FELIPE SILVA LUCAS

A AMEAÇA CIBERNÉTICA ÀS INFRAESTRUTURAS CRÍTICAS NACIONAIS

Trabalho Acadêmico – Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do certificado do Curso Superior de Segurança e Defesa Cibernética.

Orientador: Cel R1 João de Azevedo

Rio de Janeiro

2023

CSSDC2023 ESG

_____

FELIPE SILVA LUCAS

RESUMO

Este trabalho trata da ameaça cibernética às infraestruturas críticas (IC) do país. A metodologia empregada se baseou em pesquisa bibliográfica e análise documental. Inicialmente são apresentados os tipos e técnicas de ameaças cibernéticas, os conceitos de Política Nacional de Segurança de Infraestruturas Críticas, de Estratégia Nacional de Segurança de Infraestruturas Críticas e da Estratégia Nacional de Segurança Cibernética. Após isso são exemplificados ataques cibernéticos às IC de alguns países e diferentes ataques cibernéticos ocorridos no Brasil. Finalmente, busca-se trazer à luz do leitor um resumo do panorama atual das IC de comunicações do país, ressaltando a importância das transmissões por radiodifusão como meio de contingência aos ciberataques a essas IC.

Palavras-chave: ameaça cibernética; infraestruturas críticas; transmissão por radiodifusão.

ABSTRACT

This work addresses the cyber threat to the country's critical infrastructures (CI). The methodology used was based on bibliographical research and documentary analysis. Initially, the types and techniques of cyber threats, the concepts of the National Critical Infrastructure Security Policy, the National Critical Infrastructure Security Strategy and the National Cyber Security Strategy are presented. After this, cyber attacks on CIs in some countries and different cyber attacks that occurred in Brazil are exemplified. Finally, we seek to bring to light the reader a summary of the current panorama of communications CIs in the country, highlighting the importance of broadcast transmissions as a means of contingency against cyberattacks on these CIs.

Keywords: cyber threat; critical infrastructures; broadcast transmission.

SUMÁRIO

1. INTRODUÇÃO

No mundo contemporâneo, caracterizado pela era da informação e evolução tecnológica constante, diferentes sistemas e mecanismos de controle são utilizados por entes governamentais e da iniciativa privada, baseados em ativos de TI, com o objetivo de trazer dinamismo, alto nível de eficiência e eficácia nas ações e/ou serviços disponíveis ao cidadão.

Nesse contexto, percebe-se o avanço exponencial da utilização de plataformas de comando, baseadas em *software* e *hardware* que necessitam de atualizações oportunas, bem como capacitação adequada dos seus operadores, a fim de que sejam evitadas falhas durante o desencadeamento das etapas previstas de funcionamento dessas plataformas.

Se faz de grande valia destacar que as falhas acima mencionadas, em muitas oportunidades, têm ocorrido por conta da ação de cibercriminosos que aproveitando-se da descoberta de vulnerabilidades nos sistemas lógicos empregados em diversas instituições, realizam ataques cibernéticos, comprometendo a operação dos mesmos.

As motivações para a execução de um ataque cibernético estão relacionadas a fatores como: facilidade de realização de muitas ações de ataque de maneira simultânea; dificuldade de identificação do responsável pelo ataque; poder ser executado longe das fronteiras do país que sofrerá a ação cibernética; e o custo para a execução de um ataque cibernético quando comparado com um ataque cinético.

A ameaça cibernética nunca se fez tão presente em nosso cotidiano como agora, quer seja pelo risco do cidadão de sofrer uma ação de ataque durante o uso do seu microcomputador no domicílio ou então pela ação orquestrada de cibercriminosos contra infraestruturas públicas ou privadas.

Nesse sentido, fruto da possibilidade de ações cibernéticas às infraestruturas de comunicações do país perpetradas por diferentes motivações e, consequentemente, do risco de um grave dano nos meios baseados nas transmissões digitais, dependentes de conexão de dados, entende-se ser de vital importância a existência de um sistema imune aos ciberataques como as transmissões por radiodifusão, especialmente, por ondas curtas, cuja principal característica é o alcance global.

Este ensaio acadêmico tem como objetivo verificar o emprego das transmissões por radiodifusão, com o fito de mitigar os danos causados nos sistemas de comunicações do país provenientes de uma ameaça cibernética.

A metodologia empregada na elaboração deste trabalho se baseou em pesquisa bibliográfica e análise documental, o que permitiu uma verificação dos conceitos de ameaça cibernética, infraestruturas críticas e transmissão por radiodifusão, de maneira a subsidiar a linha de pensamento deste autor para o atingimento do objetivo proposto.

O tema em questão se justifica pela necessidade de criação de infraestruturas críticas dotadas de sistemas resilientes, com redundâncias de funcionamento e complementariedade, para fazer frente à ação de cibercriminosos.

2. REFERENCIAL TEÓRICO

2.1 a ameaça cibernética e suas particularidades

Pela natureza da atividade, medir a ameaça cibernética não é algo simples. O sigilo e anonimato das ações ocorrem em razão das características do próprio ambiente do sistema global de redes de computadores (internet). A identificação dos autores de ataques cibernéticos é extremamente difícil e o desenvolvimento das capacidades de ação hostil se desencadeiam em absoluto segredo por diferentes atores desse ambiente. (CORRÊA FILHO, 2016)

Todavia, conforme *o "modus operandi"* a ser utilizado nas ações cibernéticas, podemos elencar o tipo e a técnica empregada no ciberataque:

2.1.1 Malware

É a junção das letras iniciais de "*Malicious*" e finais de "*Software*", empregado em programas que exploram redes de dados com diferentes dispositivos conectados, agindo nas vulnerabilidades existentes. A partir do acesso a um anexo de e-mail ou a algum link por parte do usuário, o *malware* é instalado. O vírus é um dos tipos de *softwares* maliciosos existentes, mas nem todo *malware* é um vírus.

Os *Ransomware* "sequestro de dados" é um outro malware de grande destaque atualmente. Sua ação se baseia no "sequestro" dos arquivos da vítima criptografando-os e a condição para decriptogafá-los, consiste no pagamento de um valor aos cibercriminosos.

2.1.2 Engenharia Social

O modo de atuação se caracteriza pela realização de procedimentos por parte dos usuários, ordenados pelo cibercriminoso, como a revelação de informações pessoais, valendo-se da manipulação psicológica. A verificação antecipada de hábitos e rotinas do usuário é o requisito comum para instá-lo a clicar em um arquivo recebido e que não gere inicialmente qualquer suspeita.

Um exemplo é o ataque *Phishing*, quando o usuário alvo é incentivado a realizar uma ação, como entregar dados confidenciais ao atacante ou a se expor a downloads maliciosos.

2.1.3 *Denial-of-Service* (*DoS*) e *Distributed-Denial-of-Service (DDoS*)

O DoS, “negação de serviço”, é um ataque que sobrecarrega um determinado sistema, com o objetivo de evitar com que ele responda às solicitações de acesso de usuários legítimos. O *DDos*, “negação distribuída de serviço”, tem as mesmas características, sendo realizado a partir de mais dispositivos infectados com o *malware* sob domínio do atacante. No *DoS* a intenção é prejudicar o serviço, diferindo-se de outros ataques cujo objetivo é aumentar o domínio de um determinado sistema.

Há diferentes tipos de ciberataques *DoS* e *DDoS*; os mais comuns são o ataque *TCP SYN flood*, o ataque *teardrop*, o ataque *smurf*, o ataque de *ping* da morte, e os *botnets*.

2.1.4 *Man-in-the-Middle (MitM*)

Um ataque *MitM* ocorre quando um hacker se insere entre os meios de comunicação de um cliente e um servidor.

Um exemplo é a usurpação de sessão, isto é, o computador do atacante substitui os endereços de IP pelos do cliente confiável enquanto o servidor continua a sessão, acreditando que está se conectando com o cliente.

2.2.5 Ataques de Senha

A tentativa de acesso às senhas é uma prática comum de ataque, por se tratarem de uma ferramenta de segurança básica de todos os usuários. Podem ser obtidas de várias maneiras, por “adivinhação” de forma manual ou sistemática, por acesso às senhas trafegas em claro, pelo uso de engenharia social, ou até mesmo em anotações do próprio usuário.

Um dos processos existentes é o da Força Bruta que consiste na tentativa e erro com o uso de combinações relacionadas ao nome da pessoa, do cônjuge, data de nascimento, nome dos filhos, etc.

Diante dos conceitos elencados anteriormente, percebe-se que a ameaça cibernética tem como características a furtividade das ações de seus perpetradores, cuja técnica empregada varia conforme os objetivos a serem atingidos.

2.2. A política nacional de segurança das infraestruturas críticas (PNSIC)

Aprovada por meio do Decreto 9.573, de 22 de novembro de 2018, a PNSIC elenca em seu artigo 3º os seguintes objetivos:

> I - a prevenção de eventual interrupção, total ou parcial, das atividades relacionados às infraestruturas críticas ou, no caso de sua ocorrência, a redução dos impactos dela resultantes;
> II - o estabelecimento de diretrizes e instrumentos para salvaguardar as infraestruturas críticas consideradas indispensáveis à segurança nacional;
> III - a integração de dados sobre ameaças, tecnologias de segurança e gestão de riscos;
> IV - a identificação das relações de interdependência entre as infraestruturas críticas no País;
> V - o desenvolvimento, com enfoque na prevenção, de uma consciência acerca da segurança de infraestruturas críticas; e
> VI - o estabelecimento da prevalência do interesse da defesa e da segurança nacional na proteção, na conservação e na expansão das infraestruturas críticas. (BRASIL. Decreto 9.573, de 22 de novembro de 2018).

Vale destacar de uma forma geral o enfoque que é dado às tarefas relacionadas à prevenção de interrupções, bem como à proteção dessas infraestruturas, o que reforça a necessidade de implementação de medidas como o uso de sistemas alternativos em casos de ameaça, aliado às atividades de segurança.

2.3 A estratégia nacional de segurança das infraestruturas críticas (ENSIC)

O Decreto nº 10.569, de 9 de dezembro de 2020, aprova a referida Estratégia Nacional de Segurança das Infraestruturas Críticas, discriminando os aspectos a seguir:

> As infraestruturas de comunicações, de energia, de transportes, de finanças e de águas, entre outras, possuem dimensão estratégica, uma vez que desempenham papel essencial tanto para a segurança e soberania nacionais, como para a integração e o desenvolvimento econômico sustentável do País. Fatores que prejudiquem o adequado fornecimento dos serviços provenientes dessas infraestruturas podem acarretar transtornos e prejuízos ao Estado, à sociedade e ao meio ambiente.
>
> De maneira geral, os países buscam se preparar para possíveis imprevistos que possam afetar tais infraestruturas, identificando ações e procedimentos que permitam garantir o seu funcionamento, ainda que com algum tipo de restrição.
>
> Nesse quadro, torna-se imperativa a atividade denominada segurança de infraestruturas críticas, cuja implementação necessita do esforço conjunto do Estado e da sociedade. (BRASIL. Decreto nº 10.569, de 9 de dezembro de 2020).

O preparo do estado brasileiro frente às possíveis ações criminosas das mais variadas ordens direcionadas às infraestruturas críticas nacionais é condição essencial para a salvaguarda da soberania, além do atingimento do desenvolvimento constante do país, sendo indispensável integração entre a sociedade e o estado nesse processo.

2.4 A estratégia nacional de segurança cibernética (E-CIBER)

O Decreto nº 10.222, de 5 de fevereiro de 2020, aprova a Estratégia Nacional de Segurança Cibernética que discorre sobre os aspectos abaixo:

> Em ataques cibernéticos recentes, grupos de hackers têm considerado sistemas de governo como alvos compensadores, no intuito de provocar diferentes impactos, como: o potencial dano à imagem do Governo perante seu público interno e perante a comunidade internacional, o descrédito da população nos serviços públicos, a desconfiança de investidores internacionais na capacidade da administração pública em proteger seus próprios sistemas, a desconfiança nos processos eleitorais, e o descontentamento da população com relação à administração pública.
>
> Além da proteção do próprio Governo, outro ponto crítico refere-se à proteção cibernética das empresas representantes das infraestruturas críticas. Essas empresas precisam ter uma abordagem consistente e evolutiva em segurança cibernética para identificar e avaliar vulnerabilidades, e gerenciar o risco de ameaças, ao observar, por exemplo, as cinco funções previstas na estrutura de segurança cibernética do National Institute of Standards and Technology - NIST, que são: Identificar, Proteger, Detectar, Responder e Restaurar.
>
> Avalia-se que os principais tipos de ameaças contra essas organizações são ataques de *phishing*, negação de serviço em larga escala, vazamentos de informações privadas, espionagem e terrorismo cibernéticos e a interrupção de serviços. (BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020).

Diante do exposto, fica evidenciada a motivação dos ataques às IC por hackers atualmente, ademais, a capacidade de restauração ou resiliência, na atuação em ataques cibernéticos é condição fundamental de proteção às infraestruturas críticas do país, sendo essencial a atuação sinérgica de entes estatais ou privados e essa coordenação, a depender da escala de dano sofrida, pode ser realizada com o emprego das transmissões por radiodifusão.

3. ATAQUES CIBERNÉTICOS ÀS INFRAESTRUTURAS CRÍTICAS NO MUNDO (IC)

As ações direcionadas por cibercriminosos às IC de um determinado país, além dos impactos financeiros na maioria dos casos e danos à soberania, traz uma série de prejuízos à imagem daquela nação perante a comunidade internacional, já que passam a ser públicas as vulnerabilidades dos sistemas atingidos.

Em abril de 2007, vários ataques cibernéticos dirigidos à Estônia, do tipo *DDoS*, fez com que sites do governo ficassem inacessíveis. O ataque teria ocorrido, em razão da retirada pelo governo da Estônia de uma estátua do Soldado de bronze de Tallinn que simbolizava a vitória russa contra o nazismo. A Rússia foi acusada pelo governo estoniano dos ataques, entretanto, negou veementemente a autoria e a origem das ações cibernéticas permanece desconhecida. Esse episódio se caracterizou como o primeiro ciberataque de grande repercussão, pelo uso massivo dos serviços baseados na internet por parte da Estônia. (CLARKE, 2015).

Em 2009, ocorreu um ataque cibernético que afetou a usina nuclear de Natanz, no Irã, cuja denominação passou a ser *Stuxnet*. Sua ação consistiu no ataque ao sistema produzido pela Siemens, denominado SCADA, e empregado para o controle das centrífugas de enriquecimento de urânio. EUA e Israel foram acusados pela ação por parte do governo iraniano. Todavia, não houve comprovação de autoria (CLARKE, 2015).

Em 2015, houve um relevante ataque cibernético à infraestrutura crítica da Ucrânia, resultando na interrupção do fornecimento de energia por horas na capital do país, Kiev. A intenção dos cibercriminosos era deixar a população Ucraniana sem eletricidade no período mais frio do ano. Alguns recursos do *malware* empregado não foram executados em sua plenitude, impedindo com que a falta de energia se prolongasse por até uma semana. Os perpetradores dos ataques não foram identificados, entretanto, a Rússia foi acusada pelo presidente ucraniano de iniciar uma guerra cibernética contra o seu país. (SEGUNDO, 2019)

Em maio de 2021, ocorreu um ataque de grandes proporções no oleoduto da Empresa Colonial, nos EUA. Foram roubados cerca de 100 GB de informações por hackers, após realizarem a interrupção do fluxo de dados da rede. A costa leste dos EUA foi severamente afetada, já que quase metade do abastecimento de diesel,

gasolina e querosene de aviação provinha do duto que transportava cerca de 2,5 milhões de barris de óleo por dia. A ação fez com que o governo americano iniciasse um estado de emergência, pois houve comprometimento da infraestrutura de transporte, resultando em avarias no setor energético, o que influenciou na economia. (PINHO, 2021).

4. ATAQUES CIBERNÉTICOS NO BRASIL

A partir da década de 2010, o Brasil passou a ser sede de uma série de eventos esportivos ou religiosos em sequência e que impulsionaram a geração de uma mentalidade de proteção, pelos órgãos estatais e não-estatais, às infraestruturas suscetíveis a ataques cibernéticos. Ainda assim, o país não ficou imune à ação dos cibercriminosos.

O primeiro caso emblemático ocorrido no país foi em 2013 e envolveu um ex-agente da National Security Agency, Edward Snowden. Segundo ele, entre os vários alvos da espionagem dos Estados Unidos estariam o governo e empresas brasileiras, já que havia sido criado um programa de nome *Prism*, específico para vigilância, e que coletava comunicações de grandes companhias de internet com sede nos EUA. (CORRÊA FILHO, 2016)

Utilizando-se da técnica de engenharia social denominada *phising* (utilizado para instar o usuário alvo a realizar uma ação importante ou clicar em um link para um site malicioso), no ano de 2014, hackers acessaram mensagens de aproximadamente 1.500 diplomados brasileiros, realizando vários ataques ao sistema do Ministério das Relações Exteriores. (SEGUNDO, 2019)

Em 2015 hackers difundiram dados de cerca de 7 mil militares na internet, após interceptarem um dos sistemas do Exército Brasileiro. A motivação para esta ação teria sido uma resposta às técnicas empregadas durante um exercício de jogos cibernéticos coordenado pelo Centro de Defesa Cibernética, organização militar subordinada ao Comando de Defesa Cibernética. (SEGUNDO, 2019)

Em 2017, com o objetivo de protestar o aumento das tarifas de energia elétrica, um grupo de hackers realizou um ataque no website da Agência Nacional de Energia Elétrica, executando o *defacemen*t (alteração da página). (SEGUNDO, 2019)

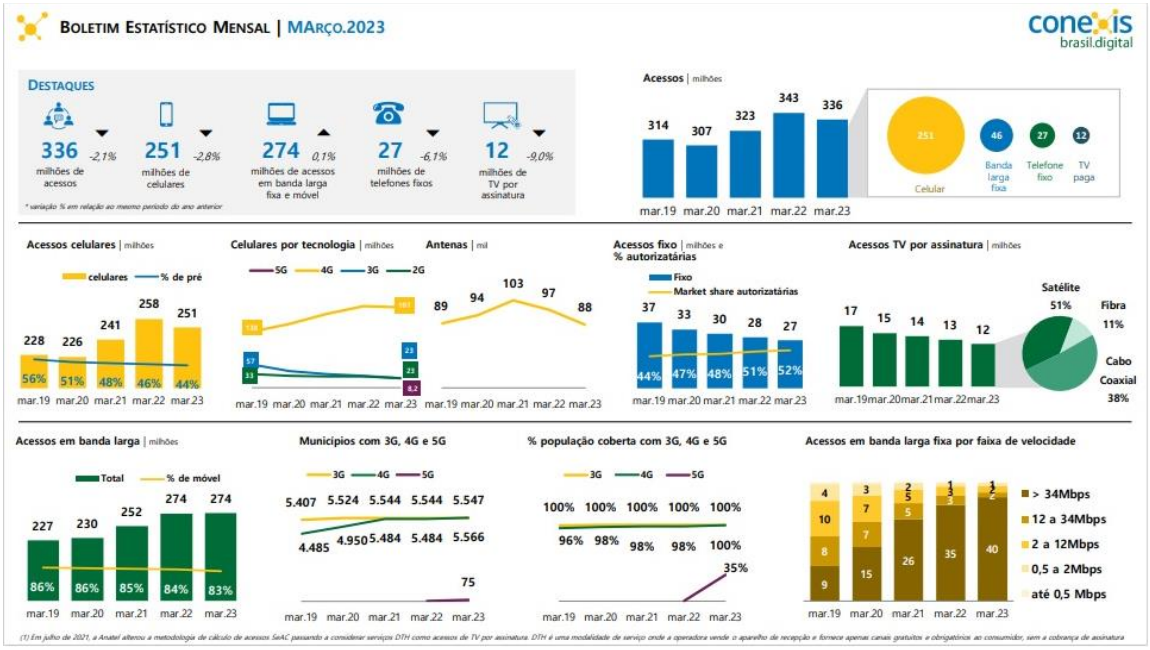
O superior tribunal de Justiça sofreu um ataque cibernético por meio da ação de *ransomwares*, em 03 Nov 20, que criptografaram todos os processos da Corte, e solicitaram o pagamento de um determinado valor, a fim de possibilitar o acesso aos dados dos referidos processos. O site do STJ ficou indisponível até 09 Nov 20, o que resultou na suspensão de prazos processuais, sessões de julgamento e audiências, durante esse período. (BOSCO, 2020).

5. PANORAMA ATUAL DAS INFRAESTRUTURAS CRÍTICAS DE COMUNICAÇÕES DO PAÍS

As infraestruturas críticas de comunicações do país abarcam os sistemas de telecomunicações, os sistemas de radiodifusão, bem como os serviços postais. Estão inseridas nos sistemas de telecomunicações as tecnologias de transmissão de dados em rede, analisadas neste trabalho e suscetíveis às ameaças cibernéticas. Importante ressaltar que os serviços de telefonia fixa, atualmente, se baseiam no sistema VoIP, ou seja, uma tecnologia que permite a transmissão de voz pela internet, o que demonstra uma grande dependência dos enlaces de dados pelas prestadoras.

Na figura 1, está a representação do nível de acesso aos diferentes serviços oferecidos pelas prestadoras, sendo possível identificar que 100% da população é contemplada com as redes celulares de 3G e 4G, e 35% com a cobertura 5G.

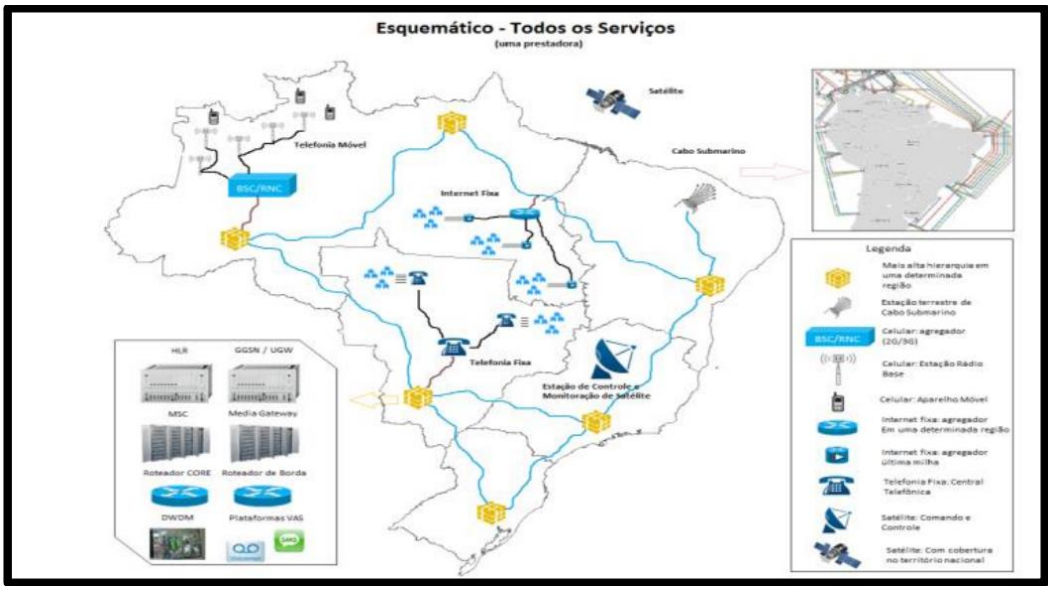
Figura 1 - Boletim de acesso aos serviços



Fonte: ESTATÍSTICAS, 2023.

Na figura 2 é possível perceber uma esquematização de instalações contempladas com os serviços de uma prestadora, para um melhor entendimento do desdobramento dos ativos ao longo do território nacional.

Figura 2 – Esquema de serviços



Fonte: BRASIL, 2023.

Existem, aproximadamente, mais de 100.000 instalações de telecomunicações no país, das quais, cerca de 361 foram selecionadas para uma análise mais profunda pelos integrantes do Grupo de Trabalho de Segurança de Infraestruturas Críticas do GSI, sendo definido, a partir de então, em torno de 134 instalações críticas de telecomunicações ao longo do território nacional. (BRASIL, 2023).

Na figura 3, a seguir, estão marcadas as 134 instalações mencionadas anteriormente, com forte predominância nas regiões sul e sudeste, que abrigam os grandes polos de industrialização do país.

Figura 3 – Infraestruturas Críticas de Comunicações

Fonte: BRASIL, 2023.

6. UTILIZAÇÃO DAS TRANSMISSÕES POR RADIODIFUSÃO COMO MEIO DE CONTINGÊNCIA

O Brasil possui uma empresa estatal com autorização para a prestação de serviços de radiodifusão pública do Governo Federal, detentora da maior estrutura de transmissão da américa latina. A Empresa Brasil de Comunicação S.A (EBC) é responsável pelo envio de programação educativa, artística, cultural, científica e informativa por todo o país, contribuindo para a integração nacional. (ALVES, 2022).

Os serviços de radiodifusão sonora, conforme art. 4 do Decreto n° 52.795/1963, se distinguem da seguinte maneira:

a) Pelas faixas de frequências utilizadas: nas Médias Frequências – MF (de 535kHz à 2.490kHz); nas Altas Frequências – HF (de 3.200kHz à 21.750kHz); e em Muita Alta Frequência – VHF (30MHz à 300MHz); e

b) Pelas técnicas de modulação (analógica): em amplitude (AM) e em frequências (FM).

A EBC possui emissões em todas as faixas acima mencionadas, entretanto, é de fundamental importância ressaltar o alcance superior proporcionado pelo uso das frequências em HF, ou ondas curtas (OC), por terem como característica a reflexão do sinal de transmissão, a partir do contato com a camada Ionosférica da Terra.

> historicamente, o sistema OC da EBC serviu para reforçar o sentimento de pertencimento e até combater o aliciamento cultural e filosófico de outros países, serviço que apoia a defesa e a soberania brasileira junto à população carente por meio dessa comunicação nacional. Isso se deu por meio de uma oferta de conteúdo de informação, utilidade pública e entretenimento por meio da programação da Rádio Nacional da Amazônia, além da interatividade por meio de cartas e telefonemas. (ALVES, 2022).

Os meios de transmissão de OC da EBC são dotados de antenas de cerca de 150 metros de altura, permitindo um alcance de sinal que supera a curvatura da Terra, podendo ser recepcionado por países de outros continentes a enormes distâncias. (ALVES, 2022).

Mesmo na ocorrência de interrupções de energia, ocorre a manutenção do sinal de transmissão, pois o sistema de alimentação de OC da EBC possui uma subestação elétrica de alta tensão e alimentação exclusiva composta por geradores a combustível. (ALVES, 2022).

Em razão das possibilidades reais de uma ação cibernética às infraestruturas críticas do país, sendo o foco deste estudo o ataque aos sistemas de comunicações, dependentes do tráfego de dados pela internet, percebe-se a importância do sistema rádio da EBC como elemento essencial para mitigação de um colapso no âmbito nacional.

As comunicações por meio das transmissões rádio não são suscetíveis a ataques por cibercriminosos, dessa maneira, mesmo havendo um comprometimento de meios de transmissão digitais, o enlace por radiodifusão seria mantido, possibilitando o acesso da população às mensagens oficiais do governo.

O emprego do sistema rádio da EBC, permite o atingimento de um dos aspectos essenciais quando se trata de segurança cibernética que é a resiliência dos sistemas, externada pela capacidade de uso de rotas alternativas para a transmissão da informação.

Numa situação hipotética de ataque cibernético que comprometa significativamente as transmissões das operadoras privadas de telefonia por meio das Estações Rádio Base (ERBs) geradoras de sinais de rede de dados 5G e voz, além de uma possível inoperância dos enlaces de dados por meio de fibra ótica ou transmissão via satélite, surgiria como opção de contingência o emprego das transmissões rádio da EBC.

Além do uso de comunicação por ondas curtas que podem chegar ao destinatário facilmente, bastando que seja utilizado um receptor para esse meio, a EBC possui uma infraestrutura robusta e que permite a operação de uma rede nacional de comunicação pública de Rádio, conforme o quadro abaixo:

Quadro 1: Estações rádio da EBC

RÁDIO	**FREQUÊNCIA**
MEC FM	RJ 99,3 MHz, BH 87,1 MHz, BSB 87,1 MHz
MEC AM	800KHz
Nacional FM	Brasília - 96,1 MHz, São Paulo - 87,1 MHz, Recife - 87,1 MHz, São Luís - 93,7 MHz
Nacional do Rio de Janeiro	FM 87,1 MHz, AM 1130 kHz
Nacional de Brasília	AM 980 kHz

Nacional da Amazônia	OC 11.780KHz, 6.180KHz
Nacional do Alto Solimões	FM 96,1 MHz

Fonte: EMPRESA BRASIL DE COMUNICAÇÃO, 2023.

A EBC possui, ainda, a TV Brasil de característica independente e democrática, cuja principal finalidade é complementar e ampliar a oferta de conteúdos.

O sistema OC da EBC está localizado no Parque de Transmissores do Rodeador, em Brazlândia-DF, conforme a figura 01 e a sua capilaridade é obtida por meio do uso de antenas que transmitem nas frequências de 6.180KHz e 11.780KHz, possibilitando o recebimento do sinal, inclusive, nas regiões mais remotas do país e, permitindo, mesmo em situações de crise, com que a população tenha acesso às informações.

Figura 4- complexo de antenas de ondas curtas

Fonte: EMPRESA BRASIL DE COMUNICAÇÃO, 2023.

O fomento aos núcleos estratégicos de desenvolvimento das emissões rádio, em especial por ondas curtas, é uma condição fundamental para a manutenção, bem como a ampliação da capacidade desse sistema funcionar efetivamente como um meio de contingência numa ação cibernética às infraestruturas de comunicações.

Quase a totalidade da infraestrutura crítica que abarca os sistemas de comunicações do país está sob o controle da iniciativa privada, em função dos processos de privatização que se iniciaram ao final da década de 90, trazendo resultados extremamente positivos em termos de expansão dos sistemas, além de

uma maior possibilidade de acesso pelo cidadão a diversos serviços com um menor custo.

Todavia, esse desequilíbrio existente nos meios de comunicações faz com que debates acerca de investimentos estatais nesse setor que é bastante caro para a soberania, venham à tona, sob pena da ocorrência de um grande incidente originado de uma ação cibernética vultuosa e que resulte em danos consideráveis, por ausência de sistemas alternativos para mitigação.

Os sistemas baseados em redes de dados permeiam de forma intensa as mais variadas esferas da administração pública federal, estadual e municipal, além de todos os mecanismos de operação e controle das infraestruturas críticas de comunicações, sob responsabilidade da iniciativa privada. Nesse sentido, na ocorrência de um ataque *DoS*, por exemplo, nas centrais de distribuição de sinal das operadoras de telefonia, impossibilitando o acesso aos serviços de dados e voz (aparelhos fixos e móveis) em todo o estado do Rio de Janeiro, a única forma de comunicação com amplitude entre as esferas federal e estadual, de maneira oficial, seria o uso das transmissões por ondas curtas ou a Rádio Nacional Rio de Janeiro nas frequências FM 87,1 MHz e AM 1130 kHz.

Assim sendo, percebe-se a capacidade de mitigação de uma ameaça cibernética por intermédio do uso de um meio de contingência, capaz de possibilitar redundância às infraestruturas de comunicações do país.

7. CONSIDERAÇÕES FINAIS

A ameaça cibernética está cada vez mais presente nos dias atuais, o risco das infraestruturas críticas do estado serem colapsadas, em razão da atuação de cibercriminosos vem sendo motivo de preocupação por diferentes atores estatais.

Como verificado nesse estudo, as técnicas e tipos de ameaças cibernéticas são inúmeras, como as ações de *Ransomwere* no superior tribunal de Justiça, em 03 Nov 20, resultando na criptografia dos processos da Corte, além dos ataques de *phishing* ao sistema do Ministério das Relações Exteriores, no ano de 2014 e ataques *DDoS* ocorridos na Estônia em 2007, impedindo o acesso a sites do governo estoniano.

Com o objetivo de salvaguardar as IC do país, em razão do crescimento de ataques cibernéticos a essas infraestruturas em todo o mundo, criou-se a PNSIC, com o foco principal na elaboração de diretrizes que visam a conscientização sobre a importância do tema e diminuição de impactos resultantes de interrupções no funcionamento das IC.

Nesse sentido a ENSIC foi estabelecida como instrumento da PNSIC e elenca objetivos estratégicos ressaltando a necessidade do trabalho conjunto entre o estado e sociedade na proteção da IC.

A criação da ENSC traz à tona o crescente ataque aos sistemas de governo, entendendo-se como alvos compensadores por cibercriminosos dada a repercussão proporcionada por este tipo de ação. Além disso, é fundamental, também, o envolvimento da iniciativa privada, por meio do controle e gerenciamento de possíveis vulnerabilidades em seus sistemas.

As infraestruturas críticas de comunicações do país, fruto da análise deste estudo, no que se refere aos meios de telecomunicações que se constitui de sistemas dependentes das tecnologias de transmissão de dados em rede, possui expressiva participação do setor privado no controle e distribuição dos serviços à população.

O altíssimo nível de acesso aos serviços digitais é traduzido pelos expressivos números de conectividade às redes 3G e 4G, 100%, todavia, demonstra a necessidade cada vez maior da execução de medidas de proteção e sistemas alternativos com vistas a permitir com que os usuários tomem conhecimento das informações de relevância, mesmo após um ataque cibernético.

Para tanto, observa-se que as transmissões por radiodifusão, são um único meio que não sofreria qualquer tipo de influência, mesmo após um grave comprometimento dos serviços dependentes do fluxo de dados em rede. Ademais, salienta-se que a única empresa nacional com capacidade e expertise para efetuar esse tipo de serviço no âmbito do território nacional é a EBC.

Diante da total dependência dos meios digitais demonstrados pela sociedade contemporânea e que impulsionam a escalada de aumento de crimes cibernéticos, torna-se indispensável a possibilidade do Brasil ter a capacidade de empregar meios analógicos, em situações de crise, como as transmissões por rádio.

Dessa maneira fica evidenciado como um relevante sistema que proporciona resiliência às IC de comunicações do país, funcionando como um meio de contingência, as emissões da EBC, com destaque para a faixa de HF (ondas curtas), pelo alcance que extrapola as fronteiras do país.

REFERÊNCIAS

ALVES, Oséias Fonseca de Aguilar Vancarlos de Oliveira. **A transmissão aberta em ondas curtas de rádio (oc) como infraestrutura crítica de comunicação e sua relação com a soberania e defesa nacionais**. Brasília, DF: Escola Superior de Defesa, 2022.

ARAUJO, José Euclides Oliveira de. **A atuação da defesa cibernética na proteção de infraestruturas críticas do Brasil**. Brasília, DF: Escola Superior de Guerra, 2020.

BOSCO, Natália**.** Ataque de hackers ao STJ é o mais grave da história do país. **Correio Braziliense**, Brasília, DF, 05 nov. 2020. Disponível em : https://www.correiobraziliense.com.br/brasil/2020/11/4886936-ataque-de-hackers-ao-stf-e-o-mais-grave-da-historia-no-pais.html. Acesso em: 30 set. 2023.

BRASIL. **Decreto n° 9.573, de 22 de novembro de 2018**. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 16 set. 2023.

BRASIL. **Decreto n° 10.569, de 09 de dezembro de 2020**. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm. Acesso em: 19 set. 2023.

BRASIL. **Decreto n° 10.222, de 05 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF: Presidência da República, 2020. Disponível em: https://www.gov.br/gsi/pt-br/dsic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf. Acesso em: 19 set. 2023.

BRASIL. **Decreto n° 52.795, de 31 de outubro de 1963**. Regulamento dos Serviços de Radiodifusão. Brasília, DF: Presidência da República, 1963. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/antigos/d52795.htm. Acesso em: 22 set. 2023.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Segurança de Infraestruturas Críticas**. Rio de Janeiro: GSI, 2023. Apresentação realizada ao Curso Superior de Segurança e Defesa Cibernética na Escola Superior de Guerra.

CLARKE, Richard. **Guerra Cibernética: a próxima ameaça e o que fazer a respeito**. Rio de Janeiro, RJ, 2015.

CORRÊA FILHO, Ivan de Souza. **A segurança cibernética no Brasil**: uma análise da situação atual. Rio de Janeiro: Escola Superior de Guerra, 2016.

EMPRESA BRASIL DE COMUNICAÇÃO. **Rádio Nacional**. Brasília, DF: EBC, 2023. Disponível em: https://radios.ebc.com.br. Acesso em: 30 set. 2023.

ESTATÍSTICAS. **Conexis Brasil.digital**, [*S. l.*], 2023. Disponível em: https://conexis.org.br/numeros/estatisticas/. Acesso em: 2 out. 2023

PINHO, Marcos Paulo Cardoso Nonato Harley de. **A integração do sistema militar de defesa cibernética (smdc) com a proteção cibernética das infraestruturas críticas de interesse para defesa nacional.** Brasília, DF: Escola Superior de Defesa, 2021.

SEGUNDO, Célio Borges Taquary. **A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos.** Escola Superior de Guerra, Brasília, 2019.