ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO

ESCOLA MARECHAL CASTELLO BRANCO

Cel Inf **ANGELO** ANDRÉ DA SILVA

O Incremento de Capacidades no Espaço Cibernético para ampliar a disseminação da Comunicação Estratégica no Exército Brasileiro

Rio de Janeiro

2024

Cel Inf **ANGELO** ANDRÉ DA SILVA

O Incremento de Capacidades no Espaço Cibernético para ampliar a disseminação da Comunicação Estratégica no Exército Brasileiro

Policy Paper apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Política, Estratégia e Administração Militar.

Orientador: Cel Cav R1 Newton Cleo Bochi Luz

Rio de Janeiro

2024

S586i Silva, Angelo André da

O Incremento de Capacidades no Espaço Cibernético para ampliar a disseminação da Comunicação Estratégica no Exército Brasileiro. / Angelo André da Silva.—2024.

38 f.: il. ; 30 cm

Orientação: Newton Cleo Bochi Luz.

Policy Paper (Especialização em Política, Estratégia e Alta Administração Militar) — Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2024.

Bibliografia: f. 37-38

1. Comunicação estratégica. 2. Cibernética. 3. Mídias Digitais. 4. Narrativas. 5. Fake News. 6. DeepFakes. 7. Dimensão informacional. 8. Público-alvo. 9. Capacitação I. Título.

CDD 370

Cel Inf **ANGELO** ANDRÉ DA SILVA

O Incremento de Capacidades no Espaço Cibernético para ampliar a disseminação da Comunicação Estratégica no Exército Brasileiro

Policy Paper apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Política, Estratégia e Alta Administração Militar.

Aprovado em 17 de setembro de 2024.

COMISSÃO AVALIADORA

Cel Cav R1 NEWTON CLEO BOCHI – Presidente
Escola de Comando e Estado-Maior do Exército

Cel Inf GLAUBER CORRÊA NETIS TELES – Membro
Escola de Comando e Estado-Maior do Exército

Cel Cav R1 FERNANDO LUIZ VELASCO GOMES – Membro
Escola de Comando e Estado-Maior do Exército

Ao nosso Grande Deus, à minha
esposa, meus filhos e meus pais,
alicerces nesta caminhada.

AGRADECIMENTOS

Agradeço primeiramente ao Grande e Poderoso Deus por iluminar meu caminho e dar-me forças em todos os momentos desta jornada.

À minha esposa, Carol, pilar da nossa família, que com paciência e amor soube compreender as minhas ausências e sempre me incentivou com palavras de apoio e carinho. Sua presença é um constante lembrete do que é mais importante na vida.

Aos meus filhos Maria Eduarda, Marina e Carlos Eduardo, que com sua alegria e amor incondicional, proporcionam a motivação necessária para seguir em frente e buscar ser uma pessoa melhor a cada dia.

Aos meus pais, que sempre estiveram ao meu lado, fornecendo um legado de valores e ensinamentos que continuam a guiar-me. Sua presença e apoio são uma fonte constante de inspiração e coragem.

Ao meu orientador, Cel Cav R1 Newton Cleo Bochi Luz, cuja sabedoria e orientação foram fundamentais para o desenvolvimento deste trabalho. Sua maneira de transmitir conhecimento e encorajar o pensamento crítico foram essenciais para o meu crescimento profissional e pessoal.

A todos eles, meu sincero agradecimento. Que possam sentir-se tão gratificados por minha jornada quanto eu sou grato por ter tido cada um deles ao meu lado.

“Nenhuma máquina é melhor do que um homem com uma máquina”

Richard Bookstaber,

Massachusetts Institute of Tecnology (MIT)

SUMÁRIO EXECUTIVO

O ambiente cibernético tem se revelado atualmente como um espaço de maior interação social do que o próprio ambiente físico. A velocidade e o alcance da informação e de narrativas têm causado impactos na opinião pública, que limitam a liberdade de ação das instituições federais no nível estratégico e, em alguns casos, no nível político. Essa liberdade de ação se dá por meio da projeção da dimensão Humana sobre a dimensão Física. Segundo o Caderno de Ensino Comunicação Estratégica, define-se como narrativa (no contexto da dimensão informacional) uma versão de um fato ou entendimento que perdura no tempo por intermédio da imprensa e da mídia digital, sendo utilizada na construção de conteúdo informacional. Essas narrativas podem ou não ser construídas e/ou disseminadas por atores determinados com ou sem o intuito de que públicos específicos as adotem como verdadeiras. É um dos fatores que balizam o planejamento da comunicação estratégica. (BRASIL, 2023). Já a opinião pública é definida como o conjunto de opiniões individuais sobre um mesmo fato, composto em um determinado momento, que pode ser medido cientificamente por meio de pesquisa, conforme o Manual de Fundamentos: Comunicação Social (BRASIL, 2017) Nesse sentido, a estratégia de comunicação do Exército não pode mais considerar o espaço cibernético apenas como uma das partes do seu Plano de Comunicação Social, para disseminar a Comunicação Estratégica do Exército, como vetor da consecução dos Objetivos Estratégicos do Exército. Mas sim, como um objetivo integrado e prioritário da instituição, sobretudo nas capacidades ligadas às mídias digitais e à inteligência artificial.

Palavras-chave: Comunicação Estratégica; Cibernética; Mídias Digitais; Narrativas; Fake News: DeepFakes; Dimensão Informacional; Público-Alvo; Capacitação.

ABSTRACT
The Cyber environment has currently been revealed as a space of greater social interaction than the physical environment itself. The speed and reach of information and narratives have impacted public Opinion, limiting the freedom of action of federal institutions at the strategic level land, in some cases, at the political level. This freedom of action occurs through the projection of the human dimension onto the physical dimension. According to the Strategic Communication Teaching Notebook, a narrative (in the context of the information dimension) is defined as a version of a fact or understanding that lasts over time through the press and digital media, being used in the construction of informational content These narratives may or may not be constructed and/or disseminated by determined actors with or without the intention that specific audiences be adopted as true. It is one of the factors that guide strategic communication planning (BRASIL, 2023). Public opinion is defined as the set of individual opinions about the fact, composed at a given moment, which can be measured scientifically through research, acording to the Fundamentals Manual: Social Communication (BRASIL, 2017) In this sense, the Army's communication strategy can no longer consider cyber space as just one part of its Social Communication Plan, to disseminate the Army's Strategic Communication, as a vector for achieving the Army's Strategic Objectives. But rather, as an integrated and priority objective of the institution, especially in capabilities linked to digital media and artificial intelligence.

Keywords: Strategic Communication; Cybernetics; Digital Media; Narratives; Fake News: DeepFakes; Informational Dimension; Target Audience; Training.

LISTA DE FIGURAS, QUADROS E TABELAS

SUMÁRIO

1 INTRODUÇÃO

Foram pouco mais de 20 anos entre a “era do computador” e a “era digital”. Bem diferente do tempo que durou a idade da pedra, a era do bronze ou a era do aço. Talvez por isso, não consigamos identificar as diferenças.

A novidade na era digital é que o poder dos computadores, associado à expansão da tecnologia da informação dita o ritmo da mudança em todas as esferas da existência. A Lei de Moore* tem se revelado espantosamente profética.

O ciberespaço atualmente se confunde com a dimensão física, humana e informacional. A comunicação por intermédio dele tem se proliferado em escala exponencial e instantânea.

O total de dispositivos conectados no Brasil pode chegar a 27,1 bilhões até 2025, segundo estimativa da ISG Provi der Lens**,** transformando as atividades humanas em “dados” e parte de um único sistema “quantificável” e “analisável”.

Segundo matéria exibida no programa de TV “Olhar Digital”: “Brasileiros passam, em média, 16 horas acordados. Dessas, gastam, aproximadamente, nove olhando para a tela do computador ou do celular. Dá 57% do tempo.”

“O mundo digital é como o alto mar. Seus perigos são intrínsecos. Por isso, ele tende a ser menos regulado, uma vez que tende a ser menos fiscalizável, como ocorre com as águas internacionais.” (Lee, pag. 37, 2022)

Com base nesses dados iniciais apresentados, a tendência atual é que cada objeto estará conectado à internet e programado para se comunicar com um servidor central ou com outros dispositivos em rede, tornando o ciberespaço estrategicamente indispensável.

As ameaças provenientes do Ciberespaço não são intrínsecas. Dependem do seu uso. Contudo, são de difícil identificação dos seus autores. Um laptop isolado pode produzir um fato de consequências globais.

Segundo KISSINGER (2015, pag. 367):

“Quando indivíduos de filiação ambígua são capazes de empreender ações cada vez mais ambiciosas e de maior penetração, a própria definição de autoridade do estado pode se tornar ambígua, encorajando possivelmente uma postura ofensiva na construção de novas capacidades.

O comandante do Cibercomando dos Estados Unidos [United States Cyber Command – uscc ou uscybercom] previu que a próxima guerra começará no ciberespaço.”

Diante dessa perspectiva, as estratégias de comunicação do Exército não podem mais considerar o espaço cibernético apenas como uma das partes do seu Plano de Comunicação Social, para disseminar a Comunicação Estratégica do Exército, como vetor da consecução dos Objetivos Estratégicos do Exército. Mas sim, como um objetivo integrado e prioritário da instituição, sobretudo nas capacidades ligadas às mídias digitais e à inteligência artificial.

Segundo o Caderno de Ensino Comunicação Estratégica, define-se Comunicação Estratégica do Exército como a unidade de ações, palavras e imagens em sintonia com sua Missão, Visão, Valores e seus Objetivos Estratégicos, na paz ou em operações, de forma alinhada, integrada e sincronizada, visando alcançar seus públicos de interesse, produzindo efeitos de longo prazo. (BRASIL, 2023).

O termo “cibernética” se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação. No campo da Defesa Nacional, inclui os recursos de tecnologia da informação e comunicações de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle (SISMC2), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais. (BRASIL. Glossário de Termos e expressões para uso no Exército - EB20-MF-03.109. Brasília, 2009)

Em um ambiente informacional de acrônimos como VUCA (Volátil, Ambíguo, Complexo e Incerto), BANI (Frágil, Ansioso, Não-linear e Incompreensível) e PSIC (Precipitação, Superficialidade, Imediatismo e Conturbação) (NUNES, 2022), os fatores tempo e espaço não são restritivos na perspectiva lógica da dimensão informacional, que inclui o espaço cibernético. Essa perspectiva lógica refere-se à onde e como as informações são obtidas, produzidas, armazenadas, protegidas e difundidas. É onde o Comando e Controle das forças militares é exercido e por meio da qual a intenção do comandante é transmitida. As ações nesta perspectiva afetam o conteúdo e o fluxo de informações.

Neste sentido, este trabalho se propõe a investigar como a espaço cibernético tem sido empregado em favor do impulsionamento da imagem do Exército Brasileiro e quais são os desafios para a implementação de uma comunicação estratégica efetiva por intermédio do ciberespaço.

2 COMUNICAÇÃO ESTRATÉGICA

O Caderno de Ensino Comunicação Estratégica, publicado em 2021, concentra o primeiro direcionamento teórico e institucional da Exército Brasileiro para elaboração, de forma sistemática, do posicionamento da Força Terrestre sobre assuntos de interesse estratégico. Em seu conteúdo foram abordadas as ferramentas de comunicação disponíveis no ciberespaço, como a Inteligência Artificial e as Mídias Sociais, como indutores do sucesso para preservação da imagem da Força na atualidade. A confecção do referido caderno teve, entre outras influências, as publicações do Centro de Excelência da Organização do Tratado do Atlântico Norte (OTAN).

Tal preocupação com o desenvolvimento dessa ferramenta se faz necessário, uma vez que as instituições não são responsáveis apenas por aquilo que elas disseminam na rede mundial de computadores, mas também por combater, com oportunidade, a desinformação a respeito dos seus processos. Essa desinformação pode ser revelar por meio de “Fake News” ou até mesmo por meio de “Deepfakes”.

Fake News (CEP, 2023) é a mensagem fraudulenta, fabricada e deliberadamente mentirosa, produzida e disseminada com a intenção de enganar e não de informar um fato e que, por isso, contribui para a desinformação. Utiliza-se, primordialmente, dos recursos da informática para imitar fontes genuínas, como instituições de Estado ou mesmo veículos consolidados de imprensa, e da velocidade, alcance e escala das mídias sociais e da internet para divulgação. Encontra solo fértil nas bolhas informacionais, principalmente, devido ao viés de confirmação.

Deepfake (NATO, 2020) é um dos produtos da inteligência artificial (IA) que é alvo das maiores preocupações, pois pode ser representado por um áudio, por imagens ou por um vídeo, gerados por “machine learning” (aprendiza de

máquina). Deepfakes costumam ser surpreendentemente realistas e às vezes difícil de distinguir se são genuínas. A IA tem sido usada para produzir Deepfakes retratando figuras políticas proeminentes, como Donald Trump e Vladmir Putin dizendo uma variedade de coisa que eles nunca disseram de fato.

A Comunicação Estratégica do Exército Brasileiro não se limita somente às inserções pelos canais técnicos, por intermédio da Rede do Sistema de Comunicação Social do Exército (RESISCOMSEx), mas também se destina a públicos-alvo prioritários, tais como influenciadores de comunicação, que podem moldar a percepção da mensagem, líderes de opinião (liderança comunitária, líderes de associações etc.) e os formadores de opinião (professores, jornalistas, líderes carismáticos etc.), bem como permear representantes dos 3 poderes (Executivo, Legislativo e Judiciário), da iniciativa privada e do setor acadêmico, conforme figura 1.

Figura 1: Interação de Com Estrt com Relações Institucionais

(BRASIL, 2023) Ao conduzir a Anl Com Estrt, deve-se ter em consideração a intenção de:

a) esclarecer o entendimento de como os atores, fatos e circunstâncias mais expressivos da dimensão informacional são ou podem ser determinantes ou apropriados pelos fluxos de informação e, assim, interferirem ou terem o

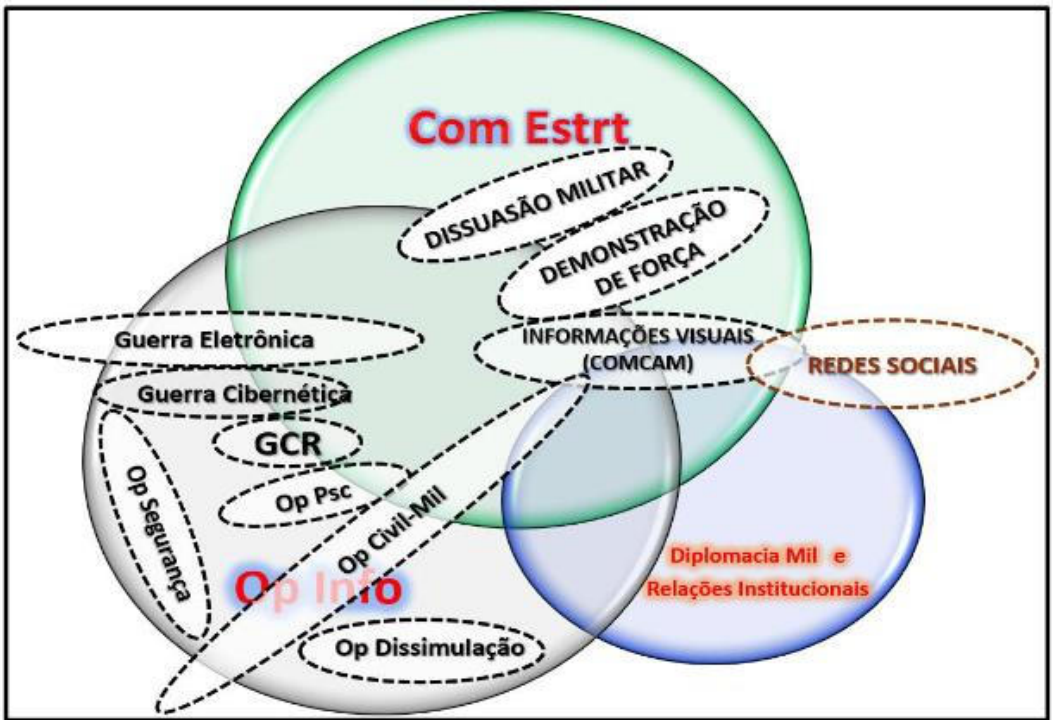
potencial de interferir na consecução dos Obj Estrt do Ex (OEE) e dos Obj de Com Estrt do Ex (OCEE); e

b) avaliar a qualidade, intensidade e abrangência dessas interferências. Nesse sentido, sugere-se o emprego de softwares específicos de aferição de mídias sociais, com o intuito de obter indicadores que retratem a efetivamente os dados que estão sendo analisados.

A “Strategic Communication” (StratCom) da Organização do Atlântico Norte (OTAN) foi uma das principais referências para o referido caderno de instrução do EB. A StratCom/OTAN tem atuado de forma efetiva no espaço cibernético, com domínio das novas tecnologias, alimentando tanto as plataformas mais acessadas pelas gerações Y, Z e A, como também servindo de fonte para materiais jornalísticos para a imprensa tradicional, que possui como público-alvo, em especial, a geração X.

A classificação das gerações por idade ajuda a identificar perfis em comum de acordo com o contexto histórico e social. As 5 Gerações atuais são: Baby Boomers, nascidos entre 1946 e 1964; a Geração X, nascidos entre 1965 e 1977; os Millennials ou Geração Y, nascidos entre 1978 e 1994; Geração Z, nascidos entre 1995 e 2010, e a Geração Alpha, nascidos a partir de 2010 (Pheula e Souza, 2016). As gerações mais jovens são os públicos prioritários no emprego das Capacidades Militares, no contexto das novas tecnologias, no ambiente informacional, conforme figura 2.

Figura 2: Com Estrt e o relacionamento das Capacidades Militares



O emprego da Comunicação Estratégica, em conjunto com as Operações de Informação e a Diplomacia Militar/Relações Internacionais, além de constituir uma ferramenta que alinha discursos descentralizados e que se beneficia da multidisciplinaridade dos seus países como fator de coesão, ela também contribui para o exercer o Soft Power da organização, conforme a figura 3.

Soft Power, conforme definido pelo estudioso político americano Joseph Nye, no final da década de 1980, ocorre quando um país faz com que outros países queiram o que eles querem (,,) em contraste com o “Hard Power”, que emite ordens a outros países. Ainda de acordo com Nye, os recursos de Soft Power incluem atração cultural, ideologia, instituições internacionais e corporações multinacionais.

(Melissem, 2005) Diplomacia de defesa é o uso da diplomacia como parte integrante da estratégia nacional de um país, destacando a importância da coordenação entre diplomatas e militares, para enfrentar desafios de segurança complexos, como a guerra assimétrica e as ameaças cibernéticas.

Figura 3: Interação de Com Estrt com Op Info e Diplomacia Mil

Por fim, a série histórica de indicadores ainda não nos permite mapear exatamente quais são as motivações políticas, econômicas e sociais de cada ator que se relaciona, por meio da Comunicação Estratégica, com o Exército Brasileiro, no nível político e estratégico. Contudo, verifica-se uma evolução exponencial dessa ferramenta, em virtude da sua capilaridade, de forma direta ou indireta, nas atividades singulares, conjuntas, combinadas ou interagências da instituição.

3 CIBERNÉTICA

O ciberespaço estreita a perspectiva. Como as informações são tão acessíveis e a comunicação instantânea, ocorre uma diminuição do foco no seu significado, ou mesmo na definição do que é significativo. A guerra da Ucrânia é repleta de exemplos dessa natureza, possibilitando visualizar que o futuro já chegou.

Segundo VALE (2024), “No campo cibernético, os russos fizeram amplo uso de TTP visando à coleta de dados negados e a disseminação de suas narrativas no meio digital. Exércitos de *trolls* (perfis em redes sociais que

tumultuam os debates em prol de determinadas organizações) insuflavam os discursos das mídias estatais russas, enquanto conversas comprometedoras entre autoridades norte-americanas, da OTAN e ucranianas eram interceptadas e tornadas públicas.

Todas essas ações na dimensão informacional foram essenciais para facilitar as ações dos rebeldes e dos russos e causar a paralisia nos centros de decisão da Ucrânia e seus aliados. Ao lograr a anexação da península da Crimeia e a independência das províncias rebeldes, sem necessidade de uma intervenção militar convencional de ampla escala, pode-se dizer que a Federação Russa alcançou a superioridade de informações."

O Brasil, como nação soberana, necessita de capacidade para se contrapor às ameaças externas, de modo compatível com sua própria dimensão e suas aspirações político-estratégicas no cenário internacional. Tal fato, possibilita ao país a consecução de objetivos estratégicos e a preservação dos interesses nacionais, além do exercício do direito de defesa assegurado pela Constituição Federal e pelo ordenamento jurídico internacional.

Na atualidade, a sociedade brasileira e suas Forças Armadas, devem estar permanentemente preparadas, considerando as atuais e futuras disputas internacionais. Nesse contexto, medidas deverão ser adotadas de modo a capacitá-las a responder oportuna e adequadamente, antecipando-se em face dos possíveis cenários adversos à defesa nacional.

No contexto do Ministério da Defesa, as ações no espaço cibernético são divididas da seguinte forma, de acordo com o nível de decisão (BRASIL, 2017):

a) nível político - Segurança da Informação e Comunicações (SIC) e Segurança Cibernética - coordenadas pela Presidência da República e abrangendo administração pública federal (APF) direta e indireta, bem como as infraestruturas críticas da informação inerentes às infraestruturas críticas nacionais;

b) nível estratégico - Defesa Cibernética - a cargo do MD, Estado-Maior Conjunto das Forças Armadas (EMCFA) e comandos das FA, interagindo com a Presidência da República e a APF; e

c) níveis operacional e tático - Guerra Cibernética - denominação restrita ao âmbito interno das FA

Pelo exposto acima verifica-se que, de acordo com nível de decisão,

podem ser ações no espaço cibernético, sejam relativas à segurança cibernética, à defesa cibernética ou à guerra cibernética a fim de manifestar o poder cibernético do país, em caso de necessidade

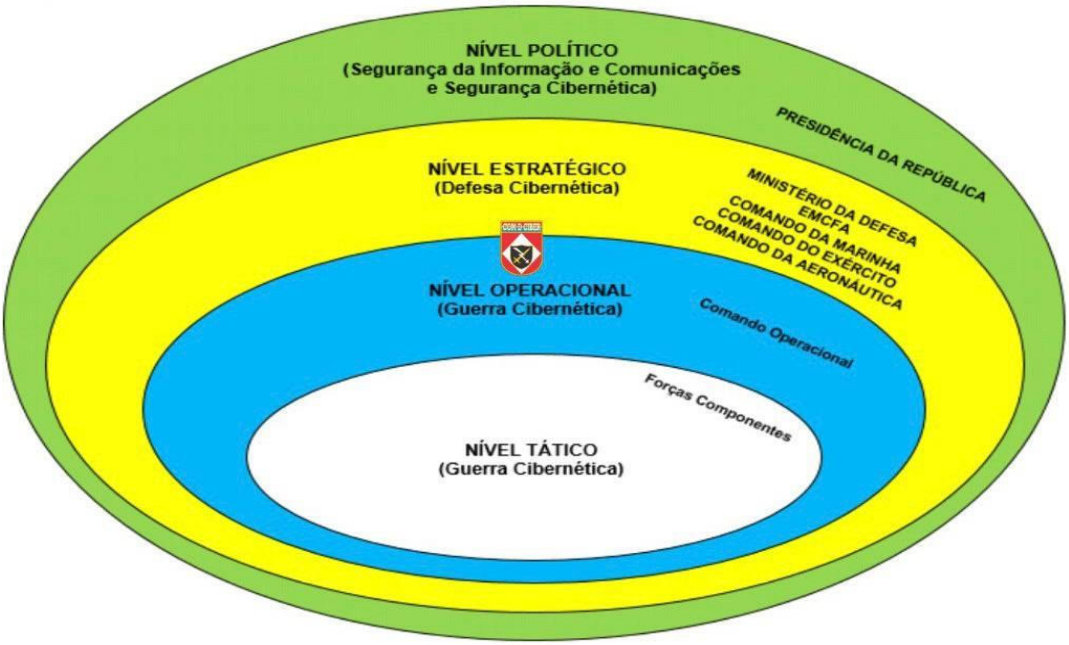
Tomando como base a atuação do Exército Brasileiro nos níveis operacional e tático, deverá ser buscado no âmbito do setor cibernético a interoperabilidade e a capacidade de atuar de forma integrada com as outras Forças Singulares, intensificar a interação com a comunidade acadêmica bem como o intercâmbio com Forças Armadas de países do entorno estratégico brasileiro como é mencionado na Estratégia Nacional de Defesa, vigente, aprovada em 2016:

> “Setor Cibernético, as capacitações destinar-se-ão ao mais amplo espectro de emprego civil e militar. Incluirão, como parte prioritária, as tecnologias de comunicações entre as unidades das Forças Armadas, de modo a assegurar sua interoperabilidade e a capacidade de atuar de forma integrada, com segurança. Para tanto, deverá ser fortalecida a atuação colaborativa entre o Setor de Defesa e a comunidade acadêmica nacional, os setores público e privado e a Base Industrial de Defesa. Adicionalmente, é importante que sejam intensificados as parcerias estratégicas e o intercâmbio com as Forças Armadas de outros países, sobretudo daqueles que compõem o entorno estratégico do Brasil.”

No Brasil, o Gabinete de Segurança Institucional da Presidência da República é responsável por gerenciar a segurança cibernética nacional. Com a finalidade de se garantir a segurança e a resiliência das infraestruturas críticas do País, foi criada a Política Nacional de Segurança de Infraestruturas Críticas e a Estratégia Nacional de Segurança Cibernética (E-Ciber). Outra iniciativa importante, foi a criação do Comando de Defesa Cibernética (ComDCiber) (conforme figura 4) órgão conjunto e permanentemente ativado, dentro da estrutura do Exército Brasileiro, cuja missão é planejar, orientar, coordenar, integrar e executar atividades relacionadas ao desenvolvimento e aplicação das capacidades cibernéticas. O ComDCiber, como órgão central do Sistema Militar de Defesa Cibernética, contribui para o uso efetivo do espaço

cibernético, impedindo ou dificultando sua utilização contra os interesses da Defesa Nacional.

Figura 4 – ComDCiber: Órgão Central do Sistema Militar de Defesa Cibernética.



No campo legal, o Brasil avançou com a regulamentação penal brasileira para crimes cibernéticos[8], por exemplo, a pena para o crime de invasão de dispositivo informático passou a ser de reclusão de um a quatro anos e multa. Da mesma maneira, a legislação brasileira prevê como ato terrorista os ataques cibernéticos contra infraestruturas estratégicas para a Defesa Nacional e serviços públicos essenciais à população brasileira. Em outra iniciativa recente, o Congresso Nacional ratificou a adesão do Brasil à Convenção de Budapeste. Esse acordo internacional tipifica os crimes cibernéticos e traz mecanismos para 1facilitar a cooperação entre seus signatários, facilitando o acesso de autoridades brasileiras às provas eletrônicas sob jurisdição estrangeira.

O trabalho colaborativo entre os setores acadêmico, público e privado é responsável pelos avanços do Brasil no cenário internacional em segurança da informação. Segundo a União Internacional de Telecomunicações, agência especializada da ONU, o Brasil melhorou 53 posições no ranking mundial de

segurança cibernética, saindo da 71ª colocação em 2018 para a 18ª em 2020, e entre os países da América está em 3º lugar, ultrapassado apenas pelos EUA/Canadá.

A título de exemplo, podemos citar as consequências negativas de um ataque cibernético contra a Usina Binacional de Itaipu, responsável por fornecer cerca de 17% da energia consumida no Brasil e 75% no Paraguai. Outro exemplo seria um ataque cibernético capaz de bloquear os sistemas do Canal do Panamá, impedindo a passagem entre os oceanos Pacífico e o Atlântico.

O Exército Brasileiro (EB) presidiu o ciclo XXXV, referente ao biênio 22/23, cujo tema é a contribuição da Conferência dos Exércitos Americanos no processo de transformação e preparação do “Exército do Futuro” para a ampliação da cooperação e integração no enfrentamento aos desafios e ameaças que possam afetar a segurança e a estabilidade do continente americano.

A identificação da origem de ataques cibernéticos é limitada, uma vez que a lógica do espaço cibernético está vinculada a aspectos técnicos e não a aspectos geográficos. Tal fato é agravado pela dificuldade no acompanhamento da evolução tecnológica na área cibernética. Essa realidade requer um compartilhamento de conhecimentos e de melhores práticas, por meio de plataformas que acelerem a identificação da ameaça, fomentando a resiliência.

O Exército Brasileiro e o Centro de Tratamento de Incidentes Cibernéticos do Governo Brasileiro (CTIR.Gov) adotam o Malware Information Sharing Platform (MISP), plataforma de inteligência de ameaças de código aberto, como metodologia de compartilhamento e identificação de ameaças e incidentes cibernéticos, contribuindo para a proteção cibernética de todos os membros contra ações adversas sobre os sistemas e ativos militares. Muitos outros exércitos americanos também adotam o MISP, incluindo a maioria dos Grupos de Resposta a Incidentes de Segurança (CSIRT — Computer Security Incident Response Team), como CERT-BR e o CERT-EU.

É importante lembrar que a evolução experimentada a partir da segunda

metade do século passado, com o uso intenso da internet trouxe inquestionáveis benefícios conferidos pela agilização do processo decisório e pela circulação da informação em tempo real e em nível mundial, contudo, tornou as pessoas, as organizações e os países altamente vulneráveis a um novo tipo de ameaça, a cibernética, que desconhece fronteiras e tem potencial para causar grandes prejuízos financeiros, paralisar as estruturas vitais de uma nação e, até mesmo, indiretamente, ceifar vidas.

O espaço cibernético, desafia conceitos tradicionais, fronteiras geopolíticas e até mesmo organizacionais, constituindo novo território, ainda inóspito, a ser desbravado pelos bandeirantes do século 21. Na atual conjuntura, a inexistência de marcos legais que disciplinem a disputa pelo domínio desse espaço cibernético transforma-o no “velho oeste” dos dias atuais, com potencial para suscitar conflitos de proporções e consequências extremamente danosas à humanidade. (BARROS, GOMES E FREITAS, 2011, p.16)

Por esta razão, é extremamente relevante adotar medidas relacionadas à segurança cibernética. Há várias providências que podem ser adotadas para fazer face à sensação de insegurança cibernética.

Segundo BARROS, GOMES E FREITAS (2011, p.91) uma das medidas mais eficazes é conscientizar a população, desde seus líderes políticos e militares até os trabalhadores das classes sociais mais baixas, sobre a possibilidade de estarem sendo alvo de levantamentos de dados, que podem comprometer indivíduos ou mesmo nações, ou de ataques, que podem ter efeitos gravíssimos.

Trazendo para o âmbito do Exército, a segurança cibernética pode ser aprimorada por meio da sensibilização do público interno (extensivo a seus familiares) quanto às ações que os tornam vulneráveis a captação de dados que podem expor sistemas e banco de dados da instituição, bem como informações pessoais de militares e servidores civis.

Para incrementar o desafio do Exército quanto à segurança cibernética ainda há, a questão geracional, a qual demonstra que de acordo com a faixa etária, os integrantes da Força, os quais ocupam diversos postos e graduações, podem ter uma conduta no espaço cibernético, intimamente ligada à sua forma de uso dos dispositivos computacionais, retratando o

comportamento da sua geração.

Nesse contexto, o Exército, por ser formado por cidadãos pertencentes de diferentes gerações, já mencionadas no capítulo “Comunicação Estratégica”, têm a desafiadora missão de conciliar as distintas visões de mundo ao seu “modus operandi”, disponibilizando ferramentas a esse público, de modo a preservar a imagem da Força, bem como contribuir com a consecução dos objetivos da Instituição no que se refere à comunicação estratégica no espaço cibernético.

4 MÍDIAS DIGITAIS

Tradicionalmente, a propaganda difundida pelos meios de comunicação, como o rádio, a TV e a internet, tem padronizado comportamentos. Contudo, isso não é um fenômeno novo. Já acontecia desde antes da invenção desses aparelhos.

Segundo Le Bon (Séc XIX), “A imitação, para qual tanta influência é atribuída como fenômeno social, é na verdade um mero efeito do contágio. Após algum tempo, esquecemos quem é o autor da frase e só lembramos dela, como se fosse verdade no subconsciente. Pessoas imitam as outras igual aos animais, onde cavalos acompanham outros cavalos que se assustaram por motivo desconhecido.”

Com a ascensão do fenômeno das mídias sociais, a disseminação da informação passou a ser realizada de forma descentralizada, influenciando de forma significativa grupos que até então não eram alcançados pelos grandes canais de comunicação.

“A informação é uma ferramenta importante para influenciar, desorganizar, corromper ou usurpar a capacidade de um adversário de tomar e compartilhar decisões, além de servir de suporte e proteção às ações amigas.” (Brasil, 2017)

“A mudança de distribuição da informação pela imprensa tradicional para a circulação da informação pelas mídias sociais sinaliza um movimento a favor de maior participação nos modelos culturais, que vê o público não como simples consumidores de mensagens predeterminadas! Mas como pessoas que moldam, compartilham e remodelam conteúdos na mídia que não poderiam ser previamente imaginados.” (Jenkins, 2018)

Para Perez & Barbosa (2007), a estratégia de mídia utilizada deve orientar aonde se quer chegar e a forma de se comunicar com seu público, definindo como os meios de comunicação devem ser utilizados. Assim, a estratégia indica o público ou segmentos a serem atingidos e a frequência na veiculação de determinado produto.

Além de descentralizadas e construídas de forma colaborativa, com base no consenso de “bolhas informacionais”. as mídias sociais estão cognificadas.

“A cognificação pode significar uma mudança da evolução pela seleção natural para uma outra orientada pela inteligência. O verbo “cognificar” que significa adicionar inteligência a um organismo, representa bem essa nova era.

O que caracteriza a cognificação é o avanço exponencial do poder computacional, a abundância de dados on-line, e também todos conectados a uma rede comum, além de tudo estar mais acessível. Significa dizer que temos o cenário ideal para criar novas formas de inteligências não limitadas pela biologia, as chamadas inteligências artificiais (IA).” (Kelly, 2019)

Kotler (2006) estabelece quatro passos para se pensar as mídias de maneira estratégica:

1) é preciso conhecer o ambiente externo: todas as escolas de pensamento estratégico entendem que é importante conhecer o ambiente externo. Algumas colocam o ambiente como protagonista, restando às organizações apenas o papel de tentar se adaptar para não desaparecer diante das ameaças ambientais. Assim, saber o que as pessoas conversam, em que ambientes e com que frequência é promissor para balizar uma estratégia em mídias sociais;

2) é preciso conhecer o ambiente interno: muitas outras escolas defendem a necessidade de se conhecer os pontos fortes e fracos da organização;

3) é preciso saber com quem falar: é importante conhecer o público para saber de suas necessidades. Isso é fundamental para que sejam desenvolvidos produtos ou serviços que gerem valor para as pessoas; mas, também, é fundamental para que sejam definidos os canais e as mensagens pelos quais elas devem transitar; e

4) é preciso checar se a iniciativa deu certo: este é um ponto fundamental para avaliar se o investimento na ação foi válido. Nenhuma instituição deve alocar recursos em atividades que não gerem valor e que não tragam resultados em satisfação de clientes, em ganho de imagem ou em utilidade pública.

“O Exército Brasileiro, Instituição tradicional e atenta à evolução da sociedade e ao aperfeiçoamento da comunicação, ingressou no campo das mídias sociais em 27 de outubro de 2010. Seguindo a vocação da comunicação mundial, a adesão a novos pontos de contato com a sociedade, por meio de plataformas de mídias sociais, visa à ampliação da divulgação das atividades da Instituição e à transmissão de informações para diversos públicos, aproximando o Exército de um grupo de usuários que passam a influenciar a opinião pública em um universo composto por todas as faixas sociais e etárias.

A administração e a gestão dos perfis nas plataformas Facebook, Instagram, Twitter, YouTube e LinkedIn está baseada nos critérios estabelecidos pela Portaria nº 453 do Estado-Maior do Exército (EME), de 19 de julho de 2021. A seção tem a missão de realizar a curadoria de material confeccionado pelas agências do SISCOMSEx; adaptar as campanhas institucionais para a linguagem de cada plataforma; gerar interação e acompanhar a ação dos usuários que se relacionam com a Instituição; monitorar e analisar os dados gerados pelas plataformas; e gerar feedback sobre as campanhas e ações que impactem a imagem do Exército Brasileiro.” (Moura, 2022)

Figura 5 - Portaria nº 453 do Estado-Maior do Exército (EME), de 19 de julho de 2021.

ESCALÃO/OM	FACEBOOK	INSTAGRAM	TWITTER	YOUTUBE	LINKEDIN	BLOG (3)
- Exército Brasileiro	SIM	SIM	SIM	SIM	SIM	SIM
- Órgão de Direção Geral - Órgão de Direção Operacional - Órgão de Direção Setorial	SIM	SIM	SIM	SIM	NÃO (1)	NÃO
- Comando Militar de Área	SIM	SIM	SIM	SIM	NÃO (1)	NÃO
- Órgão de Assistência Direta e Imediata ao Comandante do Exército - Divisão de Exército/Região Militar - Diretoria	SIM	SIM	NÃO	NÃO	NÃO (1)	NÃO
- Grande Unidade	SIM	SIM	NÃO	NÃO	NÃO	NÃO
- Academia Militar das Agulhas Negras - Escola de Sargentos das Armas - Instituto Militar de Engenharia	SIM	SIM	NÃO	SIM	NÃO (1)	NÃO

(NR - alterado pela PORTARIA – EME/C Ex Nº 1.066, DE 3 DE JULHO DE 2023)

ESCALÃO/OM	FACEBOOK	INSTAGRAM	TWITTER	YOUTUBE	LINKEDIN	BLOG (3)
- Demais Estabelecimentos de Ensino	SIM	SIM	NÃO	NÃO	NÃO	NÃO
- Colégio Militar (2)	SIM	SIM	NÃO	SIM	NÃO (1)	NÃO
- Unidade	SIM	SIM	NÃO	NÃO	NÃO	NÃO
- Subunidade Isolada	NÃO	SIM	NÃO	NÃO	NÃO	NÃO
- Tiro de Guerra	NÃO	SIM	NÃO	NÃO	NÃO	NÃO

O Exército Brasileiro tem mais de 4 milhões de seguidores no Facebook, que conferem diariamente as matérias jornalísticas que compartilham a rotina das organizações militares e campanhas publicitárias de ingresso na Força, seja por concurso, seleção de temporários ou alistamento militar. Atualmente, a Instituição ocupa a 1ª posição no ranking da categoria “Governo no Brasil” divulgado pelo site *Socialbakers*, especialista mundial em métricas de redes sociais.

No “X” (antigo Twitter), o Exército possui mais de 2 milhões de seguidores. O objetivo nesse microblog é veicular campanhas publicitárias e publicações que atraem o público jovem, sobretudo, para outras plataformas geridas pelo Centro de Comunicação Social do Exército (CCOMSEx), como o “Podcast Braço Forte”, no “spotfy” ou “soundcloud”, o site www.eb.mil.br; os vídeos do YouTube; os artigos divulgados pelo LinkedIn; ou os avisos de pauta no site do EB.

O YouTube do Exército Brasileiro, a TV Verde-Oliva, atualmente tem mais de 1 milhão e 200 mil seguidores, que consomem vídeos com alto nível de qualidade de som e imagem. O canal possui como cliente principal consumidores de vídeos em celulares e tablets ao usar linguagem que estabelece conexão direta e mais intimista com o usuário é considerado o

principal fator de sucesso de crescimento do canal. O canal do YouTube é um dos grandes responsáveis por trazer o capital social da instituição para o ambiente digital.

Na plataforma “Instagram”, o Exército possui mais de 6 milhões e meio de seguidores. A linha editorial empregada nessa plataforma visa à busca do engajamento por meio da interação com o seguidor, utilizando as ferramentas de chamada para a ação, tais como: quiz de perguntas, fotos e vídeos com links e hashtags, os movimentados e famosos Reels etc. Como segunda maior rede social do mundo, o Instagram implementa, constantemente, novidades de interação no âmbito perfil e audiência. As técnicas empregadas na gestão e análise de métricas refletem no acentuado crescimento do perfil na plataforma. O Instagram é a plataforma que mais cresce.

Outra ferramenta empregada pela Força Terrestre no campo das mídias sociais é o LinkedIn. A linha editorial busca utilizar a plataforma para aproximar o Exército da comunidade profissional, empresarial e científica. Artigos e trabalhos acadêmicos das mais diversas vertentes do ensino, das áreas de tecnologia e operacional são apresentados em publicações realizadas nessa plataforma, como forma de atrair tráfego de públicos especializados para o blog do Exército Brasileiro (EBLog) e para o site do Exército.

Em maio de 2021, o CCOMSEx lançou mais um canal de comunicação com seus públicos. O Exército Brasileiro, por meio da ferramenta Telegram, criou um *hub* de suas principais publicações, oferecendo notícias, vídeos, artigos, podcasts e informativos, direcionados tanto para o público externo quanto para o interno. O referido canal já possui mais de 55 mil seguidores.

Conclui-se, parcialmente, que o Exército brasileiro está presente em todas as mídias digitais mais conhecidas e vem desenvolvendo formas de ampliar o significativo engajamento que já possui, favorecendo a Comunicação Estratégica no ambiente cibernético.

5 CAPACITAÇÃO DIGITAL

O desafio permanente do Exército Brasileiro é manter seus quadros capacitados para enfrentar as ameaças atuais. Quando se trata de preservar a imagem da Força, por intermédio do Cyberespaço, o incremento do nível

técnico, sobretudo nas Capacidades Relacionadas à Informação (CRI), é objetivo prioritário.

O Exército Brasileiro hoje conta com estabelecimentos de ensino consolidados (Portal da Educação do Exército, 2023), que conduzem cursos e estágios voltados, direta ou indiretamente, para a disseminação de produtos que preservem a imagem da Força no espaço cibernético:

Figura 6 - Estb Ens que oferecem cursos/estágios nas CRI

Estabelecimento de Ensino	**Cursos/Estágios Oferecidos**
Centro de Instrução de Guerra Eletrônica (CIGE)	Cursos Básico/Avançado de GE para Of/Sgt e Curso de Guerra Cibernética para Of/Sgt Curso de Planejamento de Guerra Eletrônica e Cibernética em Apoio às Operações
Centro de Estudos de Pessoal (CEP)/Forte Duque de Caxias	Curso Avançado de Operações Psicológicas e o Curso de Comunicação Social/Curso de Auxiliar de Comunicação Social
1º Batalhão de Operações Psicológicas (1º B O Opsc)	Curso de Operações Psicológicas para Of/Sgt
Escola de Inteligência Militar do Exército (EsIMEx)	Curso Básico/Avançado de Inteligência para Of/Sgt
Escola Nacional de Defesa Cibernética (ENaDCiber)	Estágio Setorial de Penetration Test (Pentest) Estágio em Linguagem de Programação Python Estágio de Defesa Cibernética para Oficiais do Quadro do Estado-Maior da Ativa (QEMA)
Instituto Militar de Engenharia	Programa Institucional de Bolsas em Iniciação Científica em Desenvolvimento Tecnológico e Inovação.

Todos os cursos e estágios oferecidos estão hospedados no Portal da Educação do Exército, administrado pelo Centro de Educação a Distância do Exército (CEADEx), possibilitando que uma Organização Militar subordinada ao Departamento de Educação e Cultura do Exército (DECEx), desenvolva, pesquise e implemente ferramentas inovadoras, para emprego em proveito da Comunicação Estratégica, no Ciberespaço. Foi nesse diapasão que o CEADEx criou o “TROM”, a primeira ferramenta com Inteligência Artificial do Sistema de Educação e Cultura do Exército (SECEx), servindo de referências para iniciativas futuras no âmbito da Força.

Recentemente, foi criada a Diretriz Estratégica de Inteligência Artificial do Exército Brasileiro, para normatizar novos projetos nessa direção. (BRASIL, 2024) O documento visa promover a interoperabilidade tecnológica e a segurança cibernética, assegurando que todos os sistemas de IA sejam protegidos contra ameaças cibernéticas de forma contínua. O Exército planeja utilizar a IA para melhorar a precisão das informações e apoiar a tomada de decisão em tempo real, aumentando assim a eficácia e a eficiência operacionais.

A ampliação da “literacia digital” para as escolas de formação também poderia contribuir para a preservação da imagem da Força no espaço cibernético. (DefesaNet, 2024) No contexto da identificação de Fake News e DeepFakes, a literacia digita (ou midiática) envolve habilidades como:

1. **Verificação de Fatos**: Ensinar os usuários a verificar informações e fontes, cruzando dados com múltiplos veículos de informação confiáveis.

2. **Conscientização**: As redes sociais podem promover a conscientização sobre a existência e os perigos das fake news, incentivando o pensamento crítico.

3. **Educação Digital**: Oferecer recursos educativos que ajudem os usuários a identificar sinais de notícias falsas, como títulos sensacionalistas ou fontes duvidosas.

4. **Ferramentas de Reporte**: Disponibilizar ferramentas que permitam aos usuários reportar conteúdo suspeito, contribuindo para a sua remoção ou verificação.

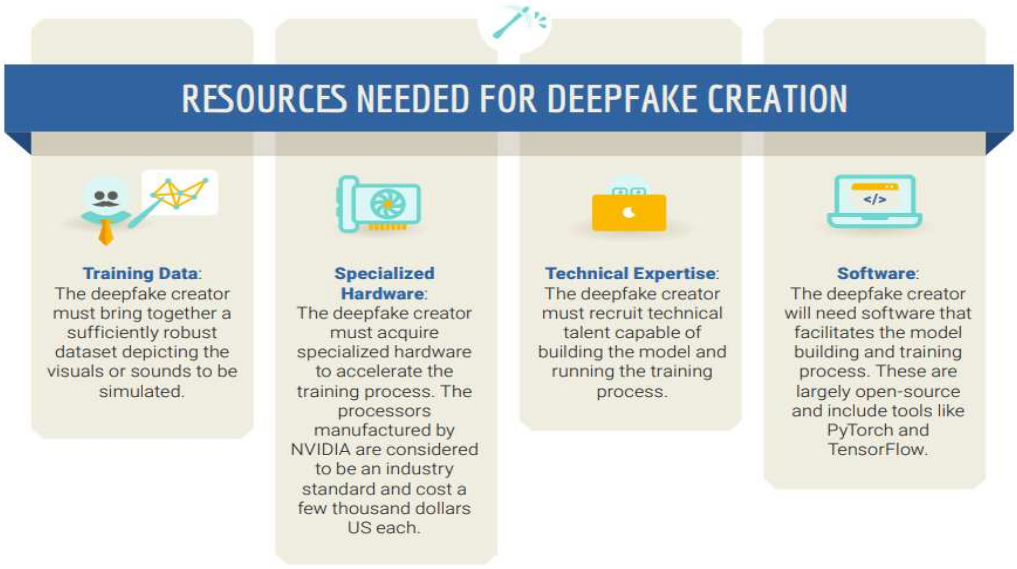
5. **Parcerias**: Colaborar com fact-checkers e organizações educativas para criar campanhas de informação e ferramentas de verificação dentro das plataformas.

Portanto, as redes sociais desempenham um papel ativo na educação dos usuários para o consumo crítico de informações, ajudando a combater a disseminação de Fake News e DeepFakes.

A Capacitação de militares para enfrentar as peculiaridades da dimensão informacional na atualidade não é exclusividade do Exército Brasileiro. Segundo a OTAN: “Nós não podemos mais acreditar no que vemos”.

(NATO, 2024) Pesquisadores conseguiram mostrar que o aprendizado de máquina pode ser usado para produzir falsificações extremamente convincentes. Mas, como me outros domínios, uma demonstração em laboratório pode estar muito longe de como uma tecnologia é finalmente usada no mundo real. O movimento de DeepFakes do laboratório para o mundo real é moldado por três tendências principais: democratização, limites da inteligência artificial e melhoria na detecção de fraudes. Esta última tendência requer conhecimento técnico para ser desenvolvida e, consequentemente, possibilitar conforme o combate a esse tipo sofisticado de desinformação, conforme figura abaixo:

Figura 7 – Conhecimento técnico (“Technical Expertise”) está entre os recursos necessários para criar e, consequentemente, combater as DeepFakes.

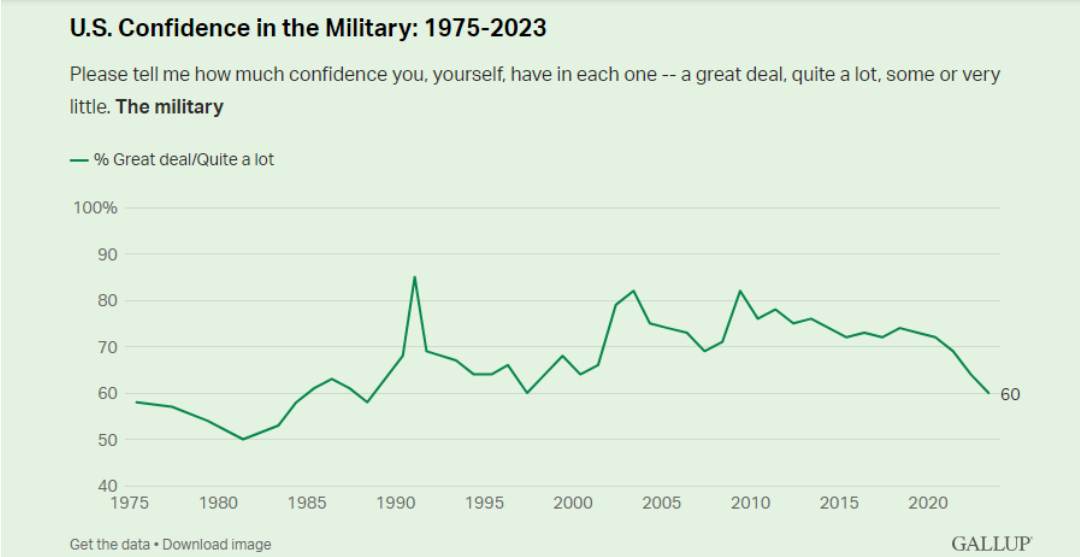


Os sistemas de detecção de DeepFakes são mais bem sucedidos quando os pesquisadores têm acesso a muitos exemplos de mídia sintética, produzida por um modelo específico. Esses exemplos são usados como base no treinamento, que por sua vez pode ser usado para criar um sistema de detecção capaz de revelar assinaturas desse modelo generativo (GAN)*

O investimento em pesquisas sobre dimensão cognitiva das DeepFakes é importante. Ainda há uma série de incógnitas importantes sobre como o público entende e responde para a mídia sintética de alta qualidade. São necessárias investigações no sentido de verificar se o nível de qualidade do vídeo ou da imagem determina o quanto crível é a mídia. Até que ponto isso é um fator preponderante? O conhecimento existente sobre DeepFakes pode tornar o indivíduo menos disposto a acreditar na mídia em geral? Se sim, quão significativo é esse efeito?

Até mesmo o Exército dos Estados Unidos da América (EUA) vem passando por quedas do índice de credibilidade pelo fato de não estar devidamente capacitado para se defender das armadilhas da dimensão informacional, conforme mostra a figura abaixo:

Figura 8 – A confiança nas Forças Armadas dos EUA é a mais baixa em mais de duas décadas



Segundo Military Review, 2024:

“O currículo que aborda as relações civis-militares na educação profissional militar deve ser obrigatório – e não opcional – durante toda a carreira de um combatente.”

Até mesmo um Presidente Americano, durante o mandato, está suscetível ao cancelamento no ciberespaço, conforme ocorreu com Donald Trump, ao ser excluído da plataforma social “Twitter”(X, atualmente), em janeiro de 2021.

De acordo com a opinião de Urben, 2021, o Departamento de Defesa precisa revisar urgentemente as normas e os regulamentos relativos às atividades políticas. A Diretriz 1344.10 do Departamento de Defesa precisa ser revisada e atualizada com maior frequência para oferecer maior clareza e contexto em relação ao “porquê” das regras relacionadas ao envolvimento de militares em atividades políticas.

Deve abordar todos os postos e graduação do serviço militar (não apenas oficiais), além de definir claramente sua aplicação a todas as categorias de militares da reserva remunerada “sujeitos aos seus dispositivos”.

A literacia mediática surge como uma solução essencial, capacitando os

indivíduos a identificar e questionar a veracidade das informações. As redes sociais têm a responsabilidade de promover essa literacia, fornecendo ferramentas e recursos educativos para combater a disseminação de fake News e DeepFakes.

Em conclusão, enquanto as fake News e as DeepFakes continuam a ser um desafio, a conscientização e a educação são as chaves para uma sociedade mais informada e menos suscetível à desinformação. É um esforço coletivo que requer a participação ativa de indivíduos, plataformas de mídia social e instituições para garantir a integridade da informação em nossa sociedade digital.

6 CONCLUSÃO

O Exército Brasileiro já possui estruturas prontas e consolidadas no ambiente cibernético. Tais estruturas têm significativo potencial de disseminar a Comunicação Estratégica da instituição, incrementando capacidades tradicionais relacionadas à credibilidade da Força Terrestre junto a públicos de interesse.

A **primeira capacidade** a ser incrementada é a **Estrutura de Tecnoloogia de Informação (TI)**. Investimentos na área de pesquisa e desenvolvimento (P&D), capitaneadas pelo Departamento de Ciência e Tecnologia (DCT), envolvendo parcerias como o Ministério da ciência, Tecnologia e Inovação (MCTI) poderiam viabilizar formas formas de acesso à internet provenientes do setor público ou privado, em todos as OM do Exército. Em todo aquartelamento poderia haver um local para ser destinado para ser estúdio de filmagem. Nesse diapasão, poderiam ser adquiridos equipamentos para tomada de imagens, como câmeras, filmadoras, drones e softwares de edição de vídeo, com o intuito de potencializar o registro das atividades e, em consequência, disseminá-las no contexto da Comunicação estratégica.

A **segunda capacidade** que poderia ser incrementada são as **Relações Institucionais**. O ciberespaço não tem limites nem fronteiras. Nesse sentido, a Força Terrestre tem condições de ampliar, com mais regularidade, a associação das suas atividades e da imagem dos seus militares à Marinha do Brasil, à Força Aérea Brasileira, aos Órgãos de Segurança Pública, ao meio acadêmico, à indústria, à imprensa, às entidades privadas, aos “influencers” das mídias sociais, selecionados pela 7ª Seção dos Comandos Militares de Área, ao Poder Judiciário, ao Poder Legislativo e ao Poder Executivo. Adcionado a isso, o Exército poderia promover sua

imagem no exterior, com vídeos, imagens e podcasts em outros idiomas. Sobretudo nos 5 idiomas mais falados do mundo: inglês, mandarim, hindi, espanhol e francês. Diante de tal iniciativa, a instituição obteria maior reconhecimento internacional, contribuindo com o estreitamento de relações institucionais e potencializando a cultura colaborativa do país.

A **terceira capacidade** com possibilidades de incremento é o **Dissuasão no Cyberespaço**. Tal capacidade exige maior engajamento do público nas páginas do Exército Brasileiro nas mídias sociais, citadas no desenvolvimento. Esse engajamento poderá ser ampliado com a integração crescente da RESISCOMSEx e do ComDCiber, pois já existem diversas ferramentas que potencializam o tráfego das postagens, que podem ser desenvolvidas de forma conjunta pelos referidos atores. Um canal que poderia ser empregado na dissuasão da Força são as campanhas para o Serviço Militar Obrigatório, cuja responsabilidade é do Ministério da Defesa (MD). Tais campanhas são direcionadas ao público adolescente e poderiam ser extendidas ao público infantil, para que seja ampliada o contato com a Força com as novas gerações. Tal iniciativa poderia ser estimulada com programas regulares nas mídias sociais, voltados para o público jovem.

A **quarta capacidade** com possibilidades de incremento é o **Combate à Desinformação**. O Exército poderia adquirir softwares que funcionam como um "antivírus" para identificar DeepFakes de vídeos, imagens e áudios, que são gerados pela inteligência artificial, possibilitando prestar esclarecimentos à sociedade de forma mais célere, quando for alvo de "hackers" maliciosos. Além disso, o CcomSEx, em coordenação com o ComDCiber, poderia ter sua própria agência de "Fact Check", possibilitando que Fake News sobre o Exército Brasileiro sejam desmentidos diariamente, disponibilizando para os órgãos de imprensa e para canais alternativos das redes sociais a versão oficial da Força Terrestre sobre cada assunto que foi veiculado de forma inadequada.

A **quinta e última capacidade** com possibilidades de incremento é a **Capacitação Digital do Público Interno**. Ainda que exista a disponibilidade de estabelecimentos de ensino conduzindo a formação de profissionais voltados para as capacidades relacionadas à informação, todo militar é um operador da informação e tem impacto direto na dimensão informacional. Sobretudo quando toma alguma conduta considerada inadequada. Nesse sentido, todo militar precisa ser capacidade a ter um comportamento ético no espaço cibernético, a fim de não haver desgastes para a Comunicação Estratégica da Força, geradas por iniciativas pontuais equivocadas, em virtude de imperícia.

Por fim, os resultados do incremento das capacidades no ambiente cibernético só

começarão a ser observadas no longo prazo, mesmo que tais propostas fossem imediatamente executadas. Diante desse quadro, é premente a necessidade de discussões a respeito desses temas, de modo a conquistar esse espaço sem fronteiras, com a Comunicação Estratégica definida pelo Exército Brasileiro.

REFERÊNCIAS

- **BRASIL**, Caderno de ensino Comunicação Estratégica - EB60-CE-11.001. Brasília, 2023.
- _____, Manual de Fundamentos: Comunicação Social - EB20-MF-03.103. Brasília, 2017.
- _____. Glossário de Termos e expressões para uso no Exército - EB20-MF-03.109. Brasília, 2009
- _____, Manual de Fundamentos: Conceito Operacional do Exército Brasileiro – EB20-07.101. Brasília, 2023.
- _____, Concepção Estratégica do Exército (Plano), Fase 4, Sistema de Planejamento Estratégico do Exército. Brasília, 2024-2027.
- _____, Boas Práticas Aplicáveis à Utilização de Mídias Digitais pela Administração Pública Federal. Brasília: Controladoria-Geral da União, Secretaria Especial de Comunicação Social do Ministério das Comunicações, 2022.
- _____, Lei No 12.232, de 29 de abril de 2010, dispõe sobre as normas gerais para licitação e contratação pela administração pública de serviços de publicidade prestados por intermédio de agências de propaganda e dá outras providências. Brasília: Casa Civil, Subchefia para Assuntos Jurídicos, 2010.
- _____, Decreto nº 11.856 em 26 de dezembro de 2023, instituiu a Política Nacional de Cibersegurança (PNCiber) **e o** Comitê Nacional de Cibersegurança (CNCiber). Brasília, 2023.
- **_____**, Portaria **nº** 1.886, de 14 de novembro de 2019, aprova o Plano de Comunicação Social do Exército para os anos de 2020 a 2023 – EB10 – P -11.001. Brasília, 2019.
- _____, Jornada de Comunicação Social 2023, Inteligência Artificial e Comunicação Institucional. Disponível em https://www.youtube.com/watch?v=B7W9TkP01pg&t=25052s Acesso em 31 Jan 2024.
- _____, Diretriz de Orientação para o incremento da Educação Assistida por Tecnologias Digitais nos Processos de Ensino e Aprendizagem no Âmbito do Sistema de Educação e Cultura do Exército. Rio de Janeiro, 2021.
- _____, Política Nacional de Defesa, Estratégia Nacional de Defesa. Brasília, 2023.
- _____, Portaria-EME/C Ex No 453, de 19 de julho de 2021. Aprova as Normas para Criação e Gerenciamento das Mídias Sociais no Âmbito do Exército Brasileiro. Brasília: SGEx, 2021.
- **NUNES, Richard Fernandez.** O Mundo em acrônimos e a Comunicação Estratégica do Exército. Disponível em https://eblog.eb.mil.br/index.php/menu-easyblog/o-mundo-em-acronimos-e-a-comunicacao-estrategica-do-exercito.html. Acesso em 20 jan 2024.
- **MOURA, Cesar Augusto Lima Campos** de. Proposta de Estruturação do Monitoramento de Mídias Sociais na Comunicação Social no Exército Brasileiro. Revista Valore, [S.l.], v. 5, p. 114-133, jul. 2021. ISSN 2526-043X. Disponível em: https://revistavalore.emnuvens.com.br/valore/article/view/771 Acesso em: 14 fev. 2024. doi:https://doi.org/10.22408/reva502020771114-133.
- _____, Cel Cesar Augusto Lima de, Caçadores de like? O que o Exército busca com seus perfis nas mídias sociais? Disponível em https://eblog.eb.mil.br/index.php/menu-easyblog/cacadores-de-like-o-que-o-exercito-busca-com-seus-perfis-nas-midias-sociais.html . Acesso em 31 Jan 2024.
- _____, Cel Cesar Augusto Lima de, Já podemos detectar socialbots nas mídias sociais? Disponível em https://eblog.eb.mil.br/index.php/menu-easyblog/cacadores-de-like-o-que-o-exercito-busca-com-seus-perfis-nas-midias-sociais.html . Acesso em 31 Jan 2024.
- **SILVA, Cel Angelo André da**, Trom: inteligência artificial a serviço da educação. Disponível em https://eblog.eb.mil.br/index.php/menu-easyblog/trom-inteligencia-

artificial-a-servico-da-educacao-militar.html . Acesso em 26 Jun 2023.
- **BRASIL, Inovação Militar: Max,** a Inteligência Artificial do Exército gradua-se como Terceiro Sargento e Intensifica Interações pelo Aplicativo Oficial. Disponível em https://noticias.bmilitar.com/exercito/2023/12/04/inovacao-militar-max-a-inteligencia-artificial-do-exercito-gradua-se-como-terceiro-sargento-e-intensifica-interacoes-pelo-aplicativo-oficial . Acesso em 12 Fev 2024.
- **LEE, Kai-Fu; QIUFAN, Chen**, 2041: Como a inteligência artificial vai mudar sua vida nas próximas décadas. 1ª edição. Rio de Janeiro: Globo Livros, 2022.
- **DOS SANTOS, Diego Maurícius Paiva *et al*.** Uma visão de futuro para a comunicação estratégica no Exército Brasileiro. A Defesa Nacional, Vol. 852, p. 31-107, 2023.
- **LATVIA,** Fact-Checking and Debunking a Best Practice Guide to Dealing With Disinformation. NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, 2021.
- _____, Robotrolling. NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, 2021.
- _____, DeepFakes – Primer and Forecast. NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, 2021.
- _____, Social Media Monitoring Tools: An In-Depth Look. NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, 2022.
- _____, Communicating Defence in Slovakia and the Czech Republic: Mapping Actors and Narratives Online. NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, 2022.
- _____, Seeking Legitimacy: Considerations for Strategic Communications in the Digital Age. NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, 2023.
- _____, Social Media Manipulation 2021/2022: Assessing the Ability of Social Media Companies to Combat Platform Manipulation. NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, 2023.
- **WEST, Geofrey,** The Universal Laws of Life and Death Scale in Organisms, Cities and Companies. United States: Penguin Books, 2018
- **JENKINS, Professor Henry *et al*.** Spreadable Media: Creating Value and Meaning in a Networked Culture. United States: New York University Press, 2018.
- **LE BON, Gustave**, Psychologie des foules. Réunion: Kult, 2018.
- VISACRO, Alessandro, A Guerra na Era da Informação. São Paulo: Editora Contexto, 2018.
- **PATRIKARAKOS, David**, War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century. United States: Hachette Book Group, 2017.
- **KRISHNAN, Armin**, Gezilte Tötung: Die Zukunft Des Krieges. Berlin: MSB Matthes & Seitz, 2012.
- **KELLY, Kevin,** Inevitável: as 12 forças tecnológicas que mudarão nosso mundo. Rio de Janeiro: Atlas Books, 2019