LUCIENE DA SILVA DEMENICIS

A REDE RÁDIO HF COMO MITIGAÇÃO DOS EFEITOS DAS AMEAÇAS CIBERNÉTICAS NAS REDES DE COMUNICAÇÃO ESTRATÉGICA DO EXÉRCITO BRASILEIRO

Trabalho de Conclusão de Curso – 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: Dr. Anderson F. Pereira dos Santos

Rio de Janeiro, RJ
2023

C2023 ESG

_____
LUCIENE DA SILVA DEMENICIS

RESUMO

Mais de 5 bilhões de pessoas em todo o mundo usufruem, por meio da Internet, de oportunidades econômicas e sociais do ambiente digital. Tecnologia de banda larga, computação em nuvem, Internet das Coisas e 4ª revolução industrial são termos já incorporados à sociedade moderna. Essa hiperconectividade entre pessoas, coisas e serviços tornou a fronteira entre a paz e a guerra muito tênue. A insegurança no espaço cibernético, conhecido como ciberespaço, é latente. No Brasil, particularmente na última década, a oferta de serviços prestados aos cidadãos, tanto na esfera pública quanto privada, cresceu vertiginosamente. Essa vasta e crescente superfície susceptível à ataque corresponde a uma grande vulnerabilidade no ciberespaço. Pesquisas recentes mostram que o Brasil ainda está em estágio bastante incipiente em suas capacidades cibernéticas. As infraestruturas críticas estão sendo alvos frequentes de ciberataques em todo o mundo, colocando em risco o funcionamento de segmentos vitais, como o setor de comunicações e energia. Nesse contexto, renascem as comunicações em altas frequência (ou ondas curtas), como uma última *ratio regis* em missões críticas, e caso de contingências. As ondas curtas, como alternativa de *backup*, podem assegurar as comunicações, viabilizando o comando e controle de operações. O Exército Brasileiro dispõe de uma Rede Rádio Fixa em alta frequência, que integra o Sistema Estratégico de Comunicações da Força. O presente ensaio busca avaliar se essa rede poderia, efetivamente, mitigar os efeitos das ciberameaças às quais as redes de comunicações estratégicas do Exército Brasileiro estão submetidas.

Palavras-chave: comunicações HF; rede de comunicações; ciberespaço; rede de contingência; Exército Brasileiro.

ABSTRACT

More than 5 billion of people around the world take advantage, using the Internet, of economic and social opportunities of the digital environment. Broadband technology, cloud computing, Internet of Things and the 4th industrial revolution are terms already incorporated into the modern society. This hyperconnectivity between people, things and services has made the edge between peace and war inaccurate (very thin or gossamer). Insecurity in cybernetic space, known as cyberspace, is latent. In Brazil, particularly in the last decade, the supply of services provided to citizens, both in the public and private spheres, has grown dramatically. This vast and growing surface susceptible to attack corresponds to a great vulnerability in cyberspace. Recent research shows that Brazil is still at a very early stage in its cyber capabilities. Critical infrastructures are being frequent targets of cyberattacks around the world, putting the functioning of vital segments, such as the communications and energy sectors, at risk. In this context, high frequency (or short wave) communications are reborn, as a last "ratio regis" in critical missions and in case of contingencies. Short waves, as a backup alternative, can ensure communications, enabling command and control of operations. The Brazilian Army has a Fixed Radio Network in high frequency, which is part of the Force's Strategic Communications System. This essay seeks to evaluate whether this network could effectively mitigate the effects of cyber threats to which the strategic communications networks of the Brazilian Army is submitted.
***Keyword**: HF communications; communications network; cyberspace; contingency network; Brazilian Army.*

SUMÁRIO

1 INTRODUÇÃO 1

2 REFERENCIAL TEÓRICO 3

2.1 O ciberespaço e os impactos das ciberameaças 3

2.2 O Brasil e o ciberespaço 10

2.3 O renascimento das comunicações via rádio em HF no mundo digital 12

2.4 O Sistema Estratégico de Comunicações do EB e a rede rádio HF 15

3 CONSIDERAÇÕES FINAIS 188

REFERÊNCIAS 23

APÊNDICE 29

1 INTRODUÇÃO

Nas duas últimas décadas, o setor de comunicações evoluiu extremamente rápido e em múltiplas áreas, tais como banda larga móvel, computação em nuvem e Internet das Coisas. Houve um aumento exponencial no processo de digitalização da economia a partir de 2019, e a espantosa demanda por acesso à Internet foi atendida por meio de infraestruturas não testadas, além de uma superexposição de informações pessoais em redes sociais sem precedentes (MARCIAL, 2023, p. 230).

Atualmente 64,4 % da população mundial (5,16 bilhões de pessoas) são usuários da Internet (MELTWATER, 2023, p. 10). As redes de voz e de dados convergiram e os dispositivos móveis, como *smartphones* e *tablets*, amplamente adotados pela população mundial, geraram uma enorme demanda por comunicações de alta capacidade. A tecnologia evoluiu a tal ponto que tudo (forno, geladeira...) pode ser considerado como se fosse um computador, e estes dispositivos estão interconectados, trazendo pontos adicionais de vulnerabilidade (SCHNEIER, 2020).

O elevado grau de conectividade associado às comunicações em banda larga proporcionou o crescimento das redes de computadores, sendo a Internet a mais relevante. Por um lado, essa conectividade trouxe muitos benefícios e uma gama de serviços *online* aos usuários, proporcionando conforto e comodidade (BRASIL, 2020).

Por outro lado, tornou a sociedade dependente e vulnerável dessa tecnologia disruptiva, que pode trazer prejuízos, com níveis distintos de impactos, para pessoas e instituições (SCHNEIER, 2020). Segundo Kallberg e Hamilton (2020), vivemos, inclusive, na “era do vício pela transmissão de dados”. A revolução digital viabilizou e conformou o modo de vida do homem moderno, ampliou o rol de vulnerabilidades no espectro dos conflitos no contexto da paz relativa (BRASIL, 2023b) e potencializou as capacidades das guerras híbridas e zonas cinzentas, dando origem ao domínio do ciberespaço (MARCIAL, 2023).

No Brasil, particularmente na última década, houve um aumento expressivo na quantidade de serviços prestados ao cidadão por meio da Internet, tanto na esfera privada quanto pública. Em 2020, 74,9 % dos domicílios, 98 % das empresas e 100 % dos órgãos federais e estaduais utilizavam a Internet. Essa vasta e crescente superfície susceptível à ataque, agrega mais vulnerabilidades que podem ser exploradas. Pesquisas mostram que o Brasil está em um estágio incipiente em suas

capacidades cibernéticas (GARCIA *et al.*, 2022). Ademais, de acordo com o relatório de 2022 do FortiGuard Labs, laboratório de inteligência de ciberameaças da líder global Fortinet®, o Brasil foi a segunda maior vítima de crimes cibernéticos da América Latina, atrás do México (BRASIL; FORTINET®; MALAGUTTI, 2020, 2022, 2022b).

As ciberameaças podem acarretar prejuízos operacionais severos com a paralisação de serviços. Há necessidade, portanto, de se proteger as infraestruturas críticas, conforme estabelecido pela Política Nacional de Segurança de Infraestruturas Críticas (BRASIL, 2022a), tornando-as mais resilientes e possuindo meios de contingência para restabelecer a prestação dos serviços, dentre eles o de comunicações. Os EUA, embora estejam na 1ª posição no *ranking* global em termos de cibersegurança (UNITED NATIONS, 2020), contam com um meio de comunicação adicional e seguro de emergências na faixa de alta frequência, para o caso de indisponibilidade das comunicações fixas ou celulares (UNITED STATES, 2023c).

É por meio das comunicações que a atividade de comando e controle é realizada, tanto no âmbito das Forças Armadas quanto no meio civil, na coordenação de operações diversas. Um tráfego eficiente de informações deve estar sempre disponível, de modo a viabilizar a consciência situacional e a tomada de decisão em tempo oportuno (BRASIL, 2015, 2022b). Os sistemas de comunicações, elencados no primeiro Objetivo Nacional de Defesa como Estrutura Estratégica, contribuem para garantir a soberania, o patrimônio nacional e a integridade territorial (BRASIL, 2016a).

Nesse sentido, por meio do método qualitativo descritivo, com base bibliográfica e entrevistas com especialistas do Exército Brasileiro, do Centro Integrado de Telemática do Exército (CITEx) e do 7º Centro de Telemática de Área (7º CTA), o problema de pesquisa indaga: uma rede rádio HF serviria como contingência para a mitigação dos efeitos das ciberameaças nas Redes de Comunicação Estratégica do Exército Brasileiro?

Diante da questão colocada este ensaio busca: i) compreender o ciberespaço e os possíveis impactos das ciberameaças nas redes de comunicação; ii) avaliar o contexto do Brasil no ciberespaço; iii) descrever o cenário das comunicações que utilizam rádio HF no mundo digital; e iv) apresentar a Rede Rádio HF do Sistema Estratégico de Comunicações do Exército Brasileiro. Finalmente, a conclusão discorre sobre o emprego da Rede Rádio HF de Comunicação Estratégica do Exército Brasileiro como contingência para a mitigação dos efeitos das ciberameaças.

2 REFERENCIAL TEÓRICO

Para introduzir conceitualmente a abordagem proposta, três conceitos básicos serão apresentados em suas tangências com o espaço cibernético: os impactos das ciberameaças; o contexto brasileiro; e o do uso das comunicações HF em pleno século XXI. Em seguida, a Rede Rádio HF do Sistema Estratégico do Exército é apresentada.

2.1 O ciberespaço e os impactos das ciberameaças

De acordo com a definição do Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência (GSI/PR), espaço cibernético

> [É o] espaço virtual composto por um conjunto de canais de comunicação da Internet e outras redes de comunicação, que garantem a interconexão de dispositivos de tecnologia da informação. Engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo, além de todas as ações, humanas ou automatizadas, conduzidas por meio desse ambiente (BRASIL, 2021).

Assim como a definição de Ganuza (2020, p.17), o ciberespaço deveria ser entendido como um conceito, um espaço imaterial dentro do ambiente da informação. Nesse sentido, nem os elementos tangíveis nem os intangíveis deveriam ser considerados parte intrínseca do ciberespaço. Porém, essa noção de ciberespaço só se concretiza, como abordado pelo autor, por meio da inter-relação das diversas camadas que materializam esse conceito, compondo o ambiente cibernético, conforme definição do referido Glossário (BRASIL, 2021), ou o ecossistema do ciberespaço, "formado por todos os elementos que estão relacionados entre si através do ciberespaço, juntamente com o mesmo ciberespaço" (GANUZA, 2020, p. 15).

No presente ensaio, então, assim como no artigo de Ďulík e Ďulík (2019), o termo ciberespaço será empregado para representar algo físico e real. As camadas que compõem o ciberespaço, segundo Ganuza (2020, p. 19), onde "as pessoas geram conhecimento que é processado em sistemas de informação que operam através de redes de telecomunicação localizadas em locais específicos no terreno", são: humana (pessoas físicas com identidade física que operam no ciberespaço); ciberhumana (identidade virtual que o usuário estabelece enquanto atua no ciberespaço, a ciberidentidade); cognitiva (ou informacional); lógica (formada pelo sistema de informação); de infraestrutura de Tecnologia da Informação e Comunicações (TIC) (dispositivos físicos de rede que permitem o transporte dos dados: hardware; software de sistema; redes com cabos ou sem fio; dispositivos eletrônicos de interconexão;

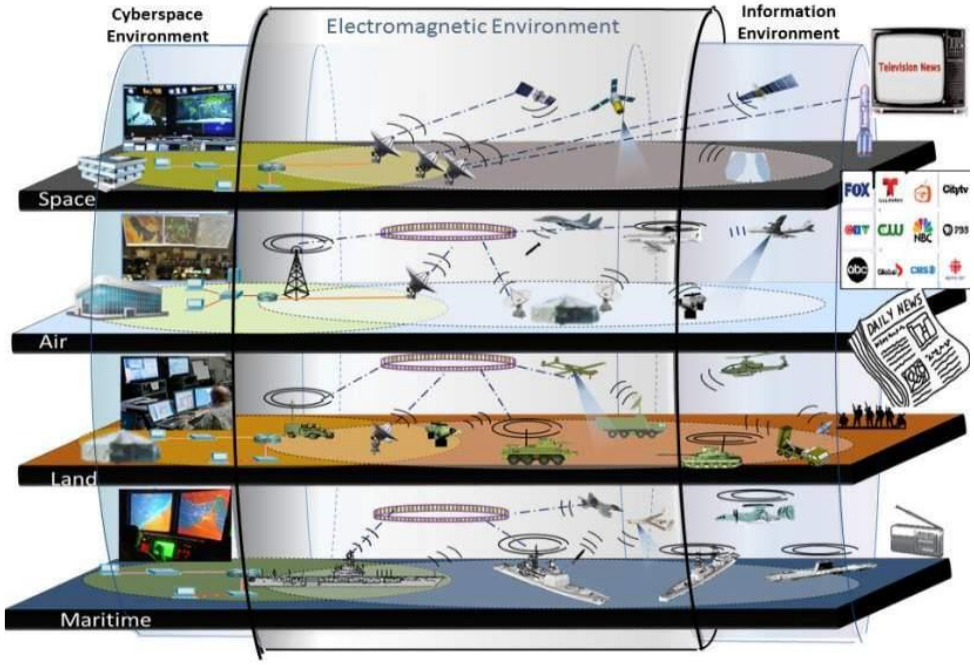
conectores; servidores; computadores; periféricos; dispositivos de segurança...) e componente geográfica (terreno ou áreas físicas correspondentes aos domínios operacionais convencionais - terra, mar, ar e espaço sideral - onde estão localizadas a infraestrutura de TIC e as pessoas que suportam o ciberespaço). Este autor ressalta (GANUZA, 2020, p. 18), ainda, dois elementos vitais para a sustentação do ciberespaço, são eles: o software e a energia elétrica.

A maioria dos autores, tal como Teixeira Júnior *et al.* (2017) e como consta no Manual de Doutrina Militar de Defesa Cibernética (BRASIL, 2023a), estrutura o ciberespaço em apenas 3 camadas, quais sejam: a física (que engloba a rede física da infraestrutura de TIC e o terreno, anteriormente citadas); sintática ou software (correspondente à rede lógica) e a semântica ou *peopleware* ou cognitiva ou ciberpersona (para as 3 demais camadas: humana, ciberhumana e cognitiva).

O ciberespaço tem conquistado grande destaque nas últimas décadas em virtude de suas características peculiares, dentre elas, ser: artificial (criado e modificado pelo ser humano); dinâmico (muda à medida que surgem novas tecnologias e serviços, e não se limita à Internet); imperceptível; ubíquo; ágil; e transversal. Além disso, com baixo custo de operação, tem alcance global com grande capilaridade e fluidez; e tem potencial para atuar como instrumento do Poder Nacional. Os efeitos dos eventos, que ocorrem no (ou por meio do) ciberespaço, podem ser percebidos em qualquer parte do mundo e de forma simultânea. A definição de fronteira para o ciberespaço é uma questão bastante polêmica, inclusive da perspectiva jurídica (GANUZA, 2020, p. 19).

Segundo Ďulík e Ďulík (2019), o ciberespaço, que no âmbito operacional foi reconhecido como quinto domínio operacional pela OTAN, é composto por sistemas eletrônicos e opera em rede, utilizando o ambiente eletromagnético para se conectar de forma transversal a todos os demais domínios operacionais: terrestre, aéreo, marítimo e espacial (GANUZA, 2020, p. 23). Além disso, ele conecta os domínios operacionais com os processos cognitivos que utilizam os dados armazenados, modificados ou trocados. Esse autor, assim como no Manual do Exército Brasileiro – Operações de Convergência 2040 (BRASIL, 2023b), classifica o ambiente eletromagnético como um sexto domínio operacional; diferentemente do Manual de Doutrina da OTAN para Guerra Eletrônica de 2020 (NATO, 2020), que considera os processos cognitivos como sexto domínio operacional, o informacional, e o ambiente eletromagnético como um sétimo domínio, tal como ilustrado na figura 1.

Figura 1 – Domínios cibernético, eletromagnético e informacional em relação aos domínios terrestre, marítimo, aéreo e espacial.



Fonte: NATO, 2020.

Independentemente de classificação, o ambiente operacional da guerra moderna tornou-se bastante complexo, heterogêneo, com diversos atores além das forças convencionais. E os múltiplos domínios operacionais tornaram-se interdependentes por meio do ambiente eletromagnético (BRASIL, 2023b).

Com a hiperconectividade, não há mais como se falar em teatros de operações delimitados, nem períodos isolados de guerra ou de paz. Dentro do ciberespaço a insegurança é latente, já que as vulnerabilidades dos ativos de informação estão, ininterruptamente, sendo exploradas por ciberameaças. As atividades ilícitas transnacionais (crime organizado, narcotráfico, corrupção...) também atuam no ciberespaço e contribuem para “[...] dificultar a diferenciação entre a paz e a guerra, o legal e o ilegal, o público e o privado.” (MARCIAL, 2023).

As ciberameaças estão se tornando cada vez mais elaboradas, difíceis de identificar e atingindo a todos os países (VAUGHAN-NICHOLS, 2023). Há 5 anos, um dos maiores especialistas em cibersegurança, Schneier (2020), já dizia que a magnitude do uso do ciberespaço vinha favorecendo as ciberameaças em muitas dimensões: ataques mais frequentes à disponibilidade dos serviços; algoritmos progressivamente autônomos e poderosos; cadeias de suprimento cada vez mais vulneráveis; e risco crescente às infraestruturas críticas em setores-chave.

Dentre os incidentes cibernéticos mais comuns, os de negação de serviço, ou do inglês *Denial-of-Service* (DoS); desfiguração de *sites* (*website defacement*) e *ransomware* foram os ressaltados pelo (UNITED STATES, 2023c). Mas outros artefatos maliciosos, atuando por vezes de forma combinada, nas diferentes camadas do ciberespaço, também têm contribuído para aumentar o caos, e sendo usados, inclusive, como ciberarmas, que são softwares, hardwares ou *firmwares* projetados ou aplicados para causar dano, por meio do ciberdomínio (BRASIL, 2021).

As vulnerabilidades do ciberespaço podem ser exploradas pelos mais diversos vetores de ataque, por meio, por exemplo, de: engenharia social; vazamento de informações confidenciais; infecções por *malwares* (sequestro de dados seguido de pedido de resgate); ameaças persistentes avançadas (APT); ataques de *phishing* (mensagens via e-mail, telefone ou texto fingindo serem de uma instituição legítima para convencer o alvo a entregar dados); e códigos maliciosos instalados em circuitos integrados (MEZIAT; SCHNEIER; 2013, 2020).

Ataques cibernéticos são ações, vindas de um oponente, sobre dispositivos, redes de computadores ou de comunicações, que geram, efeitos cinéticos e não-cinéticos, capazes de: destruir ou degradar equipamentos e sistemas; degradar a capacidade de operação; corromper dados de sistemas; negar o acesso a sistemas de interesse; e interromper o funcionamento de sistemas de interesse do oponente (BRASIL, 2023a). Oliveira de Sá *et al*. (2019) destacam, ainda, os ciberataques no domínio de atuação eletrônico ou da Guerra Eletrônica (GE), que envolvem Medidas de Ataque Eletrônico (MAE), visando prejudicar a obtenção de informações táticas.

O ataque DoS é um tipo de ciberataque que nega acesso a uma máquina, serviço ou recurso de rede, aos usuários legítimos, por meio do envio de uma quantidade exorbitante de requisições num período curto de tempo, para causar sobrecarga e saturação do sistema. Uma variante do ataque DoS é a sua versão distribuída, denominada *Distribuited Denial-of-Service* (DDoS), na qual são utilizadas múltiplas fontes diferentes que executam tarefas, sem o conhecimento nem o consentimento da vítima. Geralmente as fontes geradoras das requisições são computadores virtualmente infectados (chamados robôs ou *bots*). Ataques DDoS vêm sendo amplamente empregados para as mais diversas finalidades, inclusive para comprometer os sistemas de comunicações e outros serviços essenciais para a economia e para a sociedade, como serviços eletrônicos do governo, bancos, *sites* de jornais, entre outros (BRASIL, 2021).

Em maio de 2007, a Estônia sofreu o maior ataque DDoS da história, até então registrado, comprometendo diversos serviços naquele país, que há época se destacava pela quantidade de serviços digitais que dispunha. Esse evento durou semanas, a atribuição dele não ficou bem esclarecida (suspeita-se que os computadores que controlavam as *botnets* estavam na Rússia) e Tallinn, a capital da Estônia, tornou-se a sede do Centro de Excelência de Defesa Cibernética Cooperativa (cuja sigla em inglês é CCDCOE) da OTAN (OLIVEIRA *et al*., 2019).

Em fevereiro de 2020, um ataque à infraestrutura de comunicações do Irã, interrompeu a Internet de todo o país. Em janeiro de 2022, *hackers* desligaram o tráfego da Internet de e para a Coreia do Norte, duas vezes em duas semanas. Em março de 2022, os serviços de Internet providos pela Autoridade Nacional de Telecomunicações das Ilhas Marshall ficaram interrompidos por mais de uma semana. Em março de 2022, um importante provedor de telecomunicações israelense, tirou do ar vários *sites* do governo. Em fevereiro do presente ano, *hackers* pró-Rússia atacaram as redes de comunicações sensíveis da OTAN, interrompendo as comunicações entre a OTAN e os aviões que prestavam ajuda após um terremoto na Turquia. Nesta mesma ocasião, *sites* da OTAN ficaram fora do ar. Outros ataques DDoS se sucederam envolvendo atores estatais, espionagem e outros ciberataques que acarretaram prejuízos superiores a milhares de dólares (CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, 2020).

Nos últimos anos se intensificaram também os incidentes de *ransomwares*. Existe um mercado denominado *Ransomware-as-a-Service* (RaaS), no qual os desenvolvedores de *ransomware* o cedem a terceiros em troca de pagamento mensal ou parte dos lucros obtidos do ataque. Em 2021, esse mercado, passou a contar com serviços exclusivos para negociar o resgate de dados, assessorar as vítimas nos pagamentos e dar suporte via *chat* (FORTINET®, 2022). Ano passado, a Rede Record realizou uma série de modificações em sua programação de TV, possivelmente, devido a um ataque cibernético do *malware* BlackCat, um RaaS (CAMURÇA, 2022).

Em abril e maio de 2022, a Costa Rica sofreu dois ciberataques consecutivos de *ransomware* de grandes proporções comprometendo os sistemas: fiscal, aduaneiro, elétrico, de transporte, entre outros. O grupo *Conti* solicitou um resgate de US$ 20 milhões (que não foi pago), e o país entrou em estado de emergência em decorrência da paralisação de serviços governamentais críticos (BRITO, 2022).

Em setembro de 2023, ocorreu um dos maiores ciberataques sofridos pela Colômbia, deixando dois milhões de processos judiciais inacessíveis. Um *ransomware* foi usado para criptografar e roubar dados da empresa multinacional de telecomunicações IFX Networks, contratada pelo Poder Judiciário colombiano. Essa empresa também presta serviços a outros órgãos do governo e para 16 países da América Latina. Possivelmente, outras 700 empresas foram afetadas no Chile, Argentina e Panamá (ATAQUE, 2023).

Ciberameaças podem ser encontradas também em hardwares. Com a globalização da cadeia de fabricação de circuitos integrados (CIs ou *chips*), o aumento da complexidade na fabricação dos *chips* e a perda de controle sobre as etapas do processo produtivo, as ciberameças por meio dos hardwares foram ampliadas, sobretudo por conta da globalização (MALAGUTTI, 2022a). A ciberameaça conhecida como hardware Trojan consiste de códigos maliciosos instalados em CIs durante a fabricação, inseridos de forma dissimulada e de difícil detecção, com o objetivo de expor o hardware ou acessar dados ou softwares que estejam rodando nos sistemas que utilizam o CI (MEZIAT, 2013). Os c*hips* se encontram em uma infinidade de equipamentos (computadores, celulares, equipamentos de redes...) e o hardware Trojan pode ser utilizado para fins de: vazamento de dados, espionagem, ataques DoS, sabotagem, dentre outros. Dependendo do tipo, o hardware Trojan pode ser ativado por meio de um gatilho (*trigger*), conferindo ao atacante o poder de decisão sobre o momento mais oportuno para o ataque, podendo inclusive ocorrer em larga escala (BRUZZEGUEZ *et al.*; OLIVEIRA DE SÁ *et al.*, 2028, 2019).

Há também os ataques decorrentes de armas cibernéticas cinéticas (ou ciberarmas cinéticas), que são software, hardware e *firmware* projetados ou aplicados especificamente para causar “[...] danos físicos, direta ou indiretamente, tanto em pessoas como em equipamentos, somente por meio da exploração de vulnerabilidades dos sistemas e processos de informação” (BRASIL, 2021).

O Stuxnet foi o primeiro *worm* (ou verme) identificado, em 2010, que reprograma sistemas industriais, provavelmente desenvolvido pelos EUA e Israel. Esse *worm* foi projetado especificamente para atacar os Sistemas de Controle de Supervisão e Aquisição de Dados (SCADA), de um certo modelo da fabricante Siemens. Ele foi empregado como ciberarma cinética para danificar centrífugas da instalação em Natanz, no Irã. O Stuxnet reprogramou o SCADA para alterar a

velocidade das centrífugas da usina de enriquecimento nuclear iraniano até se danificarem, causando atraso ao programa nuclear iraniano (SCHNEIER, 2020).

Diferentemente do vírus, o *worm* (tipo complexo de *malware*) é um programa de computador capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de um computador a outro, e não necessita ser executado para se propagar. A propagação do *worm* se dá por meio da exploração de vulnerabilidades existentes ou de falhas na configuração de programas instalados em computadores (BRASIL, 2021). Foram ensaiados outros ciberataques com efeitos cinéticos de magnitude semelhante à causada pelo Stuxnets, mas sem sucesso. Até que em 2016, o código malicioso *Industroyer* ou *Crash Override* gerou um mau funcionamento de uma subestação elétrica ucraniana, ligando e desligando o fluxo de energia. A adaptabilidade desse *malware*, supostamente desenvolvido pelos russos, representa uma ameaça não apenas à infraestrutura crítica da Ucrânia, mas também às de outros países (SCHNEIER, 2020). E recentemente, em 2022, uma siderúrgica no Irã sofreu ações combinadas de ciberataques, possivelmente com a participação de Israel. O grupo *Predatory Sparrow* reivindicou a autoria do atentado, o qual incluiu um ciberataque com efeito cinético, que provocou incêndio às máquinas por meio de controle remoto, e ainda, a invasão do sistema de câmeras (para esperar funcionários deixarem o local), *ransomwar*e, entre outras ações (TIDY, 2022).

É importante destacar que um *malware* semelhante ao utilizado no ciberataque *Crash Override* foi encontrado nas redes de TIC da infraestrutura de energia elétrica na região sudeste do Brasil, conforme palestra do Prof Marcelo Antonio Osller Malagutti sobre o “Gerenciamento de vulnerabilidades diante das ameaças cibernéticas às infraestruturas críticas: proteção de ativos de informações”, ministrada no Curso Superior de Segurança e Defesa Cibernética (CSSDC), da ESG, em 17 de outubro de 2023.

Em 2022 o conflito Rússia-Ucrânia foi palco do uso combinado de ataques cinéticos com cibernéticos. Uma onda de ciberataques, com a finalidade de instaurar pânico impedindo que a população se comunicasse (SUZUKI, 2022), e um ciberataque ao serviço de banda larga por satélite (Ka-Sat) da empresa americana Viasat interrompeu os serviços de Internet em toda a Europa, incluindo as comunicações militares ucranianas (KA-SAT, 2023). As redes de telefonia celular e de Internet ucranianas foram ofensivamente destruídas e as comunicações no país só foram restabelecidas com o emprego emergencial de terminais de satélite Starlink da

empresa SpaceX. Ao utilizar os terminais Starlink para coordenar um ataque furtivo ucraniano com drones submarinos à frota naval russa, esta rede foi desabilitada pela empresa perto da costa da Criméia. Suspeita-se que o plano ucraniano foi revelado por meio de um código malicioso dos russos projetado para interceptar dados enviados aos satélites Starlink pelos comandantes ucranianos (LYNGAASDA, 2023).

2.2 O Brasil e o ciberespaço

No Brasil, diversas iniciativas governamentais promoveram o processo de digitalização do Governo Federal, tais como: a Política de Governança Digital de 2016; a Estratégia Brasileira para a Transformação Digital (E-Digital) de 2018; e a governança no compartilhamento de dados de 2019. Bilhões de pessoas acessam, por meio da Internet, recursos de TIC, e usufruem das oportunidades do ambiente digital nas esferas econômica e social. Ademais, o Brasil vem experimentando o fenômeno da 4ª revolução industrial, onde as tecnologias se conectam, o mundo físico e o ambiente virtual alcançam elevado grau de interação e os dispositivos de Internet das Coisas, proliferam em apoio aos processos produtivos (BRASIL, 2020).

Embora o Brasil tenha subido para 18ª posição (vindo da 70ª posição em 2018) no *ranking* global de países comprometidos com a agenda da segurança cibernética, e está em 3º lugar entre os países das Américas (UNITED NATIONS, 2020), a segurança da enorme superfície susceptível à ataque brasileira está aquém do que deveria ser. O Brasil está em um estágio muito primário em suas capacidades cibernéticas (MALAGUTTI, 2022b, p. 2-24).

Garcia *et al.* (2022) fizeram uma análise comparativa entre as capacidades cibernéticas brasileiras e espanholas, considerando critérios organizacionais e técnicos de avaliação. A Espanha foi selecionada para comparação por ter alcançado excelentes resultados no domínio cibernético empregando recursos que estariam ao alcance das possibilidades brasileiras. Além do mais, Espanha e Brasil se assemelham por serem as maiores economias de ambos os lados ibero-americanos do Atlântico; por possuirem objetivos geopolíticos comuns, como a estabilidade da América Latina e a supressão do crime organizado transnacional na Iberoamérica; e por fomentarem um ambiente de comércio digital saudável e seguro. Esse estudo mostrou que a Espanha tem uma capacidade cibernética nacional bastante superior à do Brasil, e que possui estratégias cibernéticas significativamente diferentes das

brasileiras. Portanto, o Brasil tem várias oportunidades de melhoria no sentido de robustecer suas capacidades.

Como pontuou o Vice-Almirante Kerr em sua aula magna, ministrada para o CSSDC 2023 da ESG, no contexto militar, enquanto os processos de tomadas de decisão forem centralizados e as instruções aos comandantes estiverem focadas em uma lista de tarefas a serem executadas, em vez de nos objetivos desejados, a dependência dos sistemas de comunicações será absoluta para apoiar o comandante na tomada de decisão e transmitir as ordens tempestivamente.

Como descrito no Manual de Operações de Convergência 2040 do Exército Brasileiro (BRASIL, 2023b), o contexto operacional que se visualiza é aquele no qual:

> 3.1.2.11 A crescente centralização em redes dos sistemas de comando e controle, comunicações e informações demandará o aporte tecnológico adequado para a sua gerência, tanto no que se refere ao seu funcionamento quanto à sua proteção. Ataques cibernéticos direcionados a infraestruturas críticas têm se tornado recorrentes, intensos e complexos, colocando em risco o funcionamento de segmentos funcionais vitais dos países afetados.

Nesse cenário, considerando a preocupação com a integridade das infraestruturas críticas, é fundamental eliminar ou reduzir as fraquezas das mesmas e torná-las mais resilientes (PEYCHEV, 2022). O Plano Nacional de Segurança de Infraestruturas Críticas (BRASIL, 2022a), como um dos instrumentos da Política Nacional de Infraestrutura Crítica (PNSIC), classifica as telecomunicações e a radiodifusão do país como setores prioritários, e todas as hipóteses de falhas dessa área devem ser consideradas.

Há 3 anos, 80 % dos municípios do estado do Amapá ficaram 22 dias consecutivos sem energia elétrica, dos quais os quatro primeiros em escuridão total e nos demais em sistema de rodízio, em plena pandemia da COVID-19. Esse problema no fornecimento de energia elétrica, decorrente da explosão de um transformador, não parece ter sido resultante de uma sabotagem, nem de ter sido gerado por um ciberataque. Entretanto, os eventos em cascata nas demais infraestruturas críticas (água, sistema financeiro, combustível...) que se sucederam trouxeram enormes transtornos à sociedade, tendo sido as comunicações a primeira infraestrutura crítica a ser impactada (FERNANDES, 2023).

O risco de ciberataques a infraestruturas críticas nacionais, como o setor de comunicações e de energia, vem aumentando, não apenas no sentido de paralisar os serviços, mas de também gerar danos à infraestrutura (SYMANTEC, 2021). Esses

dois setores possuem uma forte interdependência de serviços e infraestrutura. Uma indisponibilidade na infraestrutura de comunicações da Serra do Mendanha ou do Sumaré, apresentada por Ivo (2010), por exemplo, comprometeria severa e imediatamente as transmissões das emissoras de televisão e rádio no Rio de Janeiro.

2.3 O renascimento das comunicações via rádio em HF no mundo digital

As comunicações via rádio em HF (sigla em inglês de *high frequency*), também denominadas ondas curtas (do inglês *short waves*), operam na faixa de frequência estendida de 2 MHz a 30 MHz para serviços de rádio no meio civil e militar (ITU, 2019). A propagação de ondas HF pela ionosfera é um método de comunicação razoavelmente simples e eficaz para distâncias superiores a 160 quilômetros (que é o alcance máximo do rádio de linha de visada direta de outras faixas de frequência, como VHF e UHF), e com alcance global.

Diferentemente dos outros sistemas, as comunicações em HF requerem infraestrutura mínima, e necessitam apenas de componentes da interface/receptor, antena e fonte de alimentação (THOMPSON, 2002). Elas foram amplamente utilizadas na Segunda Guerra Mundial e na década de 1970, onde a comunicação por cabo era inviável (como em aeronaves, embarcações e outras unidades móveis, estações terrestres temporárias ou remotas) (KALLBERG; HAMILTON, 2020, p. 47).

Desde então, avanços tecnológicos nas comunicações em outras faixas de frequência do espectro eletromagnético viabilizaram uma capacidade de transmissão muito superior à do rádio. As comunicações em HF passaram a ser consideradas uma tecnologia obsoleta, frente a todas as possibilidades que as tecnologias de transmissão em banda larga trouxeram na “Era da Informação” (1950-2010). O mundo moderno tornou-se dependente dos computadores e das redes existentes para também viabilizar o comando e controle das diversas operações (SCHNEIER; UPPAL, 2020, 2021). Por meio do comando e controle e do seu ciclo, se faz a coordenação entre a emissão de ordens e diretrizes (BRASIL, 2015).

Com a hiperconectividade, os cenários operacionais passaram a ser centrados em rede (KOCH; GOLLING, 2015), e a dispor de precisão e agilidade sem precedentes nos sistemas de comunicações, pontaria, navegação no terreno, e observação do teatro de operações (LYNN, 2011). Além disso, essas facilidades

tornaram os exércitos totalmente dependentes das comunicações para capacidades aéreas, recursos médicos e cadeia logística (KALLBERG; HAMILTON, 2020).

Porém, essa vantagem militar pode desaparecer com a popularização do ciberespaço. Lynn (2011) visualiza que quando todos os países tiverem acesso a sistemas satelitais e puderem contar com banda larga praticamente infinita e ininterrupta, o diferencial e a importância atribuída a eles serão perdidas. Kallberg e Hamilton (2020, p. 48) preveem uma mudança cultural rumo a um uso mais comedido das comunicações, transmitindo-se o que de fato for essencial para a missão, tal como no passado. Esper *et al.* (2019) consideram, ainda, a hipótese de que muitas das facilidades com as quais os combatentes convivem atualmente estarão disponíveis no futuro, na melhor das hipóteses, apenas de forma intermitente.

Segundo Kallberg e Hamilton (2020), a “Era do vício pela transmissão” estaria com os dias contados, devido às diversas ameaças às quais os satélites estão expostos, particularmente no teatro de operações, tais como: interferência eletromagnética agressiva (UPPAL, 2021); colisões com lixo espacial (*debris*) (UPPAL, 2021); ataques balísticos a satélites (WHITE, 2020) e ciberataques. Em 2022, um ciberataque russo contra satélites comerciais ucranianos interrompeu e danificou permanentemente alguns terminais (THOMPSON, 2022).

Ademais, em situações críticas de grandes eventos ou calamidades, como os casos de ataque de 11 de setembro de 2001 nos EUA, do Tsunami na Ásia em 2004, e o terremoto no Haiti em 2010, o tráfego das comunicações banda larga costuma entrar em colapso por saturação da demanda, restando disponível apenas as redes rádio HF (CARDOSO; BRATHWAITE, 2018, 2011).

Na atual Guerra Rússia-Ucrânia, após 14 anos de interrupção do serviço de ondas curtas, a empresa britânica BBC precisou retomar as operações em 2022 para levar informação à população ucraniana (CASTILHO, 2022). Nesse mesmo diapasão, a Rádio Vaticano intensificou as transmissões de ondas curtas na região.

Calamidades públicas podem ocorrer em qualquer localidade do Brasil, sendo as mais recorrentes os deslizamentos de terra e as inundações. Valorizando o grande potencial dos operadores de telecomunicações em HF (CARDOSO, 2018) e seguindo o exemplo de outros países que fazem uso desse serviço (VEIGA JUNIOR, 2014), foi criada em 2001, pelo então Ministério da Integração Nacional, a Rede Nacional de Emergência de Radioamadores (RENER). Desde 2012, conforme o parágrafo X do art. 8º da Política Nacional de Proteção e Defesa Civil (PNPDEC), a mobilização e a

capacitação dos radioamadores para atuação na ocorrência de desastre competem aos Municípios (BRASIL, 2001, 2012).

A RENER, coordenada pela Liga de Amadores Brasileiros de Rádio Emissão (LABRE), é formada por radioamadores voluntários portadores do Certificado de Operador de Estação de Radioamador (C.O.E.R.), expedido pela Agência Nacional de Telecomunicações (ANATEL), e estações de rádio detentoras de Licença de Radioamadores, expedida também pela ANATEL (BRASIL, 2001). A rede foi acionada e empregada com sucesso durante os desastres: em Santa Catarina, em 2008; em São Luiz do Paraitinga e Cunha, São Paulo, em 2010; e na região serrana do estado do Rio de Janeiro, em 2011 (VEIGA JUNIOR, 2014).

Expressões como “O renascimento das ondas curtas no mundo digital” anunciam o retorno das HF, e não apenas nas comunicações globais, mas também nas locais (WHITE; WANG *et al.*, 2020, 2022). As comunicações em HF são ideais para suportar a cobertura de uma rede local, particularmente por meio da propagação de ondas de superfície em HF, oferecendo vantagens sobre as comunicações via satélite em áreas montanhosas ou latitudes mais ao norte, onde não é possível nenhuma linha de visada para satélites existentes (UPPAL; WILLIAM, 2021, 2023).

Uppal (2021) observa, ainda, que este renascimento do HF vem sendo acompanhado de aprimoramentos tecnológicos, incluindo *design* de antenas, esquemas de modulação digital e melhor compreensão da propagação na ionosfera. Os equipamentos atuais de HF são menores, mais leves e consomem menos energia, além de serem capazes de transmitir dados que requerem banda larga (imagens, mapas e outros arquivos), e contam com GPS, algoritmos de criptografia aprimorados e interoperabilidade com conjuntos legados de HF (THOMPSON, 2022).

Em 2016, pesquisadores europeus demonstraram, por meio do projeto intitulado SWING, um acrônimo em inglês para *Short Wave Critical Infrastructure Network based on a new Generation high survival radio communication system*, a viabilidade do uso de HF como contingência. Em caso de falha total das comunicações de banda larga e da Internet por longos períodos, as informações fundamentais para a gestão e controle das Infraestruturas Crítica Europeias, na região do Mediterrâneo poderiam ser mantidas com uma rede HF de *backup* (mesmo em caso de perturbações ionosféricas moderadas), mantendo um fluxo mínimo de informação essencial para a gestão e controle das mesmas (ZOLESI *et al.*, 2016).

Os comandos de operações especiais em toda a Europa estão aumentando as suas capacidades em comunicações de alta frequência para garantir a conectividade no campo de batalha, em função da baixa probabilidade de intercepção e detecção do sinal de HF (UPPAL, 2021).

Dois anos após o reconhecimento pela OTAN do domínio cibernético como sendo o quinto “domínio operacional”, foi criada, nos EUA, a Agência de Segurança Cibernética e de Infraestrutura, do inglês *Cybersecurity and Infrastructre Security Agency* (CISA), visando reduzir os riscos, de forma integrada e em âmbito nacional, para a infraestrutura digital e física. A CISA possui uma divisão dedicada exclusivamente às Comunicações de Emergência, além de considerar o Setor de Comunicações como um dos setores de Infraestrutura Crítica da Divisão de Segurança da Infraestrutura (UNITED STATES, 2023a).

Os norte-americanos contam com um meio de comunicação adicional e seguro de emergências na faixa de HF, para o caso de indisponibilidade das comunicações fixas ou celulares. Como agente de defesa cibernética e, coordenadora nacional para segurança de infraestrutura crítica, a CISA “lidera o esforço nacional para compreender, gerenciar e reduzir o risco para a infraestrutura digital e física da qual os americanos dependem [...]” (UNITED STATES, 2023b).

Os EUA dispõem do programa de rádio HF, intitulado SHAred RESources (SHARES), que em português significa “recursos compartilhados”. Esse programa visa fornecer aos norte-americanos um meio de comunicação adicional e seguro para o caso de emergências, quando as comunicações fixas e celulares não estiverem disponíveis. Os membros do SHARES utilizam os recursos de rádio HF para coordenar e transmitir mensagens necessárias ao desempenho de funções críticas, incluindo as áreas relacionadas com segurança, manutenção da lei e ordem, finanças e saúde pública. O Programa de Rádio HF SHARES dos EUA conta com mais de 3.290 estações de rádio HF, representando mais de 590 organizações federais, estaduais e industriais localizadas em todos os 50 estados, no Distrito de Columbia e em vários locais no exterior. Quase 500 equipes de planejamento e resposta a emergências participam do SHARES (UNITED STATES, 2023b).

2.4 O Sistema Estratégico de Comunicações do EB e a rede rádio HF

O Exército Brasileiro (EB) possui uma Rede Rádio Fixa (RRF) como parte integrante do Sistema Estratégico de Comunicações (SEC), que opera na faixa de HF.

A RRF está distribuída ao longo de todo o território nacional através de estações rádio, que permitem a transmissão de dados, voz (fonia), integração radiotelefonia e telegrafia, e deve funcionar como contingência para as comunicações do Exército (BRASIL, 2022b).

A RRF engloba uma base física e uma concepção flexível, subdividindo-se em Rede Rádio Fixa Principal (RRFP) e Rede Rádio Fixa Secundária (RRFS). Essa rede deve conferir, em qualquer situação, como estabelece o Manual Técnico de Telegrafia do EB (BRASIL, 2022b): “[...] rapidez, uniformidade, simplicidade e segurança [...]”; e a resiliência necessária em caso de uma eventual indisponibilidade dos demais meios de comunicação empregados no Sistema de Comunicações do Exército (SICOMEx).

A origem da RRF remonta a criação do Serviço Radiotelegráfico durante a Primeira Guerra Mundial, quando o Exército Brasileiro, acompanhando as evoluções dos demais exércitos, tenta estabelecer comunicação entre os vários escalões e o comando. Há época, o emprego do rádio tornou-se um elemento coesivo imprescindível nos campos de batalha (BRASIL, 2022b). O Serviço Rádio do Ministério Exército (SRMEx) foi criado há 108 anos, por meio do Aviso Ministerial Nº 1.243, de 23 de agosto de 1915, do então Ministério da Guerra. Por várias décadas, o Serviço Rádio foi o responsável pela transmissão de mensagens, por meio de radiogramas, entre todas as Organizações Militares (OM) do Exército, sendo a radiotelegrafia o principal meio de comunicações da Força, por onde eram enviadas todas as informações relativas à rotina administrativa das OM e dos militares em geral (dados sobre movimentações, promoções...). Na década de 90, o SEC evoluiu implantando da Rede Integrada de Telecomunicações do Exército (RITEx), visando “estabelecer comunicações telefônicas privativas, com maior segurança e praticidade, no âmbito do Exército, pavimentando assim o caminho para novas tecnologias da informação” (MOYA, 2015), dando origem à EBNet. Desde então, a Rede Rádio Fixa deixou de ser a protagonista das comunicações do Exército, passando a ser uma rede auxiliar de contingência das comunicações.

A Rede Rádio Fixa (RRF) atualmente utiliza meios de TIC, mas está previsto que em situação de contingência nas comunicações o seu funcionamento dar-se-á de forma independente de redes de computadores (locais ou externas à OM), de outros meios físicos (linhas telefônicas, fibra óptica etc.), ou de serviços terceirizados (BRASIL, 2022b). Toda a infraestrutura da RRF é instalada, manutenida e gerenciada

por profissionais do EB, conforme explica Brathwaite (2011), em seu artigo, e de acordo com entrevista realizada com o Cap R/1 Ocimar de Castilho Ribas, Assessor da RRF do SEC no 7º CTA, em 10 de setembro de 2023.

O SICOMEx é responsável pela difusão oportuna e segura da informação, ligando os escalões de comando em todos os níveis, e integrando-os ao Sistema Nacional de Telecomunicações. A base física e lógica do SICOMEx é composta pelos: SEC; Sistema Tático de Comunicações (SISTAC); e Sistema de Comunicações Críticas (BRASIL; BRATHWAITE, 2022b, 2011).

O SEC, por sua vez, é o conjunto de meios de comunicações utilizados pelo Exército “desde o tempo de paz” e está distribuído por área. Esse sistema se destina, como preconizado em manual (BRASIL, 2022b), a “assegurar as ligações necessárias ao Alto Comando do Exército, aos grandes comandos, às guarnições militares em suas sedes ou a qualquer escalão estacionado no exterior”, estabelecendo conexões de longa distância, em todo o território nacional.

A principal finalidade do SEC é permitir o funcionamento dos sistemas corporativos (sistemas automatizados do EB, de informações gerenciais e apoio à decisão) que sustentam a vida vegetativa da Força (sistemas de pessoal, de material, logístico...), atendendo às necessidades correntes e estratégicas do Exército (CAMILO *et al.*, 2020). Cabe ao SEC, também, prover pontos de acesso ao Sistema Táctico de Comunicações (SISTAC) dentro do SICOMEx. O SEC se utiliza da Rede Corporativa Privativa do Exército (EBNet) e da Rede Rádio Fixa (RRF) (BRATHWAITE, 2011).

É por meio da EBNet, uma rede de dados com alta capacidade de transmissão que interliga todas as OM do EB, que flui o tráfego de dados do SEC. A EBNet fazia amplo uso da Internet e dos serviços das operadores de telecomunicações (CAMILO *et al.*, 2020). Contudo, a partir de 2019, iniciou-se um processo de transformação histórico na rede corporativa do Exército, no sentido de prover à Força uma rede privada, independente da Internet. Atualmente, a EBNet depende apenas da rede física das operadoras de telecomunicações, ficando a gestão dos grandes enlaces (*backbones*) nacionais e regionais sob a responsabilidade do Exército, de acordo com entrevista realizada com o Coronel do Quadro de Engenheiros Militares do EB Macson José Mendes de Almeida, do CITEx, em 11 de outubro de 2023.

O Sistema de Comunicações Críticas (Sis Com Ctc), também designado por SISNACC, conforme consta na END, a Estratégia Nacional de Defesa

(BRASIL, 2016a, p. 35), não opera na faixa de HF e tem por finalidade beneficiar a Administração Pública com uma rede de comunicações para fins de coordenação e controle nos campos da Defesa Nacional, da Proteção e da Defesa Civil, da Segurança Pública, da fiscalização e da repressão a ilícitos.

A rede que compõe esse sistema é estruturada, basicamente, por capacidades oriundas do meio civil (rádios e antenas) e é empregada em situações emergenciais (BRASIL, 2016a, p. 35).

3 CONSIDERAÇÕES FINAIS

Retomando a proposição do início do ensaio, que levantou a questão acerca da pertinência do emprego de uma rede rádio HF como contingência para a mitigação dos efeitos das ciberameaças nas Redes de Comunicação Estratégica do Exército Brasileiro, conclui-se que as ameaças dentro do espaço cibernético representam um risco às comunicações estratégicas da Força e se justifica o emprego da rede rádio em HF como uma última *ratio regis*.

A total dependência do mundo moderno dos sistemas de informação deixou a sociedade, como visto no referencial teórico, vulnerável ao ciberespaço. Ao mesmo tempo que essa dependência gera muitas oportunidades, traz consigo grandes riscos. A digitalização traz para os demais setores a velocidade da computação. Mas também todas as suas vulnerabilidades que ainda não foram resolvidas por aquele setor.

O ciberespaço é um espaço onde as informações digitais transitam, são processadas e armazenadas, e se materializa, conforme apresentado no item 2.1, por meio das diferentes camadas que o compõe: humana, identidade virtual, cognitiva, lógica, de infraestrutura de TIC e componente geográfica.

É no ciberespaço que a informação é criada, armazenada, transmitida, manipulada, e é nele que o poder cibernético converte a informação em efeito estratégico, por vezes, cinético. Nele situam-se as ciberameaças cujos impactos são fortemente potencializados pelas características peculiares inerentes a esse espaço.

Dentro do ciberespaço a insegurança é latente, e os efeitos dos eventos que nele ocorrem podem ser percebidos simultaneamente em qualquer parte do mundo. As ciberameaças estão cada vez mais complexas, difíceis de identificar, e são usadas em: crimes, espionagem, terrorismo cibernéticos, entre outros; representando grande risco à sociedade e, particularmente às infraestruturas críticas, destacando-se as de comunicação e energia.

As ciberarmas podem não apenas causar danos a um elemento do ciberespaço, mas também gerar consequências físicas e caos. As ciberarmas cinéticas, por sua vez, são projetadas com o fito de gerar danos físicos.

No âmbito operacional, a capacidade de moldar o ciberespaço vem conferindo superioridade de poder de fogo e de manobra em relação aos efeitos produzidos nos demais domínios operacionais, com a grande vantagem adicional de demandar baixíssimos recursos financeiros. Embora a evolução tecnológica tenha permitido melhorar a precisão das pontarias aos alvos e mitigar efeitos colaterais, o uso combinado de ataques cinéticos com ciberamas, cinéticas ou não, elevou a criticidade dos estragos a patamares nunca antes vistos.

A superfície susceptível à ciberataque brasileira cresceu de forma surpreendente a partir de 2020, assim como a quantidade de ciberataques. Porém, a segurança cibernética desta superfície não vem crescendo na mesma taxa que deveria. Como exposto no item 2.2, a capacidade cibernética nacional brasileira ainda está em um estágio inicial. Várias oportunidades de melhorias, no sentido de robustecer essa capacidade, foram identificadas por Garcia *et al.* (2022), ao comparar com o cenário espanhol.

Ciberataques direcionados a infraestruturas críticas têm se tornado, não apenas frequentes, mas também intensos e complexos, e visam tanto paralisar os serviços quanto causar danos à infraestrutura, colocando em risco o funcionamento de segmentos funcionais vitais dos países.

Ainda no item 2.1 desse ensaio, diversas formas de ameaças ao setor de comunicações oriundas do ciberespaço foram elencadas e, como visto, o comprometimento desse setor pode se dar de forma direta ou indiretamente, atingindo o funcionamento do setor de energia elétrica, um segmento funcional vital. Ciberataques, como os Stuxnet e hardware Trojan, podem impactar os diferentes níveis de automação dos sistemas de comunicações e de infraestruturas críticas.

Além do Brasil ser um dos alvos mais visados para crimes cibernéticos, o possível ataque RaaS à rede Record, a existência de um *malware* semelhante ao utilizado no ciberataque *Crash Override* nas redes de TIC da infraestrutura de energia elétrica na região sudeste do Brasil, dentre outros incidentes cibernéticos, corroboram com a necessidade de se ter uma rede de contingência.

Em 2020, o estado do Amapá sofreu sério impacto social, ambiental, econômico e político decorrente do apagão de energia elétrica. Episódios como esses

poderão ocorrer no futuro fruto de ciberataques. Para mitigar os impactos decorrentes da indisponibilidade de infraestruturas críticas, como a de energia e comunicações, é fundamental poder contar com uma rede de contingência moderna.

Ademais, em pleno século XXI, reaparece o interesse pelas comunicações em HF como uma alternativa de *backup* em missões críticas, quando as comunicações por satélite, cabo ópticos ou a Internet não estiverem disponíveis.

Como visto no item 2.3, as redes rádio em HF permitem as comunicações de longa distância sem necessidade de retransmissão; apresentam a vantagem de alta mobilidade, viabilizando uma rede de forma flexível, expansível e com ótima capilaridade; permitem a comunicação autônoma; são mais robustas à destruição ou interferência do que outros métodos e faixas de frequência de comunicação.

O renascimento da comunicação em HF vem acompanhado de uma gama de melhorias tecnológicas. Pequenos, leves, com grande autonomia, os rádios em HF modernos permitem transmitir não apenas voz, mas também imagens, mapas, outros arquivos de dados, incluindo os de GPS, algoritmos de criptografia aprimorados, entre outras funcionalidades (WILLIAM, 2023). Técnicas avançadas, como, salto em frequência e seleção automática da frequência em função das condições da camada ionosférica por onde se propagam as ondas de HF melhoraram significativamente o desempenho das comunicações em HF (KHAWAJA; WANG, 2022).

Países como Reino Unido, EUA e a Europa estão investindo em suas capacidades em comunicações em HF. A BBC reativou as transmissões em ondas curtas na Ucrânia. Não obstante o amplo emprego das comunicações em HF nas operações militares, os EUA dispõem do programa SHAred RESources (SHARES). Pesquisadores europeus desenvolveram o projeto *Short Wave critical Infrastructure Network based on a new Generation high survival radio communication system* (SWING) e os comandos de operações especiais em toda a Europa estão aumentando as capacidades de comunicações em HF.

O Exército Brasileiro conta com uma Rede Rádio Fixa própria, integrante do Sistema de Comunicações Estratégicas (SEC) do Exército, empregada rotineiramente para envio de radiogramas, e que é uma alternativa de comunicação em caso de contingências. Como tratado no item 2.4, a RRF permite a troca de mensagens de forma eficiente, confiável, de baixo custo e própria das Forças Armadas.

Um passo muito importante foi dado no sentido de tornar a EBNet mais resiliente, frente às ciberameaças na Internet, ao torná-la uma rede privada. Sendo

privada, a disponibilidade, a integridade, a autenticidade e a confidencialidade dos dados (BRASIL, 2020) que trafegam pela rede de comunicações estratégicas do EB passam a ser muito superiores às da Internet. Contudo, há, ainda, pontos de vulnerabilidades no ciberespaço que podem ser explorados. Nas camadas lógica e de infraestrutura de TIC, por exemplo: os ativos de rede são importados; há o envolvimento de diversos prestadores de serviços nos mais variados níveis de manutenção; e a infraestrutura dos enlaces físicos não está sob o controle da Força, e depende da Internet. Outrossim, existem as vulnerabilidades das outras camadas (humana, ciberhumana, cognitiva e componente geográfica) do ciberespaço.

Para que a RRF do EB possa efetivamente cumprir a missão de prover a comunicação de contingência, foram observadas algumas oportunidades de melhoria, que se encontram no Apêndice do presente ensaio, de modo a torná-la mais efetiva, eficaz e resiliente, considerando o contexto das ameaças do ciberespaço. Dentre elas destaca-se, a importância de se fomentar o desenvolvimento do Rádio Transceptor Multibanda TRC-1222, em fase de conclusão pela Indústria de Material Bélico do Brasil (IMBEL, 2019, p. 36). Esse rádio digital também opera na faixa de HF e possui especificações técnicas que atendem a todos os requisitos mencionados e, possivelmente no final de 2024, estará disponível para encomendas. Contará com hardware, software, forma de onda, e criptografias todos proprietários. Esse produto foi projetado seguindo padrões internacionais de cibersegurança e já foram testados em campo com sucesso, no estágio de desenvolvimento em que se encontram, pelo Comando de Comunicações e Guerra Eletrônica (CComGEx), em setembro de 2022.

O Brasil possui, ainda, capacidade de fabricação das antenas log periódicas empregadas pela RRF através de empresas nacionais parceiras da IMBEL. A aquisição de rádios e antenas nacionais para a RRF, o SISTAC, a SECAF e, ainda, para o Sistema de Comunicações Críticas, além de conferir maior segurança cibernética e eletrônica (no contexto da Guerra Eletrônica) ao Sistema de Comunicações do Exército, fomentará a Base Industrial de Defesa (BID), aspecto extremamente relevante, como explica Brathwaite (2011).

Como sugestão para futuros trabalhos poder-se-ia considerar o acionamento da RENER não apenas em apoio à Defesa Civil por ocasião de deslizamentos de terra, inundações e outras calamidades públicas, mas também nos casos de ciberataques que suprimissem os serviços de telecomunicações tradicionais. Poderia, então, ser avaliado o grau de efetividade do emprego da RENER como uma rede de

contingência para mitigar os efeitos das ciberameaças, aprimorando o Sistema Nacional de Mobilização (SINAMOB), conforme previsto na Ação Estratégia de Defesa 3 (AED-3), da END (BRASIL, 2016a). A AED-3 é citada em duas Estratégias de Defesa, a ED-1 e a ED-6, que buscam, respectivamente, o fortalecimento do Poder Nacional e o desenvolvimento da capacidade de mobilização nacional. Como Duarte Frota (2020) alerta, dos ministérios integrantes do SINAMOB, apenas o Ministério da Defesa alicerçou a Doutrina de Mobilização Militar em 2015, estando carentes as diversas outras doutrinas, dentre elas a de Mobilização de Defesa Civil, sob a direção do atual Ministério da Integração e do Desenvolvimento Regional.

Outra questão que poderia ser considerada, só que no nível tático-operacional e com foco no SICOMEx, seria identificar o nível de vulnerabilidade da EBNet a ciberataques nos pontos de acesso do SISTAC, e do Sistema Crítico de Comunicações, ao SEC, sugerindo ações que robustecessem a cibersegurança de tais pontos.

Para garantir o cumprimento de uma missão deve-se sempre lembrar do acrônimo P.A.C.E., que remete à necessidade de se ter, além do plano Principal, o Alternativo, o de Contingência, e, se tudo falhar, o de Emergência (KALLBERG; HAMILTON, 2020). Nesse cenário, medidas de segurança em prol da resiliência do ciberespaço, são fundamentais, e, como, uma última *ratio regis*, o emprego da RRF.

Finalmente, conclui-se que o emprego da Rede Rádio Fixa (RRF) do Exército Brasileiro pode mitigar os efeitos das ciberameaças atuando como uma rede de contingência em prol das Comunicações Estratégicas da Força.

REFERÊNCIAS

ATAQUE à Colômbia mostra fragilidade da AL em cibersegurança, alerta especialista. **Revista Digital**, 15 set. 2023. Disponível em https://inforchannel.com.br/2023/09/15/ataque-a-colombia-mostra-fragilidade-da-al-em-ciberseguranca-alerta-especialista/. Acesso em: 9 out. 2023.

BRASIL. Decreto nº 10.222, de 05 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética (e-Ciber). **Diário Oficial da União:** seção 1, Brasília, DF, 06 fev. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 27 set. 2023.

BRASIL. Decreto nº 11.200, de 15 de setembro de 2022. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. **Diário Oficial da União:** seção 1, Brasília, DF, 16 set. 2022a. Disponível em: https://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2022/Decreto...1 of 22 27/09/2023. Acesso em: 27 set. 2023.

BRASIL. Exército. Comando de Operações Terrestre. **Manual Técnico de Exploração em Radiotelegrafia e Telegrafia - EB70-MT-10.409**. Brasília, EB, 2022b.

BRASIL. Exército. **Manual de Fundamentos Conceito Operacional do Exército Brasileiro – Operações de Convergência 2040 - EB20-MF-07.101**. Brasília, DF: EB, 2023b.

BRASIL. **Lei nº 12.608, de 10 de abril de 2012**. Institui a Política Nacional de Proteção e Defesa Civil - PNPDEC, dispõe sobre o Sistema Nacional de Proteção e Defesa Civil - SINPDEC e o Conselho Nacional de Proteção e Defesa Civil - CONPDEC, autoriza a criação de sistema de informações e monitoramento de desastres e dá outras providências. 10 abr. 2012. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12608.htm. Acesso em: 28 out. 2023.

BRASIL. Ministério da Defesa. **Conceito de Operações do Sistema Militar de Comando e Controle - MD31-S-02 (CONOPS SISMC²)**. Brasília, DF: MD, 2016b.

BRASIL. Ministério da Defesa. **Doutrina para o Sistema Militar de Comando e Controle - MD31-M03**. 3 ed. Brasília, DF: MD, 2015.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, DF: MD, 2016a.

BRASIL. Ministério da Defesa. Portaria GM-MD nº 5.081, de 16 de outubro de 2023. Aprova o Manual de Doutrina Militar de Defesa Cibernética-MD 31-M-07. ed. 2. 2023a. **Diário Oficial da União:** seção 1, Brasília, DF, n. 203, 25 out. 2023 (em vigor em 1º de novembro de 2023).

BRASIL. Ministério da Integração Nacional. Portaria nº 302, de 24 de outubro de 2001. Cria a Rede Nacional de Emergência de Radioamadores (RENER). **Diário**

Oficial da União: seção 1, Brasília, DF, n. 206, p. 131, 26 out.2001. s.1.Disponível em: https://www.gov.br. Acesso em: 28 out. 2023.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria GSI/PR nº 93, de 18 de outubro de 2021. Aprova o Glossário de Segurança da Informação. **Diário Oficial da União:** seção 1, Brasília, DF, n. 197, p. 36. 19 out. 2021.

BRATHWAITE, F. A. do Amaral. A Estratégia Nacional de Defesa e a integração dos sistemas de comunicações do Exército Brasileiro. **A Defesa Nacional**, v. 96. p. 817, 2011. Disponível em: http://www.ebrevistas.eb.mil.br/ADN/article/view/6271 Acesso em: 7 set. 2023.

BRITO, Paulo. Ataque cibernético faz Costa Rica declarar emergência. **Ciso Advisor**, maio 2022. Disponível em: https://www.cisoadvisor.com.br/ataque-cibernetico-faz-costa-rica-declarar-emergencia/. Acesso em: 05 ou 2013.

BRUZZEGUEZ, G. A.; NEUMANN, C.; SOUZA, J. C. F. O Hardware comprometido: uma importante ameaça a ser considerada pela atividade de inteligência. **Revista Brasileira de Inteligência**, Brasília, DF, n. 13, p. 113, dez. 2018.

CAMILO, Marcelo J.; MOURA, David F. C.; SALLES, Ronaldo M. Redes de comunicações militares: desafios tecnológicos e propostas para atendimento dos requisitos operacionais do Exército Brasileiro. **Rev. Mil. Ciência Tec.**, Rio de Janeiro, v. 37, p. 5-25, 2020. Disponível em: http://rmct.ime.eb.br/arquivos/revistas/RMCT_web_3_tri_2020.pdf. Acesso em: 8 out.2023.

CAMURÇA, Francisco. Rede Record sofre ataque cibernético e tem programação afetada. **Welivesecurity by ESET,** 10 out. 2022. Disponível em: https://www.welivesecurity.com/br/2022/10/10/rede-record-sofre-ataque-cibernetico-e-tem-programacao-afetada/. Acesso em 28 out. 2023.

CASTILHO, Fernando. BBC de Londres usa na Ucrânia técnica que fez a Rádio Jornal ser "Pernambuco falando para o mundo". **UOL**, 07 mar. 2022. Disponível em: https://jc.ne10.uol.com.br/colunas/jc-negocios/2022/03/14956787-bbc-de-londres-usa-na-ucrania-tecnica-que-fez-a-radio-jornal-ser-pernambuco-falando-para-o-mundo.html. Acesso em: 28 out. 2023.

CARDOSO, Daniel Moura Felix. O Concurso Verde Amarelo e a Rede Nacional de Emergência de Radioamadores. **O Comunicante**, EsCom, v. 8, n. 2, 2018.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. Significant cyber incidentes since 2006. Washington, DC: CSIS, [2020?]. Disponível em: https://csis-website-prod.s3.amazonaws.com/s3fs-public/200626_Cyber_Events.pdf. Acesso em: 08 set. 2023.

ĎULÍK, M.; ĎULÍK, M. Cyber Security Challenges in Future Military Battlefield Information Networks. **Adv. Mil. Tech**. v. 14, n. 2, p. 263–277, 15 Dec. 2019.

EDMONSON, BG Robert L.; DOYLE, II BG David; SEAGREAVES, I LC Ryan; SCHERBURNEUILDING, M Matthew G. Tactical employment considerations of HF rádios in the cavalry squadron. **The Cyber Defense Review**, Spring. 2019. p. 25.

ESPER, Mark T.; MILLEY, Mark A.; DAILEY, Daniel A. Army Senior Leaders Send Lessons from D-Day. **NCO Journal**, 01 jun. 2019.

FERNANDES, Gláucia. Estado de calamidade no Amapá: uma crise sanitária e outra energética. Fundação Getúlio Vargas (FVG). 2023. Disponível em: https://portal.fgv.br/artigos/estado-calamidade-amapa-crise-sanitaria-e-outra-energetica. Acesso em: 06 out. 2023.

FORTINET®. Comunicados à imprensa. **Relatório da FortiGuard Labs**, São Paulo, 18 ago. 2022. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/brasil-e-o-segundo-pais-que-mais-sofre-ataques-ciberneticos-na-a. Acesso em: 19 out. 2023.

GANUZA, Néstor. Guia de Defesa Cibernética na América do Sul, Orientações para o delineamento, planejamento, implantação e desenvolvimento de uma ciberdefesa militar. **Junta Interamericana de Defesa (JID)**, 2020.

GARCIA, Marcelo; MENDONCA, Fabio; DE OLIVEIRA ALBUQUERQUE, Robson. Assessments on National Cyber Capability: A Brazilian Perspective in a Comparison with Spain. *In:* 2022 17TH IBERIAN CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGIES (CISTI), 2022, Madird. **Proceedings** [...]. Madrid: IEEE, Madrid, 2022. p. 1–6. Disponível em: https://ieeexplore.ieee.org/document/9866889/. Acesso em: 7 out. 2023.

IMBEL. **Catálogo de Produtos. 2019**. Rio de Janeiro: IMBEL, 2019. Disponível em: https://www.imbel.gov.br/phocadownload/produtos/catalogo-de-produtos-imbel-2018.pdf. Acesso em: 07 set. 2023.

ITU Recommendation. **Method for the prediction of the performance of HF circuits, Recommendation**, 2019. (ITU-R P.533-14). Disponível em: https://www.itu.int/rec/R-REC-P.533-14-201908-I/en. Acesso em: 27 set. 2023.

IVO, Leonardo. Pedra do Ponto poderia vir a ser um novo Sumaré um dia. **TVs do RJ**, 26 out. 2010. Disponível em: http://www.tvsdorj.com/2010/10/edra-do-ponto-poderia-vir-ser-um-novo.html. Acesso em: 14 out. 2023.

KALLBERG, Jan; HAMILTON, Stephen S. Resiliency by Retrograded Communication-the Revival of Shortwave as a Military Communication Channel. **IT Professional**, v. 22, n. 6, p. 46–51, 1 Nov. 2020.

KA-SAT Network cyber attack overview. **Viasat,** 30 Mar. 2022. Disponível em: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview. Acesso em: 26 out. 2023.

KHAWAJA, Saleem. Protecting emergency communication systems with HF and VHF radio solutions. **Airport Technology,** 2022.

KOCH, Robert; GOLLING, Mario. Blackout and now? Network Centric Warfare in an anti-access area-denial theatre. *In*: INTERNATIONAL CONFERENCE ON CYBER CONFLICT: ARCHITECTURES IN CYBERSPACE (CYCON), 7., 2015, Tallinn. **Proceedings** [...] Tallinn, Estonia: IEEE, 2015. p. 169–184. Disponível em: http://ieeexplore.ieee.org/document/7158476/. Acesso em: 8 set. 2023.

LYNGAASDA, Sean. Elon Musk cortou sinal de satélites para impedir ataque ucraniano à frota russa, diz biografia. **CNN Brasil,** 07 set. 2023. Disponível em https://www.cnnbrasil.com.br/internacional/elon-musk-cortou-sinal-de-satelites-para-impedir-ataque-ucraniano-a-frota-russa-diz-biografia/. Acesso em: 10 out. 2023.

LYNN, William J. A Military Strategy for the New Space Environment. **The Washington Quarterly**, v. 34, n. 3, p. 7–16, ago. 2011.

MALAGUTTI, Marcelo. Cyberspace, Logistics and National Security Threats, Not Necessarily in that Order. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 16, n. 57, p. 417-441, 2022a.

MALAGUTTI, Marcelo. **Software Power**: um olhar brasileiro. Brasília, DF: Instituto Vegetius, 2022b. ISBN 978-65-997420-1-9.

MARCIAL, Cristine e PIO, Marcello José. **MEGATENDÊNCIAS MUNDIAIS 2040:** contribuição para um debate de longo prazo para o Brasil. 2023. Brasília, DF: Universidade Católica de Brasília, 2023.

MELTWATER. Global Digital Report de 2023. **Relatório da Meltwater**. 2023. Disponível em: https://www.meltwater.com/en/global-digital-trends. Acesso em: 26 set. 2023.

MEZIAT, Natália Fernandes. **Hardware Trojan and Application Backdoor:** assessing security of embedded device. 2013. Dissertação (Mestrado em Cibersegurança) – Universidade de Lancaster, 2013.

MOYA, Sylvio. Os 100 anos do ´piri-pipi`. **Montedo**, 23 ago. 2015. Dsiponível em: Disponível em: https://www.montedo.com.br/2015/08/23/os-100-anos-do-piri-pipi/. Acesso em: 30 out. 2023.

NASCIMENTO ABREU, Antônio Luiz. **SISMC² A Importância da implementação do sistema de comunicações militares de alta frequência (HF) para a interoperabilidade e contingência após a criação do Ministério da Defesa**. 2021. 39 p. Monografia (Curso Superior para Oficiais) - Escola de Guerra Naval, Rio de Janeiro, 2021.

NATO. NATO Standardization Office (NSO). Allied Joint Doctrine for Electronic Warfare (AJP-3.6). 2020. **North Atlantic Treaty Organization Allied Joint Publication**. ed. C. v. 1. mar. 2020.

OLIVEIRA DE SÁ, Alan Oliveira de Sá; MACHADO, Raphael Carlos; ALMEIDA, Nival Nunes Almeida. O Encontro da Guerra Cibernética com as Guerras Eletrônica

e Cinética no âmbito do Poder Marítimo. **Revista da Escola de Guerra Naval**, Rio de Janeiro, v. 25, n. 1, p. 89-128. jan./abr. 2019.

PEYCHEV, Alexander. **What is the measured response to a cyber attack on critical infrastructures?** Methodological, operational and legalistic approach for small states. Relatório. [*S. l.*]: Institute for Security and International Studies, 2022.

SCHNEIER, Bruce, **Clique aqui para matar todo mundo**: como sobreviver em um mundo hiperconectado. [*S. l.*]: Atlas Books, 2020.

SUZUKI, Shin. A guerra cibernética paralela entre Rússia e Ucrânia. **BBC News Brasil**, São Paulo, 01 mar. 2022. Disponível em: https://www.bbc.com/portuguese/internacional-60551648. Acesso em: 26 out. 2023.

SYMANTEC. Threat Hunter TEAM. Attacks Against Critical Infrastructure. **Symantec A Division of Broadcom White Paper**. 2021. Disponível em: https://symantec.broadcom.com/hubfs/Attacks-Against-Critical_Infrastructure.pdf. Acesso em: 24 set. 2023.

TEIXEIRA JÚNIOR, Augusto Wagner Menezes; LOPES, Gills Vilar; FREITAS, Marco Túlio Delgobbo. As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica. **Carta Internacional**, v. 12, n. 3, p. 30, 30 dez. 2017.

TIDY, Joe. Os hackers misteriosos que dizem ter provocado incêndio em fábrica no Irã. **BBC News,** 12 July 2022. Disponível em: https://www.bbc.com/portuguese/internacional-62124923. Acesso em: 11 out. 2023.

THOMPSON, Nikki. Why HF radios are mission-critical: NATO standards for military comms. **Army Technology In Association with Isode,** 16 June 2022.

UNITED NATIONS. International Telecommunication Union Development Sector. Global Cybersecurity Index 2020 Measuring commitment to cybersecurity. **ITU Publications**. [New York]; UN, 2020.

UNITED STATES. Department of Homeland Security. **U.S. Department of Homeland Security.** [*S. l.*]: DHS, 2023a. Disponível em: https://www.cisa.gov/about/divisions-offices. Acesso em: 16 set. 2023.

UNITED STATES. Department of Homeland Security. **SHAred RESources (SHARES) High Frequency (HF) Radio Program**. [*S. l.*]: DHS, 2023b. Disponível em: https://www.cisa.gov/resources-tools/programs/shared-resources-shares-high-frequency-hf-radio-program. Acesso em: 17 set. 2023.

UNITED STATES. Department of Homeland Security. **Homeland Threat Assessment 2024**. [*S. l.*]: DHS, [2023c?].

UPPAL, Rajesh. Wideband High Frequency (HF) communications provide net-centric, high-speed beyond line of sight communications in Anti-Access/Area Denial (A2/AD) battlefield environments. **Comm. & NW, Soldier.** 2021.

VAUGHAN-NICHOLS, Steven. Google Cloud, AWS, and Cloudflare report largest DDoS attacks ever. **ZDNET Tech Today**. 10 out. 2023. Disponível em: https://www.zdnet.com/article/google-cloud-aws-and-cloudflare-report-largest-ddos-attacks-ever/. Acesso em: 15 out. 2023.

VEIGA JUNIOR, João Carlos Valentim. Rede Nacional de Emergência de Radioamadores: evolução, procedimentos e aspectos legais. **Revista Jus Navigandi**, Teresina, ano 19, n. 3965, 10 maio 2014. Disponível em: https://jus.com.br/artigos/28110. Acesso em: 28 out. 2023.

WANG, Jian; SHI, Yafi; YANG, Cheng; FENG, Feng. A review and prospects of operational frequency selecting techniques for HF radio communication. **Adv. Space Res.** v. 69, p. 2989–2999, 2022.

WILLIAM, Adam**.** Why high frequency radio remains crucial for military communications. **Army Technology; Isode**. 2023. Disponível em: https://www.army-technology.com/sponsored/why-high-frequency-radio-remains-crucial-military/. Acesso em: 3 set. 2023.

WHITE, Andrew. The militar renaissance in high frequency communications. 2020. AI & ML Unmanned Battlefield Tech Space Electronic Warfare. **Cyber Industry. C4ISR**, Sept. 2020.

ZOLESI, B.; BIANCHI, C.; MELONI, A.; BASKARADAS, J. A.; BELEHAKI, J. A.; ALTADILL, J. A. e DALLE MESE, E. “SWING”: A European project for a new application of an ionospheric network. **Radio Sci.** v. 51. p. 421–428. 2016.

APÊNDICE

OPORTUNIDADES DE MELHORIA PARA A REDE RÁDIO FIXA (RRF) DO EB

Para que a Rede Rede Fixa (RRF) do Exército Brasileiro possa efetivamente cumprir a missão de prover a comunicação de contingência diante de um ciberataque, foram observadas algumas oportunidades de melhoria, a fim de torná-la mais efetiva, eficaz e resiliente considerando o contexto das ameaças do ciberespaço.

A qualificação técnica dos recursos humanos é um aspecto extremamente importante e, no contexto do presente ensaio, possui duas vertentes: a capacitação na área segurança cibernética, com ênfase nas boas práticas, uso de rede local segregada, constante atualização dos softwares, entre outras, a fim de evitar que as ciberameças se materializem; e o treinamento nas técnicas e fundamentos da transmissão HF, contemplando o modo manual, seleção de antenas, montagem de uma rede rádio e escolha correta das frequências (durante o dia e a noite) (EDMONSON *et al.*, 2019).

A RRF carece de novas antenas de alto ganho (log periódicas) para substituir as antigas e poderia se considerar a instalação de antenas adicionais em novas regiões. Poder-se-ia pensar na possibilidade de adquirir antenas para que rede rádio operasse não apenas na configuração centralizada atual, mas, em caso de indisponibilidade do Posto Diretor da Rede em Brasília, funcionasse em estrela. Novas antenas poderiam ser encomendadas no Brasil a empresas parceiras da IMBEL, que possuem capacidade de fabricação comprovada, ao menos para substituir as obsoletas.

Para mitigar as ciberameaças advindas de hardwares, ações de curto, médio (1 a 2 anos) e longo prazos poderiam ser adotadas em relação aos rádios HF utilizados na RRF e às infraestruturas de TIC empregadas. Incrementar a capacidade brasileira no setor de fabricação de *chips* seria uma meta de longo prazo a perseguir. No médio prazo, caberia a conclusão do desenvolvimento de rádios nacionais (hardware e software). No curto prazo, poderia ser implementada uma metodologia, tal como a proposta por Oliveira de Sá *et al.* (2019), para que fosse efetuado um controle dos hardwares empregados na RRF por meio de homologação e certificação de produtos cibernéticos sensíveis produzidos em ambientes não controlados, por meio de testes e ensaios sistemáticos, aos moldes do que é feito nos EUA, Alemanha e França desde, respectivamente, 2011, 2015 e 2018.

Os rádios em uso na RRFP são antigos e estão limitando a capacidade de transmissão de toda a rede RRF, e os rádios das RRFS, embora mais modernos, são, assim como os da RRFP, de empresa estrangeira (Harris). A aquisição de Rádios

Transceptores Multibanda TRC-1222 da IMBEL, que operam em diferentes faixas de frequência, incluindo HF, poderá conferir um excepcional grau de confiabilidade, segurança, disponibilidade, integridade, autenticidade e confidencialidade à RRF. Embora esse rádio digital tenha sido projetado para ser compatível com diversos modelos e tecnologias, viabilizando a interoperabilidade entre os rádios da RRFP, da RRFS e do SISTAC, todos eles poderiam ser substituídos por rádios com tecnologia nacional, se beneficiando de todas as vantagens que a produção de rádios nacionais agrega.

A aquisição desse rádio nacional poderia, ainda, ser o caminho para superar as questões de incompatibilidades técnicas advindas de uma integração das redes em HF das três Forças Armadas. Conforme observado por Nascimento Abreu (2021), cada uma dessas redes fora inicialmente projetada para atender a requisitos inerentes às especificidades de cada Força. Sendo assim, dificuldades são encontradas para viabilizar o Sistema Estratégico de Comunicações em Alta Frequência (SECAF), citado no Manual do Ministério da Defesa (BRASIL, 2016b), que tem como finalidade integrar, por meio das redes em HF, o Ministério da Defesa e as três Forças, e que pode, ainda, contar com a capilaridade geográfica das redes das Forças Singulares.

O projeto desse rádio considerou o uso por tropas do Exército, Marinha, Aeronáutica e Forças Policiais, proporcionando a troca segura de dados e de voz entre os elementos da rede de comunicação. Sendo assim, é adequado ao SECAF, além de permitir a integração do SISTAC com o SEC de forma segura.

Os artefatos maliciosos estão ficam cada vez mais especializados e tendo como alvo determinadas arquiteturas, como foi o caso do Stuxnet. Tecnologia semelhante pode ser desenvolvida para atuar em sistemas de controle de usinas de energia elétrica, ou, ainda, interferir em dispositivos eletrônicos específicos, como por exemplo, nos rádios definidos por softwares estrangeiros.

O presente apêndice não teve por finalidade esgotar o tema relativo a melhorias técnicas nos rádios HF em termos de desempenho, muito bem documentadas em outros trabalhos (CAMILO *et al.*, 2007, 2020). As sugestões aqui elencadas, buscaram apenas identificar eventuais fraquezas da RRF frente às ameaças do ciberespaço. Apesar de sempre haver novas oportunidades de aperfeiçoamentos, a RRF tem condições de assegurar a coordenação das ações de Comando e Controle em todos os níveis das ações (estratégico, operacional e tático) em tempo oportuno, em situações críticas e emergenciais nas quais as demais alternativas tenham falhado.