área cibernética poderiam ser eliminados. A criação da agência traz para o governo não só o controle das ameaças, mas

principalmente a rápida identificação dos ataques e a sinérgica aplicação de medidas para reativação de sistemas e infraestruturas atingidas.

Hoje, cada órgão possui sua Equipe ou Centro de Tratamento de Incidentes Cibernéticos (ETIR/CTIR). A agência proporcionaria a centralização do controle sobre o status das infraestruturas críticas nacionais. Seria estabelecida uma grande Central Nacional de Tratamento de Incidentes Cibernéticos (CNTIR).

Em termos de capacitação, a Escola Nacional de Defesa Cibernética, organização subordinada ao ComDCiber para a área de defesa, poderia ser o espelho para a criação da Escola Nacional de Segurança Cibernética, que ficaria a cargo da agência e responsável pelo adestramento de recursos humanos de todos os órgãos, a definição de níveis de *expertise* e a consolidação da doutrina na área da segurança. O próprio Exercício Guardião Cibernético poderia ser absorvido pela agência e expandir sua área de abrangência.

A questão da ausência de certificações de segurança cibernética em equipamentos e soluções de TIC seria sanada ao ser incorporada pela agência, assim como é realizado nos moldes europeus já abordados. O que a Anatel tem realizado, ainda de forma inicial, poderia ser ampliado e receberia o aporte financeiro necessário. O rigor nos critérios de homologação seria aumentado, salvaguardando de forma mais efetiva os sistemas e infraestruturas críticas.

No quadro abaixo estão colocadas, em forma resumida, as competências que a Agência Brasileira de Segurança Cibernética abrangeria, agindo como órgão central técnico e regulatório, com os demais elos executando ações coordenadas e sinérgicas.

Quadro 1 – Distribuição de competências para segurança cibernética nacional

Nível	Instituição	Competências
Técnico-Regulatório	Agência Brasileira de Segurança Cibernética	- Elaborar Política e Estratégia Nacionais. - Elaborar o Plano Nacional de Resiliência. - Criar a Central Nacional de Tratamento de Incidentes. - Criar a Escola Nacional de Segurança Cibernética. - Realizar a certificação cibernética de *software* e *hardware.* - Elaborar diretrizes para desenvolvimento de *software* e *hardware.* - Elaborar normativos de níveis nacionais de proteção cibernética.
Executório	Órgãos da administração pública, MD e infraestruturas críticas nacionais e privadas	- Cumpri leis, diretrizes e normas estabelecidas. - Colaborar com o esforço do governo federal para proteção do espaço cibernético nacional. - Atuar como elo interligado na identificação e reação a ataques cibernéticos.

Fonte: os autores.

5 CONSIDERAÇÕES FINAIS

O espaço cibernético sem fronteiras está ainda longe de ser um ambiente pacífico. Diversas são as ameaças advindas do atual processo de digitalização de serviços na qual o Brasil está inserido. Quanto mais digital é o país, maior é a sua exposição ao risco cibernético. Neste contexto, a segurança cibernética surge na pauta da Defesa Nacional do Estado e de interesse de vários setores da sociedade.

O espaço cibernético brasileiro é vulnerável, em maior ou menor escala. O processamento e armazenamento são, em grande parte, hospedados em servidores fora do território nacional. Destaque deve ser dado aos servidores-raiz de internet que se encontram localizados em território norte-americano.

A fim de mitigar tamanha dependência externa, o Brasil lançou, em 2017, o SGDC-1 para melhorar a autonomia e a segurança das telecomunicações estratégicas e militares. O controle do satélite é realizado no Brasil sob a coordenação da Telebrás e do Ministério da Defesa e atende, além do uso civil, os programas estratégicos de defesa, como o SISFRON, SisGAAz e SISDABRA.

A preocupação em ampliar a segurança cibernética está presente inclusive no advento das novas redes de telefonia 5G, conforme verificou-se no Edital nº 1/2021 do Ministério das Comunicações, de 2021. Nele foram introduzidos dispositivos que garantem faixas exclusivas para redes privativas de estado nas capitais dos estados federados e no Distrito Federal, além da possibilidade de inclusão de uma criptografia própria de órgão de estado.

Nos últimos anos, o GSI/PR vem desempenhando papel fundamental na tentativa de robustecer o arcabouço normativo que disciplina o setor. Salvaguardar os ativos de informação passaram a ser a prioridade do seu DSI. A estratégia adotada foi aproximar todos os atores envolvidos, haja vista o Brasil adotar a governança compartilhada entre entes públicos e privados da internet.

O Brasil despertou para a segurança na rede a partir das informações públicas apresentadas por Edward Snowden, ex-agente do Governo dos Estados Unidos, que divulgou que a Presidente da República do Brasil e altos funcionários do governo foram alvos de espionagem cibernética. Em consequência, foi editado, em 2013, o Decreto nº 8.135, referente ao combate à espionagem, que estabelece parâmetros de comunicação na administração pública e dispensa de licitação para contratações que envolvam a segurança nacional. Em resumo, toda a transmissão de dados dos órgãos de governo deixaria de ser terceirizada e passaria a ser realizada por órgãos públicos.

Além de buscar a segurança dos órgãos, o Estado buscou proteger o cidadão. Assim, após tramitar no Congresso Nacional, sem grandes polêmicas, foi editada a Lei n° 12.965, de 23 de abril de 2014, o Marco Civil da Internet.

O ano de 2018, foi importante pela edição dos principais marcos normativos do setor no âmbito da administração pública. O Decreto nº 9.573 criou a PNSIC, enquanto o Decreto nº 9.637 atualizou a PNSI. Ambas as políticas ensejaram suas respectivas estratégias. A E-Ciber, derivada da PNSI, incentiva o compartilhamento de informações entre diversos setores, públicos ou privados, ocorra de forma colaborativa.

Apesar da evolução dos marcos normativos acima, os órgãos da administração pública possuem liberdade para administrar autonomamente suas estruturas de proteção cibernética, gerenciar seus níveis de risco cibernético, além de comprar ou desenvolver produtos sem necessidade de certificações por órgãos competentes. A integração desses órgãos é apenas de caráter colaborativo, como ocorre nos Exercícios Guardiões Cibernéticos, patrocinados pelo ComDCiber. A Portaria nº 3.781/GM-MD, na qual definiu a capacidade desse comando, estabelece sua atuação colaborativa. (BRASIL, 2020f).

A 4ª versão do exercício materializou o esforço na integração e desenvolvimento de soluções compartilhadas para a proteção cibernética das infraestruturas críticas. O uso da plataforma MISP (*Malware Information Sharing Platform*) e a troca de experiências em tecnologias disruptivas tais como IA, telefonia móvel 5G, redes de cabos submarinos, computação quântica, internet das coisas (IoT), enriquecem este fórum de estudo.

Quanto à regulamentação de produtos, a Anatel aprovou, em 2019, as normas que estabelecem as regras gerais de avaliação e conformidade e de homologação de produtos para telecomunicações. A certificação é realizada pelos organismos de certificação designados e laboratórios de ensaios capacitados. Após a certificação do produto, a agência homologa o produto para sua comercialização. Para aqueles produtos que possuem acesso à internet, foram também definidos parâmetros que garantam a segurança cibernética mínima. Todavia, os requisitos de proteção cibernética não são mandatórios, cabendo ao solicitante emitir uma declaração informando quais dos requisitos atendidos e os não atendidos, com suas respectivas justificativas.

Sem dúvidas, o setor de telecomunicações é o mais avançado nos cuidados com a proteção cibernética, acompanhando a tendência mundial de regulamentação da UIT. Contudo, os regramentos da Anatel são incipientes e não abrangem todos os sistemas digitais que trafegam no espaço cibernético. Esta seria atribuição natural de uma agência especializada para o setor, como é o caso da União Europeia, que já criou sua agência regulatória para esses fins,

mesmo que admita não ser capaz de certificar e homologar produtos 100% seguros, apenas capazes de garantir sua disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados, transmitidos ou tratados.

O Brasil possui plenas condições de avançar na direção de criação de uma agência regulatória que mitigue todos os pontos abordados neste trabalho e que comprove o problema identificado, que é a vulnerabilidade do Estado brasileiro diante de ameaças cibernéticas.

Nesse sentido, foi estudada, tomando como base o conceito do paralelismo, uma agência relevante e consolidada nacionalmente e de temática similar, a ABIN, cuja criação permitiu ao Brasil a gerência das informações relativas à segurança do Estado e da sociedade brasileira. Um ponto importante identificado na ABIN é que, como centro de uma estrutura sistêmica, exerce ações de planejamento e execução da inteligência do país.

A criação da Agência Brasileira de Segurança Cibernética surge como proposta de mitigação do problema identificado, como desencadeamento lógico das etapas do estudo, que passou pela abordagem dos objetivos, geral e específicos, fruto da metodologia de pesquisa documental.

Foram descritas as atividades que esta nova agência pode realizar com escopo regulatório e de governança. Em nível normativo, o destaque foi dado à implementação de políticas, estratégias e planos nacionais de segurança cibernética que possibilitariam a governança em nível estatal. O controle das ameaças, a identificação dos ataques e a aplicação de medidas para reativação de sistemas e infraestrutura atingidas ficaria mais eficaz. As equipes e os centros de controle de todos os órgãos serão interligados e o controle passará a ser exercido por uma grande Central Nacional de Tratamento de Incidentes Cibernéticos (CNTIR).

Ao final da proposta, um quadro foi inserido, com vistas a sintetizar quais seriam as competências da agência no nível técnico e regulatório e as afetas aos demais elos do sistema no nível execução, basicamente relacionada à atuação no esforço conjunto para a segurança do espaço cibernético nacional.

É importante ressaltar que a complexidade do tema traz a constatação que o presente trabalho, apesar de explicitar diversas vantagens na adoção da criação da Agência Brasileira de Segurança Cibernética como proposta de solução para o problema identificado, possui limitações na ótica da segurança, desenvolvimento e defesa.

Dentre essas limitações, podem ser citadas a não definição da subordinação da agência e a não estruturação do sistema brasileiro de segurança cibernética e a abrangência de sua composição. São, de fato, lacunas na pesquisa, que podem ser exploradas em estudos complementares.

REFERÊNCIAS

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (Brasil). **Acesso à Informação Institucional.** Brasília, DF: ABIN, 2022. Disponível em: https://www.gov.br/abin/pt-br/acesso-a-informacao/institucional. Acesso em: 22 jul. 2022.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (Brasil). Ato n. 77, de 05 de janeiro de 2021a. Requisitos de segurança cibernética para equipamentos para telecomunicações. **Diário Oficial da União**: Seção 1, Brasília, n. 193, 7 out. 2020.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (Brasil). **Institucional**. Brasília, DF: Anatel, 2020. Disponível em: https://www.gov.br/anatel/pt-br/acesso-a-informacao/institucional. Acesso em: 14 jul. 2022.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (Brasil). Licitação Nº 1/2021-SOR/SPR/CD-ANATEL. Edital. **Diário Oficial da União**: Seção 3, Brasília, DF, n. 183, p. 9, 27 set. 2021b.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (Brasil). Resolução nº 715. Aprova o Regulamento de Avaliação da Conformidade e de Homologação de Produtos para Telecomunicações. **Diário Oficial da União**: Brasília, DF, n. 208, 2019.

BRASIL. Comando do Exército. Comando de Operações Terrestres. **Manual de Guerra Cibernética. EB70-MC-10.232**. Brasília, DF: COTER, 2010.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética E-Ciber. Brasília, DF: Presidência da República, 2020b. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm. Acesso em 18 jul. 2022.

BRASIL. **Decreto nº 10.363, de 21 de maio de 2020**. Estrutura Regimental Gabinete de Segurança Institucional da Presidência da República. Brasília, DF: Presidência da República, 2020c. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10363.htm. Acesso em: 01 ago. 2022.

BRASIL. **Decreto nº 10.455, de 30 de julho de 2020**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Agência Brasileira de Inteligência e remaneja e transforma cargos em comissão e funções de confiança. Brasília, DF: Presidência da República, 2020d. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10445.htm. Acesso em: 01 ago. 2022.

BRASIL. **Decreto nº 10.569, de 9 de dezembro de 2020.** Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas e Anexo. Brasília, DF: Presidência da República, 2020e. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm. Acesso em: 07 jun. 2022.

BRASIL. **Decreto nº 11.200, de 15 de setembro de 2022.** Aprova o Plano Nacional de Segurança das Infraestruturas Críticas. Brasília, DF: Presidência da República, 2022a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D11200.htm#:~:text=DECRETO%20N%C2%BA%2011.200%2C%20DE%2015,que%20lhe%20confere%20o%20art Acesso em 28 Set 2022.

BRASIL. **Decreto nº 6.703, de 18 de dezembro de 2008.** Aprova a Estratégia Nacional de Defesa e dá outras providências. Brasília, DF: Presidência da República, 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm. Acesso em: 14 maio 22.

BRASIL. **Decreto nº 9.573, de 22 de novembro de 2018**. Aprova a Política Nacional de Segurança das Infraestruturas Críticas. Brasília, DF: Presidência da República, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 22 maio 2022.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018.** Institui a Política Nacional de Segurança da Informação. Brasília, DF: Presidência da República, 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 14 maio 2022.

BRASIL. **Decreto-lei nº 8.135, de 4 de novembro de 2013**. Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. Brasília, DF: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d8135.htm. Acesso em: 21 jul. 2022.

BRASIL. **Lei Federal nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 jul. 2022.

BRASIL. **Lei Federal nº 13.844 de 18 de junho de 2019**. Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13844.htm. Acesso em: 29 jul. 2022.

BRASIL. **Lei Federal nº 9.883, de 7 de dezembro de 1999**. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Brasília, DF: Presidência da República, 1999. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9883.htm. Acesso em: 17 jul. 2022.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa (END)**. Brasília, DF: Ministério da Defesa, 2018c.

BRASIL. Ministério da Defesa. **MD31-M-07. Doutrina Militar de Defesa Cibernética**. Brasília, DF: Ministério da Defesa, 2014b.

BRASIL. Ministério da Defesa. **Política Cibernética de Defesa (MD31-P-02)**. Brasília, DF: Ministério da Defesa, 2012.

BRASIL. Ministério da Defesa. **Portaria nº 3.781/GM-MD, de 17 de novembro de 2020**, que cria o Sistema Militar de Defesa Cibernética. Brasília, DF: Ministério da Defesa, 2020f.

BRASIL. Ministério da Economia. **Legislação**: conheça as normas que regem as contratações de soluções de tecnologia da informação e comunicação no âmbito do SISP. Brasília, DF:

Ministério da Economia, 30 jan. 2020a. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/legislacao. Acesso em: 26 jul. 2022.

BRASIL. Ministério da Economia. **Ministério da Economia e BID criarão Centro de Integrado de Segurança Cibernética do Governo Digital**. Brasília, DF: Ministério da Economia, 2022b. Disponível em: https://www.gov.br/economia/pt-br/assuntos/noticias/2022/setembro/ministerio-da-economia-e-bid-criarao-centro-integrado-de-seguranca-cibernetica-do-governo-digital. Acesso em: 28 set 2022.

BUCHANAN, Ben. **The Hacker and the State**: cyber attacks and the new normal of geopolitics. [*S. l.*]: Harvard University Press, 2020.

COMDCIBER. **Apresentação de Atualização Doutrinária em Defesa Cibernética**. Rio de Janeiro: ESG, 2022.

CORRÊA FILHO, Ivan de Souza. **A Segurança Cibernética no Brasil:** uma análise da situação atual. 2016. Trabalho de conclusão de curso (Curso de Altos Estudos de Política e Estratégia) – Escola Superior de Guerra, Rio de Janeiro, 2016. Disponível em: https://repositorio.esg.br/bitstream/123456789/1041/1/TCC%20IVAN%20DE%20SOUSA%20CORR%c3%8aA%20FILHO.pd. Acesso em: 18 jul. 2022.

CORRÊA, Paulo. **Agência Brasileira de Inteligência (ABIN).** Rio de Janeiro: FGV/CPDOC, 2009. Disponível em: http://www.fgv.br/cpdoc/acervo/dicionarios/verbete-tematico/agencia-brasileira-de-inteligencia-abin#. Acesso em: 10 jul. 2022

DEMENICIS, Luciene. Satélite Geoestacionário de Defesa e Comunicações Estratégicas 1. **Eblog**, Brasília, DF, 26 jul. 2019. Disponível em: http://eblog.eb.mil.br/index.php/menu-easyblog/satelite-geoestacionario-de-defesa-e-comunicacoes-estrategicas-1-sgdc-1.html. Acesso em: 20 jul. 2022.

DESIDERÁ, Lucimara. Importância de Padrões Modernos para a Segurança e Proteção de Dado. In: COLÓQUIO. CTIR.Gov, 12, 2022. **Palestras [...]** Evento online, 27-29 abril 2022. Disponível em: https://www.cert.br/docs/palestras/certbr-ctirgov2022.pdf. Acesso em: 27 jul. 2022.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **About ENISA**. [*S. l.*]: ENISA, 17 abr. 2019. Disponível em: https://www.enisa.europa.eu/about-enisa. Acesso em: 21 jul. 2022.

FERREIRA NETO, Walfredo Bento. Cibernética como Setor Estratégico no Brasil e seus Reflexos para a Estrutura da Defesa (2008-2018). **Revista do Centro de Estudos Estratégicos do Exército**, Brasília, DF, v. 17, n. 3, p. 45-66, jun./ago. 2020. Disponível em: http://www.ebrevistas.eb.mil.br/CEEExAE/article/download/6409/5546/. Acesso em: 03 de maio de 2022.

FONTENELE, Marcelo Paiva. **Os Desafios da Segurança Cibernética no Mundo Contemporâneo**. Apresentação no 1 Seminário sobre segurança e defesa cibernética no mundo contemporâneo. Brasília, DF: Escola Superior de Defesa, 9 jun. 2022.

GELLMAN, Barton. Secrets, Surveillance and Snowden. **The Washington Post Magazine**, Washington, p. 1, 11 maio 2010. Disponível em: https://www.washingtonpost.com/magazine/2020/05/11/2013-edward-snowden-leaked-top-

secret-national-security-agency-documents-showing-how-us-was-spying-its-citizens-heres-what-happened-next/. Acesso em: 1 ago. 2022.

GREENWALD, Glenn. **Sem lugar para se esconder**. [*S. l.*]: Primeira Pessoa, 2014.

GREENWALD, Glenn; MACASKILL, Ewen; POITRAS, Laura. Edward Snowden: the whistleblower behind the NSA surveillance revelations: **The Guardian**, Hong Kong , 11 jun. 2013. Disponível em: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. Acesso em: 3 ago. 2022.

GUROVITZ, Hélio. Ficou claro o objetivo da NSA no Brasil. **G1.Globo**, Rio de Janeiro, 4 jul. 2015. Disponível em: https://g1.globo.com/mundo/blog/helio-gurovitz/post/ficou-claro-o-objetivo-da-nsa-no-brasil.html. Acesso em: 20 jul. 2022

HOSANG, Alexandre. **Política Nacional de Segurança Cibernética**: uma necessidade para o Brasil. Trabalho de Conclusão de Curso (Curso de Altos Estudos de Política e Estratégia) - Escola Superior de Guerra. Rio de Janeiro, 2011. Disponível em: https://abeic.org.br/Admin/Publicacoes/29/PolNacSegCib.pdf. Acesso em: 14 jun. 2022.

KURBALIJA, Jovan. Comitê Gestor da Internet no Brasil. Uma introdução à Governança da Internet. **Caderno 3**, [*S.I.*], 2016.

MEDEIROS, Sabrina Evangelista; PINTO, Danielle Jacon Ayres. Cabos submarinos e segurança cibernética no Atlântico. **Atlantic Centre**, Lisboa, jul.2022. Disponível em: https://www.defesa.gov.pt/pt/pdefesa/ac/pub/acpubs/Documents/Atlantic-Centre_PB_11.pdf. Acesso em: 19 jul. 2022.

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE. **Locked Shields**. [*S. l.*]: CCDCOE, 2022. Disponível em: https://ccdcoe.org/exercises/locked-shields/. Acesso em: 28 jul. 2022.

NONATO, Marcos Paulo Cardoso, PINHO, Harley. **A Integração do Sistema Militar de Defesa Cibernética (SMDC) com a proteção cibernética das Infraestruturas Críticas de interesse para a Defesa Nacional.** 2021. Trabalho de Conclusão de Curso (Curso de Altos Estudos em Defesa) – Escola Superior de Defesa, Brasília, DF, 2021.

RID, Thomas. **Cyber War Will Not Take Place**. Washington, DC: Oxford University Press, 2013. 218 p.

SOUSA, Ana Tereza Lopes Marra; ABRÃO, Rafael Almeida Ferreira; SANTOS, Vitor Hugo. Entre a subserviência e o pragmatismo: o Brasil perante o 5G. **Revista Oikos,** Rio de Janeiro, v. 20, n. 1, p. 71-92, 1 abr. 2021. Disponível em: http://www.revistaoikos.provisorio.ws/seer/index.php/oikos/article/view/716/353. Acesso em: 22 jul. 2022.

UNITED STATES. Department of State. International Security Advisory Board. A Framework for International Cyber Stability. *In*: UNITED STATES DEPARTMENT OF DEFENSE. International Security Advisory Board. **A Framework for International Cyber Stability**. Washington, DC: ISAB, 2 jul. 2014. Disponível em: https://2009-2017.state.gov/documents/organization/229235.pdf. Acesso em: 2 ago. 2022.

WARTH, Anne. Ministro das Comunicações defende rede privativa do governo incluída no leilão do 5G. **Estadão**, São Paulo, 11 ago. 2021. Disponível em: https://economia.estadao.com.br/noticias/geral,fabio-faria-ministro-das-comunicacoes-defende-rede-privativa-governo-incluida-leilao-do-5g,70003808114. Acesso em: 22 jul. 2022.