MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE ALEXANDRINO

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
GUERRA ELETRÔNICA

TRABALHO DE CONCLUSÃO DE CURSO

A CONVERGÊNCIA ENTRE A GUERRA ELETRÔNICA E A GUERRA CIBERNÉTICA:
O impacto para a estratégia militar e suas implicações para a segurança nacional

1ºTEN PHELIPE DE ALBUQUERQUE BARBOSA

Rio de Janeiro
2023

1ºTEN PHELIPE DE ALBUQUERQUE BARBOSA

A CONVERGÊNCIA ENTRE A GUERRA ELETRÔNICA E A GUERRA CIBERNÉTICA:
O impacto para a estratégia militar e suas implicações para a segurança nacional

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Guerra Eletrônica

Orientadores:
CC (T) Eclenice Antunes Guarany Dantas
Prof.ª Msc Beatriz Alencar Ribeiro

CIAA
Rio de Janeiro
2023

1°TEN PHELIPE DE ALBUQUERQUE BARBOSA

A CONVERGÊNCIA ENTRE A GUERRA ELETRÔNICA E A GUERRA CIBERNÉTICA:
O impacto para a estratégia militar e suas implicações para a segurança nacional

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Guerra Eletrônica.

Aprovada em 23/11/2023

Banca Examinadora:

Alessandro Roberto dos Santos, CF Dsc – CIAA _____

Eclenice Antunes Guarany Dantas, CC (T) Msc – CGAEM _____

Beatriz Alencar Ribeiro, Msc – CIAA _____

CIAA
Rio de Janeiro
2023

Dedico este trabalho a Deus e à minha família

AGRADECIMENTOS

Em primeiro lugar, a Deus, meu Criador e Salvador, porquanto não há outra razão de eu estar neste lugar e neste momento senão pela sua Providência. *Soli Deo Gloria*.

À minha família, pelo apoio e incentivo que me motivaram, e ainda me motivam, pela carreira naval.

À minha noiva, em breve esposa, Ariane, pela paciência e carinho que me foram cruciais nessa jornada.

Às minhas orientadoras, CC (T) Eclenice e Prof. Msc Beatriz, pela disponibilidade e dedicação para fornecer materiais de estudo e esclarecer diversas dúvidas.

Aos meus amigos de quarto, pela camaradagem e fraternidade, com que me ajudaram a ter dias mais agradáveis no ardor da vida de ensino.

“O coração humano é o ponto de partida de todas as coisas da guerra.”

Ardant du Picq

A CONVERGÊNCIA ENTRE A GUERRA ELETRÔNICA E A GUERRA CIBERNÉTICA

Resumo

O estudo apresenta uma visão abrangente e analítica da temática que envolve a convergência entre a guerra eletrônica e a guerra cibernética, com ênfase na estratégia militar e na segurança nacional. Inicialmente, procurou-se tratar da relação entre a guerra e a tecnologia e suas transformações ocorridas no tempo para, em seguida, discorrer sobre os assuntos da guerra eletrônica e a guerra cibernética separadamente. Com isso, foi possível tratar da convergência de ambos os domínios envolvidos, abordando seu conceito, tecnologias, questões éticas. Também, destaca-se suas aplicações para o emprego militar, com as novas adaptações de meios militares para tal fim, e para a segurança nacional, no que se refere às infraestruturas críticas, assim como os desafios e riscos envolvidos no processo da convergência. Por fim, considerou-se uma análise da convergência relacionada à Marinha do Brasil.

Palavras- chave: Convergência. Guerra Eletrônica. Guerra Cibernética.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTAS DE SIGLAS E ABREVIATURAS

AESA	*Active Electronically Scanned Array*
AIS	*Automatic Identification System*
AGE	Atividades de Guerra Eletrônica
ARP	Aeronave Remotamente Pilotada
CEMA	*Cyber Electromagnetic Activities*
CIEMA	Controle de Irradiação Eletromagnética e Acústica
CGE	Capacidade de Guerra Eletrônica
CO	*Cyberspace Operations*
DIH	Direito Internacional Humanitário
EB	Exército Brasileiro
ECDIS	*Electronic Chart Display and Information System*
ELINT	Inteligência Eletrônica
EUA	Estados Unidos da América
EW	*Electronic Warfare*
DoS	*Denial of Service*
GCS	*Ground Control Station*
GE	Guerra Eletrônica
GPS	*Global Positioning System*
GSM	*Global System for Mobile*
IA	Inteligência Artificial
IBS	*Integrated Bridge System*
IOT	*Internet of Things*
MAE	Medidas de Ataque Eletrônico
MAGE	Medidas de Apoio à Guerra Eletrônica

MB	Marinha do Brasil
MGE	Medidas de Guerra Eletrônica
NCW	*Network Centric Warfare*
MITM	*Man-in-the-Middle*
MPE	Medidas de Proteção Eletrônica
PIB	Produto Interno Bruto
OSI	*Open Systems Interconnection*
RAM	Revolução nos Assuntos Militares
RDS	Rádio Definido por *Software*
SMO	*Spectrum Management Operations*
TI	Tecnologia da Informação
WLAN	*Wireless Local Area Network*

SUMÁRIO

1 INTRODUÇÃO

No cenário global em constante transformação, a tecnologia desempenha um papel fundamental nas operações militares e na segurança nacional. Nesse sentido, a evolução tecnológica no presente século propiciou o surgimento de dois dos principais domínios que envolvem os conflitos militares modernos, a saber, a guerra eletrônica e a guerra cibernética. Com efeito, a convergência entre esses dois elementos emerge como um ponto nevrálgico para a guerra contemporânea, suscitando questões periclitantes que se somarão ao atual ambiente multifacetado, complexo e dinâmico da guerra.

Em linhas gerais, a guerra eletrônica é o uso efetivo de energia eletromagnética com o fim de interceptar, degradar ou se proteger uso do espectro eletromagnético pelo inimigo enquanto a guerra cibernética é emprego de recursos e meios computacionais para atacar ou se defender do inimigo na rede digital. Dessa forma, através de determinadas tecnologias que propiciaram uma interseção do ambiente eletrônico e do ambiente cibernético, a convergência, doravante chamada de domínio ciber-eletrônico, avança em passos acelerados alterando as necessidades dos meios de combate e redefinindo os pontos vitais para a sobrevivência da civilização moderna.

Dessa maneira, a convergência ciber-eletrônica já tem tomado forma em países cujas forças armadas estão em um nível mais avançado em relação à ciência militar, como os EUA e a Rússia. Também, já se nota o extensivo uso dos artifícios gerados pela convergência no emprego de meios e equipamentos militares da atualidade. E não só a questão militar foi profundamente afetada, mas as infraestruturas críticas tornaram-se alvos centrais deste gênero de ataque, ameaçando diretamente a estabilidade da vida em sociedade. É por isso que este assunto também tem levantado questões éticas prementes que exigirão uma postura rígida de Estados frente às ameaças de cunho não estatal, como o terrorismo.

Com isso, este trabalho tem como objetivo apresentar, de forma panorâmica e fundamentada, os principais pontos que importam a este assunto, que, como se verá, possui potenciais nítidos para impactar a guerra do futuro. Assim sendo, considerou-se de caráter fundamental adicionar alguma contribuição para a visão da Marinha do Brasil, diante da Estratégia Nacional de Defesa, a respeito das possíveis implicações da convergência ciber-eletrônica para as operações marítimas e para a defesa naval.

1.1 Apresentação do Problema

A guerra eletrônica e a guerra cibernética são dois campos de conhecimento aplicados a conflitos militares que, apesar de suas diferenças significativas, possem a capacidade de convergir a fim de alcançar objetivos comuns. As recentes transformações tecnológicas e as necessidades militares impulsionaram a comunicação e a interação entre essas duas esferas de atuação militar, de modo a produzir um espaço de interseção entre elas. Com efeito, já é possível observar ações, meios e técnicas, ora eletromagnéticas ora cibernéticas, trabalhando mutuamente no cenário geopolítico atual com finalidade de alcançar certas vantagens e determinados objetivos de forma conjunta. Estudar essa convergência é fundamental para compreender uma das principais e mais significativas novidades dos conflitos contemporâneos, tanto no aspecto militar quanto em relação à segurança nacional.

1.2 Justificativa e Relevância

Esse tema permite aprofundar o conhecimento no estudo da guerra eletrônica com o viés de sua interação com a guerra cibernética a fim de superar o conhecimento setorizado muitas vezes limitante e entender como diferentes áreas do conhecimento podem se relacionar, como é patente neste caso de convergência.

Também, esse estudo possibilita atualizar-se das mudanças mais recentes no contexto tecnológico-militar. Fazer um estreito acompanhamento do avanço científico, em acelerado desenvolvimento na indústria bélica, permite maior conscientização para tomadas de decisões que envolvam os temas da guerra eletrônica e, também, cibernética.

1.3 Objetivos

Esta seção tem como finalidade apresentar os objetivos que foram visados para a elaboração deste trabalho, consistindo em um núcleo geral e algumas metas específicas, de forma a constituir a totalidade da temática abordada.

1.3.1 Objetivo Geral

O objetivo geral deste trabalho consiste em esclarecer os efeitos potenciais e já existentes da convergência dos ambientes eletromagnético e cibernético, principalmente no que se refere a estratégia militar e a segurança nacional, através de uma pesquisa fundamentada e uma análise crítica.

1.3.2 Objetivos Específicos

Quanto aos objetivos específicos, pode-se resumi-los em:

a) Analisar a evolução tecnológica: investigar a evolução das tecnologias concernentes à guerra eletrônica e cibernética, identificando os avanços que propiciaram e impulsionaram a convergência entre ambas.
b) Avaliar estratégias de defesa: refletir sobre as estratégias de defesa existentes e emergentes em resposta à convergência entre a guerra eletrônica e a guerra cibernética, especialmente no que tange à questão militar e de segurança nacional.
c) Levantar questões paralelas: complementar o assunto, para uma compreensão mais ampla, discorrendo sobre desafios e riscos atinentes ao tema da convergência, assim como entendimentos éticos relacionados.
d) Realizar uma simulação: aplicar o conhecimento do tema de uma maneira mais prática, com o objetivo de fazer uma ilustração dinâmica do estudo.

2 REFERENCIAL TEÓRICO

2.1 Guerra e Tecnologia

"A história das guerras é, sobretudo, a história do gênio humano aplicado à destruição."

(Demétrio Magnoli)

Guerra e a tecnologia são realidades eminentemente distintas, mas que, ao longo da história, eventualmente se entrelaçam e combinam-se para, de forma funesta, formar o terror da história. Desde a descoberta das primeiras armas e maquinarias de guerra da antiguidade até as recentes inovações no campo da batalha do atual conflito na Ucrânia e em Israel, múltiplas transformações já ocorreram no âmbito do conhecimento militar. Não diferentemente, a busca por vantagens táticas e materiais nos confrontos de potências já favoreceram uma série de revoluções no âmbito científico. Essas duas correntes implacáveis do processo histórico provocaram profundas mudanças na estrutura dos conflitos humanos, na condução da política externa, na vitalidade da segurança nacional e hoje levantam questões éticas e humanitárias sem precedentes.

Particularmente em relação à guerra, muitos pensadores no decorrer da história já tentaram compreender as razões por detrás do que seria a maior manifestação de destruição da experiência humana. Isso começa, reconhecidamente, na civilização ocidental, no séc. VIII a.C., quando o poeta grego Homero escreve a *Ilíada*, na qual ressalta a nobreza e a tragédia por trás da guerra. Já no oriente, no séc. V a.C., Sun Tzu escreve o que seria o primeiro tratado de estratégia militar documentalmente conhecido, *A Arte da Guerra*. Não somente a antiguidade foi marcada pelo ávido interesse em descrever a violência nos campos de batalha, como também a Idade Média é notada pela tentativa de unir o conceito da guerra com a questão moral, através do conceito da "guerra justa", com Agostinho de Hipona e Tomás de Aquino (Carneiro, 2016). Contudo, ao romper da modernidade, surge o conceito da "guerra total"[1], que pôde ser mais fielmente expressa no fenômeno das guerras napoleônicas e na teoria militar de C. von Clausewitz em sua obra *Da Guerra*. Esse ponto de inflexão tornou possível a ocorrência de duas grandes guerras mundiais que posteriormente levaria

[1] A guerra total pode ser definida como "uma guerra que não tem restrições em termos de armas usadas, o território ou combatentes envolvidos, ou os objetivos perseguidos, especialmente aquela em que as leis da guerra são desconsideradas". Disponível em https://www.oxfordreference.com/display/10.1093/oi/authority.20110803105038425;jsessionid=B04E43773F9FA476C1ABAAC9BBCB605E. Acesso em 10 ago. 2023.

humanidade a passar um período de “equilíbrio do terror” (mistura de equilíbrio de poder entre potências nucleares e pequenas guerras por procuração) decorrente da guerra fria (Biagi, 2001). Entretanto, todo o panorama histórico da guerra seria insuficientemente explicado sem o contexto da evolução e apoio da tecnologia.

Em contrapartida, a ciência, ao contrário da guerra, possui um caráter mais construtivo (não destrutivo) e sua história na humanidade é marcadamente destacada pelas quatro revoluções industriais. No final do séc. XVIII, o surgimento da indústria através do uso do carvão para energia e da descoberta da máquina a vapor deram origem a Primeira Revolução Industrial. Em sequência, no final do séc. XIX, com a descoberta da eletricidade, a transformação do ferro em aço, dentre outras inovações, deu-se a Segunda Revolução Industrial. E a Terceira Revolução Industrial, ou também chamada de Revolução Técnico-Científica Informacional, pode ser entendida dentro dos avanços do séc. XX, como a expansão da informática, robótica, telecomunicações etc. As três primeiras revoluções científicas são muito bem consolidadas e reconhecidas no meio acadêmico (Sakurai.; Zuchi, 2018). Todavia, ainda é desafiador delimitar a Indústria 4.0, ou Quarta Revolução Industrial, uma vez que esta encontra-se em curso e em constante evolução. O que se pode dizer sobre a atual era científica são as inovações mais recentes e ainda em desenvolvimento, quais sejam, a internet das coisas, o mundo cibernético, a robótica avançada, a inteligência artificial, e outras (Sakurai.; Zuchi, 2018).

Como se pode ver, guerra e ciência têm seus devidos lugares na história e suas formas e movimentos são notavelmente observados no tempo. No entanto, ainda pode ser desafiador tentar relacionar dois conceitos e realidades aparentemente antagônicos uma vez que o primeiro é caracterizado por sua natureza agressiva e mortal ao passo que a segunda tem um aspecto mais benéfico (ainda mais visível após o advento da medicina como ciência). Malgrado as aparências, foi a interação dessas duas forças históricas que deram sentido uma a outra. A exemplo, os encouraçados norte-americanos da Guerra de Secessão tiveram mudanças significativas nas áreas de propulsão, armamento e armadura em relação aos modelos a remo e vela anteriores: a propulsão a vapor, canhões de longo alcance, e revestimentos de ferro e aço seriam impensáveis sem as invenções decorrentes da Primeira e Segunda Revoluções Industriais (Mesquita, 2021). Não somente as armas tornam-se mais sofisticadas através da ciência, mas a recíproca também é verdadeira. Na Segunda Guerra Mundial, a medicina herdou estudos bastante úteis a partir da experimentação biomédica nazista em prisioneiros de guerra e o desenvolvimento da energia nuclear só foi possível em virtude da descoberta da fissão nuclear na aplicação da bomba atômica pelo Projeto

Manhattan nos EUA (Cascais, 2003). Essas inovações tecnológicas resultaram inegavelmente em uma miríade de benefícios à humanidade, mas à custa de muitas vidas cujas perdas em guerras passaram a ser contadas na mesma proporção – em escala industrial.

Sem dúvidas, há uma estreita correlação entre esses dois elementos. Hoje e cada vez mais, a guerra moderna demanda recursos e conhecimentos em um nível de complexidade crescente. Da Guerra do Peloponeso, com os combates corpo a corpo, navegações a remo e defesas muradas, à recente Guerra na Ucrânia, com ataques a sistemas digitais de a infraestruturas críticas, uso de drones, mísseis balísticos, além da questão latente da bomba nuclear, há muito para ser estudado. De acordo com a tese de Alvin Toffler (apud Nascimento; Costa, 2017, p. 67-68), a história das guerras pode ser relacionada com a evolução tecnológica a partir de três paradigmas: (I) a primeira onda, segundo a qual as guerras eram eminentemente decididas em função da quantidade de massa humana em combate; (II) a segunda onda, cuja mecanização passa a ser o fator determinante, isto é, aquele que possui maiores quantidades de carros de combate, navios, aviões e submarinos deteria a vantagem em combate; e (III) a terceira onda, na qual se encontra a atualidade, que, dita de outra forma, é a guerra do conhecimento e da informação, que passa a empregar meios cibernéticos e eletrônicos como fatores decisivos. Portanto, é como disse o teórico militar Gus Anderson: “A combinação das funções militares de guerra eletrônica e cibernética será fundamental para manter uma vantagem política e militar no futuro”. A existência da guerra eletrônica combinada à guerra cibernética, portanto, ganha contornos impressionantes e uma proeminência *sui generis* nos dias atuais, sobretudo, em virtude da expansão massiva – e a consequente dependência – de meios que exploram o espectro eletromagnético e utilizam sistemas de redes digitais.

2.2 Guerra Eletrônica

> *"Se houver uma próxima guerra, pode ser uma guerra nuclear, pode ser uma guerra química, mas certamente será uma guerra eletrônica."*
>
> *(Bernard Brodie)*

Guerra eletrônica pode ser definida genericamente como “o conjunto de técnicas e tecnologias que tornam dispositivos capazes de neutralizar eletronicamente um sistema de armas e de desenvolver proteção contra os mesmos dispositivos” (Neri, 2006, p. 3). Em outras

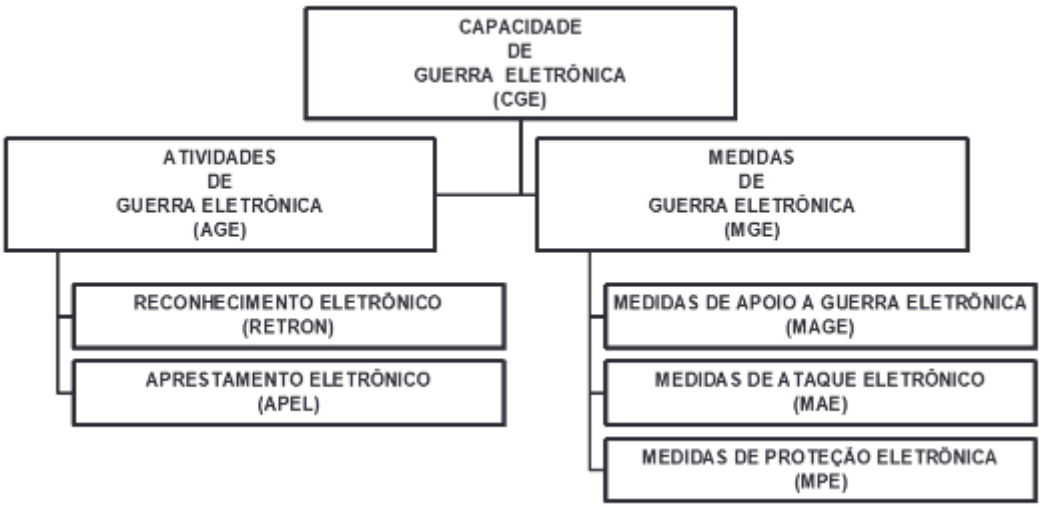
palavras, também significa a disputa pelo domínio do espectro eletromagnético e de armas direcionais com propósitos ofensivos, defensivos e informacionais em relação ao oponente (Fan, 2023). Na atualidade, a guerra eletrônica ganha um destaque especial devido a uma importante característica particular, que é sua abrangência, uma vez que os aparelhos e equipamentos de detecção, comunicação e destruição da guerra moderna possuem, em sua esmagadora maioria, dispositivos eletrônicos que, praticamente, dependem, em menor ou maior grau, das irradiações eletromagnéticas do ambiente. E, por conta disso, a guerra eletrônica acaba por não possuir limitações espaciais – desconsiderando apenas o ambiente submarino – dado que sua operação ocorre nos ambientes terrestres, marítimos e aéreos, tal é a relevância desta modalidade para a guerra moderna.

Historicamente, o conhecimento da guerra eletrônica se originou a partir dos experimentos científicos do campo do eletromagnetismo. A descoberta do físico James C. Maxwell no séc. XIX, segundo o qual havia um fenômeno na natureza que poderia ser explicado pela propagação de ondas de constituição elétrica e magnética num meio imaterial (Marques, 2023), permitiu a construção de dispositivos com a capacidade de transmitir e receber ondas de energia eletromagnética. Essa descoberta inaugurou o campo das radiocomunicações e, posteriormente, também serviu aos interesses militares. A primeira aparição de um dispositivo eletrônico sendo utilizado em combate foi na Batalha de Tsushima, na Guerra Russo-Japonesa, em 1905, com o uso do telégrafo sem fio por ambos os lados (Braga, 2023, p. 69). A criação do telégrafo sem fio, que era um aparelho que basicamente enviava mensagens através de pulsos pelo ar, rompeu as limitações físicas da época na área de comunicações navais, visto que antes os navios se comunicavam por bandeiras, galhardetes e fumaça e à noite ou em baixa visibilidade – geralmente provocada por nevoeiros – a comunicação se dava necessariamente por sinais luminosos e sonoros (Braga, 2023, p. 71). Portanto, inicialmente, a guerra eletrônica surge como uma tentativa de ultrapassar as limitações físicas da distância – e impedir que o inimigo faça o mesmo – para então evoluir e se difundir, dando origem aos então sistemas de detecção e comunicações modernos.

É importante considerar que, em virtude da multifacetada funcionalidade da guerra eletrônica, ela acaba por possuir divisões estritamente estabelecidas dentro estrutura doutrinária geral. De acordo com Neri (2006, p. 25), a guerra eletrônica pode ser dividida em: inteligência de sinais, medidas de apoio, contramedidas, medidas de proteção e guerra de informação. Entretanto, é possível simplificar ainda mais tais conceitos, de modo a permitir

uma melhor compreensão do conhecimento do tema, como se pode ver na Fig. 1, que retrata de maneira esquemática a divisão doutrinária de guerra eletrônica da Marinha do Brasil.

Fig 1 – Estrutura da Guerra Eletrônica na MB



Fonte: elaborado pelo autor (2023)

Dentro da estrutura de guerra eletrônica da Marinha do Brasil, as definições são delimitadas com base nas peculiaridades de suas divisões administrativas e operativas. No âmbito da MB, de acordo com a Doutrina Básica da Marinha (2014, p. 53), a guerra eletrônica é definida como “o emprego militar da eletrônica que diz respeito às ações que envolvem o uso de energia eletromagnética para determinar, explorar, impedir, reduzir ou prevenir o uso efetivo pelo inimigo do espectro eletromagnético e para assegurar o uso deste espectro pelas próprias forças”. Logo, as seguintes definições decorrentes podem ser expressas nas seguintes palavras, conforme a mesma publicação (Brasil, 2014, p. 53):

- Capacidade de Guerra Eletrônica (CGE): é o somatório de meios e recursos de toda ordem que permita ao Poder Naval empreender eficazmente ações de guerra eletrônica em proveito de suas operações.
- Atividades de Guerra Eletrônica (AGE): são aquelas de caráter estratégico, tático ou logístico, que visem ao estabelecimento, à reformulação ou à verificação de uma CGE e ao apoio no planejamento do seu emprego, em uma operação naval.
- Medidas de Guerra Eletrônica (MGE): abrangem as ações efetivamente realizadas no decorrer de uma operação naval. A sua natureza é fundamentalmente tática e seu emprego deve estar amparado por um planejamento e pela adequabilidade das táticas e equipamentos utilizados.

Todavia, uma vez que a estrutura de GE supracitada é ampla e se estende a limites que não se aplicam ao tema proposto, isto é, da guerra eletrônica em sua natureza tática e operativa, é necessário, dessa forma, restringir-se à área das Medidas de Guerra Eletrônica (MGE) para alcançar o fim pretendido. Nesse sentido, as MGE, como descrito acima na Fig. 1, divide-se em Medidas de Apoio à Guerra Eletrônica (MAGE), Medidas de Ataque Eletrônico (MAE), Medidas de Proteção Eletrônica (MPE). Conforme expresso na Doutrina Básica da Marinha (2014, p. 53-54), estas medidas são definidas como:

- Medidas de Apoio à Guerra Eletrônica (MAGE): são um conjunto de ações visando à busca, interceptação, identificação e localização eletrônica das fontes de energia eletromagnética irradiadas no ambiente eletrônico, a fim de permitir a análise, o imediato reconhecimento de uma ameaça ou sua posterior exploração.
- Medidas de Ataque Eletrônico (MAE): são um conjunto de ações tomadas para evitar ou reduzir o uso efetivo, por parte do inimigo, do espectro eletromagnético e, também, degradar, neutralizar ou destruir sua capacidade de combate por meio de equipamentos e armamentos que utilizem este espectro, podendo ser subdivididas em MAE não destrutivas e destrutivas.
- Medidas de Proteção Eletrônica (MPE): são um conjunto de ações tomadas para a proteção de meios, sistemas, equipamentos, pessoal e instalações, a fim de assegurar o uso efetivo do espectro eletromagnético, a despeito do emprego de MAE por forças amigas e inimigas.

Dessa maneira, essa divisão tripartida das MGE indica seu caráter multifário, a saber, informativo, ofensivo e defensivo, nessa ordem. Em relação às MAGE, tem-se os sistemas passivos de detecção e comunicação. Já as MAE são mais variadas, a saber, os bloqueios e despistamentos mecânicos e eletrônicos, tecnologia de furtividade *stealth*, armas de energia direcionada (laser de alta energia, feixe de partículas, microondas de alta potência, pulsos eletromagnéticos) e mísseis anti-radiação. E as MPE podem ser classificadas em anti-MAGE (técnicas de sistemas, CIEMA, evasivas táticas) e anti-MAE (técnicas de sistemas, controle de frequências, procedimentos operacionais) (Mossi, 2019, p. 15-17).

Conforme foi dito, o que se iniciou como uma forma de se livrar das limitações naturais do ambiente, hoje se tem uma vasta gama de artefatos eletrônicos que exploram o espectro eletromagnético com a finalidade de superar o oponente em determinada situação. Por exemplo, no meio terrestre, pode-se citar o sistema russo LEER-3, que é um interferidor de comunicação GSM, que, com apoio de drones, tem a capacidade de detectar e realizar

spoofing em sinais de celulares, e o sistema KRASUKHA-4, também russo, que realiza bloqueio eletrônico em mísseis guiados por radiofrequência e que teve fundamental atuação protegendo uma base aérea russa na Síria de bombardeiros (Mossi 2019, p. 30-31). No meio marítimo, há mísseis lançado de plataformas no mar que são capazes de discernir o contraste térmico na vertical, encontrado na linha d'água de navios, como é o caso o míssil anti-navio norueguês PINGUIM (Coutinho, 2020). No meio aéreo, é possível observar cada vez mais frequente o uso de drones com emprego de MAGE através de lançamento de plataformas marítimas ou terrestres superando as limitações naturais da curvatura da terra, como é o caso da ARP Scan-Eagle, desenvolvida pela MB, e também com emprego de MAE, acoplados de laser de alta performance, além de utilizar tecnologia *stealth* (Vieira, 2021, p. 2-4). Ao somar tudo isso, observa-se a versatilidade da guerra eletrônica nos múltiplos ambientes existentes: terrestre, marítimo e aéreo. Ademais, ainda é possível observar, um novo ambiente cuja integração com a guerra eletrônica, provocada pelas novas demandas do combate moderno, está em profunda transformação e crescimento, que é o ambiente cibernético.

2.3 Guerra Cibernética

Guerra cibernética, ou então "ciberguerra", provoca visões bastante plurais acerca da sua aplicabilidade no contexto geopolítico presente. Uma das definições mais aceitas no meio acadêmico é que a ciberguerra são "ações de um Estado-nação para penetrar nos computadores ou redes de outra nação com o objetivo de causar danos ou interrupções" (Clarke; Knake, 2010), isto é, são atividades fundamentalmente bélicas que ocorrem no meio digital, mas que podem causar impactos reais e destrutivos no ambiente físico e que, por isso, merecem uma atenção vital das autoridades competentes. Em uma visão alternativa, outro autor a define como "um ato de força instrumental e político potencialmente letal conduzido por meio de código malicioso" (Rid, 2012), porém atribuindo a mesma uma relevância menor em relação à opinião *mainstream* do assunto, pois alega que a ciberguerra nada mais é que a continuidade de práticas antigas e clássicas da guerra, como a subversão, sabotagem e espionagem e que todo alarmismo em torno do problema pode ser explicado por uma tentativa de justificar gastos militares de governos. Em outras palavras, enquanto Clarke e Knake (2010) afirmam que a guerra cibernética tem dimensões macro e com efeitos potencialmente catastróficos, Rid (2012) afirma que os ataques cibernéticos têm alcance e impacto limitados.

Sob a ótica da história, o surgimento da ciberguerra pode ser considerado recente se comparado com as outras modalidades da guerra, inclusive a eletrônica. Embora haja uma

versão mais antiga (porém controversa)[2], o primeiro incidente classificado oficialmente como um ataque cibernético foi o ocorrido na Estônia em 2007 quando os principais *sites* do governo, de bancos e de jornais estonianos receberam um ataque virtual agressivo (alegadamente de russos) através de redes *botnets*, isto é, envio de uma quantidade massiva de pedidos de informação por uma rede de computadores de vários países do mundo, obstruindo, dessa forma, os acessos aos *sites* por semanas (Landler; Markoff, 2007). Contudo, a gênese do "ciberespaço" pode ser encontrada bem antes, dentro da Revolução Técnico-Científica Informacional, nas décadas de 1980 e 1990, com a difusão da tecnologia da informação (TI) na informática, irradiando-se, em sequência, para o campo da doutrina e estratégia militares (Lobato; Kenkel, 2015). Desde então, a assimilação do domínio cibernético na arte da guerra vem ganhando amplitude e profundidade à medida que suas ocorrências se espalham pelo globo e seus impactos são mais significativos, como nos casos posteriores da Geórgia, Irã, e, inclusive, Brasil (Honório, 2016).

Antes de prosseguir, é importante apresentar o *modus operandi* desta modalidade de ataque, a ciberguerra, descrevendo os principais métodos de ataques cibernéticos existentes, costumeiramente praticados por militares sob égide de governos e ciber-criminosos independentes (Medonça, 2014):

- *Port Scanning*: consiste, basicamente, em uma técnica de invasão de dados que ocorre em duas etapas. Na primeira fase, o invasor realiza um levantamento de dados de uma ampla rede de *hosts* com a seleção e a identificação dos *hosts* mais interessantes. A seguir, na segunda fase, ele passa a fazer o escaneamento de portas propriamente dito, através do qual ele testa a vulnerabilidade da rede, explorando as falhas de segurança ao enviar pedidos de acesso a cada porta cuja resposta indicará se determinada porta está protegida ou não.
- Engenharia Social: é um conjunto de técnicas que visa explorar a falta de consciência situacional digital de membros de uma rede com o objetivo de obter acesso a dados sensíveis. Entre as principais técnicas de engenharia social, tem-se (a mais comum) o *phishing*, que trabalha com o envio de mensagens fraudulentas, normalmente através de e-mails de usuários, que aparentam proceder de fontes

[2] Há um suposto ataque cibernético ocorrido em meados de 1982. O episódio se deu com a explosão do gasoduto soviético Trans-Siberiano. A primeira versão relata que a explosão foi provocada por uma *logic bomb* adicionada furtivamente pelo serviço secreto americano no *software* canadense de controle de pressão quando a KGB o tomou e o implantou em um dos sistemas do gasoduto, causando a maior explosão não nuclear da história. Uma outra versão conta que o fato não passou de um acidente (Honório, 2016, p. 53-54).

confiáveis e seguras. E, geralmente, nestes e-mails, algumas orientações direcionam o usuário a acessar algum *link* ou anexo com o objetivo de, por exemplo, revelar seu acesso a *logins* de redes sociais ou dados bancários.

- *Denial of Service* (DoS): diferentemente dos anteriores, este ataque cibernético não visa o roubo ou a invasão de dados, mas basicamente a negação de serviços através da ocupação total da largura de banda, impedindo qualquer tráfego de rede por um longo período de tempo. Esse tipo de ataque foi semelhante ao caso supracitado da Estônia em 2007.
- *Man-in-the-Middle* (MITM): já este ataque cibernético visa interpor furtivamente o intruso entre duas partes que estão em comunicação, geralmente por meio de um roteador sem fio como mecanismo de infiltração. O objetivo deste ataque é interceptar, monitorar e até mesmo manipular as informações em tráfego na rede. É um ataque cibernético bastante típico de ações de espionagem.
- *Web Defacement*: por último, este tipo de ciberataque tem o propósito de modificar o conteúdo de determinado *site* com fins políticos e ideológicos ou simplesmente por vandalismo.

É possível ainda analisar algumas características manifestas no que se refere à ciberguerra e posicioná-la dentro do contexto da guerra convencional. Conforme o entendimento predominante, a guerra cibernética é o mais novo quinto domínio da guerra (juntamente com os domínios terrestre, marítimo, aéreo e espacial) e, devido às suas particularidades que o distingue dos demais, traz consigo algumas características singulares que tem transformado o conceito de combate na atualidade, entre as quais as mais importantes são: a superioridade do primeiro ataque, limitação de danos físicos, efeito temporário, vantagem do ataque sobre defesa, anonimato e o paradoxo cibernético[3] (Silva, 2014). No contexto mais amplo, a guerra cibernética pode ser entendida como a interação de *atores contemporâneos* existentes no ambiente cibernético, que são os Estados, as instituições, as corporações industriais/empresariais, o setor financeiro, o setor de serviços, grupos de ativistas políticos/religiosos, "*hackers*", criminosos digitais ("*crackers*", "*banckers*", etc.) e pessoas comuns, conectados em uma rede mundial, a *internet*, e fazendo o uso de *armas*

[3] O paradoxo cibernético pode ser expresso na seguinte sentença: "quanto maior a capacidade em TI de um Estado, maior a sua fragilidade à ataques cibernéticos" (Silva, 2014, p. 200), o que transforma completamente o panorama das relações internacionais e do equilíbrio de poder, visto que países extremamente informatizados como os EUA passam a ser mais vulneráveis do que os que são menos dependentes da *internet* como a Coreia do Norte e a China.

cibernéticas, que são dispositivos de *hardware* ou *software* (chaves de *hardware*, *firewalls*, *malwares*, vírus e outros programas como bombas cibernéticas) empregados durante ações no espaço cibernético, acionados remotamente ou programados por *software*, sempre com intuito de obter o domínio da informação no meio cibernético ou causar danos ao inimigo por meio de infraestruturas críticas (Silva, 2014, p. 201-202).

Além disso, muito se tem discutido sobre a relevância e o impacto do domínio cibernético na conjuntura político-estratégica da contemporaneidade. Segundo Junior et al. (2017), partindo de uma análise dos eventos históricos relacionados a hostilidades no ambiente cibernético por atores contemporâneos diversos e observando seus efeitos notáveis, conclui-se que a guerra cibernética, em razão de seu limitado potencial de danos – equiparado a meios bélicos convencionais – é incapaz de produzir coerção ou dissuasão entre Estados, em contraste com o impacto de peso político provocado pela tecnologia da bomba nuclear desde a Guerra Fria. Na verdade, a ciberguerra passa a ser mais interessante e eficaz quando utilizada no sentido de armas combinadas juntamente com os meios de força cinéticos, em missões de inteligência, reconhecimento e vigilância, o que evidencia sua função muito mais tática-operacional que político-estratégica. Nesse sentido, o Brasil vem se preparando para atuar de forma decisiva no campo cibernético conforme está estabelecido na Política Nacional de Defesa:

> [...] 2.2.16 Adicionalmente, requerem especial atenção a segurança e a defesa do espaço cibernético brasileiro, essenciais para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações de interesse nacional (Brasil, 2020, p. 8).

Ademais, a guerra cibernética tem tomado uma relevância capital no cenário estratégico brasileiro (juntamente com os projetos estratégicos nuclear e aeroespacial) cuja condução operacional tem sido capitaneada pelo Exército Brasileiro, segundo a Estratégia Nacional de Defesa:

> [...] 3.6.5 Três setores tecnológicos são essenciais para a Defesa Nacional: o nuclear, o cibernético e o espacial. Portanto, são considerados estratégicos e devem ser fortalecidos. Como decorrência de sua própria natureza, transcendem à divisão entre desenvolvimento e defesa e entre o civil e o militar [...]. Dessa forma, no Setor de Defesa, atribui-se à Marinha a responsabilidade pelo Setor Nuclear, ao Exército pelo Setor Cibernético e à Força Aérea pelo Setor Espacial (Brasil, 2020, p. 30).

Fora isso, soma-se o fato que o Brasil é um dos países que mais sofre ataques cibernéticos do mundo e o que mais sofre na América Latina (Pinto; Grassi, 2020), o que torna necessário a discussão desse assunto em um contexto mais amplo.

3 METODOLOGIA

Esta seção destina-se a abordar os princípios metodológicos empregados no estudo. De forma geral, foi adotada uma metodologia rigorosa e estrita com a finalidade de tratar o assunto de forma mais precisa possível.

3.1 Classificação da Pesquisa

A metodologia utilizada na pesquisa foi de cunho qualitativo, através da coleta de dados de maioria não numérica e mais textual e visual, buscando fazer a interpretação dos dados e a análise de textos relacionados ao assunto.

3.1.1 Quanto aos fins

O estudo realizado possui um caráter ambivalente da pesquisa quanto aos fins. A pesquisa é inicialmente descritiva por tratar de assuntos centrais ensinados no presente curso e na vida operativa da Marinha do Brasil, como os conceitos da guerra eletrônica. Mas também pode ser exploratória à medida que trata de assuntos não familiares como a guerra cibernética e a convergência de ambos os domínios, tema este aparentemente pouco discorrido no Brasil.

3.1.2 Quanto aos meios

Em relação aos meios, pode-se dizer que o estudo possui uma essência majoritariamente formada por uma pesquisa bibliográfica, com a revisão de artigos, livros e diversos trabalhos científicos do assunto. Porém, não é irrelevante considerar a contribuição de manuais oficiais da Marinha do Brasil e do Ministério da Defesa que permitiram reforçar o conhecimento de determinadas áreas; logo, tratando-se também de uma pesquisa documental.

3.2 Limitações do Método

Os métodos utilizados possuem limitações inerentes a especificidade do tema. Como o tema se trata ainda de um assunto incipiente no meio militar, principalmente no Brasil se comparado às grandes potências, as produções científicas a respeito da convergência ainda demonstram estar em fase de observação, visto que ainda possui grande potencial para

evoluir. Outra coisa, é o fato do assunto ser evidentemente militar, o que reduz as possibilidades de encontrar fontes abertas e confiáveis a respeito de equipamentos em desenvolvimento de forças armadas estrangeiras.

3.3 Coleta e Tratamento de Dados

A coleta de dados constituiu-se de um levantamento cuidadoso e criterioso de obras de autores consagrados no meio acadêmico. Inicialmente, foi necessário compilar trabalhos mais didáticos que possibilitassem uma compreensão mais acessível do tema por parte do autor. Depois, foi possível buscar literaturas mais sofisticadas que abordassem e correlacionassem o tema a outras áreas de interesse. Por fim, utilizou-se esses dados para desenvolver o assunto de forma mais exaustiva possível assim como para realizar a simulação no Simulink.

4 A CONVERGÊNCIA

4.1 Conceituação

A priori, é absolutamente indispensável estabelecer e delimitar o conceito do tema em questão, isto é, do que realmente se trata a então convergência entre a guerra eletrônica e a guerra cibernética. Para esse fim, é necessário, antes de tudo, esclarecer suas diferenças exclusivas, que são aquelas que irremediavelmente constituem a natureza de determinada modalidade de guerra, ou seja, sua essência, que a distingue das demais. Conforme se discorreu nas seções acima, pode-se definir, cada um nos seguintes termos: a guerra eletrônica envolve o uso de tecnologias e técnicas para controlar o espectro eletromagnético, incluindo o uso de sinais de rádio, micro-ondas, laser e outras frequências para atingir objetivos militares, como interferência em comunicações inimigas, bloqueio e análise de sinais de radiofrequência, ou neutralização de sistemas de armas inimigos; por outro lado, a guerra cibernética envolve o uso de tecnologias e ferramentas para conduzir operações ofensivas e defensivas no ciberespaço, como ataques a sistemas de computadores, redes e grandes infraestruturas. De forma mais elucidativa, pode-se também sistematizar essas características no quadro abaixo:

Quadro 1 – Características das guerras eletrônica e cibernética

	Guerra Eletrônica	Guerra Cibernética
Ambiente	Atua predominantemente no espectro eletromagnético.	Opera em redes digitais e sistemas de informação.
Alvos	Seus ataques são basicamente direcionados a alvos desde aparelhos e sistemas de comunicações até equipamentos e sistemas de deteção radar, sistemas de navegação e dispositivos eletrônicos em geral.	Sua ofensiva é voltada eminentemente para alvos como computadores, redes, bancos de dados, sistemas de controle industrial e infraestruturas críticas.
Métodos	Podem variar desde medidas de apoio (interceptação eletrônica) de ataque (*jamming*, *spoofing* e outros) além de defesa (circuitos de proteção e suas variações).	Também possui métodos varáveis que vão desde a inserção de um simples código malicioso (*malware*) até métodos de negação de serviço (DoS), engenharia social, roubo de dados etc.

Fonte: elaborado pelo autor (2023)

Em termos simples, essas são as principais características que permitem entender o domínio eletrônico e o cibernético como dois conceitos notoriamente distintos. Contudo, embora haja diferenças explícitas no que tange a cada categoria, as recentes pesquisas na área da tecnologia militar têm descoberto um espaço de interseção entre ambos, unindo os meios eletrônicos e cibernéticos para alcançar resultados outrora impossíveis.

Com a crescente expansão do conhecimento científico e da tecnologia bélica em uma razão praticamente geométrica, as mudanças provocadas na estratégia e na doutrina militar se moldam na mesma proporção. De acordo com o historiador e teórico militar Martin van Creveld (2009), as diferentes modalidades da guerra, impulsionadas pelas fortes mudanças no âmbito dos conflitos e estratégias militares, tendem a uma convergência de forma inexorável. Conforme o autor, a guerra convencional, guerra híbrida, guerra cibernética, guerra psicológica e demais estão se tornando cada vez mais interdependentes e entrelaçadas, de modo que se observa uma tendência natural e geral das diferentes modalidades da guerra se influenciarem mutuamente resultando em um emprego cada vez mais complexo no que se chama na terminologia militar de armas combinadas[4]. Dessa forma, é evidente que há um contexto maior em que a diversidade do combate tem tomado um caráter *interoperável*, isto é, as ramificações da guerra e suas especializações que tornam o

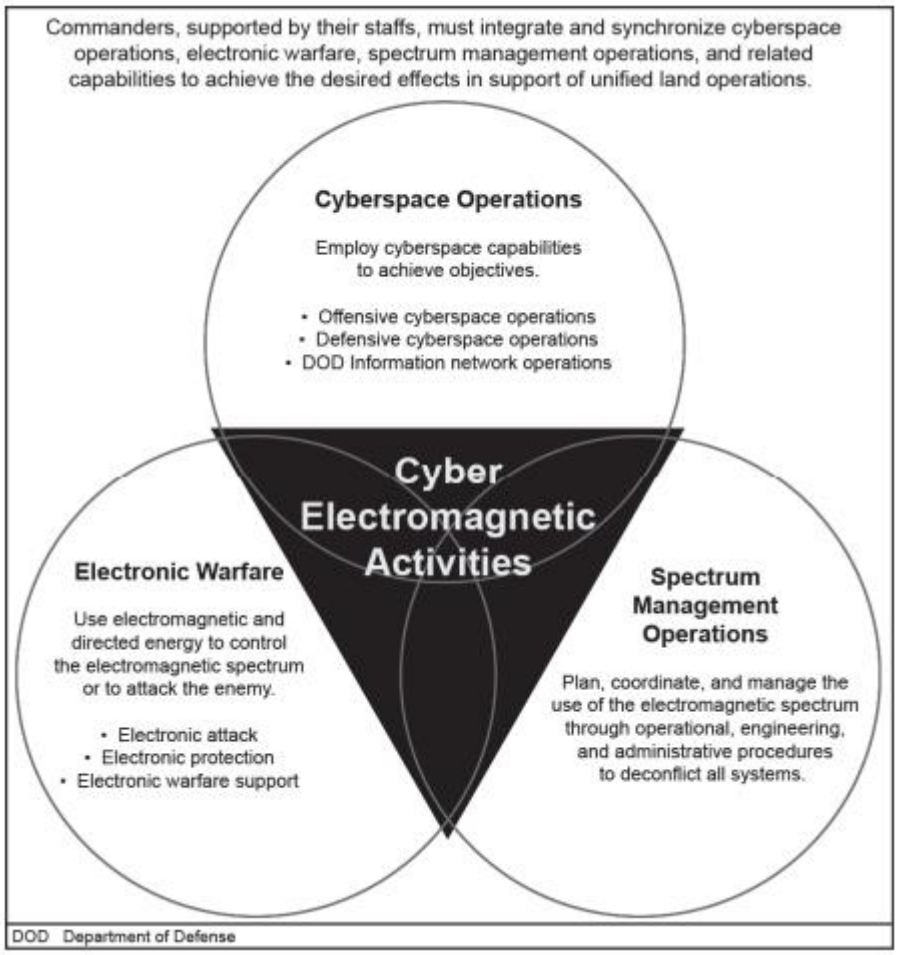
[4] O conceito de armas combinadas consiste basicamente no uso coordenado de armas de diferentes naturezas explorando suas utilidades conforme a situação a fim de maximizar a eficácia de resultados. Um emprego famigerado de armas combinadas na história pode ser observado tática de Blitzkrieg (House, 2008).

combate eventualmente diverso têm se mesclado a fim de obter resultados mais eficazes. Com isso, a tendência a uma convergência não é um fato exclusivo dos domínios eletrônico e cibernético, mas se trata de um fenômeno macro em que eles estão incluídos.

Além disso, a integração de ambos os domínios, eletrônico e cibernético, já é um entendimento consolidado por parte de algumas das forças armadas mais relevantes do mundo. É o caso do exército norte-americano, que, na vanguarda, já tem demonstrado interesses e preocupações quanto a essa questão, como se pode ver no documento doutrinário FM 3-38, que, em outras palavras, declara que a guerra eletrônica e a guerra cibernética consistem, na verdade, em uma única matéria chamada de "atividades ciber eletromagnéticas" – em inglês, *Cyber Electromagnetic Activities* (CEMA). Nesse caso, o CEMA integra e sincroniza as funções de operações no ciberespaço (CO – *cyberspace operations*), guerra eletrônica (EW – *electronic warfare*) e operações de gestão no espectro[5] (SMO - *spectrum management operations*) para produzir efeitos complementares e de reforço. Conforme o mesmo documento norte-americano, é de fundamental importância a realização desta atividade tríplice de forma coordenada de modo que, se qualquer uma delas atuar de forma independente, pode prejudicar o seu emprego eficiente e causar conflitos e interferências mútuas entre elas. Logo, os CO, EW e SMO são sincronizados para causar efeitos específicos em momentos decisivos com a finalidade de apoiar a operação global. Estes elementos podem ser mais detalhadamente expressos na figura 2:

[5] A ideia de "operações de gestão no espectro", ou SMO na sigla em inglês, pode ser comparada, no âmbito doutrinário da Marinha do Brasil, ao CIEMA (Controle das Irradiações Eletromagnéticas e Acústicas), que é a efetiva administração de todas as emissões eletromagnéticas e acústicas de uma força ou unidade, para obter a máxima vantagem tática. No entanto, a comparação não é perfeita uma vez que esta visa estabelecer a política de irradiação eletromagnética e acústica enquanto aquela apenas eletromagnética.

Fig 2 – Atividades Ciber Eletromagnéticas



Fonte: United States Army (2014)

Outrossim, a Rússia já toma o fato da convergência até com mais solidez do que os EUA. De forma peculiar, os russos nunca pensaram na guerra eletrônica e cibernética como entidades separadas, diferentemente dos ocidentais. A doutrina russa de “guerra de informação” une, ao mesmo tempo como uma única e indissolúvel arma, a guerra eletrônica, a guerra cibernética, as operações psicológicas e inteligência de sinais (O’Shea, 2017, p. 16). Inclusive, a habilidade russa na guerra de informação se observa de forma evidente em seu uso intensivo, não somente durante todas as fases do conflito, mas especialmente em tempos de paz para fomentar as condições necessárias de uma intervenção militar em locais de interesse. Ademais, a guerra de informação aparenta ser atraente aos russos graças ao seu baixo custo em relação às armas convencionais e de apresentar resultados precisamente eficazes de forma a abrir o caminho para possível emprego de efeitos cinéticos (O’Shea, 2017, p. 16). Com isso, devido à histórica filosofia russa de armas combinadas, a ideia de convergência não faz sequer sentido para o pensamento russo uma vez que eles nunca os trataram como domínios separados, sendo a ideia de uma arma única muito mais natural.

No âmbito militar brasileiro, não existe qualquer definição oficial que abarque a guerra eletrônica e a guerra cibernética em uma ideia convergente; ao contrário, o que parece é que as forças armadas brasileiras ainda consideram a questão – ao menos doutrinariamente – como dois domínios não correlacionáveis. Contudo, é possível buscar um conceito razoavelmente comum através de uma síntese dialética, analisando dois pensamentos predominantes sobre o tema, mas aparentemente conflitantes – tese e antítese. A primeira via é a de que a convergência ocorre de forma estrita, como defende o Tenente-Coronel da *US Air Force*, Ryan J. Worrell (2020), que afirmou: "Esses conceitos – CO e EW – são dois lados da mesma moeda", visto que qualquer ação eletrônica pode ser suprimida por uma ação cibernética e vice-versa, como se a separação dos ambientes eletromagnético e cibernético fosse mais formal do que prática. A segunda via afirma que não ocorre uma convergência, num sentido literal, *stricto sensu*, mas uma coordenação entre os dois domínios, conforme o Major do *Marine Corps*, Devlin O'Shea (2017), explica: "Esses dois campos têm semelhanças e aspectos sobrepostos, mas, em última análise, são independentes um do outro", além de que uma convergência operacional seria prejudicial para missões e nada efetivo. Como se vê, há, dentro desse espaço teórico, dois tipos de pensamentos sensivelmente controversos a respeito do fenômeno da convergência, mas o que se conclui é que, de fato, existem conexões tangíveis e inextrincáveis entre os dois lados em questão e que a ideia da interseção, seja compreendida como uma convergência tênue ou uma poderosa coordenação, emerge de forma evidentemente firme e gradativa.

Além disso, o conceito de convergência entre os aspectos eletrônico e cibernético pode ser derivado de outro conceito fundamental que está contido na Revolução nos Assuntos Militares[6] (RAM): a guerra centrada em rede. À vista disso, a guerra centrada em rede, ou NCW – sua sigla em inglês, *Network Centric Warfare* – pode ser definida como ações que buscam a supremacia no domínio da informação, seja por intrusões em computadores, pelas interferências em equipamentos de telecomunicações, pela destruição física de antenas e camuflagem de unidades e instalações (Teixeira, 2009, p. 74). Em outras palavras, a NCW transforma superioridade de informações em poder de combate, pela interligação de todas as entidades que produzem algum tipo de conhecimento relevante no espaço de batalha e em tempo real – soldados, navios, aviões etc –, com a finalidade de obter maior consciência

[6] Revolução nos Assuntos Militares é um conceito empregado para definir o processo histórico de transformação das técnicas militares e da natureza da guerra que foram motivadas fundamentalmente pela integração de alguma nova tecnologia de combate ou de alguma mudança específica de organização ou até mesmo de ambos (Teixeira, 2009, p. 51-52).

situacional e sincronização de ações, ao mesmo tempo que impede o adversário do mesmo, explorando os domínios da computação (guerra cibernética), das emissões eletromagnéticas (guerra eletrônica) e adicionalmente das técnicas de dissimulação e camuflagem (a técnica russa de Maskirovka[7]) (Teixeira, 2009, p. 74). Portando, de forma exemplar, a convergência pode ser compreendida dentro do conceito da guerra centrada em rede.

4.2 Tecnologia da Convergência

Conforme foi abordado no discorrer das seções acima (mais explicitamente no quadro 1), os ambientes em que ocorrem a guerra eletrônica e a guerra cibernética são como dois mundos distintos. Enquanto a primeira ocorre livremente no mundo físico através da propagação de ondas eletromagnéticas no espaço, a segunda existe estritamente dentro do mundo digital por meio de fluxos de dados. A integração entre esses dois espaços não é trivial. Diferentemente dos ambientes terrestre, marítimo e aéreo que eventualmente se cruzam, como, por exemplo, um avião que realiza um bombardeio em terra ou um sistema de defesa costeira que se opõe a um navio, as naturezas do ambiente eletrônico e cibernético não possuem um contato claro, a não ser por duas tecnologias que romperam as fronteiras existentes entre elas e potencializaram os riscos envolvidos na guerra pela informação, quais sejam: *wireless* e automação. Ademais, somado ao fato de que as transformações sociais levam, cada vez mais, a uma maior dependência de computadores e a uma circulação intensa de informações em rede, o impacto dessas tecnologias na modernidade tem crescido em uma razão exponencial.

A tecnologia *wireless*, em termos gerais, é um recurso que permite estabelecer uma rede livre de cabos físicos entre dois ou mais pontos materialmente distantes seja através de radiofrequência, radiação infravermelha ou sinais via satélite. O dispositivo se dá por meio do *Access Point* (Ponto de Acesso), que envia os dados em forma de ondas de rádio para todos os pontos conectados à rede comum (Ribeiro, 2012). Atualmente, a tecnologia *wireless* é popularmente conhecida pela difusão de aparelhos celulares com *bluetooth*, redes *wi-fi*, serviços de telefonia etc., que são responsáveis por fornecer uma miríade de facilidades tais como a conectividade e a comunicação instantânea. Já a automação, por sua vez, serve para controlar, automaticamente e com capacidade de autorregulagem, sistemas de quaisquer

[7] A técnica de Maskirovka, originalmente russa e que traduzida quer dizer “dissimulação”, é um recurso militar que procurar efetuar ilusão em sistemas de detecção através de alvos falsos (Teixeira, 2009, p. 74). De modo análogo, pode-se entender esta técnica como as ações de despistamento mecânico (*chaff*) e eletrônico, já reconhecidamente existentes dentro da doutrina de guerra eletrônica.

naturezas sejam, mecânico, eletroeletrônicos, computacionais etc. (Bayer, 2011, p. 15). Muito comum no meio fabril, a automação hoje é indispensável para o controle da produção mundial agrícola, industrial e comercial cujo volume produzido seria impensável apenas com o esforço humano. De forma superficial, essas são as duas inovações que permitiram a formação de uma área cinzenta comum entre os domínios eletrônico e cibernético, sobre as quais se discorrerá mais detalhadamente a seguir.

No começo da computação, o tráfico de rede acontecia invariavelmente por cabos físicos, o que propiciava ao ambiente cibernético uma característica de estanqueidade em relação ao meio externo. Contudo, com o advento da tecnologia *wireless*, que hoje se estende a, praticamente, quase todos os dispositivos eletrônicos em virtude das diversas facilidades proporcionadas, as redes se tornaram suscetíveis a um novo tipo de dano além do cibernético: o ataque eletrônico. Com os dados agora se propagando no ar, a informação transmitida passa a ser vulnerável à interceptação eletrônica em modens e roteadores *wi-fi*, mesmo que eventualmente a operação tenha se decorrido sem acesso à *internet*. Dentre as técnicas existentes capazes de efetuar invasões em uma rede *wireless* usando-se basicamente de sinais de radiofrequência, estão: *WLAN Scanners*, *Man in the Middle Attack*, Ataque de Inundação UDP, Ponto de Acesso Falso, Ataques *Sniffers*, *Denial of Service (DoS)* e *Port Scanning* (Gonçalves et al., 2021, p. 7) – já tratados acima. Dessa forma, o aumento do uso das de conexões *datalink*[8] e a dependência de sistemas integrados em redes pavimentou o caminho para as medidas de guerra eletrônica intervirem diretamente no espaço cibernético (Worell, 2020, p.7-8).

Não somente o ciberespaço se tornou vulnerável às armas eletrônicas, mas também os equipamentos e dispositivos eletrônicos, com seu avanço culminando na automação, tornaram-se reféns de técnicas e a ataques cibernéticos. O desenvolvimento da engenharia de *software* propiciou uma série de benefícios para a modernidade, tais como o aumento da produtividade, redução de custos, melhor precisão de tarefas e maior segurança do trabalho (Drumond, 2023). Dessa maneira, o trabalho autônomo das máquinas vem "aposentando", gradativamente, seus operadores tradicionais, o que, inclusive, está se tornando cada vez mais tangível para a realidade militar. Possuir um sistema de armas

---

[8] *Datalink*, ou enlace de dados, é a segunda das sete camadas do modelo *Open Source Interconnection* (OSI), que basicamente serve para assegurar a transferência confiável de dados entre sistemas conectados em rede. Disponível em: https://www.teleco.com.br/tutoriais/tutorialosi/pagina_6.asp. Acesso em 15 de set. 2023. No meio militar, é amplamente utilizado com o objetivo de evitar ou diminuir o uso de comunicação por voz entre as unidades militares.

completamente autônomo, livre de intervenção ou supervisão humana, capaz de selecionar alvos e engajá-los sem probabilidades de erros é o sonho utópico de qualquer força armada. Apesar de não ter alcançado o estado da arte, o uso armas militares com a integração de IA tem se tornado cada vez mais comuns, como é o caso do famigerado sistema de defesa antimísseis israelense *aerodom* (Beja, 2023, p. 17). Entretanto, apesar dos inumeráveis benefícios de se substituir os riscos humanos pela máquina, é necessário saber que há um custo envolvido, que é a vulnerabilidade cibernética. Uma vez invadido o sistema de algum equipamento eletrônico automatizado, o invasor consegue alterar algoritmos de decisão do programa, como, inclusive, já foi comprovadamente testado em sistemas de navegação de carros autônomos (Fantinato, 2021).

Consequentemente, como se observa, com a aparição da tecnologia *wireless* e com o desenvolvimento da automação, tanto redes de computadores sem fio ficaram suscetíveis a medidas de ataque eletrônico quanto os equipamentos eletrônicos autônomos passaram a ser vulneráveis à ataques cibernéticos. Essa mudança de paradigma favorece uma abordagem que permite apresentar uma clara zona de convergência entre os dois domínios, eletrônico e cibernético, que tem modificado drasticamente não somente a vida civilizada, mas também os preceitos da guerra convencional. Ademais, é nitidamente observável que o constante avanço tecnológico nesse sentido vai abrir ainda mais possibilidades capazes de alterar as condições da guerra no futuro.

4.3 Emprego Militar e Segurança Nacional

A crescente complexidade e interconectividade do modo de vida humano têm provocado profundas transformações no âmbito global, mormente nas esferas política, econômica, social e militar. Esses fatores não foram tão drasticamente afetados desde o advento da bomba termonuclear, que se pode dizer que foi a inovação científica-militar de maior relevância do século XX em razão da magnitude de seu poder destrutivo. No entanto, o século XXI se abre com outras novidades – de cunho bem menos agressivo, mas igualmente importantes – como a circulação de informações através do uso difundido de *smartphones*, da alta adesão de redes sociais, ampliação do mercado de criptomoedas e *blockchain*, a popularização e militarização de drones, o desenvolvimento da inteligência artificial etc. Ou seja, mudanças profundamente ligadas à área eletrônica e digital, que fortuitamente poderão ser exploradas pelas nações em função de seus interesses no jogo político, ou na extensão dele na visão clausewitzana, isto é, na guerra. Não menos importante do que as relações

internacionais, as preocupações internas quanto à segurança nacional também estão em relativa tensão quando outro fator originado no século XXI entra em cena em antagonismo com os Estados, que é o terrorismo.

É notório que, nos tempos atuais, uma série de mudanças tem ocorrido no campo militar, principalmente com a criação de novas armas, equipamentos, treinamento e doutrina. Mas o que se pode dizer sobre a convergência dos domínios eletrônico e cibernético? Anteriormente, quando o domínio eletrônico só afetava a primeira camada do modelo OSI – a camada física –, a guerra eletrônica só conseguia causar efeitos no ciberespaço de forma indireta com o emprego de armas *hardkill*, por exemplo, o uso de armas de energia direcionada, como de pulso eletromagnético ou de microondas de alta potência, em nós físicos de rede (Worrell, 2020, p. 10). Agora, com a abertura do espaço cibernético para as transmissões via *wireless*, a guerra eletrônica passou a trafegar na quarta camada do modelo OSI – a camada de transporte –, o que possibilitou um emprego mais diversificado de armas eletrônicas com o fim de afetar o ciberespaço (O'Shea, 2017, p. 20). Dessa forma, para melhor detalhamento, é imprescindível seguir com alguns exemplos concretos e aplicações de emprego militar.

Um dos evidentes produtos resultantes da convergência são os meios que foram estruturalmente modificados para servir aos dois empregos, eletrônico e cibernético, como é o caso da aeronave de ataque eletrônico EC-130H da *US Air Force*, também chamada de *Compass Call*, apresentada na figura 3. Essa aeronave que antes operava basicamente com fins de guerra eletrônica, com grande capacidade de realizar bloqueio eletrônico de comunicações, radar, e sistemas de navegação inimigos, agora, em sua última modernização, recebeu um aprimoramento em seu sistema de ataque para transmitir códigos maliciosos de computador para dispositivos sem fio usando basicamente radiofrequência (Theohary; Hoehn, 2019). Nesse tipo de ataque, pode-se injetar códigos maliciosos de computador mesmo em redes fechadas – isto é, sem acesso à *internet* – desde que esteja recebendo emissões em radiofrequência. Adicionalmente, o efeito pode variar desde ataques de negação de serviço (DoS) até danos físicos a componentes de computador.

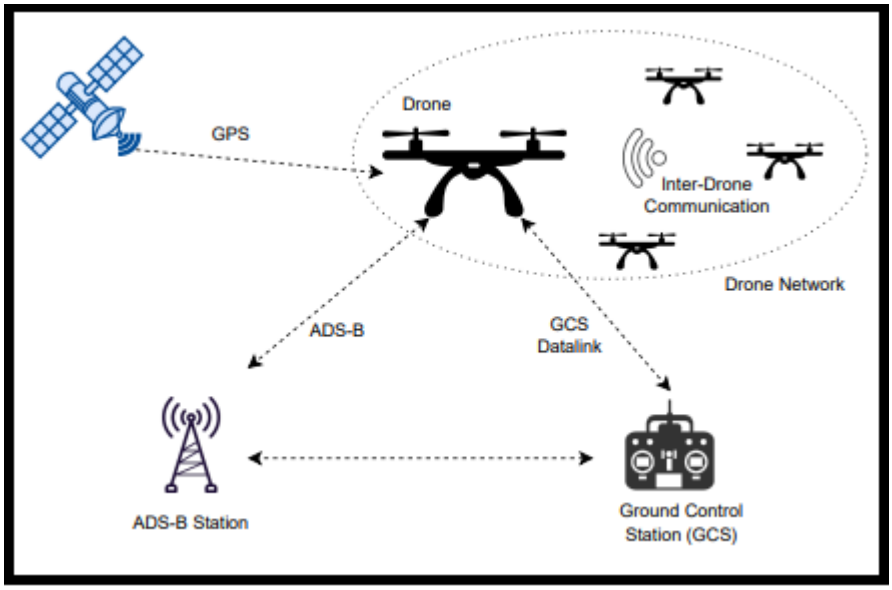
Fig 3 – Aeronave EC-130H

Fonte: Theohary; Hoehn (2019)

Não somente aeronaves militares de ataque eletrônico estão recebendo atualizações para se adequar à guerra cibernética, mas também uma novidade da guerra do século XXI está se apresentado bastante receptiva à mudança: os drones. Esses veículos aéreos não tripulados possuem, em geral, tarefas que vão desde operações militares, como inteligência, vigilância, aquisição e reconhecimento de alvos, até aplicações civis, como monitoramento, busca e salvamento, jornalismo, transporte e usos recreativos. Em seu emprego militar, os drones originalmente sempre estiveram imersos na guerra eletrônica em virtude do poder de coletar informações de inteligência eletrônica (ELINT) e efetuar ataques eletrônicos sobre comunicações, radares e sistemas eletrônicos diversos (Frackiewicz, 2023), e também por ser suscetível aos mesmos tipos de ataques em virtude de sua alta dependência de sinais[9] de rádio e *wi-fi*, como exposto na figura 4. Fora isso, os drones também estão recebendo atualizações para serem empregados na guerra cibernética com a instalação de *softwares* maliciosos capazes de transmitir *malwares* para redes (Frackiewicz, 2023). Inclusive, já existem kits instaláveis em drones que os habilitam ao emprego eletrônico-cibernético, como é o caso do *SkyJack*, que permite aos drones detectar, desconectar e assumir integralmente o controle de outros drones via *wireless* e de forma completamente autônoma, com possibilidade de "recrutar" um exército de drones zumbis (Hartmann; Giles, 2016). A proposta de equipar drones com essa capacidade é altamente vantajosa para o meio militar.

[9] Os drones possuem tipicamente pelo menos três tipos de comunicações, quais sejam: redes de estações de controle terrestre (GCS), de sistemas de controle de tráfego aéreo (ADS-B), e de sistemas de navegação por satélite (GPS). Adicionalmente, alguns drones mais sofisticados podem possuir comunicações extras, tais como redes entre drones (Sihag et al., 2023).

Fig 4 – Arquitetura típica de drones



Fonte: Sihag et al. (2023)

Por outro lado, diversos equipamentos eletrônicos têm se demonstrado vulneráveis a ataques cibernéticos em virtude da dependência de sistemas informáticos para gerirem suas operações no espectro eletromagnético. Por exemplo, os radares de varredura eletrônica ativa (AESA) tem como característica principal a capacidade de controlar eletronicamente a direção do feixe de radar sem a necessidade de movimento mecânico da antena. Eles utilizam um tipo de antena faseada com vários elementos ativos cujos módulos de transmissão e recepção são controlados por computador. Semelhantemente, os rádios definidos por *software* (RDS), que dependem de um sistema eletrônico controlado por *software*, fazem o processamento e modulação do sinal digitalmente – ao invés do aparato físico de um rádio convencional. Em ambos os equipamentos, uma eventual intrusão maliciosa no sistema pode alterar as configurações pré-ajustadas e deteriorar o desempenho padrão, como atenuar a intensidade dos feixes radar em determinada direção desejada ou impedir que rádios recebam transmissões em uma frequência específica (Theohary; Hoehn, 2019).

Em relação à segurança nacional, diferentemente da questão militar, os interesses internos são mais levados em consideração para a implantação de políticas públicas que promovam a proteção do patrimônio nacional. E, não diferentemente da questão militar, um mundo mais digital e interconectado favorece um ambiente mais complexo e sensível com as pessoas cada vez mais dependentes de sistemas de comunicações além da existência de infraestruturas vitais para o funcionamento comum da sociedade. Contudo, toda questão em

torno do assunto da segurança nacional reside na problemática entre a convergência existente e a soberania nacional, isto é, o limite “fronteiriço” do espaço cibernético impulsionado pelas emissões eletromagnéticas em relação à autonomia de um país sobre seu território. Por isso, a valorização da informação bem como a infraestrutura moderna de serviços junta à realidade de novas ameaças transnacionais e do inerente terrorismo digital estão diretamente correlacionados com a fragilização da segurança nacional dos povos (Wesley, 2013).

Nesse sentido, sabe-se que, atualmente, a capacidade alcançada pela guerra cibernética não se limitou a apenas promover o roubo de informações, mas também a desestabilizar infraestruturas críticas de cunho vital para uma determinada região. Dentro desse contexto, pode-se entender que serviços essenciais como energia, transporte, telecomunicações, abastecimento de alimentos e água e sistemas financeiros estão gradativamente ficando mais suscetíveis a este gênero de ataque à medida que se automatizam. Um caso emblemático foi o ataque *hacker* a três centros de controle elétrico na Ucrânia em 2015, que provocou um *blackout*. para cerca de 225 mil pessoas em todo o país por várias horas (Whitehead et al., 2017). Em resumo, as empresas ucranianas foram vítimas de um ataque que incluiu inicialmente técnicas de engenharia social por *e-mails* fraudulentos que habilitavam o acesso à rede interna da central (*spear phishing*) até o estabelecimento de controle remoto das estações efetuando a interrupção de energia (Whitehead et al., 2017). Segundo Pate-Cornell, et al. (2018), o sucesso da invasão *hacker* se deu muito em favor do nível de automação e conectividade das redes de distribuição de modo que os invasores conseguiram não apenas migrar da rede corporativa para a rede de controle com facilidade (visto que a conexão se dava por roteadores simples), mas também conseguiram abrir os disjuntores de 30 subestações de forma completamente remota por sinais de rádio. Logo, uma rede inteligente pode oferecer um serviço com maior eficiência e baixo custo ao passo que ganha maior exposição a ataques ciber-eletrônicos.

Não obstante, o domínio espacial também é severamente afetado pelas ações decorrentes do binômio eletrônico-cibernético. Os satélites são operados por estações terrestres por meio de um transponder que transmite e recebe sinais de radiofrequência da estação. Esses sinais geralmente servem para enviar comandos diretos para o satélite manter sua posição em órbita. Entretanto, sistemas do satélite não são completamente seguros, havendo ações que visam provocar danos ou perda de controle. Uma delas consiste na possibilidade de algum oponente, furtivamente, invadir os computadores da estação terrestre controladora e transmitir, por meio dela, códigos de comando alternativos ao satélite, forçando-os sair de posição ou desligando seus sistemas críticos (Theohary; Hoehn, 2019).

Isso exige um grande preparo para realizar tarefas complexas, como enganar o receptor GPS do satélite e resolver desafios de criptografia. Um caso semelhante ocorreu quando *hackers* éticos invadiram o sistema de um satélite da Agência Espacial Europeia para testar sua cibersegurança (Brandão, 2023).

Assim sendo, é impressionante a dimensão alcançada pelo poder que equipamentos e técnicas conseguiram produzir ao integrar recursos do espectro eletromagnético e do ambiente cibernético em um só plano. Meios militares estão sendo atualizados para esse novo tipo de confronto ao passo que equipamentos já em uso estão tendo suas medidas de proteção repensadas para se adequar às novas ameaças. Também, a existência de serviços públicos automatizados, apesar de todo benefício que proporcionam, estão prestes a se tornar alvos cada vez mais frequentes de terrorismo e vandalismo digitais. Logo, não somente os Estados e suas forças armadas absorvem a necessidade de se preparar para os desafios dessa convergência, mas também a vida humana em sociedade passa a estar sujeita ao risco essa nova realidade. Com isso, numa projeção futura, desafios e riscos serão inerentes ao curso dessa atividade ao mesmo tempo que questões éticas e legais devem ser discutidas a fim de promover a proteção da vida e a limitação de danos.

4.4 Perspectiva futura: Desafios e Riscos

À medida que o mundo se desenvolve tecnologicamente com adversários geopolíticos modernizando suas forças militares e grupos digitais sediciosos aumentando em quantidade e alcance, emerge o imperativo para a resolução de novos problemas gerados dos meios cibernético e eletromagnético. Esses problemas constituem os desafios que, em primeiro lugar, exigem uma resposta imediata dos Estados nacionais a fim de proteger sua soberania dos diversos atores contemporâneos desse ambiente complexo e multifacetado; e, em segundo lugar, os riscos que afetarão, em maior proporção, as próximas gerações, que viverão em um mundo sob os efeitos das ações providenciadas no presente. Dessa maneira, para abordar esse assunto com maior profundidade e clareza, deve-se separar os tópicos na seguinte lógica: desafios político-estratégico, operativo-tático e tecnológicos; e riscos individuais e coletivos.

O desafio central em torno da questão da convergência começa, prioritariamente, no âmbito político-estratégico. O nível mais alto de decisão de um Estado é responsável por determinar as diretrizes oficiais do interesse da alta administração estatal para a atividade da guerra de modo a permitir que os órgãos operativos subordinados desenvolvam, de forma

apropriada, a pesquisa, a doutrina e treinamento. Logo, a conscientização acerca do tema pelas autoridades estatais competentes é o fator primordial que, invariavelmente, decide o nível de esforços e recursos empregados sobre os assuntos militares. Conforme já visto nas seções acima, os países mais avançados na questão militar tiveram a percepção da existência de uma convergência cada vez mais estreita entre a guerra eletrônica e a guerra cibernética a ponto de se reorganizarem administrativamente para se adequar à realidade emergente, como os EUA, Rússia e até mesmo outros países de menor expressão geopolítica[10]. Nos EUA, por exemplo, observa-se um estreito envolvimento institucional para promover o avanço da atividade:

> A versão do Senado da Lei de Autorização de Defesa Nacional para o ano fiscal de 2023 orientou o Pentágono a desenvolver uma estratégia para a guerra cibernética e eletrônica convergente conduzida por meios militares e de inteligência destacados. (Pomerleau, 2022)

Da mesma maneira, os desafios ligados à área operativa e tática não devem ser desprezados, visto que a construção da doutrina e aplicação de treinamento são pré-requisitos fundamentais para o desempenho de qualquer força armada para o combate. Por exemplo, em virtude das evidentes diferenças em cada domínio (eletrônico e cibernético), é imprescindível que o nível de coordenação tático entre os diferentes meios de uma força esteja perfeitamente ordenado e sincronizado de modo a impedir um possível fratricídio na forma de interferências mútuas (Worell, 2020, p. 9). Também, outro desafio a respeito da convergência, numa perspectiva mais operativa, seria a unificação das equipes de operadores e técnicos de guerra eletrônica e guerra cibernética, visto que os trabalhos de operação e manutenção ocorrendo de forma mais centralizada evitaria duplicação de esforços com objetivos opostos e conflitantes (O'Shea, 2017, p. 18). E de forma mais abrangente, o desafio se intensifica ainda mais ao se tentar integrar os trabalhos do Exército, Marinha e Força Aérea, cujo alinhamento é importante para produzir sinergia e troca de conhecimento (Pomerleau, 2022).

Todavia, mesmo superadas as dificuldades das esferas política-estratégica e operativa-tática, permanece ainda o desafio concernente à sua natureza tecnológica, uma vez que as mudanças decorrentes da convergência estão em rápido e constante desenvolvimento. Em relação a isso, há um sem-número de inovações do campo científico na atualidade que

---

[10] Por exemplo, a Austrália, em sua organização administrativa militar, possui um órgão que contempla a guerra eletrônica e a guerra cibernética em uma única divisão chamada *Cyber and Electronic Warfare Division*. Disponível em: https://www.dst.defence.gov.au/divisions/cyber-and-electronic-warfare-division. Acesso em 25 set. 2023.

impactam diretamente os equipamentos eletrônicos e o ambiente cibernético, quais sejam, inteligência artificial, computação quântica, redes 5G e 6G, inteligência das coisas etc. A inteligência artificial (IA), impulsionada pelas funções de *machine learning* e *deep learning* e análise de *big data*, alcançou uma envergadura sem precedentes no mundo digital, sendo hoje o suprassumo da automação (Bittencourt, 2019). Em princípio, a IA pode fornecer inúmeras aplicações para a defesa cibernética, com seus algoritmos de aprendizado, poder de computação e dados disponíveis (Guyonneau; Le Dez, 2019, p. 109). Não somente isso, a IA propicia um nível formidável de autonomia aos equipamentos eletrônicos para classificação de alvos através da otimização da análise de sinais e inferência de sinal, com aplicações para a coleta, interpretação e análise de informações (ELINT, MASINT), simulação de guerra e veículos não tripulados (Sharma et al., 2020).

Outro fator que será determinante para os desafios tecnológicos relativos à convergência é a internet das coisas (IOT). A conectividade em profusão é a nova realidade da internet das coisas, que propicia a integração de diferentes dispositivos sob uma rede comum. As principais características de dispositivos IOT são: operação sem supervisão humana, comunicação através de redes sem fio e incapacidade de suportar esquemas de segurança complexos (Abomhara; Køien, 2015, p. 68). Por isso, em virtude desses aspectos, claramente se deduz a existência de fragilidade de sistemas IOT e o aumento da superfície de ataque principalmente de cunho eletrônico-cibernético, como negação de serviço (DoS) e ataques de acesso remoto (Abomhara; Køien, 2015, p. 73). Outras tecnologias que estão intimamente relacionadas – já existentes ou em desenvolvimento – tais como a tecnologia quântica[11], redes 5G e 6G[12], *smart cities*[13] e *blockchain*[14], associados à IA e à IOT, comporão

[11] A tecnologia quântica – ou mais especificamente a computação quântica – é uma inovação em desenvolvimento que tem o potencial de elevar exponencialmente a capacidade atual de processamento computacional. Em suma, ela pode fornecer vantagens para a guerra cibernética como os vetores de ataque às atuais criptografias assimétricas (baseadas na fatoração de inteiros, no logaritmo discreto ou no problema do logaritmo discreto de curva elíptica) (Krelina, 2021, p. 24). Para a guerra eletrônica, é possível que a melhor contribuição seja o desenvolvimento de analisadores de espectro de RF aprimorados (Krelina, 2021, p. 35).

[12] As tecnologias de redes de telecomunicações 5G (quinta geração) e 6G (sexta geração) – esta última ainda em desenvolvimento – vão expandir abruptamente as capacidades de conexão e transmissão de dados. Com isso, uma maior dependência de *software* e expressiva quantidade de pontos de entrada abrem inúmeras possibilidades para ataques ciber-eletrônico. E isso, somado aos fatos de que muitos dispositivos estão sendo fabricados com segurança insuficiente e de que desde o início do processo de conexão existe certa deficiência de criptografia, agrava sobremodo os riscos associados à tecnologia (Oliveira, 2021, p. 9).

[13] As *smart cities*, isto é, cidades inteligentes, são áreas urbanas tecnologicamente modernas que são conectadas através de muitas redes de *software*, comunicação e interface (IOT) para fornecer uma infraestrutura de serviços públicos inteligente para a sociedade (Matuszak, 2023). Logo, se o nível de conectividade é diretamente proporcional ao nível de vulnerabilidade eletrônica-cibernética, então as *smart cities* são um dos principais desafios a se enfrentar, principalmente quanto à segurança de privacidade e de infraestruturas críticas.

a lista de desafios atinentes à revolução tecnológica em curso que impactará inexoravelmente a zona de convergência eletrônica e cibernética.

Além disso, a consideração de riscos deverá ser constante no processo de convergência, sendo esses individuais ou coletivos. Os riscos individuais se resumem àqueles relativos às pessoas comuns, no que tange, principalmente, à privacidade. Como tem se tornado comum, dados pessoais cada vez mais circulam livremente por redes diversas, o que faz com que informações privadas fiquem o tempo todo expostas a ataques de invasores cabendo às medidas de segurança impedirem tal acesso. Uma evidência disso é o *malware Chameleon*, criado na Universidade de Liverpool, que tem a capacidade de se transmitir via redes *wi-fi* ativas, infectando estrategicamente pontos de acesso, o que lhe dá um forte potencial de criar uma epidemia digital agressiva (Cannell, 2014). Já os riscos coletivos residem no nível segurança do patrimônio comum. Em relação a estes, cabem às autoridades corporativas assegurarem a preservação do bem público cuja instabilidade pode provocar danos severos para a vida em sociedade. À vista disso, sabe-se que, nos últimos anos, setores vitais receberam fortes investimentos de tecnologia IOT, como a saúde e o agronegócio (Fulgêncio, 2023), sobre os quais um ataque sistêmico poderia causar efeitos drástico para a população de determinada região.

Dessa forma, fica exposto que resta ainda grandes lacunas para prever os efeitos finais do fenômeno da convergência. À proporção que as guerras eletrônica e cibernética continuam a se desdobrar, é inevitável que surjam desafios significativos e riscos complexos. O futuro tem reservado um cenário em que as operações militares e de segurança nacional serão cada vez mais dependentes de tecnologias avançadas, como a inteligência artificial, as redes 5G e 6G, a computação quântica, entre outros. Logo, é crucial que haja uma conscientização nacional acerca da necessidade de desenvolvimento de pesquisa voltada para os setores estratégicos e táticos da nação. Enquanto isso, resta encontrar o delicado equilíbrio entre a aplicação da ciência e tecnologia para o conforto humano e a segurança face às ameaças de um mundo cada vez mais interconectado e digitalizado.

---

[14] A tecnologia *blockchain* é uma estrutura cujos dados são armazenados em blocos com cada bloco vinculado a outro, linearmente, utilizando um link criptográfico para formar uma cadeia (Ossamah, 2020, p. 5). Por depender de criptografia como mecanismo de segurança, o *blockchain* possui uma lógica que garante alta proteção de dados, podendo, inclusive, ser utilizado como segurança cibernética para dispositivos IOT (Ossamah, 2020, p. 3).

4.5 Considerações Éticas e Legais

A paz e a segurança internacionais sempre foram preceitos fundamentais que regeram as relações entre países, blocos e alianças. Todavia, isso jamais foi possível sem o esforço contínuo de estabelecer um grau de cooperação entre as nações na forma de tratados e convenções internacionais. Nesse contexto, a atual temática da convergência entre a guerra eletrônica e cibernética tem suscitado um espaço para discussões na esfera ética e jurídica, principalmente em razão das características anárquica e transnacional do ciberespaço. O uso irregular do ambiente cibernético impulsionado em alcance pela propagação no espectro eletromagnético tem requerido um diálogo a fim de delimitar a margem da legalidade no que diz respeito à relação entre os Estados e ao direito do cidadão comum. No mais, é extremamente necessário o enquadramento jurídico das possibilidades da convergência, visando a garantia das liberdades individuais, da soberania nacional, dos direitos humanos e demais convenções universais.

Eticamente, a convergência pode ser tratada segundo os parâmetros do conceito filosófico-militar da *guerra justa*. Em síntese, para efeito de guerra justa, qualquer ação visando a esse fim deve ter, pelo menos: uma autoridade para legitimar a ação, causa justa e intenção justa (Carneiro, 2016). Portanto, tal princípio preconiza apenas Estados como atores contemporâneos legítimos para o emprego da força além de condenar a arbitrariedade para tomada de ações. Além disso, o princípio do duplo efeito também pode ser válido para determinar a qualidade ética de um ataque. Para isso, deve-se considerar a proporcionalidade e os efeitos colaterais de um ataque (Carneiro, 2016). Por isso, a questão ética pode ser desafiadora para a convergência principalmente quando se tem a existência latente do terrorismo no ciberespaço que repetidamente ignora a legitimidade do Estado bem como da comunidade internacional, além de práticas como a espionagem e a sabotagem irrestritas que ferem o direito à privacidade de pessoas comuns e põem em risco vidas humanas dependentes de determinadas infraestruturas críticas vitais.

A Convenção de Budapeste foi o primeiro tratado internacional que buscou abordar o problema da cibercriminalidade e oferecer às legislações nacionais princípios gerais, melhorar as técnicas de combate às infrações e aumentar a cooperação entre os países (Lima, 2017, p. 40). Entretanto, o Brasil não foi convidado a aderir à Convenção – visto ser um Comitê fechado –, o que, contudo, não impede o país de criar uma legislação apropriada para o combate de crimes na *internet*. Nesse sentido, a necessidade de criar tais leis deve acompanhar o respeito absoluto por princípios fundamentais. Por exemplo, o Projeto de Lei

Substitutivo do Senador Eduardo Azeredo (PSDB-MG) sobre crimes cibernéticos que visava "tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares" estabelece um Estado supervigilante e um amplo policiamento digital, comprometendo, inclusive, dados alheios a possíveis empresas transnacionais, caindo numa flagrante desconsideração aos direitos de privacidade e da soberania nacional (Souza; Pereira, 2009).

Em suma, os princípios da soberania nacional e de direitos humanos não devem ser vilipendiados frente às ações contra o crime da era digital. De fato, o conceito de território nacional é completamente inadequado se tratando do ciberespaço, cujas características são de um ambiente transnacional e anárquico. Com efeito, a presença de atores não estatais e do terrorismo digital utilizando armas cibernéticas afrontam a soberania nacional dos países. Diante disso, muitos Estados têm exercido jurisdição penal sobre cibercrimes e regulado inúmeras atividades no ciberespaço (Barros, 2018, p. 145). Todavia, deve-se lembrar que a condição *sine qua non* para o reconhecimento e consolidação da soberania nacional é a própria cooperação dos atores internacional, que, à vista disso, devem somar esforços contra cibercrimes. Em relação aos direitos humanos, os Estados são responsáveis por sua garantia frente a atores não estatais e frente à sua própria atuação, em caso de excessos. A necessidade de monitoramento não deve superar os direitos fundamentais, tais como o direito à privacidade, a liberdade de expressão e o acesso à informação.

Face ao exposto, é necessário entender que os principais desafios éticos e legais sobre o tema da convergência residem na atuação de atores estatais e não estatais diante de princípios jurídicos universalmente estabelecidos como a soberania nacional e os direitos relativos à liberdade individual. Os direitos fundamentais do ser humano não devem ser violados sobre o pretexto de segurança jurídica, mas sim protegidos. O Estado deve procurar intensificar e estreitar a cooperação internacional de modo a conter os crimes e enfraquecer o terrorismo, hoje em franca atividade no ciberespaço. Destarte, entende-se que é preciso tratar os aspectos jurídicos e éticos do tema da convergência com máxima responsabilidade e equilíbrio possíveis.

2.5 O FUTURO DA MARINHA DO BRASIL: IMPLICAÇÕES DA CONVERGÊNCIA E UMA REFLEXÃO SOBRE A ESTRATÉGIA NACIONAL DE DEFESA.

O mar desempenha um papel fundamental na história, economia e segurança do Brasil, destacando-se como um dos principais elementos que moldaram a identidade nacional. Com uma extensa linha costeira que se estende por mais de 8.500 quilômetros, o país possui uma vasta riqueza de recursos marinhos que incluem petróleo, gás natural, minerais, peixes e uma biodiversidade única. Por causa disso, praticamente 95% do comércio marítimo ocorre em via marítima além de que 90% do PIB nacional e 93% da produção industrial se concentram na zona costeira brasileira (Biazon, 2017, p. 5). De fato, o Brasil é uma nação eminentemente marítima, o que lhe propiciou criar o conceito estratégico para denominar a porção de águas que compreende seu território marítimo de "Amazônia Azul"[15]. Com efeito, além do seu valor econômico, o mar também exerce uma utilidade crucial na defesa e segurança do país, sendo o cenário das operações da Marinha do Brasil, que protege as águas territoriais e garante a soberania nacional, conforme expresso na Estratégia Nacional de Defesa:

> [...] 3.6.2 A Marinha do Brasil tem como missão preparar e empregar o Poder Naval, a fim de contribuir para a defesa da Pátria; para a garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem; para o cumprimento das atribuições subsidiárias previstas em lei; e para o apoio à política externa (BRASIL, 2020, p. 47).

Em contrapartida, o crescimento do tráfego marítimo com o número crescente de embarcações no mar está intimamente relacionado à automação e conectividade dos meios. A indústria naval está construindo navios cada vez mais modernos, automatizados, com sistemas mais funcionais e integrados. A automação e a conectividade dos meios permitem diminuir os custos operacionais de manutenção de meios e aumentar a eficiência e, com isso, elevar a produtividade e otimização de serviços. Essa revolução digital tem impactado positivamente a operação de navios tanto comerciais quanto militares, como, por exemplo, a substituição (ou

[15] Amazônia Azul é a região que compreende a superfície do mar, águas sobrejacentes ao leito do mar, solo e subsolo marinhos contidos na extensão atlântica que se projeta a partir do litoral até o limite exterior da Plataforma Continental brasileira. Ela deve ser interpretada sob quatro vertentes: econômica, científica, ambiental e de soberania (Brasil, 2020, p. 75).

complementação) das cartas náuticas impressas pelo ECDIS[16]. Hoje, em virtude do advento da IA, de *softwares* mais sofisticados e de sensores mais precisos, já é possível viabilizar a construção de navios autônomos ou remotamente pilotados, o que parece ser uma tendência global irrefreável (Faria et al., 2022). Contudo, conforme já mencionado, meios com este nível de automação são mais propensos a ataques ciber-eletrônicos à medida que se desfazem do trabalho humano para obter autonomia.

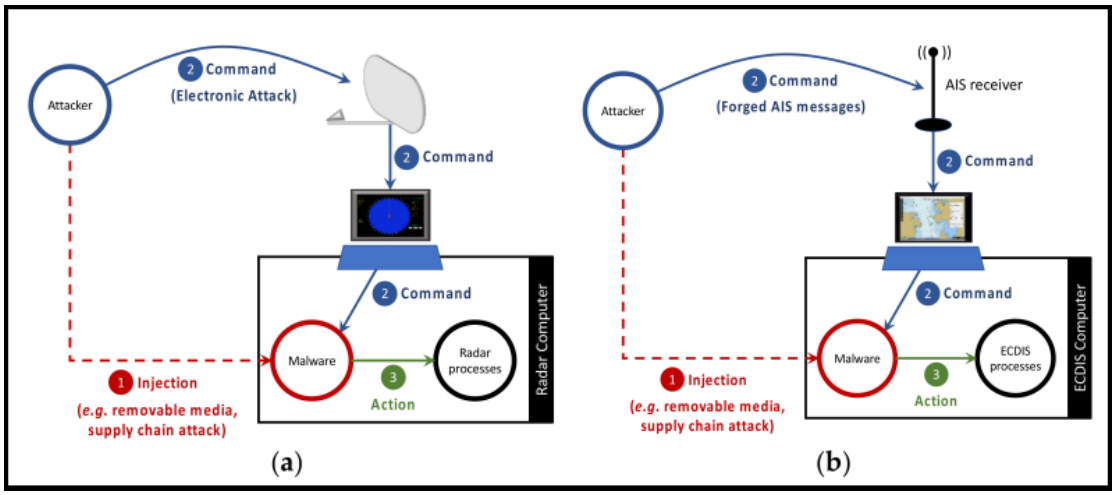
Os sistemas de radar para os meios marítimos são utilizados como sensores fundamentais para a segurança da navegação ou como fonte de informação para sistemas de navegação integrados. Inclusive, um sistema de radar ineficiente pode causar sérios riscos à segurança das embarcações, podendo resultar em acidentes, prejuízos econômicos, poluição e perdas de vida humana. Uma das causas que pode reduzir a confiabilidade de um sistema radar é justamente a possibilidade de ataques ciber-eletrônicos. Por exemplo, Israel já conseguiu desencadear um ataque cibernético no sistema computacional de um radar sírio por meio de um ataque eletrônico, com o envio de comandos falsos para o radar através do espectro eletromagnético, o que possibilitou um posterior ataque cinético aéreo sem ser notado (Junior et al., 2021). Por isso, a injeção de dados falsos em sistemas de radar com operação remota tem preocupado a gestão militar. Não à toa, a mesma preocupação se aplica ao AIS dos navios, cuja função é fornecer informações de outras embarcações como posição, identificação etc. Como esses sistemas são, via de regra, integrados a sistemas radar e ECDIS, sua carência de mecanismos de segurança pode afetar a segurança da navegação em geral.

Hoje, há mecanismos pelo qual um invasor localizado fora do navio, a uma distância razoável, consegue explorar a antena de sistema de radar ou o receptor de AIS a bordo como portas abertas para, remotamente, por pulsos eletromagnéticos, enviar comandos desejados para um *malware* hospedado no sistema, mesmo que os sistemas do navio não estejam conectados a outras redes (Junior et al., 2021, p. 2). Na figura 5, pode-se entender como funciona a cinemática de um ataque a sistemas de navegação a bordo. Primeiro, o invasor realiza a injeção do *malware* no sistema alvo por métodos furtivos (mídias removíveis ou cadeia de fornecimento), depois envia ao *malware*, de forma remota, um comando forjado e, por fim, o *malware* manipula o radar ou o computador do ECDIS conforme o comando

[16] ECDIS (Sistema Eletrônico de Informações e Exibição de Cartas, em português) é um sistema de cartas eletrônicas usado em navegação por navios. Inclui também informações integradas com o GPS e outros sensores como o AIS.

transmitido pelo invasor[17] (Junior et al., 2021, p. 6). Há um outro tipo de ataque especial, chamado *"meacoming"*, segundo o qual ciberinvasor rastreia e registra as emissões eletromagnéticas entre o satélite e o navio, como o sinal GPS, e o retransmite como um sinal mais forte e com atraso ao navio alvo, fazendo o receptor ler o sinal falso dominante (Mednikarov, 2020, p. 37). Dessa forma, percebe-se que a integração de sistemas radar, de identificação automática (AIS), de cartas eletrônicas (ECDIS), de posicionamento global (GPS) e demais tecnologias, apesar das facilidades e da eficiência proporcionadas à operação marítima, fragiliza esses mesmos sistemas a ataques invasores de natureza eletrônica-cibernética.

Fig 5 – Padrão de ataque em (a) um radar e (b) um AIS/ECDIS



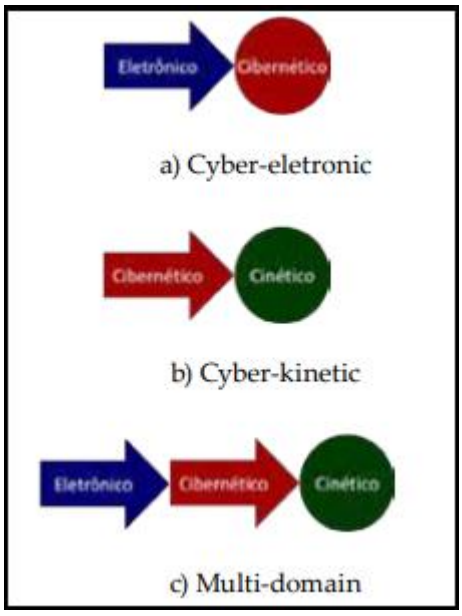
Fonte: Junior et al. (2021)

Esses ataques convergentes no mar são tipicamente voltados para sistemas que integram equipamentos de transmissão e recepção de emissões eletromagnéticas e com sistemas de computador que processam e fornecem as informações, como, por exemplo, os sistemas integrados de passadiço (IBS) ou os chamados sistemas *smartship* (De Sá, 2019, et al., p. 108). Para os meios navais, sistemas integrados têm como vantagens reduzir o tamanho da tripulação, aumentar a prontidão do navio, simplificar o treinamento, elevar a consciência situacional e diminuir a carga administrativa sobre o pessoal. Não obstante, a depender do nível de integração dos sistemas de um navio, um ciberinvasor pode afetar até mesmo o

[17] É possível empreender diversas ações maliciosas em sistemas de navegação com *malware* hospedado, tais como: reiniciar o sistema, interromper a atualização da posição na apresentação radar, ou mesmo gravação e repetição de cenários (Junior et al., 2021, p. 7).

controle da propulsão de um navio através de comandos recebidos por uma antena a bordo[18] (De Sá, et al., 2019, p. 109). Embora esses tipos de ataques ciber-eletrônicos não tenham a capacidade de causar uma destruição massiva sobre um alvo no mar, eles são úteis para preparar ao atacante a oportunidade de um ataque cinético ao debilitar o autocontrole do alvo, caracterizando um estilo de ataque "multidomínio", como representado na figura 6. Portanto, em termos táticos, a convergência impacta diretamente o combate naval, principalmente nos preparativos pré-engajamento cinético.

Fig 6 – Fluxo de ataque multidomínio



Fonte: De Sá et al. (2019)

Além disso, sabe-se que, atualmente, existe certa tendência da indústria naval em desenvolver embarcações autônomas ou remotamente pilotadas para atividades comerciais e até mesmo militares, em proveito de se evitar a necessidade de pôr de vidas humanas em risco. Particularmente, no que tange à indústria da guerra, os meios militares mais demandados foram as embarcações de tamanho relativamente pequeno com propósitos específicos, como por exemplo o *USV Supressor*, construído pela EMGEPROM em parceria com a TIDEWISE, cuja missão é atuar em missões de contramedida de minagem (Padilha, 2022). No entanto, apesar das vantagens inerentes da tecnologia, deve-se considerar que as

[18] Isso pode ser mais comum em navios mercantes modernos onde o a interconexão IBS com sistemas de propulsão e controle de leme permite ao navio funcionar no piloto automático, eliminando até mesmo a necessidade da presença ininterrupta de um timoneiro. A adesão desse método para os meios militares é bastante improvável visto que a prontidão e a vigilância são fatores inegociáveis para a operação naval.

embarcações autônomas ou remotamente pilotadas são naturalmente suscetíveis aos ataques convergentes. A infiltração em sistemas operacionais de veículos autônomos é feita sob a mesma lógica utilizada para invadir sistemas eletrônicos de navegação – conforme explicitado acima. O efeito deste tipo de ataque pode variar desde assunção de controle, alteração de rota, cometimento de ataque suicida ou fratricida, sequestro de embarcação para roubo de tecnologias etc. (Cho et al,, 2022, p. 14).

Desse modo, uma vez que as forças armadas estão cada vez mais modernizadas e dependentes de tecnologias que envolvam o espectro eletromagnético e o ambiente cibernético, é imprescindível adotar medidas de prevenção frente a essas ameaças no cotidiano. Por isso, a Marinha tem empregado esforços positivos nesse sentido, como possuir sua própria rede de dados, chamada de Rede de Comunicações Integradas da Marinha (RECIM), que é a infraestrutura que possibilita o tráfego de informações digitais e analógicas na MB e que interliga todas as redes extra-MB, inclusive o Sistema de Comunicações Militares por Satélite (SISCOMIS), provendo segurança para as comunicações navais[19] (Souza, 2012, p. 33). Também, cabe ressaltar que cada OM centraliza o gerenciamento de redes em militares apropriadamente adestrados para tal serviço, que são as figuras do Oficial de Segurança das Informações Digitais (OSID) e do Administrador de Redes Locais (ADMIN) (Souza, 2012, p. 34).

Outra perspectiva igualmente importante ao emprego tático naval da atividade convergente, é a questão da segurança nacional que cabe à Marinha do Brasil. De acordo com a Estratégia Nacional de Defesa, a Marinha do Brasil tem a responsabilidade de assegurar e defender o patrimônio brasileiro localizado nas águas territoriais, inclusive, contra às ameaças de cunho eletrônico-cibernético:

> [...] 3.6.2 O Poder Naval deve explorar suas características intrínsecas de mobilidade, de permanência, de versatilidade e de flexibilidade. [...] A versatilidade permite alterar a postura militar, mantendo a aptidão para executar uma ampla gama de tarefas. Isto inclui os diferentes níveis de prontidão exigidos pelos vários cenários, as capacidades de operar, ofensiva ou defensivamente, contra alvos nos ambientes aéreo, submarino, superfície, terrestre, cibernético e eletromagnético [...]. As capacidades para controlar áreas marítimas, negar o uso do mar e projetar o Poder Naval terão por foco incrementar a segurança e a habilitação para defender as infraestruturas críticas marítimas, os arquipélagos e as ilhas oceânicas nas águas jurisdicionais brasileiras ou onde houver interesses nacionais, assim como responder prontamente a qualquer ameaça às vias marítimas de comércio (Brasil, 2020, p. 47).

[19] Somado a isso, inclui-se o sistema *Dreadnought* desenvolvido pela Marinha que tem como função segregar o tráfego de redes, realizar análise histórica dos eventos de segurança, identificar, bloquear e reportar ameaças cibernéticas, entre outras capacidades (JUNIOR, 2022).

Nesse contexto, é importante ressaltar que a segurança nacional dentro do âmbito da convergência consiste principalmente na defesa às infraestruturas críticas. No território marítimo, pode-se entender que a principal infraestrutura crítica a proteger, além daquelas que possam se concentrar na faixa litorânea, é a estrutura de cabos submarinos.

Os cabos submarinos de conectividade são a principal infraestrutura crítica localizada no ambiente marinho. Um dano sobre a rede de cabos submarinos de um país pode produzir um colapso sem precedentes em sua estrutura cibernética de conectividade e comunicação, provocando uma reação em cadeia em outras infraestruturas críticas dependentes. Particularmente o Brasil possui sua maior interconexão de dados e de comunicação feita via cabos submarinos, cuja maior concentração encontra-se na região do 3º Distrito Naval (Lopes, 2021). Na verdade, há várias formas de sabotagem nestes cabos marítimos, como o uso de ferramentas de corte, lançamento de âncoras, dispositivos de dragagem, dispositivos explosivos (minas submarinas) etc. Mas também, há também modos mais sofisticados, como a perturbação eletromagnética, conforme descrito em um relatório da OTAN, que cita um método russo que se utiliza de um minissubmarino lançado de meios como contratorpedeiros, fragatas ou navios patrulhas e que tem a capacidade de efetuar técnicas de interferência eletrônica sobre os cabos submarinos (Soames, 2019, p. 4).

Em contrapartida, embora seja claro o entendimento que as implicações cibernéticas se estendem a todos os domínios físicos, inclusive o marítimo, é preciso entender que a Estratégia Nacional de Defesa segrega os setores estratégicos, quais sejam, nuclear, cibernético e espacial, e os divide sob a responsabilidade das três forças armadas em razão da elevada complexidade inerente a cada projeto e, também, da necessidade de uma liderança centralizada. No caso, a responsabilidade do desenvolvimento estratégico do setor cibernético fica a cargo do Exército Brasileiro, enquanto a Marinha do Brasil tem a competência do programa nuclear (Brasil, 2020, p. 59). Logo, com o objetivo de construir uma política de avanço quanto à tecnologia da convergência eletrônica e cibernética, é imprescindível que haja iniciativas no sentido de estabelecer um esforço conjunto por parte do EB e da MB, principalmente por efeito das características que envolvem a natureza de operação de cada força, visto que a maior capacidade de guerra eletrônica encontra-se substancialmente na Marinha e o capital de guerra cibernética reside no Exército.

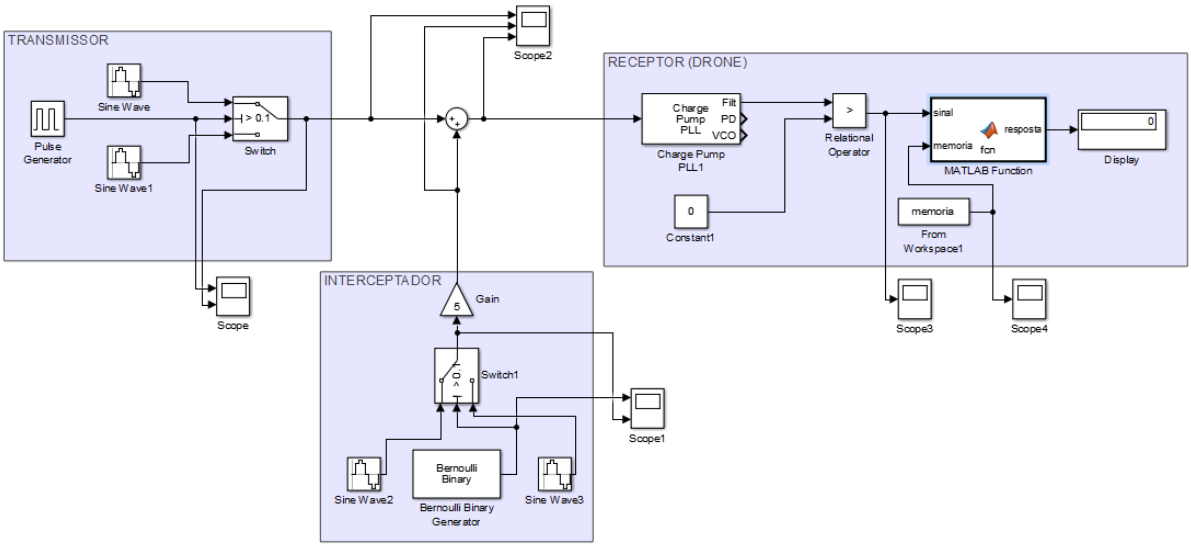
Por conseguinte, o fenômeno convergente entre a guerra eletrônica e a guerra cibernética tem impactos notáveis no ambiente marítimo. Os sistemas integrados de navegação, como ECDIS e AIS, atualmente importantes para a navegação moderna, estão

expostos às possíveis invasões maliciosas; igualmente, pode-se dizer das embarcações autônomas e remotamente pilotadas. Também, o valor estratégico dos cabos submarinos de conectividade como infraestrutura crítica marítima não deve ser subestimado diante da possibilidade de um ataque agressor afetar a segurança nacional. Por isso, é interessante que o Brasil estabeleça uma estratégia de cooperação entre seus organismos responsáveis pela operação eletrônica e cibernética, visto que, em um cenário de hostilidade, quem for mais capaz de atacar e resistir aos ataques convergentes estará em franca vantagem no mundo atual. Logo, não é trivial a ideia de Sun Tzu: em mundo amplamente conectado e digitalizado, uma guerra pode ser previamente vencida sem exposição de tropas ao debilitar a atividade econômica de um inimigo e inabilitá-lo para empregar sua força militar apropriadamente.

6 SIMULAÇÃO DE UMA INTERCEPTAÇÃO ELETRÔNICA COM EFEITOS CIBERNÉTICOS NO SIMULINK (MATLAB)

A simulação proposta visa representar uma interceptação eletrônica com manipulações cibernéticas em dispositivos eletrônicos. Para efeitos de ilustração, foi considerado simbolicamente um drone remotamente pilotado sofrendo interceptação em seu sistema. Para isso, foi utilizado o Simulink, que é uma ferramenta para modelagem, simulação e análise de sistemas dinâmicos. O conhecimento empregado no programa foi com base na pesquisa realizada neste trabalho bem como nos ensinamentos em sala de aula. O objetivo deste programa é simular, de forma básica e genérica, um ataque ciber-eletrônico. Ademais, não está no escopo desta seção representar fielmente os componentes de um drone autônomo ou de um dispositivo eletrônico qualquer, visto que a intenção proposta é mais ilustrativa do que didática. A figura abaixo (figura 7), mostra, de forma holística, o programa realizado e em sequência tem-se as figuras de suas partes separadas (transmissor, interceptador e receptor, respectivamente).

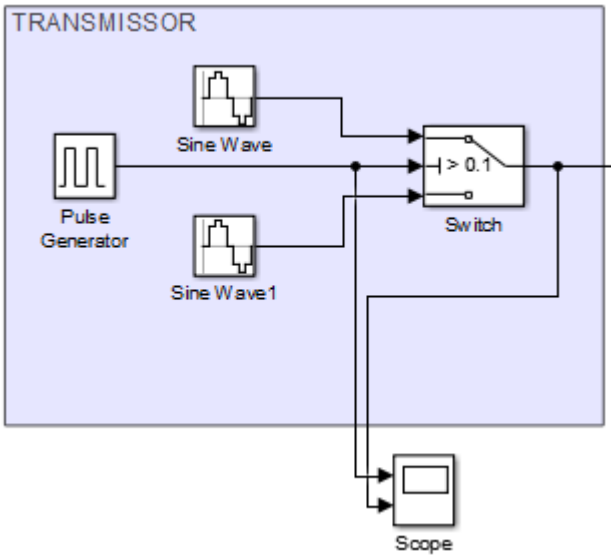
Figura 7 – Visão holística da simulação



Fonte: elaborado pelo autor (2023)

Abaixo (figura 8), é a representação do transmissor que realiza a comunicação e os comandos do operador com o drone (sinal GCS). Optou-se por simular uma transmissão digital modulada em frequência (FSK), bastante típica dos drones modernos. Para isso, utilizou-se um bloco gerador de pulso e blocos de ondas senoidais configuradas de forma discreta como entradas em uma switch. Cabe ressaltar que, para fins de simulação, estabeleceu-se mil amostras por segundo de máquina.

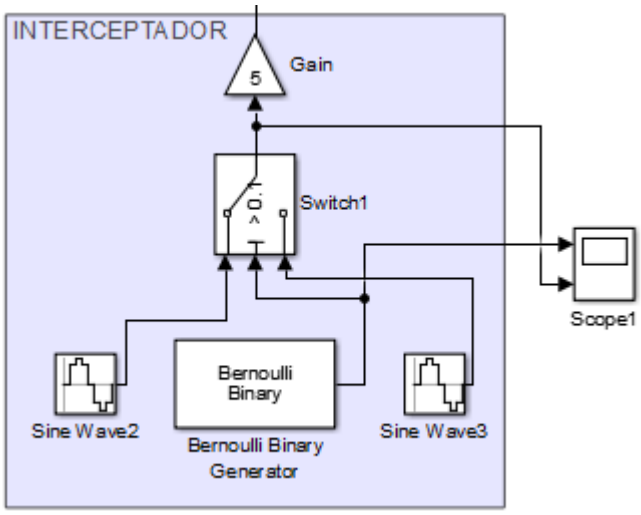
Figura 8 – Transmissor da simulação



Fonte: elaborado pelo autor (2023)

No caso do interceptador (figura 9), procurou-se estabelecer uma configuração que fornecesse um sinal com os mesmos parâmetros do transmissor, mas com uma informação modulada diferente e intensamente mais forte, de forma a se sobrepor ao sinal do transmissor durante a soma. Para isso, foram utilizados um gerador aleatório de Bernoulli, com blocos de onda senoidal como entradas de uma switch além de um amplificador (5x).

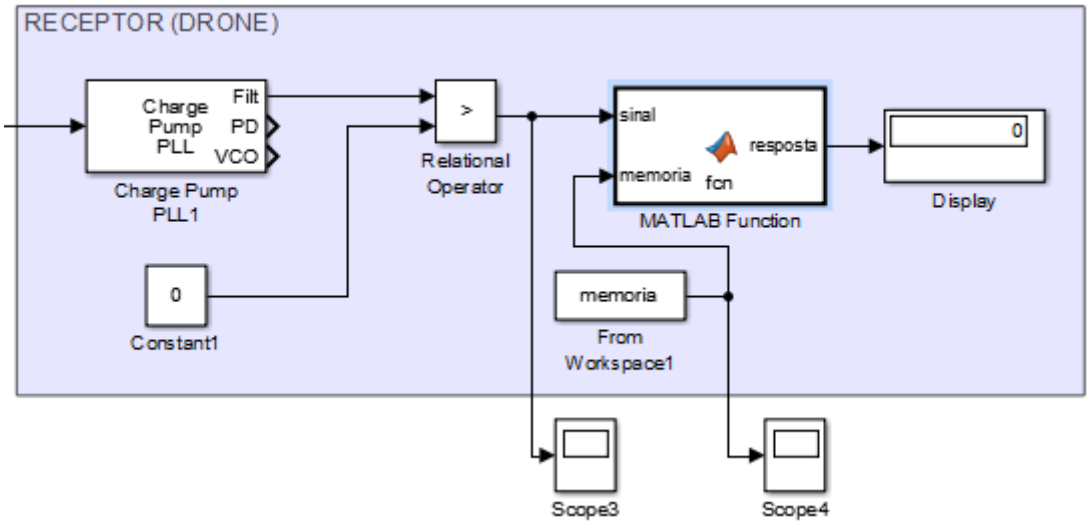
Figura 9 – Interceptador da simulação



Fonte: elaborado pelo autor (2023)

Em relação ao receptor (figura 10), foi preferível fazer um determinado arranjo de blocos que simulasse a demodulação do sinal com sua posterior leitura. Nesse caso, aplicou-se uma função do MATLAB que recebe duas entradas, a saber, o sinal e a memória. A memória consiste num banco de dados previamente determinado com a mesma sequência de informações dos sinais do transmissor. Basicamente, o MATLAB *function* (figura 11), que simula o algoritmo do sistema do drone, faz a correlação do sinal recebido com o padrão esperado na memória. Se o sinal do controlador (transmissor) chegar integralmente ao drone, o receptor processa e sinaliza “cumprir a missão” e envia o comando “1010” para os demais componentes do sistema (atuadores, sensores etc). Se não (em caso de interceptação), aparece a mensagem “abortar a missão” e o comando alternativo “1001” (erro) é enviado para o sistema.

Figura 10 – Receptor da simulação



Fonte: elaborado pelo autor (2023)

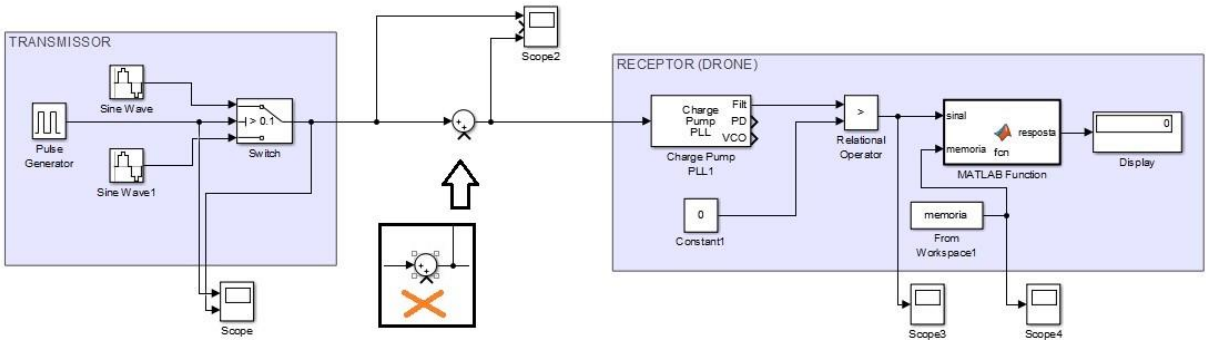
Figura 11 – Algoritmo da simulação

```
function resposta = fcn(sinal,memoria)
%% simulação da leitura da informação
% se resposta 1010, sistema ok; se 1001, erro no sistema (interceptação)
resposta = 0;
if isequal(sinal, memoria)
    disp('Cumprir missão');
    resposta = 1010; % mensagem impressa no display
else
    disp('Abortar missão');
    resposta = 1001; % mensagem impressa no display
end
end
```

Fonte: elaborado pelo autor (2023)

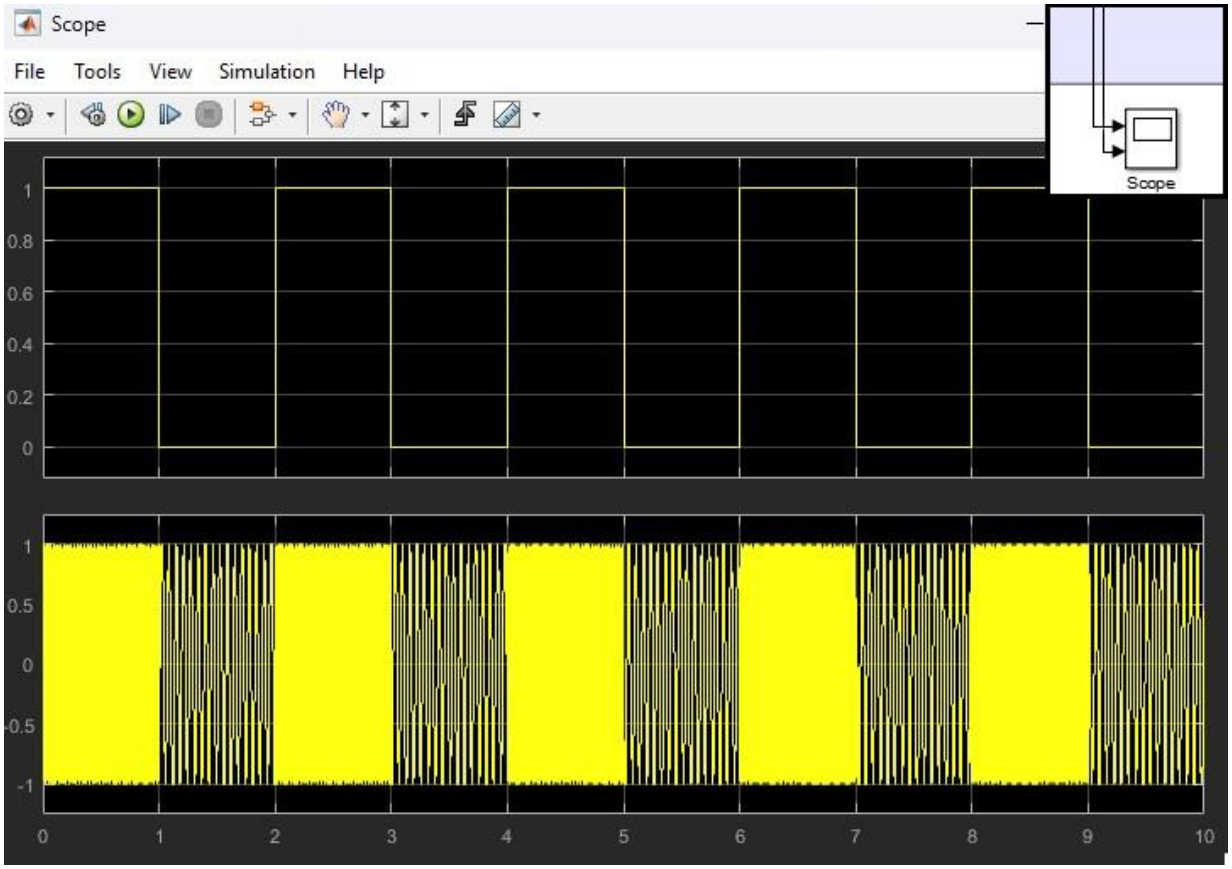
Inicialmente, testou-se a simulação do controle do drone sem interferência (figura 12). Pode-se atestar o sinal digital modulado em frequência medido no scope do transmissor (figura 13). Esse mesmo sinal chega ao receptor onde é demodulado e decodificado na função. Nesse caso, como o sinal não sofre interferências, sua operação ocorre normalmente no sistema do drone (figura 14).

Figura 12 – Transmissão livre da simulação



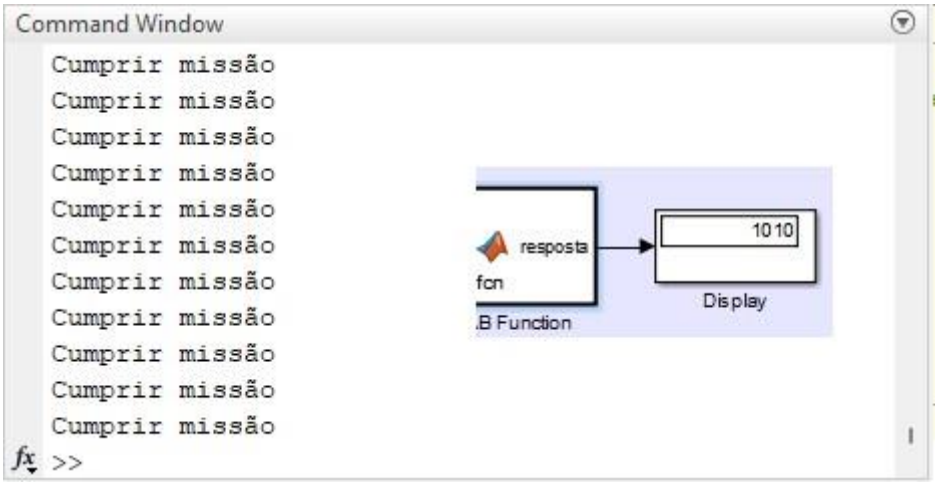
Fonte: elaborado pelo autor (2023)

Figura 13 – Sinal transmitido modulado em frequência



Fonte: elaborado pelo autor (2023)

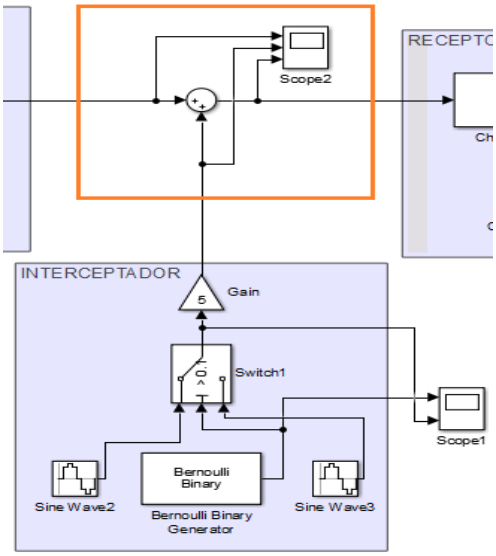
Figura 14 – Resposta da operação da transmissão livre



Fonte: elaborado pelo autor (2023)

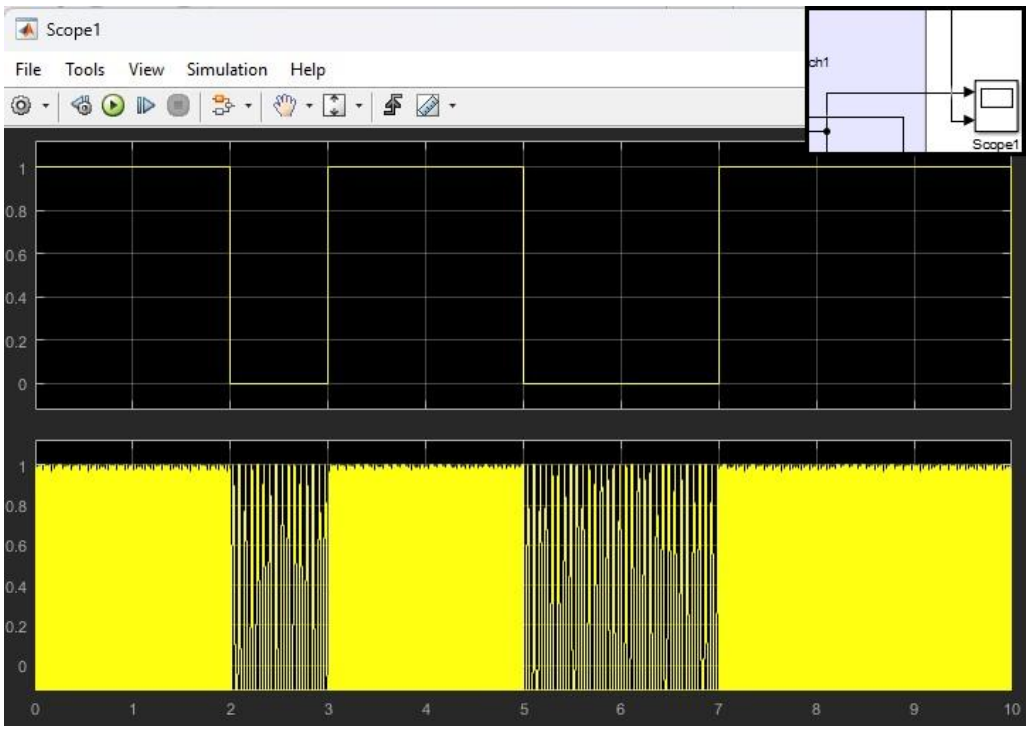
Ao simular a interceptação, conectou-se o dispositivo junto ao transmissor em um somador, simbolizando a entrada do receptor em meio ao espaço eletromagnético livre (figura 15). O sinal do interceptador, também digital modulado em frequência, é evidentemente destoante do transmissor no scope1 (figura 16), representando a intenção do invasor de enviar uma informação diferente para o drone. Na figura 17, no scope2, observa-se na primeira linha o sinal do transmissor e na segunda linha o sinal do interceptador e que, na terceira linha, apresentando o somatório de ambos os sinais, prevaleceu o sinal do interceptador em detrimento do controlador (transmissor). Isso ocorreu em virtude da maior intensidade do interceptador (cinco vezes maior), característica comum de medidas de ataque eletrônico.

Figura 15 – Transmissão com interceptação da simulação



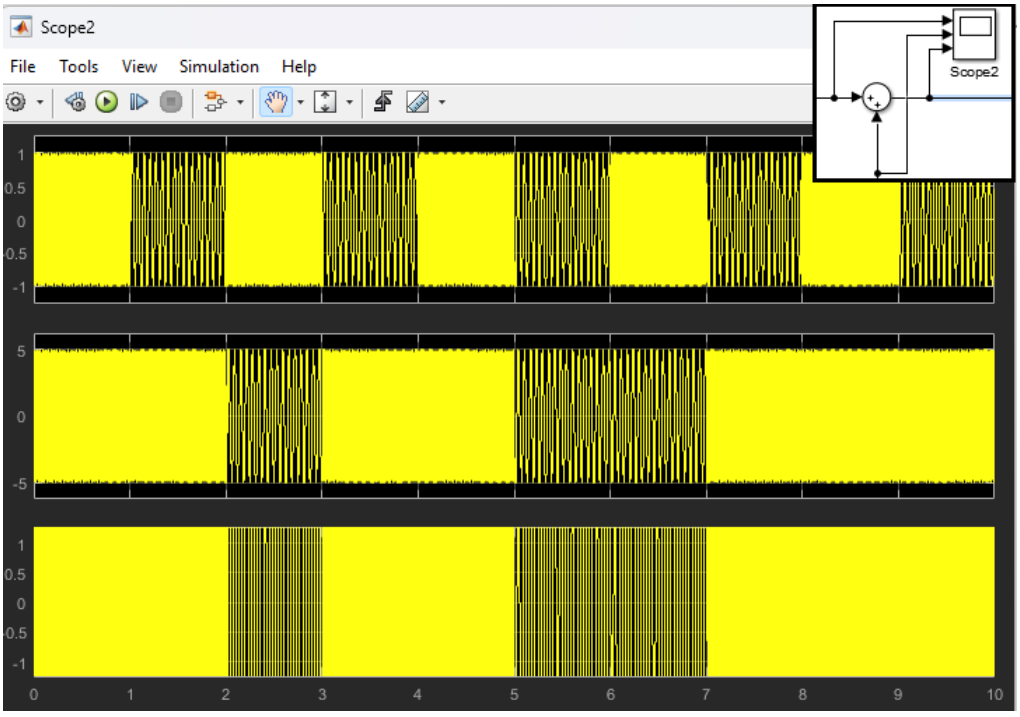
Fonte: elaborado pelo autor (2023)

Figura 16 – Sinal de interceptação modulado em frequência



Fonte: elaborado pelo autor (2023)

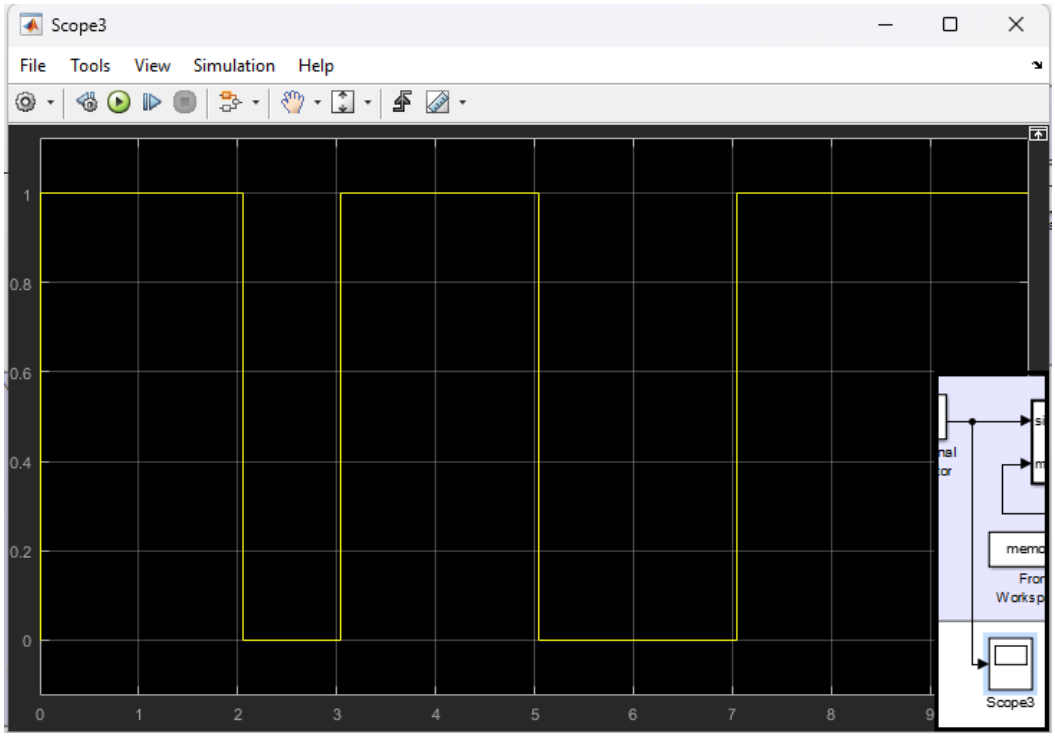
Figura 17 – Sinais da transmissão e interceptação sobrepostos



Fonte: elaborado pelo autor (2023)

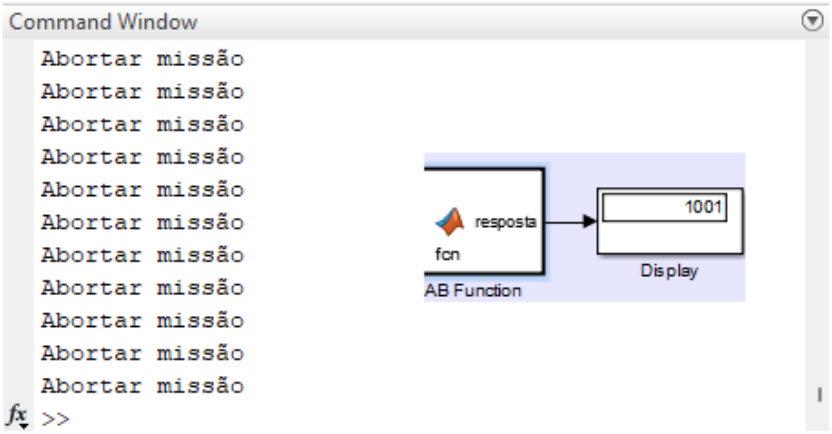
Após isso, ao se medir o sinal demodulado no receptor no scope3, percebe-se que o sinal do controlador foi totalmente obliterado em proveito do sinal do interceptador que é recebido praticamente sem prejuízos no receptor do drone (figura 18). Com isso, o leitor de código automaticamente interpreta a informação do sinal como fora da memória programada. Dessa forma, o sistema imprime a ordem de “abortar a missão”, constando o sinal de erro “1001” no display.

Figura 18 – Sinais do interceptador demodulado



Fonte: elaborado pelo autor (2023)

Figura 19 – Resposta da operação com interceptação



Fonte: elaborado pelo autor (2023)

Portanto, essa é uma simples e breve ilustração da dinâmica de um ataque ciber-eletrônico sobre o qual se discorreu durante todo o trabalho. Cabe ressaltar que a simulação realizada acima é um esforço para representar uma interceptação de um dispositivo eletrônico genérico, com todas as limitações de um *software* de simulação para tal aplicação, e que, por isso, consiste em uma situação simples, podendo variar o nível de complexidade na realidade.

7 CONCLUSÃO

Em suma, tendo em conhecimento o conteúdo supracitado e os fatos apresentados, torna-se clarividente a existência de uma interseção entre a guerra eletrônica e a guerra cibernética que permite integrar informações, ataques e efeitos diversos trafegados ora no meio eletromagnético ora no espaço cibernético em um só ambiente comum. Essa interseção, então chamada convergência ciber-eletrônica, foi possível graças à evolução de tecnologias fundamentais, a saber, o advento da automação e a tecnologia *wireless*, sem as quais ambos os domínios continuariam a ser tratados como espaços estritamente desconexos. Com isso, o desenvolvimento da técnica relacionada à convergência permitiu que ataques eletrônicos, por meio do espectro eletromagnético, pudessem afetar diretamente o espaço cibernético ao passo que operações cibernéticas, como a inserção de códigos maliciosos, pudessem degradar o funcionamento de equipamentos eletrônicos.

Como foi abordado, muitos países que se encontram na vanguarda do desenvolvimento científico-militar já possuem suas doutrinas e técnicas bem consolidadas a respeito da convergência ciber-eletrônica. Não apenas possuem documentos oficiais que normatizam tal atividade para suas forças armadas como também já possuem armas desse gênero voltadas para a operação militar. Nessa perspectiva, dois aspectos se tornam relevantes para os efeitos convergentes: o emprego militar e a segurança nacional. O primeiro se deve, sobretudo, ao uso de artifícios para desestabilizar os sistemas do inimigo como forma de preparar o cenário tático para um ataque efetivamente cinético, o que se torna – ou se tornará – típico de confrontos entre meios militares modernos. Já o segundo, por sua vez, se refere à defesa de infraestruturas críticas vulneráveis a esta categoria de ataque, o que acaba por comprometer a estabilidade da vida civilizada.

Em contrapartida, é preciso lembrar que essa novidade traz consigo claros desafios e riscos em um ponto de vista futuro. Desafios políticos, operativos e tecnológicos vão necessariamente fazer parte do desenvolvimento da atividade convergente enquanto riscos individuais e coletivos deverão ser considerados para uma evolução salutar. Desse

modo, é mister levantar ponderações éticas que servirão como base legal e jurídica para delimitar determinadas ações que visam superar princípios e direitos inultrapassáveis, tais como a soberania nacional, direito à privacidade, à transparência, entre outros. Por isso, torna-se desejável a busca por um equilíbrio razoável entre as ações do Estado e a liberdade do indivíduo.

Por conseguinte, é absolutamente necessário reconhecer o lugar da Marinha do Brasil no que tange à guerra ciber-eletrônica. Com navios cada vez mais automatizados e dependentes dos domínios eletrônicos e cibernéticos, a Marinha precisa adaptar suas estratégicas, doutrinas e investir recursos para se adequar à essa nova realidade em evidente crescimento. Precisa-se entender que uma das principais vitalidades desse gênero no país encontra-se justamente no domínio marítimo, na estrutura de cabos submarinos, elemento crucial para a estabilidade nacional. Portanto, pode-se entender que a convergência ciber-eletrônica não apenas redefine os paradigmas da guerra contemporânea como também cria novas tendências para o cenário geopolítico do futuro.

REFERÊNCIAS

ABOMHARA, Mohamed; KØIEN, Geir M. **Cyber Security and The Internet of Things**: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, p. 65–88, 2015.

ANDERSON, Gus; HADLEY, Mark. **The Invisible War**: The Convergence of Cyber and Electronic Warfare. p. 33-38, 2015.

BARROS, Renata Furtado. **Guerra Cibernética**: A Definição de Soberania na Responsabilização dos Estados pelas Cortes Internacionais nas ações de Guerra por Meio Eletrônico sob a Luz da Teoria Sistêmica de Luhmann. Direito Internacional Público e Privado em Faces Contemporâneas, p. 134-150, 2018.

BAYER, Fernando M.; ECKHARDT, Moacir; MACHADO, Renato. **Automação de sistemas**. Santa Maria: Rede E-tec Brasil, 2011.

BEJA, Louise A. **Aplicação militar da inteligência artificial nos sistemas de armas autónomas letais em tempos de guerra**. Livro de Resumos, p. 17-20, 2023.

BIAGI, Orivaldo Leme. **O imaginário da Guerra Fria**. Revista de História Regional, 2001.

BIAZON, Tássia. **Mentalidade Marítima**. INFOCIRM, p. 4-8, 2017.

BITTENCOURT, Nathália V. **Do Aumento À Automação**: O Novo Dilema Da Revolução Dos Assuntos Militares. 2019.

BRAGA, Cláudio C. **Comunicações Navais na Guerra da Independência e Sua Evolução Até os Dias Atuais**. Revista do Clube Naval, p. 68-73, 2023.

BRASIL. Marinha do Brasil. EMA-305. **Doutrina Básica da Marinha**. Brasília, 2014.

BRASIL. Ministério da Defesa. END. **Estratégia Nacional de Defesa**. Brasília, 2020.

BRASIL. Ministério da Defesa. PND. **Política Nacional de Defesa**. Brasília, 2020.

BRODIE, Bernard. **Strategy in the Missile Age**. Nova York: Harcourt, Brace and Company, 1946.

CANNELL, Joshua. **O vírus Chameleon WiFi se espalha como um resfriado**. 2014. Disponível em: https://www-malwarebytes-com.translate.goog/blog/news/2014/03/chameleon-wifi-virus-spreads-like-a-cold?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=wapp. Acesso em 22 set. 2023.

CARNEIRO, Pedro Erik. **Teoria e Tradição da Guerra Justa**: Do Império Romano ao Estado Islâmico. 1. ed. Campinas: Vide Editorial, 2016.

CASCAIS, António Fernando. **Guerra (In)Justa, Ciência (Im)Pura**. Revista da Faculdade de Ciências Sociais e Humanas, p. 91-119, 2003.

CHO, Sungbaek et al. **Cybersecurity Considerations in Autonomous Ships**. NATO Cooperative Cyber Defence Centre of Excellence: Tallinn, Estonia, 2022.

COUTINHO, Ricardo. **A Guerra Eletrônica No Espectro Óptico**. Disponível em: https://www.academia.edu/17323271/A_Guerra_Eletr%C3%B4nica_no_Espectro_%C3%93ptico. Acesso em 22 ago. 2023.

CLARKE R.; KNAKE R. **Guerra Cibernética**: a próxima ameaça à segurança e o que fazer a respeito. 1. ed. Rio de Janeiro: Brasport, 2015.

CLAUSEWITZ, Carl Von. **Da Guerra**. 3. ed. São Paulo: WMF Martins Fontes, 2010.

DE SÁ, Alan Oliveira; MACHADO, Raphael Carlos Santos; ALMEIDA, Nival Nunes. **O encontro da Guerra Cibernética com as Guerras Eletrónica e Cinética no âmbito do Poder Marítimo**. Revista da EGN, p. 89-128, 2019.

DRUMOND, Bruno. **Automação industrial**: o que é, quais os benefícios e formação. 2023. Disponível em: https://adequada.eng.br/automacao-industrial/. Acesso em 15 set. 2023.

FAN, Ricardo. **Controle do Espectro Eletromagnético – Criando Dominância do Ar**. 2023. Disponível em: https://www.defesanet.com.br/aviacao/noticia/1050901/and-in-brazil-the-government-wants-to-create-a-law-to-silence-the-independent-and-free-media-brazil-government-is-heading-toward-the-dream-of-facism/. Acesso em 19 ago. 2023.

FANTINATO, Giovanna. **Carros com IA são mais vulneráveis a ataque hacker, diz relatório**. 2021. Disponível em: https://www.tecmundo.com.br/seguranca/211495-carros-ia-vulneraveis-ataque-hacker-diz-relatorio.htm. Acesso em 15 set. 2023.

FARIA, Luis C. F., et al. **Os Navios Autônomos e os Novos Desafios da Responsabilidade Civil**. 2022. Disponível em: https://www.migalhas.com.br/coluna/migalhas-maritimas/358299/os-navios-autonomos-e-os-novos-desafios-da-responsabilidade-civil. Acesso em 04 out. 2023.

FRACKIEWICZ, Marcin. **Explorando o crescente uso de drones militares na guerra cibernética**. 2023. Disponível em: https://ts2.space/pt/o-papel-dos-drones-militares-na-guerra-cibernetica-e-na-guerra-eletronica/. Acesso em 21 set. 2023.

FULGÊNCIO, Caio. **Saúde e Agronegócio: As Principais Aplicações da IoT no Brasil**. 2023. Disponível em: https://www.meioemensagem.com.br/proxxima/saude-e-agronegocio-as-principais-aplicacoes-da-iot-no-brasil. Acesso em 27 set. 2023.

GUYONNEAU, Rudy; LE DEZ, Arnaud. **Artificial Intelligence in Digital Warfare**. The Cyber Defense Review, p. 103-116, 2019.

GONÇALVES, Josiane P.; CASTILHO, Marta V. **Segurança em Redes sem Fio**: principais formas de ataques, testes de invasão e modelos de segurança. 2021.

HARTMANN, Kim; GILES, Keir. **UAV exploitation**: A new domain for cyber power. 8th International Conference on Cyber Conflict (CyCon), p. 205-221, 2016.

HOUSE, Jonathan M. **Combinação das Armas**: A Guerra no Século XX. Rio de Janeiro: Biblioteca do Exército, 2008.

HOMERO. **Ilíada**. São Paulo: Penguin-Companhia, 2013.

HONÓRIO, Thiago J. **Segurança na Era da Informação: Reflexões Teóricas sobre a Ciberpolítica Internacional**. Niterói, 2016.

JÚNIOR, Augusto W. M. T.; LOPES, Gills V.; FREITAS, Marco T. D. **As Três Tendências da Guerra Cibernética**: novo domínio, arma combinada e arma estratégica. Carta Internacional, p. 30-53, 2017.

JUNIOR, Salvador M.; MARTINS, Norival L. **Sistema Dreadnought**. Revista Passadiço, p. 50-50, 2022.

JUNIOR, Walmor C. L. et al. **A Triggering Mechanism for Cyber-Attacks in Naval Sensors and Systems**. 2021.

KRELINA, Michal. **Quantum technology for military applications**. EPJ Quantum Technology, 2021.

LANDLER M.; MARKOFF J. **Estônia protagoniza primeira guerra virtual**. 2007. Disponível em: https://g1.globo.com/Noticias/Tecnologia/0,,MUL45961-6174,00-estonia+protagoniza+primeira+guerra+virtual.html. Acesso em 23 ago. 2023.

LIMA, Angelo S. **Cibercrimes e sua Configuração no Plano Jurídico Nacional e Internacional**. 2017.

LOBATO, Luisa; KENKEL, Kai M. **A Ciberguerra é moderna! Uma investigação sobre a relação entre tecnologia e modernização na guerra**. Contexto Internacional, p. 629-660, 2015.

LOPES, Michael S. **O Sistema de Cabos Submarinos de Conectividade no Brasil sob a Ótica da Segurança Marítima enquanto Infra-Estrutura Crítica de Comunicação**. Revista Hoplos, p. 28-50, 2021.

MAGNOLI, Demétrio (org.). **História das Guerras**. 4. ed. São Paulo: Contexto, 2019.

MARQUES, Domiciano. **Maxwell e a integração da luz com o magnetismo**. Brasil Escola. 2023. Disponível em: https://brasilescola.uol.com.br/fisica/maxwell-integracao-luz-com-magnetismo.htm. Acesso em 19 de agosto de 2023.

MATUSZAK, Justyna. **The Rise of IoT in Smart Cities**. Disponível em: https://knowhow.distrelec.com/internet-of-things/the-rise-of-iot-in-smart-cities/#:~:text=For%20data%20collection%20and%20analysis,and%20services%2C%20among%20other%20things. Acesso em 27 set. 2023.

MEDNIKAROV, Boyan; TSONEV, Yuliyan; LAZAROV, Andon. **Analysis of Cybersecurity Issues in The Maritime Industry**. Information & Security, p. 27-43, 2020.

MENDONÇA, Cláudia S. **Guerra Cibernética**: Desafios de uma Nova Fronteira. Rio de Janeiro, 2014. Disponível em: https://pantheon.ufrj.br/bitstream/11422/3340/1/CMendon%C3%A7a.pdf. Acesso em 24 ago. 2023.

MESQUITA, João L. **Navios de Guerra a Vapor, Os Primeiros Navios Blindados**. 2021. Disponível em: https://marsemfim.com.br/navios-de-guerra-a-vapor-os-primeiros-navios-blindados/. Acesso em 16 ago. 2023.

MOSSI, Welder P. **Comparação entre o Emprego da Guerra Eletrônica (GE) nas Guerras de Terceira e Quarta Geração:** A GE na Guerra do Golfo e na Guerra Civil Síria. Resende, 2019.

NASCIMENTO, Vinícius D.; COSTA, João M. D. **Paradigma Tecnológico e Guerra: A Importância da Inovação para o Poder de Combate**. Revista da Escola Superior de Guerra, p. 61-74, 2017.

NERI, Filippo. **Introduction to Electronic Defense Systems**. Artech house radar library. Boston: Artech House, 2006.

NETO, Ricardo B. G. **Guerra Cibernética/Guerra Eletrónica-Conceitos, Desafios e Espaços de Interação**. Revista Política Hoje, p. 201-217, 2017.

OLIVEIRA, Ângela B. C**. Tecnologia 5g e Possíveis Impactos para a Segurança Nacional**. 2021.

O'SHEA, Devlin R. **Electronic Warfare and Cyberspace Operations**: Coordination, not Convergence. Marine Corps University, 2017.

OSSAMAH, Almotery. **Blockchain as a solution to drone cybersecurity**. IEEE 6th World Forum on Internet of Things (WF-IoT). IEEE, p. 1-9, 2020.

PADILHA, Luiz. **USV 'Suppressor':** A Solução da EMGEPRON e TIDEWISE para a Guerra de Minas. 2022. Disponível em: https://www.defesaaereanaval.com.br/naval/usv-suppressor-a-solucao-da-emgepron-e-tidewise-para-a-guerra-de-minas. Acesso em 05 out. 2023.

PATÉ-CORNELL, M.-Elisabeth et al. **Cyber Risk Management for Critical Infrastructure**: a risk analysis model and three case studies. Risk Analysis, p. 226-241, 2018.

PINTO, Danielle J. A.; GRASSI, Jéssica M. **Guerra Cibernética, Ameaças às Infraestruturas Críticas e a Defesa Cibernética do Brasil**. Revista Brasileira de Estudos de Defesa, 2020.

POMERLEAU, Mark. **Services Working to Convergence EW, Cyber Warfare Capabilities.** 2022. Disponível em: https://defensescoop.com/2022/09/30/services-working-to-convergence-ew-cyber-warfare-capabilities/. Acesso em 25 set. 2023.

RIBEIRO, Carolina. **Como funciona a tecnologia Wireless**. Disponível em: https://www.techtudo.com.br/noticias/2012/04/como-funciona-tecnologia-wireless.ghtml. Acesso em 15 set. 2023.

RID, Thomas. **Cyber war will not take place**. Oxford University Press, 2013.

SAKURAI, R.; ZUCHI, J. D. **As Revoluções Industriais até a Industria 4.0**. Revista Interface Tecnológica, p. 480–491, 2018. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/ article/ view/386. Acesso em: 10 ago. 2023.

SHARMA, Purabi; SARMA, Kandarpa K.; MASTORAKIS, Nikos E. **Artificial Intelligence Aided Electronic Warfare Systems-Recent Trends and Evolving Applications**. IEEE Access, p. 224761-224780, 2020.

SIHAG, Vikas et al. **Cyber4Drone**: A Systematic Review of Cyber Security and Forensics in Next-Generation Drones. Drones. 2023.

SILVA, Júlio C. B. L. **Guerra cibernética**: a guerra no quinto domínio, conceituação e princípios. Revista da Escola de Guerra Naval, p. 193-211, 2014.

SOAMES, Nicholas. **Evolving Security in The North Atlantic**. Sub-Committee on Transatlantic Defence and Security Cooperation (DSCTC), 2019.

SOUZA, Gills L. M.; PEREIRA, Dalliana V. **A Convenção de Budapeste e as Leis Brasileiras**. Seminário Cibercrime e Cooperação Penal Internacional, 2009.

SOUZA, Tulio A. **A Guerra Cibernética e a Marinha Do Brasil**: As Ameaças Cibernéticas e a Defesa da MB. Rio de Janeiro, 2012.

TEIXEIRA, Márcio L. **Por que revolução nos assuntos militares.** Revista da Escola de Guerra Naval, p. 51-81, 2009.

THEOHARY, Catherine A.; HOEHN, John R.. **Convergence of Cyberspace Operations and Electronic Warfare**. Congressional Research Service, 2019.

TZU, Sun. **A Arte da Guerra**. 1. ed. Barueri: Novo Século, 2014.

UNITED STATES. Army. FM 3-38. **Cyber Eletromagnetic Activities**. 2014. Disponível em: https://irp.fas.org/doddir/army/fm3-38.pdf. Acesso em 09 set. 2023.

VAN CREVELD, Martin**. Transformation of War**. Simon and Schuster, 2009.

VIEIRA, Antônio F. J. **Emprego de Drones na Guerra Eletrônica**. Revista Passadiço, p. 18-21, 2021.

WESLEY, Maria H. A. **Cibernética e Cultura: Transição e Conflitos na Segurança e na Soberania**. Disponível em: http://www.brasilbrasileiro.pro.br/eceme%20-mhaw%20-%202013%20ccm.pdf. Acesso em 24 set. 2023.

WHITEHEAD, David E. et al. **Interrupção de Energia Induzida por Ataque Cibernético na Ucrânia: Análise e Estratégias Práticas de Mitigação**. Schweitzer Engineering Laboratories, Inc, 2017.

WORRELL, Ryan J. **EW and Cyber Convergence**: Beyond Information Warfare. Air University, 2020.