BRENO ZABAN CARNEIRO
DAVID RODRIGUES DOS SANTOS

DEFESA CIBERNÉTICA DE INFRAESTRUTURA CRÍTICA: PADRÕES DE SEGURANÇA DO OPERADOR NACIONAL DO SISTEMA ELÉTRICO

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. Carlos Maurício de Borges Mello - Maj QCO R1 EB

Brasília
2021

BRENO ZABAN CARNEIRO

DAVID RODRIGUES DOS SANTOS

BRENO ZABAN CARNEIRO
DAVID RODRIGUES DOS SANTOS

DEFESA CIBERNÉTICA DE INFRAESTRUTURA CRÍTICA: PADRÕES DE SEGURANÇA DO OPERADOR NACIONAL DO SISTEMA ELÉTRICO

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, 18 de AGOSTO de 2021

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

ALCIMAR SANCHES RANGEL – Prof. MSc. (ITI)
Membro 1

CINTIENE SANDES MONFREDO MENDES - Profa. Dra (ESD)
Membro 2

Defesa Cibernética de Infraestrutura Crítica: padrões de segurança do Operador Nacional do Sistema Elétrico

Breno Zaban Carneiro[1]
David Rodrigues dos Santos[2]

RESUMO

Este trabalho discute padrões de segurança cibernética adotados pelo Operador Nacional do Sistema Elétrico - ONS. O texto inicia-se com descrição do contexto de defesa cibernética no mundo e no Brasil, destacando o efeito da evolução tecnológica e o crescimento de incidentes de ataques. Em seguida, discutem-se as dificuldades específicas de defesa do setor elétrico. São também apresentados padrões de avaliação de segurança cibernética no setor elétrico adotados por autoridades dos Estados Unidos da América e do Reino Unido. A seção final relata e analisa informações obtidas sobre os padrões adotados para orientação da defesa cibernética do ONS. Estas informações foram obtidas em entrevistas conduzidas com autoridades do setor elétrico e de defesa cibernética brasileira. Observou-se que o ONS não utiliza os padrões de segurança dos Estados Unidos da América ou do Reino Unido, preferindo utilizar soluções de mercado para as quais seja mais fácil obter padrões de comparação e avaliação. O texto conclui com ponderações sobre o estado atual e o futuro da defesa cibernética no âmbito do setor elétrico brasileiro.
Palavras-chave: Defesa cibernética. Infraestruturas críticas. Securitização. Sistema elétrico.

Cyber Defense of Critical Infrastructure: Safety Standards of the National Electric System Operator

ABSTRACT

This paper discusses cybersecurity standards adopted by Brazil's National Electric System Operator - ONS. The paper starts by describing the cyberdefense environment in Brazil and the world, highlighting the effects of technologic development and the increase in cyber attack incidents. The paper then addresses specific issues observed in defending the electricity sector. This includes a description of cybersecurity standards for the electricity sector adopted by authorities in the United States of America and in the United Kingdom. The final section reports and analyzes information regarding cybersecurity standards that guide the ONS' cyber defense. The information was obtained in interviews conducted with Brazilian authorities in the electricity sector and cyber defense fields. ONS was found not to employ the standards adopted by the USA or the UK, preferring instead to employ market solutions that allow easier benchmarking and evaluation. The paper concludes by commenting on the current state and the future of cyber defense in the context of the Brazilian electricity sector.
***Keywords**: Cyber defense. Critical infrastructures. Securitization. Electric system.*

---

[1] Especialista em Políticas Públicas e Gestão Governamental (EPPGG) do Ministério da Economia.
[2] Mestre em Desenvolvimento Sustentável, com ênfase em Políticas Públicas e Gestão Ambiental, Tenente-Coronel do Corpo de Bombeiros Militar do Distrito Federal.
Trabalho de Conclusão do Curso de Altos Estudos em Defesa (CAED) da Escola Superior de Defesa (ESD), 2021.

1 INTRODUÇÃO

O risco de ataques cibernéticos à infraestrutura elétrica não é uma novidade recente. Em 2007, especialistas do governo dos EUA foram capazes de invadir o sistema de controle de um gerador a diesel de grande porte, causando sua autodestruição (CYBER..., 2011). Desde então, o risco tem se majorado em razão do aumento da sofisticação de ataques simultaneamente ao aumento do uso, no setor elétrico, de sistemas sofisticados de automação e controle.

O ataque à rede elétrica ucraniana em 2015 é um incidente ilustrativo tanto das dificuldades de implementação de um ataque, como dos potenciais prejuízos em caso de sucesso. Por um lado, as dificuldades de sucesso de um ataque podem ser vislumbradas pelo nível de dedicação e recursos alocado pelos atacantes. Estima-se que o ataque tenha demandado meses de planejamento e dezenas de pessoas trabalhando de forma coordenada; mesmo com toda essa dedicação, o ataque conseguiu interromper o fornecimento de energia por apenas 6 horas, e para apenas 250 mil pessoas (HOW..., 2017).

Mesmo a melhor tecnologia pode ser superada em caso de erro humano. Por outro lado, há elementos para se sustentar o que se chama de defesa em profundidade (*defense in depth*). Trata-se de uma combinação de medidas cuja adoção simultânea diminua a probabilidade de um ataque ser bem-sucedido:

> Defesa em profundidade não é uma solução única, e sim uma combinação de avaliações de risco, arquitetura de cyber segurança e de rede, conscientização de empregados, monitoramento de segurança, e planejamento e resposta a incidentes (...) Aplicar uma estratégia de defesa em profundidade em um ambiente de sistemas de controle industriais aumenta o 'custo' de ataques, aumentando simultaneamente habilidades de detecção e defesa contra operadores maliciosos. O objetivo é diminuir a quantidade de chances que um antagonista tem de se mover com sucesso dentro de uma rede ou sistema da rede elétrica (CLEMENTE, 2018, p. 32-33).[3]

Neste contexto, uma medida essencial de segurança em profundidade é assegurar que práticas de defesa modernas estejam inseridas em segmentos e instâncias diferentes da operação do setor: tecnologia, recursos humanos, capacidade de resposta etc. Mesmo que se admita que

[3] Livre tradução de "Defense in depth is not a single solution, but rather a combination of risk assessments, cyber security and network architecture, employee awareness, and security monitoring, incident planning, and response.(…) Applying a defense in depth strategy in an ICS setting increases the "cost" to hack simultaneously increasing defense and detection abilities from malicious operatives. Decreasing the amount of chances an antagonist is able to successfully maneuver within any given power grid's network or system is the objective".

uma defesa perfeita seja pouco provável, cada camada de proteção adicional atende ao objetivo de diminuir a capacidade de implementação de um novo ataque.

Surge então a questão: quais são as práticas de defesa adequadas, e como verificar se estão sendo implementadas adequadamente ao longo de aspectos distintos da operação de organizações do setor elétrico?

Este trabalho aborda a segurança cibernética do setor elétrico brasileiro. Mais especificamente, discute o padrão de segurança cibernética adotado pelo Operador Nacional do Sistema Elétrico - ONS. O objetivo é descrever as práticas atuais e verificar se são compatíveis com algum padrão de segurança internacional.

O trabalho é dividido em quatro seções principais. Esta primeira seção buscou caracterizar o desafio da segurança cibernética de ativos de infraestrutura no mundo moderno.

A seção 2 introduz questões relacionadas à evolução humana e suas consequências relacionadas aos ataques cibernéticos, em especial voltados às infraestruturas críticas do setor elétrico. Neste contexto, é apresentado o conceito de securitização, a partir do qual se realizará um *overview* sobre o processo de securitização[4] de defesa cibernética no Brasil. Esta seção também discute a inserção do tema cibersegurança nos documentos de Defesa, por meio da Política Nacional de Defesa, Estratégia Nacional de Defesa e Estratégia Nacional de Defesa Cibernética, com os reflexos no Sistema Interligado Nacional - SIN, o Operador Nacional do Sistema Elétrico - ONS e a defesa cibernética de infraestruturas críticas, indicando casos reais de ataque cibernético para exemplificar o tema.

A seção 3 apresenta padrões e guias internacionais de segurança cibernética no setor elétrico, apresentando algumas das melhores práticas internacionais para defesa cibernética do setor elétrico em âmbito internacional adotadas nos Estados Unidos da América e no Reino Unido.

Por fim, na seção 4, registram-se as informações coletadas em entrevistas com autoridades de defesa cibernética e representantes do ONS, com a finalidade de um diagnóstico comparativo entre os modelos adotados pelos EUA, Reino Unido e Brasil, vislumbrando os padrões de defesa do agente central do sistema elétrico brasileiro.

---

[4] Securitização: Termo definido por Buzan, Waever e Wilde (1998, p. 23 e 29) como sendo a versão mais extrema da politização. Securitização significa apresentar uma questão como urgente e existencial, tão importante que não deve ser exposta à discussão normal de políticas, mas deve ser tratada com decisão pelos principais líderes antes de outras questões. (Livre tradução dos autores de: “Securitization can thus be seen as a more extreme version of politicization. Securitization means to present an issue as urgent and existential, as so important that it should not be exposed to the normal haggling of politics but should be dealt with decisively by top leaders prior to other issues”.)

2 CONTEXTO HISTÓRICO - DEFESA DE INFRAESTRUTURA CRÍTICA NO MUNDO E NO BRASIL

2.1 TECNOLOGIA, DESENVOLVIMENTO E DEFESA

O desenvolvimento da sociedade moderna pode ser medido, dentre outros parâmetros, pelo nível de modernização dos seus processos de produção. Ao considerar que o homem pré-histórico partiu de uma situação de sobrevivência em um ambiente hostil, no qual seus desafios estavam ligados ao meio ambiente no qual habitava, é notável que, por meio da sua adaptabilidade, associada ao desenvolvimento de ferramentas e aperfeiçoamento do uso destas, tenha vencido os desafios que o ambiente lhe impunha.

Diamond (2013) descreve em sua obra sobre a evolução da humanidade ao longo da história, as principais causas de sucesso ou fracasso das diferentes sociedades. Para o autor, estas causas associam-se ao desenvolvimento, capacidade de adaptação e uso de três elementos básicos: armas, germes e aço. No contexto histórico apresentado, a maior capacidade de emprego de armas, a proteção contra agentes patogênicos externos (vírus) e o uso de novas tecnologias, permitiram a proteção, resistência e evolução. Transportando os conceitos para o tempo-espaço atual referente ao espaço cibernético, a capacidade de repelir ataques e proteção das infraestruturas críticas contra agentes externos será um divisor para assegurar a soberania de um país no campo cibernético.

Cruz Júnior (2013) aponta em seu texto que sistemas de informações e comunicação constituem a base do desenvolvimento econômico e social de um país e que a sociedade está a cada dia mais dependente da internet e de sistemas de informações. O autor faz uma comparação entre, de um lado, a aplicação da segurança e defesa cibernética no ramo empresarial, que visa assegurar o sigilo das informações classificadas do parque industrial nacional e proteger o conhecimento estratégico desenvolvido no meio industrial que representa uma vantagem competitiva do país, e, de outro lado, a segurança e defesa cibernética no campo governamental, cujas ações visam proteção contra ataques e sabotagens das infraestruturas críticas de uma nação, como por exemplo o sistema elétrico, das telecomunicações, de transportes, de segurança, do sistema financeiros, dentre outros.

McCaul (2012, apud CRUZ JÚNIOR, 2013) cita, como exemplo de tais ataques, o caso do vazamento de dados do desenvolvimento dos caças da Força Aérea Norte-americana F-35 e

F-22. O autor observou que, dois anos após o vazamento, a China apresentou caças com características muito semelhantes àqueles cujo repositório de dados foi invadido e copiado.

2.2 A SECURITIZAÇÃO DA SEGURANÇA E DEFESA CIBERNÉTICA NO BRASIL

Buzan, Waever e Wilde (1998, p. 1) citam em sua obra clássica que o conceito de segurança vem sofrendo alterações em virtude da incorporação de novos elementos. Passa-se de uma visão estadocêntrica centrada na política, representada por organizações (incluindo o Estado) e sua expressão militar, do qual surge o conceito tradicional dos estudos de segurança (conhecido também como estudos estratégicos), a qual foi muito difundida nos Estados Unidos. Em contraponto, surge outra visão oriunda do meio acadêmico, por meio de pesquisas sobre a paz, feminismo, economia política internacional e dos estudos de segurança (e estudos estratégicos), difundido principalmente na Europa.

Ainda segundo Buzan, Waever e Wilde (1998, p. 4), do confronto entre essas duas abordagens surge uma proposta de visão mais radical dos estudos de segurança, explorando ameaças a objetos referentes (indivíduo *versus* Estado) e a securitização dessas ameaças, que podem ser não-militares e também militares, incorporando as contribuições da visão ampla trazida pelos tradicionais estudos críticos de segurança e pesquisa da paz, sem abandonar a visão tradicional, por meio do estudo de diferentes tipos de ameaças.

Buzan, Waever e Wilde (1998) definem os setores dos estudos de segurança nos seguintes termos:

> De um modo geral, a **Segurança Militar** diz respeito à interação em dois níveis da capacidade ofensiva armada e defensiva dos estados, e a percepção das intenções de cada um dos estados. A **Segurança Política** diz respeito à estabilidade da organização dos estados, sistemas de governo e as ideologias que lhes dão legitimidade. A **Segurança Econômica** diz respeito ao acesso aos recursos, finanças e mercados necessários para sustentar níveis aceitáveis de bem-estar e poder do Estado. A **Segurança Social** diz respeito à sustentabilidade, dentro de condições aceitáveis para a evolução, dos padrões tradicionais de linguagem, cultura e identidade e costumes religiosos e nacionais. A **Segurança Ambiental** diz respeito à manutenção da biosfera local e planetária como o sistema de suporte essencial do qual todos os outros empreendimentos humanos dependem (BUZAN, WAEVER e WILDE, 1998, p. 8, tradução e grifo nossos).

Do estudo dos setores de segurança, emerge o termo securitização, assim descrito pelos autores:

> A maneira de estudar securitização é estudar o discurso e as constelações políticas: quando um argumento dentro desta estrutura retórica e semiótica específica atinge um efeito suficiente para fazer um público tolerar violações das regras que, de outro modo, deveriam ser obedecidas? Se, por meio de um argumento acerca da prioridade e da urgência de uma ameaça existencial, o ator securitizante conseguiu se libertar dos procedimentos ou das regras aos quais ele ou ela deveria estar vinculado (a), estamos testemunhando um caso clássico de securitização (BUZAN, WAEVER e WILDE, 1998, p. 25).

Buzan e Hansen (2012, p. 324) explicam a evolução dos temas que passam pelo processo de securitização, no qual uma questão pública, inicialmente tratada como não-politizada (o Estado não lida com isso e não faz disso um assunto de debate público e de decisão), passado na fase seguinte a ser politizado (a questão é parte das políticas públicas, exigindo decisão governamental e alocação de recursos) até chegar a securitização (determinada questão não é debatida como assunto político, mas tratada com velocidade acelerada e de maneiras que possam violar regras legais e sociais comuns).

Rudzit e Nogami (2010) citam que a segurança nacional somente pode ser entendida como um problema político quando se tem uma ideia razoavelmente clara sobre a natureza de uma ameaça e as vulnerabilidades do objeto ao qual as ameaças são dirigidas. Segundo Goldman (1982, apud RUDZIT E NOGAMI, 2010), os Estados podem procurar reduzir as suas inseguranças através da diminuição de suas vulnerabilidades ou enfraquecendo as fontes de ameaças.

Souza e Almeida (2016) exemplificam a aplicação dos conceitos da Escola de Copenhague ao contexto brasileiro, ao analisarem um processo de securitização ocorrido durante os protestos populares no Brasil em 2013, por meio do qual trilhou-se todas as suas etapas da securitização citadas por Buzan et al. (1998), culminando com ações “não discursivas” de monitoração das redes sociais pelo Centro de Defesa Cibernética (CDCiber) e pela Agência Brasileira de Inteligência (ABIN). No caso apresentado, os Órgãos de Inteligência, como Agentes Securitizadores, identificam uma ameaça (à paz social) e convencem as autoridades (Poder Executivo) a adotar medidas securitizadoras, atuando assim na monitoração das redes sociais.

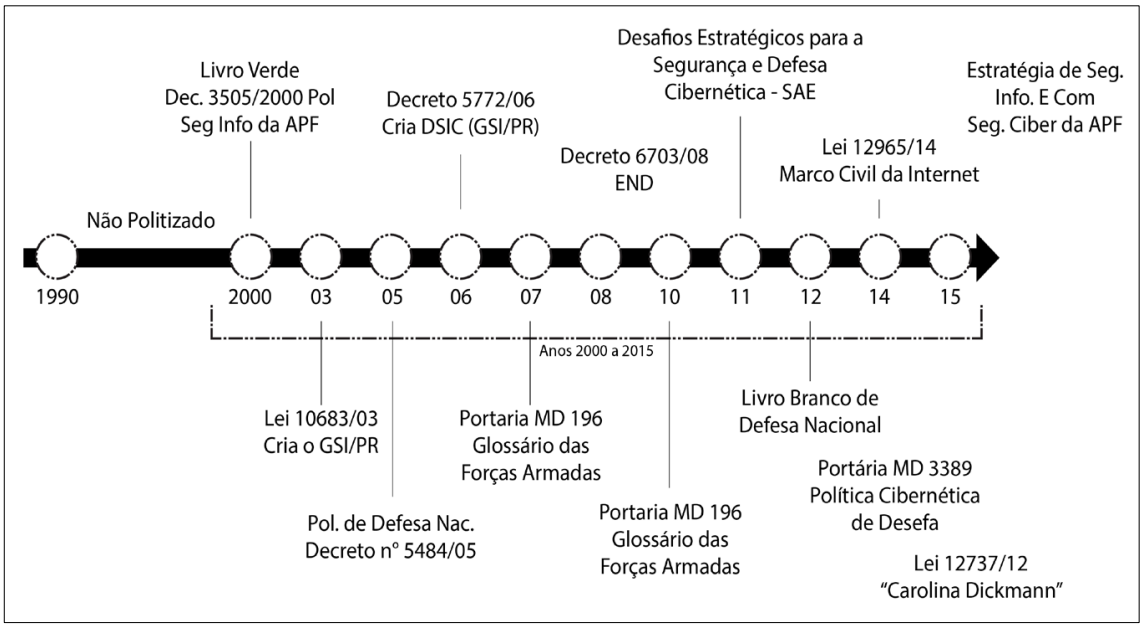
De acordo com Buzan et al. (1998, p. 25, apud SOUZA E ALMEIDA, 2016), dependendo de como se enquadra uma questão, as respostas a ela irão variar. Assim, quanto mais securitizado for um evento social, mais excepcional e extremo podem ser as respostas

governamentais a ele. Tratar da mesma forma o ativismo, os crimes, o terrorismo e os atos de guerra cibernéticos seria um erro.

Souza e Almeida (2016) avaliam que o tratamento da segurança cibernética pelo Brasil possui três marcos conceituais, utilizando a teoria da securitização de Buzan: até o ano 2000, fase não-politizado; entre 2000 e 2008, fase politizado; e de 2008 em diante, se inicia um processo de securitização. Tem-se o marco inicial do processo de politização da questão de Segurança e Defesa Cibernética com o Livro Verde da Sociedade da Informação no Brasil, do Ministério da Ciência e Tecnologia. Em termos de segurança cibernética (até então denominado segurança da informação), no mesmo ano, o governo publicou o Decreto No. 3.505 de 13 de junho de 2000, instituindo a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, aplicando a definição de pressupostos básicos, conceituações, objetivos, diretrizes, alocação de recursos e de responsabilidades.

Souza e Almeida (2016) apresentam a seguinte síntese da securitização:

Figura 1 - Arcabouço Político-Administrativo do Espaço Cibernético Brasileiro



Fonte: Souza e Almeida (2016)

No Brasil, foram instituídos dois documentos que norteiam a defesa nacional: a Política Nacional de Defesa e a Estratégia Nacional de Defesa.

Segundo Muller (2021), a Política Nacional de Defesa é o documento de mais alto nível do país em questões de Defesa, baseado nos princípios constitucionais e alinhado às aspirações e aos Objetivos Nacionais Fundamentais. Sua primeira edição ocorreu ainda em 1996 com o

título de Política de Defesa Nacional, sendo que, após a criação do Ministério da Defesa em 1999 e do advento da Lei Complementar 136, de 25 de Agosto de 2010, houve a obrigatoriedade da confecção e revisão, a cada 4 anos, da Política Nacional de Defesa, Estratégia Nacional de Defesa e Livro Branco de Defesa Nacional. A Política Nacional de Defesa expressa os objetivos a serem alcançados com vistas a assegurar a Defesa Nacional e atua no sentido de contribuir para a percepção de um estado de Segurança Nacional, definindo os objetivos fundamentais e os princípios que devem nortear as ações do País na área de Defesa.

A Estratégia Nacional de Defesa definiu as estratégias que deverão nortear a sociedade brasileira nas ações de defesa da Pátria, tratando das bases sobre as quais deve estar estruturada a defesa do país. Apresenta as Capacidades Nacionais de Defesa, as Ações de Diplomacia e os Setores Estratégicos. Nos setores estratégicos, destaca-se o setor cibernético, inicialmente à cargo do Exército Brasileiro e atualmente tratado no nível estratégico por meio do Comando de Defesa Cibernético (ComDCiber). A preocupação das autoridades brasileiras com a questão da defesa cibernética de instalações críticas está prevista desde a publicação da Estratégia Nacional de Defesa em 2008, que atribuiu o status de setor estratégico à cibernética (FERREIRA NETO, 2020, p. 18).

Em razão da interdependência entre o sistema elétrico e as demais infraestruturas críticas do país, existe uma grande preocupação quanto à necessidade em se rever a relação entre público e privado, no que diz respeito à gestão cibernética de infraestruturas críticas, à exemplo do modelo estadunidense, conforme citado pelo General de Divisão Amin Naves, Comandante de Defesa Cibernética, em audiência pública na Comissão de Relações Exteriores do Senado Federal, em setembro de 2019 (FERREIRA NETO, 2020, p. 255).

Mais recentemente, foi aprovada a Estratégia Nacional de Defesa Cibernética pelo Decreto nº 10.222, de 5 de fevereiro de 2020. A estratégia destaca a necessidade de proteção a infraestruturas críticas, identificadas como as pertencentes ao setor de Telecomunicações, ao setor de Transportes, ao setor de Energia, ao setor de Água e ao setor Financeiro.

Neste contexto, destacam-se os papéis de dois agentes-chave da defesa cibernética brasileira: o GSI - Gabinete de Segurança Institucional, Órgão da Presidência da República responsável pela segurança da informação no âmbito da administração pública federal, incluindo a segurança cibernética (Art.10, V, da Lei nº 13.844/19) e o ComDCiber -Comando de Defesa Cibernética, órgão central do Sistema Militar de Defesa Cibernética, possuindo amplas competências para a coordenação e execução de ações de defesa cibernética (Art.10 da Portaria nº 3.781/GM-MD/2020 do Ministério da Defesa).

2.3 O OPERADOR NACIONAL DO SISTEMA ELÉTRICO

Infraestrutura é essencial para o funcionamento de um país. A atividade humana moderna depende de rodovias e ferrovias para escoamento logístico, de telecomunicações para troca de informações e tomada de decisões e de saneamento para preservar a saúde da população. Manter a integridade da infraestrutura deve ser, portanto, uma prioridade de qualquer estrutura de defesa nacional.

Este trabalho enfoca a defesa de um dos ativos de infraestrutura mais críticos do Brasil: o Sistema Interligado Nacional - SIN. Conforme o Operador Nacional do Sistema Elétrico - ONS (OPERADOR NACIONAL DO SISTEMA ELÉTRICO, 2021a), o SIN pode ser definido da seguinte forma:

> O sistema de produção e transmissão de energia elétrica do Brasil é um sistema hidro-termo-eólico de grande porte, com predominância de usinas hidrelétricas e com múltiplos proprietários. O Sistema Interligado Nacional é constituído por quatro subsistemas: Sul, Sudeste/Centro-Oeste, Nordeste e a maior parte da região Norte.
> A interconexão dos sistemas elétricos, por meio da malha de transmissão, propicia a transferência de energia entre subsistemas, permite a obtenção de ganhos sinérgicos e explora a diversidade entre os regimes hidrológicos das bacias. A integração dos recursos de geração e transmissão permite o atendimento ao mercado com segurança e economicidade.[5]

O SIN é um ativo de valor inestimável para o Brasil. Se os geradores do Sudeste observam dificuldades, o SIN permite o despacho de energia do nordeste ou do sul. Se for mais eficiente gerar energia solar no Nordeste, o SIN permite a instalação de capacidade geradora lá para atender demandas em outros locais.

A gestão do SIN depende da atuação do Operador Nacional do Sistema Elétrico - ONS[6], uma pessoa jurídica de direito privado autorizada e fiscalizada pela Agência Nacional de Energia Elétrica - ANEEL. De acordo com a Lei nº 9.648/98, competem ao ONS as “atividades

---

[5] Disponível em: http://www.ons.org.br/paginas/sobre-o-sin/o-que-e-o-sin. Acesso em: 21 abr. 21.

[6] Lei nº 9.648/98: Art. 13. As atividades de coordenação e controle da operação da geração e da transmissão de energia elétrica integrantes do Sistema Interligado Nacional (SIN) e as atividades de previsão de carga e planejamento da operação do Sistema Isolado (Sisol) serão executadas, mediante autorização do poder concedente, pelo Operador Nacional do Sistema Elétrico (ONS), pessoa jurídica de direito privado, sem fins lucrativos, fiscalizada e regulada pela Aneel e integrada por titulares de concessão, permissão ou autorização e consumidores que tenham exercido a opção prevista nos arts. 15 e 16 da Lei no 9.074, de 7 de julho de 1995, e que sejam conectados à rede básica.

de coordenação e controle da operação da geração e da transmissão de energia elétrica integrantes" do SIN. Trata-se, assim, de um agente crítico para a infraestrutura nacional.

2.4 CONCEITOS DE DEFESA CIBERNÉTICA DE INFRAESTRUTURAS CRÍTICAS

Conforme o Glossário de termos das Forças Armadas do Brasil, o conceito de defesa cibernética é o conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (BRASIL, 2015, p. 85).

Segurança Cibernética é a arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas (BRASIL, 2015, p. 249).

Infraestruturas Críticas são instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade (BRASIL, 2015, p. 147).

Considerando que o objeto deste estudo são as infraestruturas críticas, apresenta-se ainda outro conceito complementar que considera as instalações, serviços, bens e sistemas que exercem significativa influência na vida de qualquer pessoa e na operação de setores importantes para o desenvolvimento e manutenção do país, como é o caso do setor industrial. Elas são importantes pelas facilidades e utilidades que fornecem à sociedade e, principalmente, por subsidiarem, na forma de recurso ou serviço, outras Infraestruturas Críticas, mais complexas ou não (BAGHERY, 2007).

Antes de concluir esta seção sobre defesa de infraestruturas críticas, cabe destacar que o Conselho Nacional de Pesquisa Energética - CNPE instituiu, em 01 de março de 2021, um Grupo de Trabalho - GT para estabelecimento de diretrizes sobre segurança cibernética no Setor Elétrico (BRASIL, 2021a). Esse GT, composto por representantes do setor elétrico e pelo Gabinete de Segurança Institucional - GSI da Presidência da República, recebeu a missão de propor diretrizes relacionadas ao tema, no prazo de sessenta dias a contar de sua criação.

2.5 INCIDENTES DE ATAQUES CIBERNÉTICOS

Ataques cibernéticos a infraestruturas críticas são uma realidade no mundo atual. Em 2010, teve-se notícia de que o *worm Stuxnet* foi utilizado para destruir centrífugas no centro de enriquecimento de urânio de Natanz, no Irã (MCAFEE, 2021). Em 2016, a Rússia foi acusada de realizar um ataque cibernético que causou quedas generalizadas de energia na Ucrânia (CABLE NEWS NETWORK, 2016).

A ameaça de ataques cibernéticos é majorada pelo fato de que agentes não governamentais frequentemente possuem as capacidades e o interesse em realizar ataques. É o que se observou em 2020, quando as operações do Superior Tribunal de Justiça - STJ foram paralisadas por um agente que pediu pagamento para não destruir os dados do sistema (POLÍCIA..., 2020).

O Brasil, pela sua ascensão econômica e pela recente organização de grandes eventos de interesse mundial, tem se destacado e atraído a atenção para país, o que coincidiu com o aumento dos ataques de *hackers*. Segundo dados do Grupo de Resposta aos incidentes de segurança - CTIR Gov (BRASIL, 2021b), só em 2021, foram reportados 14.091 notificações de ataques a *sites* públicos, onde fica demonstrado que o risco de ataque cibernético é uma preocupação real que deve permear a agenda de prioridades dos setores estratégicos do país, haja vista seu potencial de danos.

A frequência desses incidentes não deve ser interpretada como indicativa de que ataques cibernéticos são inevitáveis ou que meios de defesa estejam fora do alcance de autoridades nacionais. Pelo contrário: mesmo ataques contra instalações bem defendidas podem ser extremamente difíceis de executar, como descrito por Rovner[7]:

---

[7] Livre tradução pelos autores de: “Operations against closely guarded facilities require elaborate preparations. In these cases, the widely held belief that the offense has the advantage in cyberspace is usually false.19 Gaining access to hard targets and delivering payloads with significant effect is extremely difficult without time, expertise, and substantial organizational resources. A good deal of luck is required. Target characteristics must stay the same long enough for cyberspace developers to work on “exploits.” Success also depends on key personnel staying in place. Among other problems, personnel changes mean new passwords and security procedures that make it difficult to retain access into adversary networks. Success ultimately depends on cooperative adversaries, whose poor operational security leaves them at risk of attack. It is much easier to go on the offensive against adversaries who practice poor cyber hygiene, who are sloppy about vetting personnel, who do not encrypt communications, and who fail to update software routinely. Even in these cases, success is fleeting, because access is fragile. Minor network changes can spell doom for once-promising cyberspace operations; even mediocre defenders of hard targets can make life difficult for attackers seeking to degrade them.
Access to adversary networks is a prerequisite to any cyberspace operation. Access is hard to gain and easy to lose. Capable defenders practice routine updates, educate their workforce about the importance of cybersecurity, and test their systems against real and imagined intruders. Mediocre defenders are easier to target, but even they can do things to frustrate OCO.”

> Operações contra instalações bem protegidas demandam preparações complexas. Nestes casos, **a impressão geral de que o atacante tem vantagem no ciberespaço é normalmente falsa**. Ganhar acesso a alvos bem protegidos e fazer armas chegarem a seu alvo com efeito é extremamente difícil sem tempo, conhecimento especializado e recursos substanciais. **Uma boa dose de sorte é necessária. As características do alvo devem se manter as mesmas por tempo suficiente para serem "exploradas". O sucesso também depende de pessoal-chave ser mantido**. Entre outros problemas, mudanças de pessoal significam novas senhas e novos procedimentos de segurança que dificultam manter acesso em redes de adversários. **O sucesso acaba dependendo de cooperação dos adversários, cuja fraca segurança operacional deixa-os sob risco de ataque. É muito mais fácil atacar adversários com higiene cibernética fraca, que não criptografam comunicações e que não fazem *update* de software. Mesmo nesses casos, o sucesso é fugaz, já que o acesso é frágil**. Pequenas mudanças de rede podem representar o fim de operações promissoras no ciberespaço; mesmo defensores medíocres de alvos defendidos podem dificultar a vida de atacantes buscando degradá-los. Acesso a redes de adversários é um pré-requisito a qualquer operação no ciberespaço. Acesso é difícil de se obter e fácil de perder. **Defensores capazes praticam atualizações de rotina, educam sua força de trabalho sobre a importância de cibersegurança, e testam seus sistemas contra intrusos reais e imaginários**. Defensores medíocres são mais fáceis de atacar, mas mesmo eles podem tomar medidas para frustrar operações cibernéticas ofensivas. (ROVNER, 2020, p. 86-87, grifos nossos)

Uma dificuldade para a defesa cibernética é a incerteza sobre que soluções disponíveis são eficazes. Ian Levy, diretor técnico do *National Cyber Security Centre* – NCSC do Reino Unido, comentou que boa parte da indústria de segurança cibernética funciona como "feitiçaria medieval": "compre meu amuleto mágico e você estará seguro". Para Ciaran Martin, que liderou a criação do NCSC, consertar essa situação depende do desenvolvimento de padrões comuns para avaliar o quão bem um *software* de segurança cibernética funciona (CRIMS..., 2021).

É possível argumentar que padrões comuns são úteis não só para avaliação de *software*, como também para avaliar as práticas de gestão de segurança e riscos de organizações. Em outras palavras, a disponibilidade de guias de melhores práticas de conduta pode auxiliar entidades privadas e autoridades públicas a identificar vulnerabilidades e determinar medidas de segurança. Na próxima seção, serão apresentados exemplos de melhores práticas dos Estados Unidos da América e do Reino Unido.

3 MELHORES PRÁTICAS INTERNACIONAIS PARA SEGURANÇA CIBERNÉTICA DO SETOR ELÉTRICO

Dado o papel crítico da infraestrutura elétrica para o funcionamento da economia e de serviços públicos, governos nacionais tendem a liderar esforços para a defesa do setor contra cyber ataques. Como estes esforços normalmente envolvem interação com agentes privados envolvidos na geração, transmissão e distribuição de energia, é comum a divulgação de guias e melhores práticas para conhecimento público. Esta seção discutirá melhores práticas publicadas por outras nações e entidades.

3. 1 CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

Como ponto de partida, serão descritas as orientações da *Cybersecurity and Infrastructure Security Agency* (CISA), agência do governo dos Estados Unidos da América dedicada a promover infraestrutura segura e resiliente (UNITED STATES, 2021a). Em 2015, a CISA publicou o seu plano específico para o setor de energia (UNITED STATES, 2015a). O plano parte da premissa de que, como a maioria das infraestruturas de energia são controladas pelo setor privado, esforços de segurança e resiliência são uma responsabilidade compartilhada entre governo e este setor.

O plano estabelece três prioridades para defesa do subsetor elétrico: a primeira consiste em desenvolver ferramentas e tecnologias para aprimorar consciência situacional e segurança. Essa prioridade inclui a instalação de tecnologia governamental proprietária em sistemas de empresas para permitir compartilhamento de informações máquina-a-máquina e percepção de ameaças à rede.

A segunda prioridade é assegurar que “inteligência para ação” (*actionable intelligence*) e indicadores de ameaças sejam comunicados no menor tempo devido entre governo e empresas.

A terceira prioridade é planejar e treinar respostas coordenadas a um ataque, incluindo (1) desenvolvimento de guias e capacidades de coordenação de esforços empresas-governo de resposta e recuperação e (2) monitoramento contínuo de programas de compartilhamento de equipamentos.

O plano prevê que o Conselho Coordenador do Subsetor Elétrico (ESCC em inglês) atue como agente de ligação entre o governo federal e o setor na preparação e resposta a ameaças. O ESCC é formado por diretores de empresas e líderes de associações representando todos os

segmentos do setor. Ele fala diretamente com o Conselho Coordenador de Governo para Energia (GCC em inglês), composto por representantes do Departamento de Energia e do Departamento de Segurança Doméstica, bem como representantes do governo dos Estados Unidos e Canadá.

O plano registra que, em 2013, o Presidente assinou a Ordem Executiva 13.636, que estabeleceu políticas para defesa contra ameaças cibernéticas. No âmbito do setor elétrico, o Departamento de Energia e parceiros desenvolveram o "*Energy Sector Cybersecurity Framework Implementation Guidance*" (UNITED STATES, 2015b). O Departamento de Energia também desenvolveu o manual de programa Modelo de Maturidade de Capacidade de Cyber segurança (C2M2), e também lidera um programa de pesquisa e desenvolvimento chamado "*Cybersecurity for Energy Delivery Systems*".

Nota-se que uma abordagem ampla à gestão de riscos pode permitir desenvolver uma estratégia de cyber segurança personalizada para as necessidades de cada ativo específico de energia elétrica. Nessa linha de desenvolvimento autônomo, associações do setor também tem tomado iniciativa de conduzir seus próprios projetos de segurança cibernética.

O plano ressalta que o setor também enfrenta riscos de segurança física sobre a infraestrutura que controla os componentes cibernéticos. De especial interesse é a interdependência do setor elétrico com outras infraestruturas, como transporte, tecnologia da informação, comunicação, água e serviços financeiros. O Programa Regional de Avaliação de Resiliência (RRAP) avalia a infraestrutura física local para identificar dependências, interdependências, efeitos em cascata, resiliência e capacidades/insuficiências regionais. Note-se que as informações produzidas nessa avaliação são confidenciais por lei e não podem ser usadas para fins regulatórios.

O plano destaca a relevância de construção progressiva de confiança e planejamento, por meio de exercícios simulados. Informações sobre vulnerabilidades são sensíveis e agentes do setor podem não confiar o suficiente no governo ou em parceiros para compartilhá-las; é necessário construir relações de confiança entre tomadores de decisão. A essência de exercícios de preparação e planejamento está na flexibilidade e adaptabilidade para incorporar nova informação em um ambiente de mudança de práticas e informações.

Do ponto de vista de reação a eventos de segurança, registra-se que o governo federal dos EUA desenvolve Funções de Suporte em Emergência (FSE) para coordenar apoio federal em resposta a um incidente. Exercícios simulados, como o "*Cyber Storm*", permitem que os interessados avaliem cenários que têm impacto em suas operações e testem atividades de

resposta, mitigação e recuperação. O plano ressalva que, embora o subsetor de eletricidade tenha se dedicado à avaliação de riscos, o desenvolvimento de métricas para segurança ainda é um trabalho inacabado.

O *Energy Sector Cybersecurity Framework Implementation Guidance* (UNITED STATES, 2015b) visa permitir às organizações do setor de energia: caracterizar sua situação atual e seu alvo; identificar fraquezas em sua segurança energética; reconhecer as diretrizes, ferramentas e padrões existentes no setor; demonstrar suas práticas de gestão de riscos a interessados internos e externos.

Um elemento fundamental do *framework* é o *Cybersecurity Capability Maturity Model* (C2M2). Elaborado em parceria com o setor privado, o C2M2 oferece vantagens de padronização, orientação específica a cada subsetor e avaliação própria. A versão mais recente do C2M2, de julho de 2021 estabelece os seguintes domínios e propósitos (UNITED STATES, 2021c)[8]:

Quadro 1 - Domínios e Declarações de Propósitos C2M2

DOMÍNIO	**DECLARAÇÃO DE PROPÓSITO (*PURPOSE STATEMENT*)**
Asset, Change, and Configuration Management	*Manage the organization's IT and OT assets, including both hardware and software, and information assets commensurate with the risk to critical infrastructure and organizational objectives.*
Cybersecurity Program Management	*Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with both the organization's strategic objectives and the risk to critical infrastructure.*
Identity and Access Management	*Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.*
Event and Incident Response, Continuity of Operations	*Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and incidents, and to sustain operations during cybersecurity incidents, commensurate with the risk to critical infrastructure and organizational objectives.*
Risk Management	*Establish, operate, and maintain an enterprise cyber risk management program to identify, analyze, and respond to cyber risk the organization is subject to, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.*

[8] Optou-se por manter estas citações no original em inglês devido à relevância da escolha de cada elemento da linguagem na formulação de cada uma destas frases.

Situational Awareness	*Establish and maintain activities and technologies to collect, analyze, alarm, report, and use operational, security, and threat information, including status and summary information from the other model domains, to establish situational awareness for both the organization's operational state and cybersecurity state*
Threat and Vulnerability Management	*Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (such as critical, IT, and operational) and organizational objectives*
Workforce Management	*Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives*
Third-Party Risk Management	*Establish and maintain controls to manage the cyber risks arising from suppliers and other third parties, commensurate with the risk to critical infrastructure and organizational objectives.*
Cybersecurity Architecture	*Establish and maintain the structure and behavior of the organization's cybersecurity architecture, including controls, processes, technologies, and other elements, commensurate with the risk to critical infrastructure and organizational objectives.*

Fonte: O Autor adaptado de UNITED STATES, 2021c.

O C2M2 descreve 342 práticas de segurança cibernética, divididas nos 10 domínios citados acima. Para avaliar a segurança de uma organização, o modelo estabelece indicadores de maturidade (*Maturity Indicator Levels*, ou MIL), que variam do menor nível MIL0 até o nível mais avançado MIL3.

Para ilustrar este modelo, apresentam-se na tabela abaixo as práticas associadas à gestão de ativos de tecnologia da informação e operacional, no âmbito do domínio *Asset, Change, and Configuration Management*:

Quadro 2 - Exemplo de Progressão de Maturidade

PRÁTICA	MIL1	MIL2	MIL3
There is an inventory of IT and OT assets that are important to the delivery of the function; management of the inventory may be ad hoc	✓	✓	✓
The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective		✓	✓

The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, operating system and firmware versions)		✓	✓
Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function		✓	✓
Prioritization criteria include consideration of assets within the function that may be leveraged to achieve a threat objective		✓	✓
The IT and OT asset inventory is complete (the inventory includes all assets used for the delivery of the function)			✓
The IT and OT asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes			✓
The IT and OT asset inventory is used to identify cyber risks, such as asset end of life or end of support and single points of failure			✓
Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life			✓

Fonte: O Autor adaptado de UNITED STATES, 2021c.

O setor elétrico dos Estados Unidos da América também observa padrões estabelecidos pela *North American Electric Reliability Corporation* - NERC, uma autoridade regulatória supranacional (*NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION*, 2021). A NERC estabelece padrões específicos para cada questão de segurança cibernética. Por exemplo, o *Standard* CIP 006-6 visa especificar um plano de segurança física para proteger sistemas cibernéticos de sistemas elétricos de grande porte (*Bulk Electric Systems – BES)*. O *Standard* CIP 008-6, por sua vez, estabelece condições de respostas a incidentes para mitigar o risco à operação de BES em razão de um incidente de segurança cibernética.

3.2 CYBER ASSESSMENT FRAMEWORK (CAF)

No Reino Unido, o *Office of Gas and Electricity Markets* – OFGEM, autoridade regulatória governamental, publicou em 2018 o *Ofgem Competent Authority Guidance for Downstream Gas and Electricity in Great Britain* (REINO UNIDO, 2018). A função deste guia é servir como ponto de referência para a interpretação, pela OFGEM, da norma intitulada *Network and Information Systems Regulations 2018* (NIS).

O público-alvo do guia consiste em operadores de serviços essenciais (OES em inglês). O guia deve ser usado em consonância com os 14 princípios do NIS e o *Cyber Assessment Framework* (CAF), ambos divulgados pelo *National Cyber Security Centre* (NCSC) e descritos a seguir.

Quadro 3 - Objetivos e Princípios do CAF

OBJETIVO	PRINCÍPIOS
Managing Security Risk	*1. Governance* *2. Risk Management* *3. Asset Management* *4. Supply Chain*
Protecting Against cyber attack	*5. Service Protection Policies and Processes* *6. Identity and Access control* *7. Data Security* *8. System Security* *9. Resilient Networks and Systems* *10. Staff Awareness and Training*
Detecting Cyber Security Events	*11. Security Monitoring* *12. Proactive Security Event Discover*
Minimizing the Impact of Cyber Security Incidents	*13. Response and Recovery Planning* *14. Lessons Learned*

Fonte: O Autor adaptado de UNITED KINGDOM, 2019.

Os princípios são elaborados em termos de resultados a serem atingidos, sem se especificar uma lista de checagem sobre o que deve ser feito. No âmbito de cada princípio, são oferecidos Indicadores de Boas Práticas (IGPs, em inglês). Os IGPs estabelecem classificação por cores de acordo com as características típicas de organizações, sendo os que alcançam (cor verde), alcançam parcialmente (cor âmbar) ou não alcançam os resultados pretendidos (cor vermelha). O NCSC destaca que os IGPs visam auxiliar a avaliação por especialistas, mas não oferecem uma definição exaustiva de tudo que o avaliador deve considerar.

Para ilustrar o exposto, tome-se o exemplo do princípio B3 – Segurança de Dados (UNITED KINGDOM, 2019). O princípio, em termos gerais, envolve práticas de proteção contra acessos não autorizados. Dentro deste princípio, consta o item B3.d – Dados Móveis (*Mobile Data),* que enfoca a segurança de dados em telefones ou outros dispositivos móveis. Para avaliar o nível de adesão a boas práticas neste item, são utilizados os seguintes critérios.

Quadro 4 - IGPs para *B3.d Mobile Data*

NÃO ALCANÇADO	PARCIALMENTE ALCANÇADO	ALCANÇADO
Pelo menos uma das seguintes declarações é verdadeira	Todas as declarações a seguir são verdadeiras	Todas as declarações a seguir são verdadeiras
You don't know which mobile devices may hold data important to the operation of the essential function. *You allow data important to the operation of the essential function to be stored on devices not managed by your organisation, or to at least equivalent standard.* *Data on mobile devices is not technically secured, or only some is secured.*	*You know which mobile devices hold data important to the operation of the essential function.* *Data important to the operation of the essential function is only stored on mobile devices with at least equivalent security standard to your organisation.* *Data on mobile devices is technically secured.*	*Mobile devices that hold data that is important to the operation of the essential function are catalogued, are under your organisation's control and configured according to best practice for the platform, with appropriate technical and procedural policies in place.* *Your organisation can remotely wipe all mobile devices holding data important to the operation of essential function.* *You have minimised this data on these mobile devices. Some data may be automatically deleted off mobile devices after a certain period.*

Fonte: O Autor adaptado de UNITED KINGDOM, 2019.

Os OES devem avaliar sua situação de acordo com o CAF e indicar que medidas de segurança são devidas. O OFGEM pode, quando apropriado, revisar a autoavaliação e aconselhar medidas adicionais de cyber segurança, assim como demandar auditorias e inspeções. O guia prevê atividades de autoavaliação e revisão para permitir início de auditorias em 2019.

Os OES têm a obrigação de relatar ao OFGEM incidentes que possam ter um efeito adverso sobre a segurança de sistemas de rede e informação. O OFGEM não atua na resposta a incidentes; para obter suporte em tais situações, o OES deve contatar o NCSC. O NIS define alguns parâmetros para que um incidente se qualifique como adverso. Por exemplo, no caso de distribuição de eletricidade, considera-se como adverso um incidente em que 50 mil usuários deixaram de ser atendidos por mais de 3 minutos.

Cabe notar que a ocorrência do incidente adverso, em si, não constitui necessariamente uma violação a ser punida. A não comunicação do incidente, por outro lado, constitui em si

uma violação. O OFGEM define punições financeiras por condutas indevidas de forma proporcional, observando o limite máximo de 17 milhões de libras esterlinas.

Os OES devem relatar quais são os sistemas de redes e informações que são críticos ao serviço essencial prestado. O objetivo desse relatório (*scoping*) é identificar os sistemas, ativos e responsabilidades de interesse. O guia lista alguns sistemas que podem ser críticos, tais como controle de turbinas e desligamento de emergência.

A perspectiva do governo britânico é que uma abordagem baseada em princípios é mais eficaz do que a fixação de regras prescritivas. O motivo para tanto é a rápida mudança percebida no campo de cyber segurança. Os OES devem entender seu próprio negócio melhor do que qualquer entidade externa e devem ser capazes de tomar decisões adequadas.

Originalmente, o OFGEM considerou demandar que OES contratem e paguem os serviços de auditoria e inspeção dentro de uma lista pré-aprovada de agentes independentes acreditados. Posteriormente, pretendeu-se usar recursos próprios para financiar auditorias e inspeções.

Vale notar que o NCSC acredita produtos e serviços de segurança cibernética. Em sua página oficial (UNITED KINGDOM, 2021b), são indicados fornecedores cujos produtos foram avaliados independentemente com base nos critérios do NCSC do que se qualifica como “bom” dentro de cada área específica de segurança. Faz-se a ressalva que os fornecedores podem também oferecer outros produtos que não tenham sido avaliados.

3. 3 CONSIDERAÇÕES SOBRE AS PRÁTICAS INTERNACIONAIS OBSERVADAS

Com base na observação das práticas avaliadas, conclui-se que tanto é possível estabelecer padrões de conformidade e maturidade baseados em regras e pontos de checagem específicos, como é o exemplo do C2M2, quanto também é possível estabelecer padrões baseados em princípios e resultados, sem pontos de checagem específicos, como é o caso do CAF.

4 PADRÕES DE DEFESA CIBERNÉTICA DO ONS

4.1 PERSPECTIVAS DE AUTORIDADES BRASILEIRAS DE DEFESA CIBERNÉTICA

Em julho de 2021, os autores deste trabalho conduziram entrevistas com representantes do Gabinete de Segurança Institucional da Presidência da República e do Comando de Defesa

Cibernética do Exército Brasileiro - ComDCiber. Em razão da pandemia de COVID-19, as entrevistas foram conduzidas por via eletrônica, tendo os entrevistados manifestado concordância em participar da pesquisa e com o uso das informações coletadas, por meio do termo de consentimento livre e esclarecido cujo modelo segue no Apêndice C. As entrevistas tiveram como linha-mestra o questionário constante no Apêndice A. Esta seção apenas registra as respostas recebidas, deixando análises para a seção 4.3.

A entrevista foi iniciada com perguntas sobre se as autoridades brasileiras exigem a observância de algum padrão ou tecnologia para defesa cibernética e, em caso positivo, quais (perguntas 1 e 2). O objetivo destas perguntas era verificar se o Brasil segue o exemplo dos EUA e do Reino Unido de impor a observância de padrões ou tecnologias.

Em resposta, recebeu-se a informação de que não se conhece de exigência, por autoridades do governo brasileiro, de uso de qualquer padrão formal de avaliação de segurança cibernética (como o C2M2 ou o CAF). A única perspectiva que se conhece de criação de padrão de tal natureza envolve o trabalho do GT do CNPE.

Em seguida, foi perguntado como as autoridades brasileiras oferecem orientações e apoio para entes privados se estruturarem (perguntas 3, 5 e 7). O objetivo destes questionamentos era sondar o nível de suporte oferecido a entidades privadas no momento da entrevista. Em resposta, obteve-se a informação de que não se conhece de tecnologias específicas de segurança de tecnologia da informação que sejam oferecidas (ou impostas) pelo governo brasileiro para uso por agentes do setor elétrico. Não há, no âmbito do GSI ou do ComDCiber, credenciamento de produtos ou tecnologias, nem de agentes independentes, para prestação de serviços de segurança cibernética. Também não se oferece serviço para checar adequação de estruturas de defesa cibernética de agentes privados. E não se oferece orientação sobre localização e proteção de infraestrutura física que controle componentes cibernéticos do setor elétrico.

Perguntou-se então se existe canal institucional para permitir que dirigentes de empresas privadas que operem infraestrutura crítica comuniquem-se diretamente com autoridades de defesa cibernética (pergunta 4). O objetivo deste questionamento é verificar o nível de facilidade de comunicação por pessoas-chave da defesa cibernética brasileira. Em resposta, foi indicado o Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos. Este decreto é de observância obrigatória para órgãos e entidades da administração federal direta, autárquica e fundacional, e de observância facultativa para

empresas públicas e sociedades de economia mista federais. Entidades privadas podem eventualmente ser convidadas a integrar a rede[9].

No que se refere a iniciativas ou esforços para fazer pessoas-chave se conhecerem e criarem confiança mútua, informou-se a princípio que há orientação de que, para se ter acesso a informações classificadas, órgãos devem ser habilitados de acordo com a Lei de Acesso à Informação (LAI) e Decreto nº 7845, de 14 de novembro de 2012.

Questionou-se se as autoridades brasileiras conduzem exercícios simulados de defesa cibernética (pergunta 6). O objetivo da pergunta é registrar se e como o Brasil segue práticas internacionais de exercícios liderados por autoridades. Em resposta, foi destacada a realização anual do exercício Guardião Cibernético. Trata-se de simulação construtiva que emprega "gabinetes de crise" no âmbito de áreas de tecnologia da informação, comunicação social, jurídica e alta administração. O exercício culmina em simulação virtual, onde são reproduzidos sistemas computacionais utilizados pelos especialistas dos órgãos e empresas participantes

O exercício envolve as Forças Armadas, órgãos parceiros e entidades públicas e privadas de setores de infraestrutura crítica. No âmbito do setor elétrico, destaca-se a participação de entidades privadas independentes e empresas, tais como a Enel, que atua nos setores de geração, transmissão e distribuição de energia elétrica, e o próprio ONS. Atualmente, o Guardião Cibernético é o único exercício cibernético de âmbito nacional.

4.2 PADRÕES E PRÁTICAS ADOTADOS PELO ONS – RELATO DE ENTREVISTAS

Em julho de 2021, os autores deste trabalho conduziram entrevistas com representantes do ONS responsáveis pela gestão de sua política de segurança cibernética. Em razão da pandemia de COVID-19, as entrevistas foram conduzidas por via eletrônica, tendo os entrevistados manifestado concordância em participar da pesquisa e com o uso das informações coletadas, por meio do termo de consentimento livre e esclarecido cujo modelo segue no Apêndice C. As entrevistas tiveram como linha-mestra o questionário constante no Apêndice B deste trabalho. Esta seção apenas registra as respostas recebidas, deixando análises para a seção 4.3.

---

[9] Art. 5º (...) 3º Observado o interesse do Estado em relação à segurança cibernética nacional, outras entidades públicas ou privadas poderão ser convidadas pelo Gabinete de Segurança Institucional da Presidência da República para integrar a Rede Federal de Gestão de Incidentes Cibernéticos, por meio de ofício, desde que cumpridos os requisitos de que trata o art. 7º.

Questionou-se se o ONS segue algum padrão internacional de segurança cibernética e, em caso positivo, qual (pergunta 1). O objetivo era verificar, logo de início, se o ente nacional segue práticas consolidadas no exterior. Em resposta, informou-se que, desde 2018, o ONS utiliza, como padrão de segurança cibernética, o ISF Framework. Trata-se de um padrão comercial oferecido por uma entidade chamada *International Security Forum*.

O ONS optou pelo ISF porque este padrão permite comparação com outras entidades. Entendeu-se que, embora padrões como o C2M2 constituam ferramentas eficazes para sondagem de vulnerabilidades, não há base pública de dados que permita averiguar se os padrões de uma organização são comparáveis a outras organizações similares no mundo. O ISF, por outro lado, permite comparações (anonimizadas) com grupos de pares ao redor do mundo. No caso do ONS, buscou-se comparar a organização com empresas de prestação de serviços públicos (*utilities*) ao redor do mundo.

Perguntou-se sobre como é a estrutura de governança do ONS para decisões sobre segurança cibernética (pergunta 2). O objetivo do questionamento era identificar o método de tomada de decisão sobre práticas de defesa cibernética e utilização de tecnologia. Em resposta, informou-se que, no ONS, a política de segurança cibernética é proposta pela Diretoria de Tecnologia da Informação, Relacionamento com Agentes e Assuntos regulatórios, e aprovada pela diretoria colegiada. O ONS considera que a execução da política de segurança cibernética existente é um dever de todos seus funcionários. Nesta linha, destaca-se que, em todos os ataques cibernéticos recentes ao setor elétrico, tem-se observado um elemento de engenharia social envolvido na estratégia de ataque. Registre-se, ainda, o papel da auditoria interna no "policiamento" (*enforcement*) do cumprimento da política de segurança existente no âmbito da organização.

Perguntou-se então como decisões sobre operação do sistema são tomadas e comunicadas, com especial interesse em identificar o que depende de interação humana e o que é feito automaticamente por sistemas cibernéticos (perguntas 3 e 4). O objetivo desta linha de questionamento era verificar se a operação do sistema poderia ser interrompida remotamente por via exclusivamente cibernética, ou se a necessidade de intervenção humana conteria eventuais ataques de tal natureza.

Em resposta, obteve-se a informação relevante de que *nenhuma decisão de operação do sistema elétrico é tomada de forma cibernética (ou seja, exclusivamente por meios de sistemas eletrônicos e de automação) pelo ONS*. Embora o ONS receba telemetria de sistemas

automáticos de supervisão de controle e aquisição de dados (SCADAs[10]) e equipamentos de agentes de forma eletrônica, eventuais decisões do ONS de operação e despacho não são efetivadas por meio cibernético. A decisão é comunicada e efetivada por meios humanos; por exemplo, se houver necessidade imediata de desligamento de um equipamento, haverá um contato telefônico entre uma pessoa do ONS e uma pessoa do agente envolvido.

Cada centro regional de operação atua de acordo com diretrizes enviadas para o dia seguinte. O sistema conta com uma estratégia de substituição de centros para assegurar continuidade do serviço: caso um centro deixe de operar, outro centro poderá assumir seu lugar provisoriamente.

Questionou-se que critérios o ONS utiliza ao decidir pela aquisição de produtos e serviços de segurança cibernética, com especial interesse em identificar a adesão a padrões internacionais (pergunta 5). O objetivo da pergunta era verificar como o ONS decide confiar em uma tecnologia, e sondar se os credenciamentos realizados por autoridades estrangeiras são úteis para este esforço.

Em resposta, informou-se que, no Brasil, não existe certificação centralizada de serviços de segurança cibernética para auxiliar a tomada de decisão sobre aquisições de defesa cibernética. O ONS aborda esta demanda por meio da contratação de consultoria, com destaque para a empresa Gartner Group. Ao contratar esta empresa, eles têm acesso a documentos, análises e contato direto com analistas. Não se trata de um método estruturado em si como seria a aquisição de produtos certificados; trata-se de uma abordagem eficaz para se obter um produto bom e confiável. Representantes do ONS também buscam se manter atualizados sobre tendências do setor por meio da participação em eventos e congressos sobre o tema de segurança cibernética.

Finalmente, perguntou-se como o ONS interage com autoridades públicas e com outros entes privados para aprimorar segurança cibernética do setor elétrico, com destaque para a participação em exercícios (perguntas 6 e 7). O objetivo das perguntas era sondar como o ONS aproveita sua posição chave no setor elétrico para promover práticas eficazes de defesa cibernética.

Em resposta, informou-se que o ONS tem liderado esforços para o desenvolvimento de padrões nacionais de defesa cibernética no setor elétrico. Neste contexto, cabe destaque à

---

[10] Sistemas supervisão de controle e aquisição de dados, ou SCADAs, é uma expressão utilizada para se referir a software desenvolvido como aplicação para sistemas operacionais comerciais, e atua supervisionando e monitorando, quando muito alterando, as variáveis provenientes dos controladores no chão de fábrica.

proposta de procedimento de rede para defesa cibernética, concluído em dezembro de 2019. Este procedimento foi elaborado a partir de intenso diálogo com agentes do setor, inclusive no âmbito de um seminário e dois *workshops* em que se discutiu o procedimento item a item. Trata-se da primeira iniciativa no setor elétrico brasileiro de instituição de padrões de defesa cibernética.

O procedimento de rede foi encaminhado à ANEEL, cuja aprovação é necessária para que a norma passe a ser obrigatória por demais agentes do setor. A ANEEL já conduziu consulta pública sobre o tema, que foi incluído em sua agenda regulatória com previsão de definição em 2022. Há notícias de que a agência pretende expedir normas mais abrangentes para o setor elétrico, e não restritas aos procedimentos de rede discutidos.

No meio tempo, o ONS tem acelerado o processo de sofisticação da defesa cibernética no setor elétrico mediante a divulgação de rotinas operacionais. Estas rotinas, que não demandam aprovação pela ANEEL, têm envolvido práticas que não demandem investimentos expressivos pelos agentes afetados. Neste contexto, destaca-se a Rotina Operacional RO-CB.BR.01 - Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético (OPERADOR NACIONAL DO SISTEMA ELÉTRICO, 2021b). Entre as disposições contidas nesta rotina, destaca-se a obrigação de comunicação de incidentes ao ONS. Note-se que, em tais casos, o ONS não atua no tratamento e resposta a incidentes; o objetivo da exigência é apenas permitir ao ONS conhecer da ocorrência de ataques mais amplos antes que maiores impactos sejam percebidos.

Em 2019, o ONS participou do exercício "Guardião Cibernético" conduzido pelo Comando de Defesa Cibernética. O ONS também conduz testes próprios de vulnerabilidade, contratando empresas para realizar periodicamente testes de invasão para documentar e corrigir fragilidades.

Do ponto de vista de proteção física dos seus ambientes críticos, o ONS estabeleceu controle de acesso por biometria a seu *data center*. Nem mesmo diretores possuem acesso a tais ativos sem acompanhamento especial. Para o restante do setor elétrico, não há ainda procedimento de rede demandando diligência similar.

4.3 CONSIDERAÇÕES SOBRE AS INFORMAÇÕES COLETADAS

As entrevistas com autoridades brasileiras de defesa cibernética tinham quatro objetivos. A seguir descrevem-se as perspectivas dos autores acerca do conteúdo das respostas relatadas.

O primeiro objetivo era verificar se o Brasil segue o exemplo dos EUA e do Reino Unido de impor a observância de padrões ou tecnologias. Conclui-se das respostas que não há exigência de padrões ou tecnologias de modo equivalente aos EUA ou ao Reino Unido.

Segundo, buscou-se sondar o nível de suporte oferecido pelo poder público às entidades privadas, no momento da entrevista. Com relação às respostas obtidas, entendeu-se que não há oferta, pelo governo, de tecnologias proprietárias certificadas que garantam a segurança cibernética aos operadores do sistema elétrico. Tampouco existe o credenciamento de fornecedores ou a prestação de serviços de auditoria ou congêneres pelo governo, que garantam a integridade dos sistemas elétricos em relação à segurança cibernético.

Terceiro, buscou-se verificar o nível de facilidade de comunicação dos gestores privados do sistema elétrico com pessoas-chave da defesa cibernética brasileira. Extraiu-se das respostas que não há fórum dedicado à comunicação de diretores de empresas envolvidas em infraestruturas críticas.

Finalmente, buscou-se verificar se o Brasil segue práticas internacionais de exercícios liderados por autoridades. Das respostas recebidas, teve-se a perspectiva de que o Brasil já possui iniciativa de condução de exercícios de defesa cibernética, destacando-se para tanto o Exercício Guardião Cibernético, com a participação efetiva do ONS no exercício.

As entrevistas com o ONS tinha cinco objetivos. A seguir descrevem-se as perspectivas dos autores acerca do conteúdo das respostas relatadas.

Primeiro, visou-se investigar se o ente nacional segue práticas consolidadas no exterior. Das respostas recebidas, entendeu-se que o ONS não adota os modelos internacionais estudados, embora haja a preocupação quanto ao comparativo com entidades congêneres em relação à segurança cibernética dos seus sistemas, por meio da adoção do ISF Framework.

Segundo, buscou-se identificar a estrutura de tomada de decisão sobre práticas de defesa cibernética e utilização de tecnologia. Nas respostas, observou-se a clara liderança da Diretoria de Tecnologia da Informação, Relacionamento com Agentes e Assuntos Regulatórios, associada à compreensão, na organização, de que esta é uma responsabilidade compartilhada.

Terceiro, buscou-se verificar se a operação do sistema poderia ser interrompida remotamente ou se a necessidade de intervenção humana conteria eventuais ataques de tal natureza. As respostas permitiram constatar que este é um risco reduzido, uma vez que não há tomada de decisão por vias estritamente eletrônicas. Em caso de alteração na operação do sistema, haverá intervenção humana.

Quarto, visou-se verificar como o ONS decide confiar em uma tecnologia, e sondar se os credenciamentos realizados por autoridades estrangeiras são úteis para este esforço. Das respostas, observou-se que o ONS usa dos serviços de uma consultoria especializada para buscar tecnologias e equipamentos adequados à operação.

A definição da aquisição é realizada pelos representantes do ONS, que se mantêm atualizados sobre tendências do setor por meio da participação em eventos e congressos sobre o tema de segurança cibernética. Entretanto, não há um processo estruturado baseado em fornecedores credenciados certificados pelo governo.

Finalmente, buscou-se sondar como o ONS aproveita sua posição chave no setor elétrico para promover práticas eficazes de defesa cibernética. Observou-se que o ONS já exerce liderança em tentar desenvolver padrões e orientar outros agentes do setor elétrico a segui-los, com destaque para a submissão da Rotina Operacional RO-CB.BR.01 - Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético para aprovação da ANEEL.

As informações coletadas permitem aduzir duas constatações gerais. A primeira refere-se ao contexto incipiente de regulação e defesa em que o ONS atua. Ainda não há diretrizes, regras ou orientações consolidadas a orientar a atuação de agentes privados. Nota-se esforço e evolução constantes de autoridades neste sentido, como se observa com a publicação do Decreto nº 10.748/21 e com a instituição do grupo de trabalho para diretrizes de segurança cibernética no setor elétrico. Observou-se ainda distância entre a situação brasileira e a observada em outros países, em que já se disponibilizam padrões, normas e serviços de apoio a entidades privadas, inclusive com o credenciamento de soluções de tecnologia.

A segunda refere-se à tomada de decisão do ONS acerca dos padrões que devam orientar sua defesa cibernética autônoma. O ONS conhece os padrões estabelecidos por autoridades estrangeiras e considera que tais padrões possuem utilidade relativamente reduzida devido à impossibilidade de obter dados de comparação relevantes. Essa impossibilidade pode ser o resultado, em parte, da primeira constatação: na ausência de um ambiente regulatório e de defesa conducente ao compartilhamento de informações entre agentes, a opção pelo uso de um padrão externo implica uma decisão isolada e pouco informada. Em tal contexto, a opção por um serviço de consultoria externo, ainda que não dedicado exclusivamente ao setor elétrico, apresenta-se como uma solução imediata mais sustentável em evidências empíricas concretas.

5 CONSIDERAÇÕES FINAIS

Este trabalho buscou descrever as práticas de segurança cibernética do ONS e verificar sua compatibilidade com os padrões e tecnologias de segurança cibernética internacionais. Inicialmente, buscou-se apresentar o embasamento teórico para dar sustentação à discussão quanto à aderência do padrão adotado pelo ONS em relação à segurança cibernética.

Apontou-se a importância dos sistemas de informações e comunicação para o desenvolvimento econômico e social de um país e que a sua proteção representa uma vantagem competitiva, cabendo ao governo e aos entes privados prover a segurança e defesa cibernética, citando casos de ataques cibernéticos a infraestruturas críticas contra indústrias nucleares, sistemas elétricos e sistemas governamentais corporativos, como o caso do Superior Tribunal de Justiça, informando que foram reportados 14.091 notificações de ataques a *sites* públicos no Brasil em 2021.

Com o objetivo de apresentar a evolução da segurança cibernética como prioridade na definição e aplicação de políticas públicas, a pesquisa fundamentou-se nos conceitos da Escola de Copenhague, apresentando a evolução do conceito de segurança e as fases percorridas por um tema até que ele seja securitizado, analisando o processo de securitização ocorrido durante os protestos populares ocorridos em 2013 no Brasil.

O estudo prosseguiu apontando a preocupação das autoridades brasileiras com a defesa cibernética de instalações críticas, materializado por meio da publicação da Política Nacional de Defesa, Estratégia Nacional de Defesa e Livro Branco de Defesa, atribuindo o status de setor estratégico à cibernética. Mais recentemente, foi aprovada a Estratégia Nacional de Defesa Cibernética em fevereiro de 2020, destacando a necessidade de proteção a infraestruturas críticas, identificadas como as pertencentes aos setores de Telecomunicações, Transportes, Energia, Água e Financeiro.

Passou-se então à apresentação dos modelos de segurança cibernética aplicados ao setor elétrico nos Estados Unidos - C2M2 e Reino Unido - CAF. De forma sucinta, cada modelo foi apresentado, com suas características e peculiaridades. Em seguida, por meio da entrevista com gestores do ONS, buscou-se identificar o modelo adotado pelo Brasil, concluindo que o ONS adota o padrão do ISF Framework, uma solução de mercado apresentada pela consultoria internacional contratada e que permite a comparação em relação aos seus congêneres internacionais, de forma anônima.

O estudo aponta que existe uma possibilidade de alteração neste quadro nos meses e anos que se seguirem à conclusão deste trabalho, haja vista que tanto as autoridades de defesa cibernética como as autoridades do setor elétrico têm tomado medidas para sofisticar o aparato de segurança. Exercícios como o Guardião Cibernético têm permitido testar condições atuais e construir relacionamentos e confiança tendentes ao aprimoramento da segurança. Iniciativas de institucionalização de boas práticas, inclusive com a especificação de medidas no âmbito do setor elétrico, tendem a oferecer um ambiente regulatório mais propício à tomada de decisão segura por executivos do setor.

Concluindo, os riscos de vulnerabilidades cibernéticas tendem a crescer com o aumento da sofisticação tecnológica da sociedade brasileira e a importância do Brasil no contexto regional e mundial. Por outro lado, há uma série de medidas conhecidas que podem ser adotadas para aumento da segurança: desenvolvimento de padrões, acreditação de serviços e tecnologias, monitoramento constante e sanções regulatórias em caso de inobservância, dentre outras.

Documentos e modelos de segurança cibernética existem e estão disponíveis, havendo a necessidade de um maior estreitamento dos laços entre o poder público e os entes privados responsáveis pela operação do sistema elétrico brasileiro.

Iniciativas como do exercício Guardião Cibernético são o caminho para o aprofundamento nesta relação, com a maior inserção da Academia no desenvolvimento de tecnologias e sistemas proprietários, promovendo o desenvolvimento de padrões adequados às necessidades do país.

Tomando por base os modelos apresentados neste estudo, sugere-se a criação de uma agência reguladora voltada à segurança cibernética, nos moldes da *National Cyber Security Centre* do Reino Unido, que poderá liderar o desenvolvimento de padrões adequados às necessidades do país. Outra iniciativa que pode ser adotada e que serviria de embrião da futura agência seria a criação, no Ministério das Minas e Energia, de uma secretaria análoga à Secretaria de Produtos de Defesa do Ministério da Defesa, a qual seria responsável pela certificação dos produtos de segurança cibernética voltados às infraestruturas críticas do setor elétrico.

REFERÊNCIAS

BAGHERY, E. et al. **The State of the Art in Critical Infrastructure Protection**: a framework for convergence. Faculty of Computer Science, University of New Brunswick,

Fredericton, N.B. Canada, 2007. Disponível em: http://glass.cs.unb.ca/~ebrahim/papers/CIPFramework.pdf. Acesso em: 25 jun. 2021.

BRASIL, Ministério da Defesa. **Glossário das Forças Armadas**. 5. ed. Brasília, DF: Ministério da Defesa, 2015. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf. Acesso em: 25 jun. 2021.

BRASIL. Conselho Nacional de Política Energética. Resolução nº 1, de 10 de fevereiro de 2021a. Institui Grupo de Trabalho - GT para estabelecer diretrizes sobre segurança cibernética no Setor Elétrico que abordem aspectos relativos à prevenção, tratamento, resposta a incidentes e resiliência sistêmica. **Diário Ofcial da União**: seção 1, Brasília, DF, ed.40, n. 85, p. 11, 02 mar. 2021.Disponível em: https://www.in.gov.br/en/web/dou/-/despacho-do-presidente-da-republica-306193929. Acesso em: 22 jul. 2021a.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo. CTIR Gov. **Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos**. Brasília, DF: GSI, 2021. Disponível em: https://emnumeros.ctir.gov.br. Acesso em: 10 jul. 2021b.

BUZAN, Barry; WAEVER, Ole; WILDE, Jaap de. **Security:** a new framework for analysis. Londres: Lynne Rienner Publishers, 1998.

BUZAN, Barry, HANSEN, Lene. **A Evolução dos estudos de segurança internacional**. tradução Flávio Lira. São Paulo: Ed. Unesp, 2012. 576p.

CLEMENTE, Jason F. **Cyber security for critical energy infrastructure**. 2018. Dissertação (Mestrado em Estudos de Segurança*)* -Homeland Security and Defense, Naval Postgraduate School, Monterey,2018. Disponível em: https://calhoun.nps.edu/handle/10945/60378. Acesso em: 22 jul. 2021.

CRIMS and spooks unite and fight - Ransomware highlights the challenges and subtleties of cybersecurity. **The Economist,** London, 19 jun. 2021. Disponível em: https://www.economist.com/briefing/2021/06/19/ransomware-highlights-the-challenges-and-subtleties-of-cybersecurity. Acesso em: 22 jun. 2021.

CRUZ JÚNIOR, S.C. **A Segurança e Defesa Cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. Textos para discussão 1850: Rio de Janeiro: Ipea, 2013.
CYBER attacks mounting fast in U.S**. CBS NEWS** , *[S. l.]*, 30 set. 2011. Disponível em: https://www.cbsnews.com/news/cyber-attacks-mounting-fast-in-us. Acesso em: 22 jul. 2021.

DIAMOND, J. **Armas, Germes e Aço:** os destinos das sociedades. Tradução de Nota Assessoria, Silva de Souza Costa. 15. ed. Rio de Janeiro: Record, 2013.

FERREIRA NETO, W.B. **Uma Estratégia Nacional de Defesa para além da guerra:** geopolítica cibernética e seu transbordamento econômico-tecnológico no Brasil (2008-2018). 2020. 318p. Tese (Doutorado em Economia Política Internacional) - Instituto de Economia, Universidade Federal do Rio de Janeiro 2020.

HOW Power Grid Hacks Work, and When You Should Panic. **Wired,** 13 out. 2017. Disponível em: https://www.wired.com/story/hacking-a-power-grid-in-three-not-so-easy-steps/. Acesso em: 22 jul. 2021.

MCAFEE. **What Is Stuxnet?**. Disponível em: https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware/what-is-stuxnet.html. Acesso em: 22 jul. 2021.

MULLER. **Power Point Presentation.** Curso de Altos Estudos em Defesa, Escola Superior de Guerra, *Campus* Brasília, 26 ago. 2021.

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION. **CIP Standards**. Washington, DC: NERC, 2021 Disponível em: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx. Acesso em: 22 jun. 2021.

OPERADOR NACIONAL DO SISTEMA ELÉTRICO. **O sistema interligado nacional**. Rio de Janeiro: ONS, 2021. Disponível em: http://www.ons.org.br/paginas/sobre-o-sin/o-que-e-o-sin. Acesso em: 22 jul. 2021a.

OPERADOR NACIONAL DO SISTEMA ELÉTRICO. RO-CB.BR.01. **Rotina Operacional Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético**. Vigência em 09/07/2021. Rio de Janeiro: ONS, 2021.Disponível em http://www.ons.org.br/paginas/sobre-o-ons/procedimentos-de-rede/mpo. Acesso em: 16 jul. 2021b.

POLÍCIA Federal identificou hacker que invadiu sistema do STJ, diz diretor-geral. **G1,** .Brasília, 6 nov 2020. Disponível em: https://g1.globo.com/politica/noticia/2020/11/06/policia-federal-identificou-hacker-que-invadiu-sistema-do-stj-diz-diretor-geral.ghtml. Acesso em: 22 jul. 2021.

ROVNER, Joshua. Cyberspace and Warfighting. *In:* SCHNEIDER, Jacquelyn G. et. al..Ten Years In: implementing strategic approaches to cyberspace. **Newport Papers**, 45, 2020.

RUDZIT, Gunther e NOGAMI, Otto. **Segurança e Defesa Nacionais: conceitos básicos para uma análise**. Revista Brasileira de Política Internacional [online]. 2010, v. 53, n. 1. Disponível em: https://doi.org/10.1590/S0034-73292010000100001. Acesso em: 17 ago. 2021.

SOUZA, E, A, A; ALMEIDA, N.N. A questão da segurança e defesa do espaço cibernético brasileiro, e o esforço políticoadministrativo do estado . **Revista da Escola de Guerra Naval,**. Rio de Janeiro. v. 22, n. 2, 2016, p. 381-410. Disponível em: https://www.proquest.com/docview/2400886741?pqorigsite=gscholar&fromopenview=true. Acesso em: 17 ago. 2021.

UNITED KINGDOM. Office of Gas and Electricity Markets. **Ofgem Competent Authority Guidance for Downstream Gas and Electricity in Great Britain**. 2018. Disponível em: https://www.ofgem.gov.uk/system/files/docs/2018/11/ofgem_ca_guidance_for_dge_gb_v1.0_final.pdf. Acesso em: 22 jun. 2021.

UNITED KINGDOM. National Cyber Security Centre. **Cyber Assessment Framework V3.0**. Versão de 30/09/2019. Disponível em: https://www.ncsc.gov.uk/files/NCSC_CAF_v3.0%20.pdf. Acesso em: 16 set. 2021.

UNITED KINGDOM. National Cyber Security Centre. **Cyber assessment framework.** Disponível em: https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework. Acesso em: 23 jun. 2021a.

UNITED KINGDOM. National Cyber Security Centre. **CAF assured products & services**. Disponível em: https://www.ncsc.gov.uk/section/private-sector-cni/products-services. Acesso em: 23 jun. 2021b.

UNITED STATES. Department of Homeland Security. **Energy Sector-Specific Plan 2015a**. Disponível em: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf. Acesso em: 15 jun. 2021.

UNITED STATES. Department of Energy. Office of electricity delivery and energy reliability. **Energy Sector Cybersecurity Framework Implementation Guidance.** Jan 2015b. Disponível em: https://www.energy.gov/sites/default/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf. Acesso em: 21 jun. 2021.

UNITED STATES. Cybersecurity and Infrastructure Security Agency. **About CISA**. Disponível em: https://www.cisa.gov/about-cisa. Acesso em: 15 jun. 2021a.

UNITED STATES. Department of Energy. **Cybersecurity Capability Maturity Model (C2M2) Program**. Disponível em: https://www.energy.gov/ceser/energy-security/cybersecurity-capability-maturity-model-c2m2-program. Acesso em: 15 jun. 2021b.

UNITED STATES. Department of Energy. **Cybersecurity Capability Maturity Model (C2M2)**. Versão 2.0, Julho de 2021c. Disponível em: https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf. Acesso em: 16 set. 2021.

U.S. OFFICIAL blames Russia for power grid attack in Ukraine**. CNN**, *[S. l.]*, 12 fev. 2016. Disponível em: https://edition.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/index.html. Acesso em: 22 jul. 2021.

APÊNDICE A – Questionário Autoridades Defesa Cibernética

1. O governo brasileiro exige a observância, por agentes privados envolvidos em infraestrutura crítica nacional, a observância de algum padrão específico formal de avaliação de segurança cibernética como o C2M2 ou o CAF?
    a. Se sim, quais são os padrões exigidos?
    b. Se não, há perspectiva de criação de padrão próprio ou adesão a padrão internacional?
        i. Se sim, qual é o estado da arte desta criação ou adesão?

2. O governo brasileiro oferece (ou impõe) o uso, por agentes do setor elétrico, de alguma tecnologia específica de segurança de tecnologia da informação?
    a. Se sim, quais tecnologias proprietárias do governo são oferecidas/ impostas, e quais tecnologias de terceiros são impostas?
    b. Se não, há planos de desenvolvimento de tais tecnologias próprias ou definição de obrigação de uso de tecnologia de terceiros?
        i. Se sim, qual é o estado da arte desta criação ou adesão?

3. O governo brasileiro credencia (a) produtos e tecnologias ou (b) agentes independentes para prestação de serviços de segurança cibernética?

4. Existe um canal institucional formado por meio do qual Diretores de empresas do setor elétrico e autoridades de defesa cibernética possam se comunicar para relatar ameaças ou se planejar contra riscos?
    a. Se sim, qual é, e como funciona na prática? Se não, há planos de cria-lo?
    b. Existe um canal institucional similar para contato com autoridades de Estados, do Distrito Federal e dos Municípios?
    c. Existe alguma iniciativa ou esforço contínuo de fazer as pessoas chave se conhecerem melhor para criar confiança e facilitar comunicação de informações confidenciais ou sensíveis?

5. O ComDCiber oferece algum serviço para empresas para checar a adequação de sua estrutura de defesa cibernética?
    a. Se sim, como tais serviços são divulgados e ofertados?
    b. Há algum plano de realizar tal serviço, seja diretamente por cobrança de taxas ou indiretamente por credenciamento de empresas especializadas?
    c. Há alguma orientação sobre como contratar serviços de segurança cibernética?

6. O ComDCiber, ou alguma outra autoridade, realiza exercícios simulados de resposta a incidentes de segurança cibernética?
    a. Caso positivo, com que frequência?

7. Há orientações sobre onde localizar e como proteger a infraestrutura física que controla os componentes cibernéticos do setor elétrico?

APÊNDICE B – Questionário Autoridades Operador Nacional do Sistema

1. O ONS segue, em seus próprios sistemas e instalações, algum padrão específico de segurança cibernética para a gestão de riscos (como o C2M2 ou o CAF)?
    a. Se não, qual é a sua perspectiva sobre a adesão, pelo ONS e outras entidades do setor elétrico, a padrões internacionais de avaliação de segurança cibernética como o C2M2 (EUA) ou o CAF (Reino Unido)?

2. Quem é responsável pela definição da política de segurança cibernética dentro do ONS? E quem é responsável pela execução desta política?
    a. Existem pontos prioritários para aprimoramento da segurança cibernética do ONS?

3. Quais decisões de operação do sistema elétrico nacional são tomadas pelo Centro Nacional de Operação do Sistema – CNOS e pelos centros regionais?
    a. Quais decisões são tomadas e executadas por pessoas, e quais são tomadas e executadas automaticamente por sistemas cibernéticos?

4. Como é feita a comunicação entre agentes do setor elétrico e terceiros com o ONS para operações do setor elétrico?
    a. A ONS impõe a observância de alguma norma ou padrão para a realização dessa comunicação?

5. Ao decidir adquirir produtos ou serviços de tecnologia e cyber segurança, quais são os critérios de segurança observados pelo ONS?

6. Como o ONS e outros agentes do setor elétrico tem interagido para desenvolver padrões de segurança cibernética?

7. O ONS e outros agentes do setor elétrico realizam ou realizaram exercícios simulados para testar suas condições de segurança cibernética?
    a. Se sim, com que frequência?

APÊNDICE C – Modelo de Termo de Consentimento Livre e Esclarecido

Convidamos o senhor (a) a participar como voluntário da pesquisa intitulada “Defesa do sistema interligado nacional de eletricidade: condições de segurança física e cibernética do operador nacional do sistema”, desenvolvida para conclusão do Curso de Altos Estudos em Defesa, da Escola Superior de Guerra, Brasília, Distrito Federal.

Este documento é chamado de Termo de Consentimento Livre e Esclarecido (TCLE) e tem esse nome porque você só deve aceitar a participação na pesquisa, depois de ter lido e entendido este documento. Leia as informações com atenção e converse com o pesquisador responsável pela pesquisa sobre quaisquer dúvidas que você tenha. Caso haja alguma palavra ou frase que você não entenda, solicite mais esclarecimentos. Caso prefira, converse com os seus familiares e amigos antes de tomar a decisão de participar. Se você tiver dúvidas depois de ler estas informações, entre em contato com o pesquisador responsável.

Após receber todas as informações e/ou o esclarecimento de suas dúvidas, você poderá fornecer seu consentimento, rubricando e/ou assinando em todas as páginas deste Termo, em duas vias (uma do pesquisador responsável e outra do participante da pesquisa), caso queira participar. Esta pesquisa será realizada com atores-chave de autoridades de regulação e operação do setor elétrico e de defesa cibernética nacional.

O estudo tem como objetivo geral estudar as condições de defesa cibernética de um agente-chave do setor elétrico brasileiro, o Operador Nacional do Sistema Elétrico - ONS. A pesquisa pretende descrever o processo pelo qual o ONS define padrões e práticas de segurança cibernética para suas operações.

A sua participação se dará por meio de uma entrevista. Você foi selecionado e convidado a participar por ser um ator-chave do setor elétrico ou de autoridades de defesa cibernéticas brasileiras, entretanto a sua participação não é obrigatória. A qualquer tempo, você poderá desistir da entrevista, sendo que a sua recusa ou desistência não lhe trará qualquer prejuízo. A sua participação lhe trará risco mínimo, poderá trazer um desconforto mínimo pois exigirá tempo para realizar a entrevista. Não haverá remuneração decorrente da participação, assim como, não implicará em gastos. A sua participação poderá trazer benefícios para o seu trabalho, para sociedade brasileira e para comunidade internacional ao contribuir para o aprimoramento do conhecimento sobre práticas de defesa cibernética em ambiente regulado.

Caso você concorde em participar, a entrevista será realizada pelos pesquisadores principais, preferencialmente de forma presencial, em ambiente reservado. Devido ao

isolamento social e às restrições de locomoção decorrentes do enfrentamento da pandemia pelo novo Corona vírus, a entrevista poderá ser realizada a distância por videoconferência, ou ser respondida por escrito por e-mail.

Se você optar pela sua participação nesta pesquisa, os dados obtidos por meio da entrevista não serão divulgados individualmente, seus dados pessoais serão mantidos de maneira confidencial e sigilosa. Apenas os pesquisadores autorizados terão acesso aos dados individuais. O seu nome não será relacionado às respostas dadas para responder às perguntas da entrevista. Quando realizada a gravação, ela será transcrita. O áudio e o documento digital (transcrição ou reposta por e-mail) serão guardados em uma pasta de computador protegida por senha, e que somente a investigadora terá acesso. Mesmo que estes dados sejam utilizados para propósitos de divulgação e/ou publicação científica, a sua identidade permanecerá em segredo.

A sua participação é voluntária e sua recusa em autorizar esta participação não acarretará quaisquer penalidades. Você poderá retirar seu consentimento a qualquer momento do estudo sem qualquer prejuízo.

Caso concorde em participar nesta pesquisa, deverá assinar duas vias deste documento, uma delas será sua e a outra dos pesquisadores principais. Você terá a garantia de acesso, em qualquer fase da pesquisa, sobre qualquer esclarecimento de eventuais dúvidas e inclusive para tomar conhecimento dos resultados desta pesquisa. Neste caso, você pode entrar em contato com os responsáveis pela pesquisa: Breno Zaban Carneiro, e-mail breno.zaban@mme.gov.br e David Rodrigues Santos, e-mail david.rodrigues@cbm.df.gov.br.

CONSENTIMENTO

Li as informações acima e entendi o objetivo do estudo. Ficou claro para mim que serei submetido a uma entrevista, os riscos, os benefícios e a garantia de esclarecimentos permanentes.

Ficou claro também que minha participação é isenta de despesas e que eu terei a garantia de acesso aos dados e de esclarecimento de dúvidas a qualquer tempo.

Entendo que o meu nome não será publicado e que será assegurado meu anonimato.

Concordo voluntariamente com a minha participação nesta pesquisa e sei que posso retirar o consentimento a qualquer momento, sem penalidade ou prejuízo ou perda de qualquer benefício que eu possa ter adquirido.

Eu, **(participante da pesquisa)**, por intermédio deste, concedo livremente meu consentimento para minha participação nesta pesquisa.

Brasília - DF, _____/_____/_____

Nome do participante	Data	Assinatura

Nome do pesquisador/entrevistador	Data	Assinatura

Nome da Testemunha (se o voluntário não souber ler)	Data	Assinatura

Observação: 1ª Via Entrevistador/Pesquisador; 2ª Via Voluntário(a).