ESCOLA DE GUERRA NAVAL

CC (T) Marli Marques Jares de Medeiros

O EMPREGO DAS OPERAÇÕES DE INFORMAÇÃO NOS CONFLITOS MODERNOS: A (DES)INFORMAÇÃO COMO ARMA

Rio de Janeiro

2020

C-Sup/2020

O EMPREGO DAS OPERAÇÕES DE INFORMAÇÃO NOS CONFLITOS MODERNOS: A (DES)INFORMAÇÃO COMO ARMA

Monografia apresentada à Escola de Guerra Naval como requisito parcial para a conclusão do Curso Superior.

Rio de Janeiro
Escola de Guerra Naval
2020

CC (T) Marli Marques Jares de Medeiros

O EMPREGO DAS OPERAÇÕES DE INFORMAÇÃO NOS CONFLITOS MODERNOS: A (DES)INFORMAÇÃO COMO ARMA

Monografia apresentada à Escola de Guerra Naval como requisito parcial para a conclusão do Curso Superior.

Orientador: CF Daniel Gomes Padilha

Rio de Janeiro
Escola de Guerra Naval
2020

AGRADECIMENTOS

Agradeço primeiramente a Deus, que permitiu a minha existência e por seu amor incondicional a mim.

Ao meu pai, Antonino, e minha mãe, Martha, que me ajudaram a ser quem eu sou.

Ao meu marido, Reginaldo, que me acompanha nesta jornada.

Aos meus filhos, Patrícia e Felipe, que, muitas vezes, não puderam ter a minha companhia, mas entenderam.

A todos que cruzaram o meu caminho e me orientaram, oraram por mim, se alegraram ou trouxeram conforto quando eu precisava.

Ao meu orientador, CF Daniel, pelas orientações durante o curso, as quais me permitiram alcançar o aprendizado necessário à conclusão desta monografia.

DEDICATÓRIA

Dedico esta vitória a Deus, que me deu a vida, e ao meu marido, que abdicou de minha companhia e auxiliou meus familiares em momento de pandemia.

O meu sincero carinho a todos que me ajudaram a concluir este trabalho.

RESUMO

Mudanças tecnológicas ao longo dos anos trouxeram reflexos para a sociedade, influenciando tanto o modo de fazer política como a tarefa de planejar a Defesa da Pátria. Ao mesmo tempo, essas transformações aumentaram a vulnerabilidade de sistemas e colocaram a sociedade sob constante ameaça de ataque cibernético. Grupos que respondem a Estados ou hackers perceberam essas vulnerabilidades, e também que a dimensão informacional é fundamental para as operações militares, pois ela permite o seu planejamento, condução e busca de vantagens competitivas. Ao mesmo tempo, facilita a coleta de informações sem autorização ou a publicação de informações falsas, que são rapidamente compartilhadas e consideradas como verdadeiras, podendo, inclusive, desestabilizar governos ou instituições. A Marinha do Brasil possui diversos sistemas, tanto administrativos quanto operativos, que podem ser alvo de ataques desse tipo, mas ela também se preocupa com a sua imagem, cujo fortalecimento é realizado por meio da Comunicação Social e que pode, inclusive, ser uma aliada indispensável nas operações de informação, ajudando no fortalecimento da imagem da Instituição e no esclarecimento da população.

Palavras-chave: Informação. Desinformação.

LISTA DE ABREVIATURAS E SIGLAS

AI	Inteligência Artificial
AUMF	*Authorization for the Use of Military Force*
CCOMSEx	Centro de Comunicação Social do Exército
CCSM	Centro de Comunicação Social da Marinha
CENTCOM	Comando Central dos Estados Unidos
CEO	*Chief Executive Officer*
CIA	Central Intelligence Agency
CRI	Capacidades Relacionadas à Informação
CSIS	Center for Strategic and International Studies
CTIM	Centro de Tecnologia da Informação da Marinha
DoD	Departamento de Defesa dos EUA
EUA	Estados Unidos da América
GAN	Generative Adversarial Network
IOR	*Information Operations Roadmap*
ISO	Sensibilidade do sensor da câmera à luz
MD	Ministério da Defesa
NIST	National Institute of Standards and Technology
NSA	National Security Agency
Op Info	Operações de Informação
OTAN	Organização do Tratado do Atlântico Norte

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Graças à evolução tecnológica, a informação é disseminada cada vez mais em tempo real, mas também é manipulada e coletada para diversas finalidades na busca pela superioridade de informações.

As Operações de Informação (Op Info) contribuem nesse esforço pela busca da superioridade de informações e consistem na atuação de potencialidades para informar e influenciar grupos e pessoas, afetar a decisão de oponentes e evitar ou neutralizar os adversários na Dimensão Informacional.

Os conflitos modernos evoluem de acordo com o desenvolvimento da tecnologia e, muitas vezes, em meio a batalhas no ambiente informacional (ANTONOVICH, 2011), trazem consequências reais. Ao mesmo tempo, essa evolução é acompanhada por novas necessidades quanto à segurança e defesa, além de alterar profundamente a sociedade, transformando, inclusive, a forma de se comunicar e trabalhar.

O objetivo deste trabalho é, a partir de pesquisas bibliográficas em literaturas técnicas e artigos acadêmicos: efetuar uma análise comparativa das estratégias utilizadas nas Op Info pelos EUA e Rússia, verificar os impactos destas estratégias para o Brasil e responder à seguinte questão: como fortalecer a imagem da Marinha frente aos perigos da desinformação?

Em síntese, este trabalho é estruturado em sete seções, incluindo a Introdução. A segunda seção trata da definição de operações de informação. A terceira seção aborda como os EUA e a Rússia usam a informação como arma estratégica nos conflitos modernos. A quarta faz referência a como os EUA e a Rússia usam a desinformação como arma estratégica nos conflitos modernos. A quinta seção trata da comparação entre as estratégias dos EUA e da Rússia. A sexta seção trata dos impactos das estratégias destes dois países para o Brasil. A sétima seção trata do fortalecimento da imagem da Marinha.

2 OPERAÇÕES DE INFORMAÇÃO

O conceito doutrinário da agregação de instrumentos para atuar na informação começou em 1986, nos EUA, com o nome de *Command and Control Warfare*, durante a Guerra Fria (BRASIL, 2018), mas somente em 1996 surge o termo "Operações de Informação", com a divulgação da "Visão Conjunta 2010", sendo um grande sucesso na 1ª Guerra do Golfo (BRASIL, 2018). O termo passou a representar uma coordenação integrada das Capacidades Relacionadas à Informação (CRI) para efetuar ou ajudar outras operações, informando e

influenciando pessoas ou grupos, para atingir os objetivos e minar o processo decisório dos adversários (BRASIL, 2018).

As Op Info são definidas nos EUA da seguinte forma: como complementares das questões de apoio e de melhora dos dados para combater e conquistar o campo de batalha; como contínuas dentro do campo informacional onde se encontram; que ajudam a proteger com sua capacidade e obter vantagem no ambiente da informação ou atrapalhar a decisão do oponente (UNITED STATES, 1996) e podem ser usadas para ajustar o ambiente de operações por meio de ações de natureza "não militar", por meio da verificação de possíveis perigos, reduzindo confrontos e instabilidades, e interrompendo processos que possam gerar o início de uma crise.

Em uma sociedade cada vez mais dependente da informação, os conflitos modernos podem ser travados na dimensão informacional, que é o lugar em que os decisores e sistemas automatizados utilizam e agem de acordo com as informações, sendo o principal ambiente de tomada de decisão (BRASIL, 2014). O ambiente informacional tem grande importância, uma vez que as transformações sociais estão fundamentadas na capacidade de transmissão, acesso e compartilhamento da informação (BRASIL, 2014), e seu domínio por uma força militar pode permitir um melhor conhecimento do espaço de batalha em relação aos seus inimigos, mas também pode ocasionar instabilidade no cenário mundial e o surgimento de conflitos. O conflito ocorre pelo choque de vontades, envolvendo interesses antagônicos (GIDDENS; SUTTON, 2016) e são acompanhados pela mídia, que contribui para o entendimento da opinião pública.

A dinâmica da evolução tecnológica exige mudanças cada vez mais rápidas junto à sociedade no ambiente operacional, fazendo com que as Op Info sejam um instrumento integrador de várias capacidades. As Op Info passam, então, a integrar as CRI, reunindo diversos vetores com o objetivo de informar e influenciar públicos-alvo adversários e neutros, ajudando a confundir os oponentes ou até mesmo impedir ou neutralizar as ações adversárias na dimensão informacional. Nesse contexto, a popularização da televisão, da Internet e, principalmente, das redes sociais, acelerou exponencialmente a circulação da informação, na base da sociedade da informação, a tal ponto que o espaço físico e o ciberespaço refletem suas ações entre si e aumentam a preocupação quanto à proteção de informações e em como combater notícias falsas. Portanto, as Op Info devem encarar essas mudanças e buscar a atualização dos fatores de decisão por eles analisados de forma mais integrada, na busca pela melhor decisão possível.

A informação e a desinformação podem ser utilizadas como instrumento para ataque ou defesa, uma arma estratégica capaz de destruir ou manipular o inimigo.

3 A INFORMAÇÃO COMO ARMA: EUA E RÚSSIA

O campo da informação é de grande importância em todos os conflitos. Conseguir o conhecimento e utilizá-lo ou negá-lo ao inimigo de acordo com as decisões estratégicas, é de extrema importância, capaz de definir qualquer conflito. O impacto do desenvolvimento tecnológico computacional, as mídias sociais e o surgimento da Inteligência Artificial (AI), também têm grande importância na sociedade, alterando tanto a forma de se pesquisar como a forma de se utilizar esta informação. A informação pode ser disseminada rapidamente, mas se for modificada a ponto de perder a percepção de realidade contribuirá para a propagação da desinformação. Assim, a dimensão informacional é fator de decisão nos conflitos modernos. A informação pode ser utilizada nas Op Info para ataque ou proteção contra o oponente, e, por isso mesmo, é uma arma que pode neutralizar, confundir ou destruir o inimigo.

3.1 Estratégia

Nos próximos subitens, serão abordadas as estratégias de uso da informação dos EUA e da Rússia.

3.1.1 EUA

A superioridade da informação é a capacidade de ter uma quantidade maior de informações, com qualidade maior do que a do adversário. Permite o controle da dimensão informacional para usar as informações de sistemas e recursos e alcançar uma vantagem operacional em um conflito ou controlar a situação em operações de guerra, enquanto nega estas capacidades para o adversário.

A forma com que a informação é conduzida, aumenta a importância de se combater as dificuldades da visão global, pois as informações são compartilhadas cada vez mais rapidamente através de modernas tecnologias. Tomar uma decisão se tornou cada vez mais um desafio dinâmico e multidimensional, pois as operações devem ocorrer simultaneamente a decisões e planejamento sobre operações futuras.

Os EUA foram o primeiro país a desenvolver doutrinas voltadas para o uso da informação no ambiente de conflito, além do termo Operações de Informação (UNITED STATES, 1996), mas foi a inquietação sobre a integração das Op Info no contexto militar e civil que permitiu que este conceito fosse colocado na *Joint Publication* 3-13 (UNITED STATES, 2012). A NSA é a mais importante agência de segurança da informação dos EUA,

ela é responsável pela proteção do espaço cibernético daquele país, pelo setor de segurança e inteligência e é formada por vários escritórios que trabalham juntos ou isolados.

Após os atentados do 11 de setembro de 2001, entretanto, houve a criação da *Quadrennial Defense Review* (UNITED STATES, 2006) e o governo passou a identificar o valor destas operações como capacidade essencial na resolução de conflitos juntamente com as Forças Armadas.

O medo provocado pelos atentados passou a ser usado pelo governo com a finalidade de legitimar suas ações (BAUMAN *et al.,* 2014) e houve a "securitização do terrorismo" (BALKIN, 2008), ou seja, estabeleceu-se uma prerrogativa de emergência para justificar atos que garantissem o retorno ao estado normal; e, assim, as autoridades criaram um plano para espionar, autorizado por meio de legislação emergencial: a *Authorization for the Use of Military Force* (*AUMF*)[1] e o *Patriot Act*[2]. O *Patriot Act*, por exemplo, permitiu que diversos abusos à privacidade fossem praticados por agências de vigilância, como a NSA (REES, 2006), uma das mais conhecidas dos EUA, e apontada como responsável por abusos quanto ao direito à privacidade e segurança. Em 2003, foi aprovada a *Information Operations Roadmap* (*IOR*), tornando as Op Info uma atribuição militar essencial, com orientações e objetivos para todos os agentes de defesa, iniciando em períodos de paz até ocorrer a estabilidade. De todas as normas, a JP 3-13 descreveu melhor o assunto.

O ambiente da Internet é livre, ou seja, não existe um órgão ou nação que seja responsável pela aplicação de penalidades em caso de crimes ou abusos cometidos nesse ambiente. Assim, os Estados utilizam o ambiente do ciberespaço como querem.

Em 2011, o governo americano anunciou uma série de medidas, uma delas foi afirmar sua tática para proteger o ciberespaço (UNITED STATES, 2011), em que confirmou a importância do assunto e quais seriam as vantagens de se obter o domínio deste ambiente. Por meio da *Executive Order,* definiu quais informações poderiam ser obtidas, armazenadas e divulgadas; e pelo *Patriot Act* permitiu tipificar o "terrorismo doméstico", ou seja, qualquer pessoa pode ser considerada terrorista de acordo com suas atitudes (HASTEDT, 2011). O estado de vigilância surgiu com o monitoramento de todos e foi justificado pelo terrorismo (BAUMAN *et al.,* 2014). Em 2013, Edward Snowden, ex-funcionário da NSA, divulgou para a imprensa informações que seriam, segundo ele, da agência:

---

[1] *Authorization for the Use of Military Force* (*AUMF*) decreto que foi transformado em lei, autorizando o uso das Forças Armadas dos EUA contra os responsáveis pelos ataques de 11 de setembro (UNITED STATES, 2001a).

[2] *Patriot Act* é um decreto que autoriza órgãos de segurança e de inteligência dos EUA a interceptar ligações telefônicas e e-mails de possíveis envolvidos com o terrorismo, sem necessidade de autorização da Justiça (UNITED STATES, 2002).

–

– existência de uma rede de vigilância usada pela NSA para coletar informações de indivíduos dentro do território dos EUA (YOO, 2007) e de pessoas fora do território nacional (UNITED STATES, 2008);
– que a empresa Google ajuda na coleta de informações para o programa que treina os agentes (PRISM);
– que o ECHELON (POTENGY, 2000) era usado para coletar informações, inclusive de uso militar (COSTA, 2003);
– que interceptava ligações feitas por telefone (UNITED STATES, 2008); e
– que coletava e armazenava informações da Web (BAUMAN *et al.*, 2014).

A capacidade do governo dos EUA de influenciar as percepções e a tomada de decisão de outros afeta muito a eficácia da dissuasão, a projeção de poder e outros conceitos estratégicos. Em tempos de crise, a informação pode dissuadir adversários de iniciar ações prejudiciais aos interesses do governo dos EUA ou contra seus aliados. Dessa forma, o governo norte-americano utiliza seu poder, inclusive, na dimensão informacional, para impedir que seus adversários possam prejudicá-lo ou a seus aliados.

3.1.2 Rússia

O conceito de Op Info, para a Rússia, é definido como a tentativa de influenciar a mentalidade de um grupo adversário ou a população, e ele tem sido usado ao longo da história para afetar os resultados da guerra (THOMAS, 2019).

O pensamento militar russo está mudando devido às inúmeras conquistas tecnológicas, resultando em conceitos mais antigos sendo reorganizados, atualizados ou até mesmo sendo descartados. Como o caráter do conflito e o potencial para a guerra mudaram, os níveis educacional, profissional e de instrução seguem o mesmo caminho (HALPIN *et al.*, 2006). Comandantes e professores ensinam subordinados a como tomar iniciativa em combate e desenvolver aplicações novas e criativas de arte militar. Devido aos desenvolvimentos de alta tecnologia em inteligência artificial, computação quântica e outras áreas, os pontos de vista também estão se atualizando, e, assim, os oficiais russos fazem previsões de guerra futura a cada quatro ou seis meses por meio de novas tecnologias.

Os oficiais russos pensam, também, que o desenvolvimento da técnica militar deve verificar o que é feito no Ocidente, ou seja, deve entender como pensa o inimigo para poder

avaliar seu plano de ação, estimar precisamente suas forças, recursos e potencial para ter sucesso em uma operação ou batalha. Não deve copiar o que outros exércitos fazem, mas deve aprender com seus erros e acertos, além de aprender o que os outros países pensam sobre o pensamento militar russo, evitando estereótipos. Assim, os russos utilizam diversas estratégias para a obtenção de informação, conforme seu pensamento e doutrina, tais como:

– camuflando as próprias tropas; desorganizando as tropas adversárias; reduzindo a aplicação da eficiência do armamento e dos ativos eletrônicos do adversário; e garantindo a estabilidade da força amiga no controle de suas próprias tropas e armas. (MORGAN, 2016);

– desenvolveram granadas capazes de auxiliar em missões de vigilância que geram imagens de vídeo com alcance de 2.500 metros utilizando sistemas com conceito reflexivo controle (RC) baseado na *maskirovka* (MORGAN, 2016). A *maskirovka é* uma percepção russa em que se transmite a um inimigo informações falsas para o levar a tomar a decisão desejada por quem iniciou a ação. Um exemplo dessa técnica são as cópias infláveis de sistemas de mísseis de defesa aérea S-300PM russos utilizados para enganar os adversários quanto à sua localização real;

– utilizam o engodo nas Op Info: ao longo da campanha presidencial dos EUA, a Rússia produziu ataques de informações falsas, tendo como objetivo eleger um certo candidato, mas, principalmente, minar a tomada de decisão democrática (THOMAS, 2019; UNITED STATES, 2012);

– utilizam a dissuasão: compreendem que a dissuasão não é dominar o adversário no campo de batalha, mas dar a ele uma visão de derrota, ou seja, é um jogo reflexivo, com visão de vitória, derrota e danos; e que existem dois termos para defini-la: *sderzhivanie* e *ustrashenie*. O primeiro define como contenção, usado para limitar o desenvolvimento de armas ou o uso de atividades militares. O outro é definido como dissuasão por meio de intimidação ou medo (ECKERT, 2004);

– criam impasses de informações estratégicas: para desorganizar militares e civis, enganar um adversário e manipular a opinião pública;

– ser capaz de interromper, se necessário, os fluxos de informação de um adversário: a respeito disso, a Rússia está se concentrando nas transportadoras de informação, ou seja, cabos subaquáticos, satélites e meios de guerra eletrônica, para controlar ou interromper o fluxo de dados. Uma das formas é por meio do uso do navio Yantar, que pode submergir a uma profundidade de mais de 6.000 metros e obter dados de cabos submarinos; ou utilizando

recursos REB, que exigem o mapeamento da rede de informações do oponente para causar confusão ou perturbação;

– uso de “informação hostil” (técnica da informação psicológica): pode violar a soberania do estado ou interferir nos assuntos internos de um país; (THOMAS, 2019);

– criação de tropas de operação de informação;

– uso de grupos de hackers com alto estado organizacional, identificados como “Ameaças Persistentes Avançadas” (APT): Em geral, que tenham prejudicado sistemas operacionais por meio de e-mails com anexos ou links maldosos e cujos assuntos despertam o interesse das vítimas (WEEDON, 2015). Esses hackers procuram fragilidade nas redes de informação do oponente para poder explorar as falhas de seus sistemas. Destes grupos, destacam-se os hackers APT28: CyberBerkut, Fancy Bear e Pawn Storm (KOVAL, 2015). O CyberBerkut, por exemplo, atacou o sistema da Ucrânia responsável pelas Eleições, já a ameaça Sofacy, usada pelo Fancy Bear, prejudicou diversos sistemas operacionais das forças armadas da Ucrânia (MEYERS, 2016) e foi implantado em simpósios militares ucranianos, através de um aplicativo que permitiu obter a localização das tropas (MEYERS, 2016). O Pawn Storm, por sua vez, atacou por e-mail diversos sistemas corporativos militares, políticos e civis e publicou estes dados (PAGANINI, 2017);

– uso do *clickbait*: essa técnica de marketing é usada para instalar vírus nos computadores e roubar informações; e

– divulgou um documento chamado “Visões conceituais sobre as atividades das Forças Armadas da Federação da Rússia no espaço de informação”, no qual constavam as estratégias utilizadas no campo cibernético, incluindo ajuda e interação com outros Estados, possibilidade de as Forças Armadas utilizarem de todos os meios possíveis como disfarce operacional, informações privadas, proteção de sistemas, entre outros (CRUZ JÚNIOR, 2013).

3.2 Vulnerabilidades

Nos próximos subitens, serão abordadas as vulnerabilidades do uso da informação pelos EUA e pela Rússia.

3.2.1 EUA

Os EUA possuem grande poder tecnológico e econômico. Quanto maior este poder, maior também tem que ser o investimento em segurança e maior é sua vulnerabilidade, pois o

país será alvo de diversos outros países. Dentre as vulnerabilidades apresentadas em relação à informação, destacam-se:

– Falha de informação: em 1953 quando Stalin faleceu, o Presidente dos EUA soube do ocorrido por meio da mídia e não por meio de sua agência de segurança, o que provocou o descrédito da NSA (AID, 2009);

– Possibilidade de que um adversário use um software malicioso para avaliar a vulnerabilidade das informações nas redes e que utilize vírus para prejudicar sistemas militares ou civis: 1) em 1988, houve o primeiro caso de um vírus de computador autorreplicante, conhecido como *Worm*, sendo as Forças Armadas o maior alvo deste ataque; 2) em 1994, um hacker conseguiu invadir o Centro de Desenvolvimento da Força Aérea de Griffiss e corrompeu mais de trinta sistemas governamentais; 3) em 2008, adversários dos EUA invadiram os sistemas do Comando Central dos Estados Unidos (CENTCOM), enganando acessos, *firewalls* e criptografias, por meio de drives contaminados e abandonados perto daquele comando. Militares, movidos pela curiosidade, conectaram os dispositivos, comprometendo todo o sistema (HABIGER, 2010), e, por este motivo, foi proibido o uso de dispositivos removíveis; 4) em 2015, a energia da Ucrânia foi desligada devido a um ataque cibernético contra os ucranianos, originado em Moscou. O chamado *malware "Black Energy"* (THREATSTOP, 2016), que causou o evento, foi detectado também nos EUA. Apagando as luzes em Kiev, Moscou mostrou que é capaz de penetrar na rede americana e enviou um aviso aos EUA: para não tentarem um ataque no estilo do vírus cibernético Stuxnet sobre seu país ou sobre seus aliados. Nesta visão, a Rússia usa uma estratégia de dissuasão para limitar as ações de seu inimigo; 5) em 2017, o Presidente dos EUA proibiu o uso do antivírus Kaspersky em agências civis e militares, por alegar que hackers russos podem explorar uma vulnerabilidade e invadir sistemas do governo e de empresas, mas esse antivírus já era comercializado há anos no país, inclusive sendo usado pela NSA, que teve informações roubadas por um hacker russo;

– Uso de *fake news*: foram usadas, por exemplo, para confundir a sociedade americana nas eleições de 2016, nos EUA, e durante a pandemia de COVID-19;

– Uso de *deepfakes*: podem ser usadas para confundir a sociedade, desmoralizar, criar conflitos. Com imagens cada vez mais próximas da realidade, são um grande perigo, podendo levar a conflitos;

– Perigo do *clickbait*: milhares de computadores são contaminados por vírus ou têm suas informações roubadas por meio dessa técnica de marketing;

– Sabotagem de sistemas: em 2018, a Amazon.com Inc. informou às autoridades dos EUA ter sofrido um ataque à sua cadeia produtiva, por meio de *chips* inseridos em seus sistemas críticos, afetando indústrias e atingindo, inclusive, o Departamento de Defesa dos EUA (DoD), a CIA e navios de guerra americanos; e

– Hackers russos utilizam as redes sociais para incitar a violência, confundir e desestabilizar o governo americano: em 2020, o Presidente Trump editou um decreto para regular as redes sociais no país, para diminuir a propagação de ondas de violência causadas por hackers russos.

3.2.2 Rússia

A Rússia, após a Guerra Fria, investiu muito em tecnologia, mas tem como principal opositor os EUA. Sentindo que seus sistemas possam ser ameaçados, os russos buscam soluções para suas vulnerabilidades:

– Internet global: a Rússia utiliza a rede cujo domínio é dos EUA. A preocupação com uma possível negação dessa rede ou seu uso para danificar seus sistemas de armas nucleares, gerou inquietação, e Putin, então, resolveu substituir a Internet global pela Runet, ou seja, uma solução nacional;

– A visibilidade dos conflitos modernos: a tropa também pode sofrer influência da estratégia da desinformação para afetar o seu moral, pois a presença da imprensa nos conflitos modernos pode facilitar a circulação de notícias falsas;

– Desenvolvimento de sistemas de criptografia quântica (MENDES; PAULICENA; SOUZA, 2011) e sistemas de criptografia pós-quântica para proteger as informações; (THOMAS, 2019); e

– O uso deliberado de *software* malicioso: a Rússia está deixando de usar o Windows por alegar que ele possui falhas que podem ser usadas pelos EUA para sabotar seus sistemas nucleares e de defesa.

4 A DESINFORMAÇÃO COMO ARMA: EUA E RÚSSIA

A desinformação pode ser utilizada nas Op Info para ataque ou proteção contra o oponente e, por isso mesmo, é uma arma que pode neutralizar, confundir ou destruir o inimigo.

A circulação de informações sempre foi importante para a sociedade, mas alguns fatores aumentaram a rapidez da disseminação de informações que não são verdadeiras, tais como:

- a perda da confiança da sociedade na mídia e nas corporações;
- a facilidade no acesso à rede;
- a ausência de educação no mundo digital (ALBRECHT, 2015);
- a ausência de crítica; e
- a preocupação em monetizar, por meio do *clickbait* (ALEXANDER *et al.*, 2017).

Na era digital, é muito mais fácil publicar informações falsas do que verdadeiras, pois as falsas despertam interesse e são rapidamente compartilhadas e tomadas como verdadeiras, espalhando-se em uma verdadeira cascata de informação[3], muitas vezes, por meio do uso de *bots* e *trolls*. Enquanto as notícias falsas são aquelas que parecem verdadeiras, mas possuem distorções intencionais para atrair a atenção, as *fake news* são mentiras produzidas para enganar os leitores com finalidade política ou financeira (ALLCOTT; GENTZKOW, 2017).

Apesar de o termo *fake news* não ser recente, apenas agora foi notada a intenção do seu uso para controlar e gerar confusão na sociedade (BOTEI, 2017). Sua disseminação é favorecida pelo fato de o espaço cibernético e a mídia sobrecarregarem a sociedade com grande volume de notícias, muitas delas falsas (WARDLE; DERAKHSHAN, 2017), levando à desinformação. A desinformação, inclusive, é usada, muitas vezes, com o objetivo de confundir e criar instabilidade (FRIAS FILHO, 2018). Um exemplo disso ocorreu no período da pandemia da COVID-19, quando diversas *fake news* foram disseminadas por meio da mídia para confundir a população (MALYSHEV, 2000, p. 2-8) quanto ao tratamento e, assim, criar instabilidade no governo.

Enquanto algumas pessoas debatem se o termo *fake news* abrange ou não a notícia que não é verdadeira, ou como impedir que se propague, a tecnologia está em constante evolução, permitindo que se associe com a inteligência artificial, surgindo os *deepfakes* (BLITZ, 2018, p. 62). *Deepfake* é um método que manuseia som, imagem e fala por meio de inteligência artificial. Liga e superpõe imagens, vídeos e sons que existem a um novo arquivo, sendo assim, a junção dos termos *deep learning* e *fake media* (DENG, 2014).

A popularização dos *deepfakes* é uma das maiores preocupações de governantes (HASAN; SALAH, 2019), juristas, jornalistas e especialistas em cibersegurança, pois esse recurso destrói a confiança em algo que, até então, tinha credibilidade: a gravação em vídeo. Se

[3] Cascata de informação ocorre quando temos um tipo de comportamento (ou decisão) que é repetido por vários atores com base na observação dos demais (influência), e não em uma análise a partir das informações recebidas a respeito.

um corrupto fosse filmado recebendo propina, não poderia dizer que não cometeu o delito; entretanto, com os *deepfakes* e o alto nível de realidade das imagens, um dia não será mais possível distinguir entre a realidade e uma manipulação de imagens, gerando impactos na sociedade mundial (PECEQUILO, 2016).

Portanto, a sociedade é diariamente atingida pela desinformação, que tem por objetivo influenciar a liderança e a opinião pública de estados estrangeiros (DONSKOV, 2005); ela se espalha pelas redes sociais rapidamente, podendo provocar desestabilização política, econômica ou financeira, além de poder gerar conflitos.

4.1 Estratégia

Nos próximos subitens, serão abordadas as estratégias de uso da desinformação pelos EUA e pela Rússia.

4.1.1 EUA

Quando as pessoas contestam o Estado informacional e o controle estatal, esquecem-se de que grande parte do que é produzido e disponibilizado nas redes é oriundo de tecnologia dos EUA (DANTAS, 2002), permitindo, assim, a manipulação da informação por seus serviços de inteligência e informação.

Dessa forma, a capilaridade social é atingida por meio do domínio das ferramentas de desinformação e pela hegemonia informacional, por meio de satélites e redes sociais, que influenciam nas decisões por meio da mídia (DUNNIGAN; NOFI, 2001). As redes sociais são a maior forma de disseminação de desinformação nos Estados Unidos.

4.1.2 Rússia

Os russos consideram que existem dois tipos de guerra de informação, de acordo com o objetivo a ser alcançado, a saber:

– guerra psicológica da informação para afetar os militares e a população; e

– guerra de tecnologia da informação (para afetar sistemas técnicos que recebem, coletam, processam e transmitem informações durante guerras e conflitos armados) (KVACHKOV, 2019).

O conceito desinformação (*dezinformatsiya*), é entendido como uma técnica militar para confundir e levar o adversário a errar (OAS, 2017), sendo propósito da inteligência russa, cuja KGB e o GRU são os principais agentes e onde o Departamento de Desinformação

substituiu o “Disinformburo” (COMITÊ CENTRAL DO PARTIDO COMUNISTA DA UNIÃO SOVIÉTICA, 1923).

A estratégia da desinformação é utilizada pelo governo russo da seguinte forma:

– por meio do controle dos meios de comunicação que são controlados pelo governo, que atinge seus objetivos, uma vez que a maioria dos russos acredita nessas informações manipuladas (KHALDAROVA; PANTTI, 2016);

– por meio do *Deepfake*, ou seja, combina os termos *deep learning* com *fake media*, e designa uma estratégia de manipulação de vídeo e áudio com uso de AI para desinformar: em 2017, o Presidente da Rússia, declarou que a inteligência artificial fará parte do futuro das pessoas, mas que há perigos difíceis de serem previstos. Dois anos depois, o Centro de Inteligência Artificial da Samsung em Moscou apresentou um novo *software*, capaz de criar vídeos *deepfakes* (MORAES, 2017) com apenas uma imagem, utilizando a tecnologia de GAN (ESG, 2019).

4.2 Vulnerabilidades

Nos próximos subitens, serão abordadas as vulnerabilidades do uso da desinformação pelos EUA e pela Rússia.

4.2.1 EUA

A desinformação é uma grande ameaça para Estados democráticos como os EUA. Por meio de técnicas de *fake news* e *deepfakes*, mentiras são disseminadas para desestabilizar o governo e sua economia, além de tentar desmoralizar instituições e pessoas. Dentre os exemplos desse tipo de ataque, muitas vezes iniciados por hackers, estão:

– Em 2016, o Facebook foi apontado como responsável por ajudar a disseminar desinformação durante as eleições de Trump para a presidência dos EUA (ALLCOTT; GENTZKOW, 2017). A empresa então resolveu implantar bloqueios contra publicações falsas, e firmar parcerias com *fact checkers* para a identificação de conteúdo suspeito; o Google também foi indagado por facilitar a visualização de resultados de busca por notícias falsas e, por isso, passou a apoiar o First Draft News, uma ONG voltada ao jornalismo sério e ao combate às *fake news*, criando o Cross Check. Criou também um mecanismo para identificar *fake news* e uma ferramenta de denúncia.

– Em 2017, pesquisadores da Universidade de Washington utilizaram tecnologia *deepfake* para fazer um vídeo falso do ex-presidente Barack Obama que impressionou pela imagem

realista. O diretor Jordan Peele procurou alertar as pessoas sobre o perigo desses vídeos para o mundo (FONTES, 2019).

4.2.2 Rússia

A desinformação é muito utilizada pela Rússia interna e externamente, por meio de *fake news* e *deepfakes,* mas os EUA podem usar o seu domínio tecnológico para prejudicar ou atrapalhar o avanço tecnológico, militar e econômico dos russos, por meio de:

– Domínio do espaço e ciberespaço: os EUA podem utilizar seus satélites contra os sistemas e satélites da Rússia, impedindo o controle das comunicações e permitindo a manipulação da mídia pelo oponente, podendo disseminar a desinformação para confundir a população russa ou suas tropas (HALPIN, 2006); e

– Dependência da Internet global: 1) Em 2019, a Rússia testou com sucesso uma alternativa russa para substituir a Internet mundial. Sendo dependente Internet global a Rússia é vulnerável a ciberataques, e por isso, desenvolveu a Runet, para poder controlar seu fluxo de dados ou impedir seu acesso fora do Estado quando quiser; 2) No mesmo ano, os EUA demonstraram que a preocupação dos russos tinha fundamento, pois interromperam a Internet da Agência IRA, ligada ao governo russo, usada para disseminar desinformação.

5 COMPARAÇÃO ENTRE AS ESTRATÉGIAS

A análise das estratégias usadas pelos EUA e pela Rússia permite concluir que utilizam essas técnicas para:

– desvalorizar e deslegitimar pessoas e organizações;
– aumentar preconceitos e gerar conflitos;
– controlar e manipular sistemas;
– negar, quando quiser, acesso à informação;
– sabotar governos, instituições e empresas, inclusive por meio de *hackers*;
– buscar a superioridade da informação;
– manobrar a opinião pública;
– desestabilizar governos;
– criar desestabilização política e econômica; e
– roubar informações que possam ser usadas contra seu adversário.

6 IMPACTOS DAS ESTRATÉGIAS PARA O BRASIL

O Estado brasileiro adota diversas medidas para se proteger de ataques cibernéticos, tais como a adoção de procedimentos e normas de segurança e esclarecimento sobre o problema da desinformação. Entretanto, com o desenvolvimento de novas tecnologias e estratégias de Op Info, devem aumentar os ataques cibernéticos dentro do território nacional.

Nenhum país está imune a ciberataques, e o Brasil, segundo relatório da Symantec, está classificado em terceiro lugar, quanto aos países que mais sofreram esse tipo de ataque em 2019, ficando atrás dos EUA e da Rússia (IMASTERS, 2019).

As estratégias usadas por estes dois países para manter o controle e a superioridade das informações trazem os seguintes impactos para o Brasil:

– o aumento de ataques cibernéticos por *hackers* com solicitação de resgate: é facilitado por meio de empresas interconectadas à rede global de computadores e com a participação de empresas brasileiras de comunicação. Em 2017, por exemplo, ocorreu um grande ciberataque, governamental, usando um *ransomware* que criptografou dados e exigiu resgate por cada equipamento atacado de empresas como a Petrobras e o INSS.

– crescimento de tentativas e golpes para obtenção de dados confidenciais, inclusive sobre reservas energéticas e de petróleo (SAMPEDRO, 2015);

– monitoramento de cidadãos e autoridades brasileiras com roubo de dados, prejudicando a privacidade como um direito humano;

– aumento de sabotagem e de roubo de informações industriais;

– vulnerabilidade de sistemas, inclusive militares, que podem sofrer ataques ou negação de uso diante da dependência à rede global de computadores e ao sistema GPS (ESG, 2019);

– aumento de *fake news* e *deepfakes*: 1) que o Ministro Paulo Guedes anunciou o fim do auxílio-reclusão; 2) que o BNDES teria emprestado dinheiro ao país de Obiang Mangue; 3) que usar máscara para prevenir COVID-19 deixa o sangue ácido e enfraquece o sistema imunológico;

– aumento do uso de *trolls* e *bots* para disseminar desinformação (RUSSIAN FEDERATION, 2000);

– aumento do risco à integridade de estruturas estratégicas essenciais e ao controle de diversos sistemas e órgãos que, se afetados, poderão impactar a Segurança Nacional;

– aumento de ataques cibernéticos visando acessos a sistemas críticos e roubo de informações: a Marinha do Brasil passou a adotar medidas de orientação quanto aos procedimentos de

segurança e operação por meio do Centro de Tecnologia da Informação da Marinha (CTIM), incluiu, em suas normas, medidas que devem ser observadas pelos usuários para aumentar a segurança e impedir a ação maliciosa dentro do espaço cibernético;

– aumento do uso de *fake news* para enfraquecer e desmoralizar a imagem das Forças Armadas diante da sociedade: o Exército Brasileiro resolveu utilizar o Centro de Comunicação Social do Exército (CCOMSEx) para ajudar no fortalecimento da imagem institucional do Exército, por meio do uso da AI e criação da figura do Soldado MAX (FIGURA 1), um *chatbot* com interação homem-máquina (MORENO *et al.*, 2015) e campanhas de combate *às fake news*; e

– empresas nacionais estão preocupadas com a desmoralização institucional por meio das *fake news*: o Magazine Luiza, rede varejista brasileira, criou a primeira *influencer* digital do Brasil, a "Lu", com mais de 14 milhões de seguidores; é um *chatbot* com aparência feminina (FIGURA 2). O objetivo da personagem é conquistar a confiança e simpatia dos usuários e poder responder a perguntas sobre assuntos relevantes, inclusive sobre *fake news* e *deep fakes*.

7 O FORTALECIMENTO DA IMAGEM DA MARINHA

A MB também adota medidas de proteção e de esclarecimento, mas, devido ao crescimento alarmante de tentativas de acesso indevido e de tentativas de ofuscar a imagem da Instituição, coloca-se aqui a sugestão de criação de um *chatbot* para a Instituição, usando como exemplo a experiência do EB com a criação do "Soldado Max".

Apesar de os personagens irreais não votarem, não tomarem vacina, não transmitirem doenças, eles são capazes de capturar a atenção dos usuários e criar uma opinião pública artificial, ou seja, a atuação desses personagens nas redes sociais, ao se confundirem com usuários comuns, pode orientar o comportamento dos humanos e alterar de maneira significativa a tomada de decisão.

A doutrina militar naval tem uma narrativa que não aceita a desinformação. A resposta adequada a estas ameaças depende do monitoramento do espaço cibernético com ferramentas tecnológicas que permitam a análise e o combate aos perigos deste ambiente informacional. Nessa tarefa, a comunicação estratégica, a inteligência e a defesa cibernética precisam estar integradas, de modo a permitirem um assessoramento e uma tomada de decisão à altura da ameaça a ser enfrentada, sem perda de tempo e com as medidas que se fizerem necessárias. A desinformação é oportunista e não pode ser desprezada, por conta dos prejuízos que ela possa causar, daí a necessidade de vigilância constante por meio de tecnológicas próprias de monitoramento e segurança. Deixar de desenvolver capacidades e estratégias nessa

área poderá acarretar sérios prejuízos ou danos à Estrutura Militar de Defesa e ao futuro do País.

O grande problema com a disseminação da desinformação e principalmente, com as *deepfakes,* será o grande impacto que causarão, inclusive no Brasil.

Por meio do Centro de Comunicação Social da Marinha (CCSM), a comunicação social pode ser utilizada de modo estratégico para combater às *fake news* e *deepfakes,* permitindo o fortalecimento de sua imagem institucional, de sua reputação e confiança junto à sociedade brasileira. Nesse sentido, conquistar o apoio da opinião pública confere legitimidade à obtenção de liberdade de ação para atingir os objetivos estratégicos e operacionais da Força.

Nesse sentido, a proposta de criação de um *chatbot* para a MB poderá:

– fortalecer a imagem da Instituição;

– conscientizar o público interno e externo dos perigos existentes na disseminação de *fake news*;

– alertar sobre o perigo dos *deepfakes*;

– ajudar na divulgação de campanhas e eventos da instituição; e

– aproximar o público-alvo, pois a representação da personagem por uma figura feminina, com imagem modelada tridimensional, humanizará este contato.

Assim, o *chatbot* seria uma "boneca virtual", com imagem realista (FIGURA 3), com as seguintes características:

– Posto: Primeiro-Tenente;

– Corpo: Quadro Técnico;

– Formação: Comunicação Social;

– Nome: Mariana;

– Personalidade: simpática e educada;

– Objetivo: gerar empatia e aproximar-se mais da população, ajudando a fortalecer a imagem da Instituição e a esclarecer dúvidas.

Durante o desenvolvimento, deverá ser montada uma equipe constituída por profissionais de diversas áreas, responsável pela criação da história da personagem, que deverá estudar seu comportamento desejado e suas falas para cada situação.

8 CONCLUSÃO

A pesquisa apontou a importância da informação e como ela é compartilhada cada vez mais rapidamente graças à evolução tecnológica, mas também como pode ser manipulada para desinformar, explorando a vulnerabilidade de sistemas e a falta de educação digital. Nesse sentido, também foi possível apresentar as estratégias e as vulnerabilidades dos EUA e da Rússia nos conflitos modernos, os quais utilizam a informação e a desinformação como arma estratégica. Também foram analisados os impactos de suas estratégias para o Brasil.

A pesquisa apontou que a evolução tecnológica permite que a informação seja compartilhada, mas também pode ser manipulada para confundir o adversário ou o público. Assim, a imprensa, cada vez mais presente nos conflitos na busca pela transparência, exerce influência sobre a população. O apoio da população ajuda a conseguir a legitimidade para as ações que a Força tiver que desempenhar, na busca dos objetivos estratégicos nacionais.

Portanto, a comunicação social pode ser uma grande aliada para combater as *fake news* e *deepfakes*, e, por esse motivo, foi apresentada a proposta de criação de um *chatbot* para ajudar a fortalecer a imagem da Instituição, partindo da experiência bem-sucedida do EB.

Face ao exposto nesse trabalho, conclui-se que as ameaças cibernéticas estão em constante evolução, acompanhando o desenvolvimento tecnológico, e, portanto, a MB deve utilizar — além das medidas para garantia de sua segurança e de seus objetivos estratégicos já adotados em sua expertise — a comunicação social, para reforçar a imagem da Instituição e aproximá-la da população, por meio da criação de um *chatbot* com características humanizadas e realistas.

REFERÊNCIAS

AID, Mathew M. **The Secret Sentry:** The untold History of the National Security Agency. Nova York: Bloomsbury Press. 2009.

ALBRECHT, J. P. **Hands off our data!** Europa: The Greens/EFA, 2015.

ALEXANDER, Contributors Jenny *et al.* **Understanding fake news, the nature of the problem and potential solutions.** 2017.

ALLCOTT, Hunt; GENTZKOW, Matthew. Social Media and Fake News in the 2016 Election. **Journal of Economic Perspectives.** Volume. 31:2, Spring, 2017.

ANTONOVICH, P. Cyberwarfare: Nature and Content. **Military Thought**, Nº 3, Vol. 20, p. 35-43, 2011.

BALKIN, J. The Constitution in the National Surveillance State. **Minnesota Law Review,** Minneapolis, v. 93, n. 01, 2008.

BARROS, José Benedito de Moreira. A nova geopolítica mundial e seus reflexos para o Brasil. **Revista da Escola Superior de Guerra,** v. 23, n. 48, p. 5-6, p. 21-39, 2007.

BAUMAN, Zygmunt *at al.* After Snowden: Rethinking the Impact of Surveillance. **International Political Sociology,** v. 8, issue 2, p. 121-144, 2014.

BLITZ, Marc Jonathan. Lies, line drawing, and (deep) fake news. **Okla.** V. 72. L. Rev. 59. 2018.

BOTEI, Mircea. Misinformation with fake news. Transilvania University of Brasov. **Series VII, Social Sciences, Law,** v. 10, p. 133-140, 2017.

BRASIL. Exército Brasileiro. **EB20-MC-10.213:** Manual de Campanha — Operações de Informação. 1. ed. Brasília, DF, 2014.

BRASIL. Marinha do Brasil. **EMA-335:** Doutrina de Operações de Informação. Brasília, DF, 2018.

CAMPOS, Carolina. **Engajamento gerado pelos públicos na página corporativa do Magazine Luiza no Facebook e suas implicações na comunicação organizacional digital.** 2015. Monografia (para obtenção do título de Bacharel em Relações Públicas) — Universidade Federal do Pampa. São Borja, RS, 2015. Disponível em: http://cursos.unipampa.edu.br/cursos/relacoespublicas/files/2015/04/ENGAJAMENTO-GERADO-PELOS-P%C3%9ABLICOS-NA-P%C3%81GINA-CORPORATIVA-DO-MAGAZINE-LUIZA-NO-FACEBOOK-E-SUAS-IMPLICA%C3%87%C3%95ES-NA-COMUNICA%C3%87%C3%83O-ORGANIZACIONAL-DIGITAL.pdf. Acesso em: 25 ago. 2020.

COMITÊ CENTRAL DO PARTIDO COMUNISTA DA UNIÃO SOVIÉTICA. Resolução do Politburo do Comitê Central do RCP “Sobre a desinformação”. Publicado em: 11.01.1923.

Hrono.ru. Disponível em: http://hrono.ru/dokum/192_dok/19230111ck.php. Acesso em: 25 jul. 2020.

COSTA, Silvio. O Sistema Echelon de espionagem global ou a lei do vale tudo. **Revista Espaço Acadêmico,** ano II, n. 22, março de 2003. Disponível em: http://www.espacoacademico.com.br/022/22ccosta.htm. Acesso em: 4 ago. 2020.

CRUZ JÚNIOR, Samuel César da. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual.** Texto para discussão 1850 / Instituto de Pesquisa Econômica Aplicada. Brasília: Ipea, 2013. Disponível em: http://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=19183. Acesso em: 8 jun. 2019.

DANTAS, Marcos. **A lógica do capital informação:** a fragmentação dos monopólios e a monopolização dos fragmentos num mundo de comunicações globais. Rio de Janeiro: Contraponto, 2002.

DEFESANET. EB no combate às "fake news" e no combate à "desinformação". Publicado em: 22 de agosto de 2018. **DefesaNet,** 2018. Disponível em: https://www.defesanet.com.br/ghbr/noticia/30295/EB-no-combate-as-%E2%80%9Cfake-news%E2%80%9De-no-combate-a-%E2%80%9Cdesinformacao%E2%80%9D-/. Acesso em: 25 ago. 2020.

DENG, Li; YU, Dong. Deep Learning: Methods and Applications. **Foundations and Trends® in Signal Processing:** Vol. 7: No. 3-4, p 197-387, 2014. Disponível em: http://dx.doi.org/10.1561/2000000039. Acesso em: 25 ago. 2020.

DONSKOV, Yu Ye; NIKITIN, O. G. Operações especiais de informação em conflitos armados. **Pensamento Militar,** vol. 14, 2005.

DUNNIGAN, James F.; NOFI, Albert A. **Victory and deceit:** deception and trickery at war. San Jose: Writers Club Press, 2001.

ECKERT, D. **Le monde russe.** Paris: Hachette, 2004.

ESG. Escola Superior de Guerra. **Cadernos de Estudos Estratégicos.** ESG, 2019. Disponível em: https://www.esg.br/publi/arquivos-cadernos/copy_of_EdiodeMarode2019.pdf. Acesso em: 25 ago. 2020.

FONTES, Swami de Holanda. Muito além das fake News: as deepfakes. **DefesaNet,** 2019. Disponível em: https://www.defesanet.com.br/tecdi/noticia/34804/Muito-alem-das-fake-news--as-deepfakes//. Acesso em: 25 jul. 2020.

FRIAS FILHO, O. O que é falso sobre fake news. **Revista USP,** n. 116, p. 39-44, 2018.

GIDDENS, Anthony; SUTTON, Philip. **Conceitos essenciais da Sociologia.** 1. ed. São Paulo: UNESP, 2016.

HABIGER, Eugene E. **Cyberwarfare and Cyberterrorism:** the need for a new U.S. Strategic Approach. EUA: The Cyber Secure Institute, 1 fev. 2010.

HALPIN, E. et al. **Cyberwar, Netwar and the Revolution in Military Affairs.** New York: Houndmills, 2006.

HASAN, H. R.; SALAH, K. Combating Deepfake Videos Using Blockchain and Smart Contracts. **IEEE Access,** vol. 7, p. 41596-41606, 2019.

HASTEDT, Glenn. **Spies, Wiretaps, and Secret Operations: an encyclopedia of American Espionage.** Santa Bárbara: ABC-CLIO, LLC, 2011.

IMASTERS. Brasil é terceiro país que mais recebe ataques cibernéticos, diz relatório. Publicado em: 27 MAR, 2019. **iMasters,** 2019. Disponível em: https://imasters.com.br/noticia/brasil-ataques-ciberneticos. Acesso em: 11 jun. 2019.

KHALDAROVA, Irina; PANTTI, Mervi. **Fake News:** The narrative battle over the Ukrainian conflict. Journalism Practice, 2016. Disponível em: https://doi.org/10.1080/17512786.2016.1163237. Acesso em: 5 set. 2020.

KOVAL, Nikolay. Revolution Hacking Cys Centrum LLc, 2015. In: GEERS, K (ed.). **Cyber War in Perspective:** Russian Aggression Against Ukraine. NATO CCDCOE Publications: Tallinn, 2015.

KVACHKOV, V. **Спецназ России** (Russia's Special Purpose Forces). 2019.

MALYSHEV, V. Использование возможностей средств массовой информации в локальных вооруженных конфликтах (Making use of the media in local armed conflicts), **Zarubezhnoye voyennoye obozreniye,** No. 7, p. 2-8, 2000.

MENDES, A. J. B.; PAULICENA, E. H.; SOUZA, W. A. R. Criptografia Quântica: Uma Abordagem Direta. **Revista de Sistemas de Informação da FSMA,** v. 7, n. 39-48, p. 9, 2011.

MEYERS, Adam. Danger close: fancy bear tracking of Ukrainian field artillery units. Publicado em: 22/12/2016. **CrowdStrike.** Research & Threat Intel. 2016. Disponível em: https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/. Acesso em: 3 set. 2020.

MORAES, Cristiane Pantoja de. **"Deepfake" como ferramenta de manipulação e disseminação de "fake news" em formato de vídeo nas redes sociais.** 2017. Disponível em: https://pdfs.semanticscholar.org/40e6/2f4d88b9c1ac944ef229b2e7ab09c0d34076.pdf?_ga=2.119991503.636816415.1595723789-2027430841.1595723789. Acesso em: 25 jul. 2020.

MORENO, F.; MANFIO, E.; BARBOSA, C. R.; BRANCHER, J. D. Tical: Chatbot sobre o Atlas Linguístico do Brasil no WhatsApp. XXVI Simpósio Brasileiro de Informática na Educação. **Anais […].** SBIE, 2015. Disponível em: https://www.br-ie.org/pub/index.php/sbie/article/view/5170/3561. Acesso em: 3 ago. 2020.

MORGADO, Flávio Roberto Bezerra. Fatores da decisão. **Revista PADECEME,** v. 15, n. 24, Rio de Janeiro. 2020.

MORGAN, Maier. **A Little Masquerade:** Russia's Evolving Employment of Maskirovka. United States Army. School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas, 2016.

OAS. Organization of American States. **Join Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda.** 2017. Disponível em: http://www.oas.org/en/iachr/expression/showarticle.asp?artID=1056&lID=1. Acesso em: 21 ago. 2020.

OLIVEIRA, Filipe. Os segredos da Lu do Magalu, a primeira influenciadora digital do Brasil. **#TMJ,** 2019. Disponível em: https://tmjuntos.com.br/inovacao/o-que-esta-por-tras-da-lu-primeira-influenciadora-virtual-do-brasil/. Acesso em: 25 jul. 2020.

PADECEME. A dimensão informacional. **Revista PADECEME,** V. 15 n. 24. 01/2020. Disponível em: http://webcache.googleusercontent.com/search?q=cache:6-ZUgRT5bnwJ:www.ebrevistas.eb.mil.br/index.php/PADECEME+&cd=1&hl=pt-BR&ct=clnk&gl=br/. Acesso em: 25 jul. 2020.

PAGANINI, Pierluigi. **Back in BlackEnergy:** BlackEnergy Used as a Cyber Weapon Against Ukrainian Critical Infrastructure, 2017.

PECEQUILO, Cristina Soreanu. **Teoria das Relações Internacionais, o mapa do caminho:** estudo e prática. São Paulo: Alta Books, 2016.

POTENGY, Silvio. "Echelon" X Segurança Nacional. **Revista da Escola Superior de Guerra,** nº 39, Brasil, 2000.

REES, Wyn. **Transatlantic counter-terrorism cooperation:** the new imperative. 2006. Disponível em: https://catalogue.nla.gov.au/Record/3793556. Acesso em: 25 jul. 2020.

RUSSIAN FEDERATION. **National Security Concept of the Russian Federation.** Approved by Presidential Decree No. 24 of 10 January 2000. Disponível em: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768. Acesso em: 27 ago. 2018.

SAMPEDRO, Victor. **O quarto poder em rede.** 2015. Disponível em: http://www4.pucsp.br/neamp/downloads/o-quarto-poder-em-rede-portugues.pdf. Acesso em: 25 jul. 2020.

THOMAS, Timothy L. Russian Military Thought: Concepts and Elements. McLean, VA. Publicado em: agosto de 2019. **MITRE,** 2019. Disponível em: https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf. Acesso em: 24 ago. 2020.

THREATSTOP. **Black Energy.** Security Report by ThreatSTOP. Publicado em: fevereiro de 2016. Disponível em: https://threatstop.com/sites/default/files/ThreatSTOP_BlackEnergy.pdf, Acesso em: 3 ago. 2020.

UNITED NATIONS. **Public Law 107-40.** Sept. 18, 2001a. 107th Congress. Disponível em: https://www.congress.gov/107/plaws/publ40/PLAW-107publ40.pdf. Acesso em: 4 set. 2020.

UNITED NATIONS. **Resolution 1373.** 2001b. Disponível em: http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1373%282001%29. Acesso em: 3 ago. 2020.

UNITED STATES. Congressional Research Service. P. L. 110-55, **the Protect America Act of 2007:** Modifications to the Foreign Intelligence Surveillance Act, 14 fev. 2008. Disponível em: https://www.fas.org/sgp/crs/intel/RL34143.pdf. Acesso em: 4 ago. 2020.

UNITED STATES. Congressional Research Service. **The USA Patriot Act:** A Sketch, 18 abr. 2002. Disponível em: http://fas.org/irp/crs/RS21203.pdf. Acesso em: 4 ago. 2020.

UNITED STATES. Department of Defense — DoD. **IOR.** Roteiro para as Op Info. Publicado em: 30/10/2003. Departamento de Defesa/EUA, 2003. Disponível em: http://www.iwar.org.uk/iwar/resources/io/io-roadmap.pdf. Acesso em: 5 set. 2020.

UNITED STATES. Department of Defense — DoD. QDR. **Quadrennial Defense Review.** [Revista Quadrienal do Departamento de Defesa dos EUA]. Publicada em: 6 de fevereiro de 2006. Washington, D.C., 2006.

UNITED STATES. **Joint Publication 3-13.4:** Military Deception. Publicado em: 26/01/2012. Washington, D.C.: Government Printing Office, 2012. Disponível em: https://info.publicintelligence.net/JCS-MILDEC.pdf. Acesso em: 6 ago. 2020.

UNITED STATES. The White House. **International strategy for cyberspace:** prosperity, security, and openness in a networked world. Publicado em: maio de 2011. Washington, D.C., 2011. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Acesso em: 4 set 2020.

UNITED STATES. The White House. **National Security Presidential Directive — NSPD 5,** 9 maio 2001c. Washington, D.C., 2001. Disponível em: http://fas.org/irp/offdocs/nspd/nspd-5.pdf. Acesso em: 4 set 2020.

UNITED STATES. United States Army. **FM 100-6.** Information Operations. Documento Doutrinário do Exército dos EUA, 27 de agosto de 1996. Disponível em: http://www.jya.com/fm100/fm100-6.htm. Acesso em: 4 ago. 2020.

WARDLE, C.; DERAKHSHAN, H. Information Disorder: Toward an interdisciplinary framework for research and policy making. **Council of Europe report DGI,** 2017. Disponível em: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c. Acesso em: 3 ago. 2020.

WEEDON, J. Beyond Cyber War: Russia´s use of Strategic Cyber Espionage and Information Operations in Ukraine. In: GEERS, K (ed.). **Cyber War in Perspective:** Russian Aggression Against Ukraine. NATO CCDCOE Publications: Tallinn, 2015.

YOO, John. **The Terrorist Surveillance Program and the Constitution.** 14 Geo Mason L. Rev 565. 2007.

APÊNDICE — FIGURA

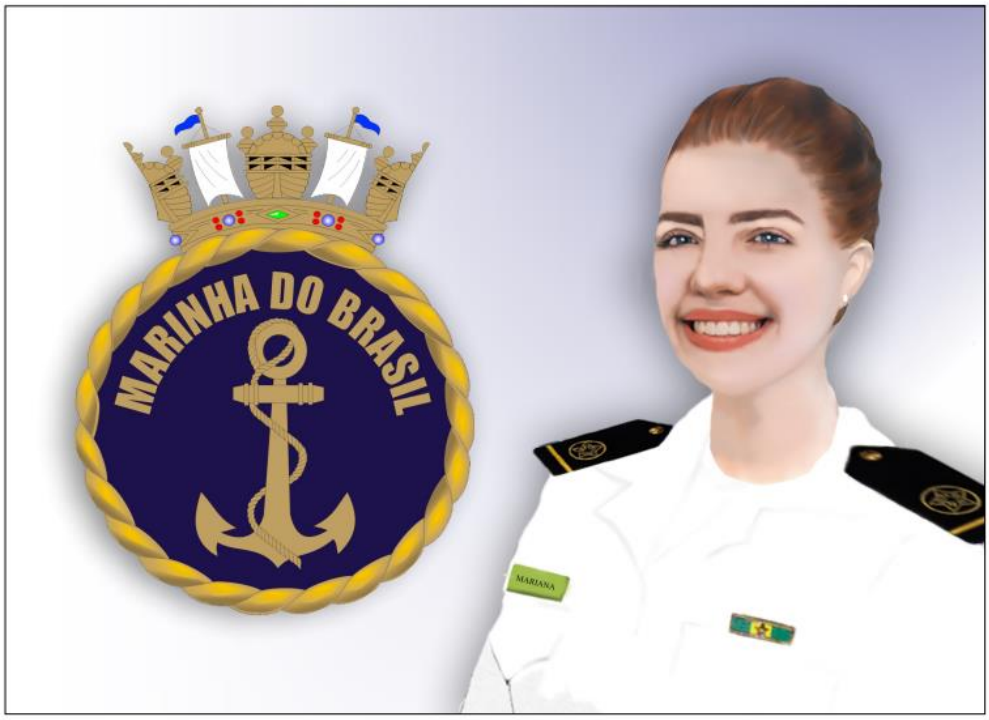

FIGURA 3 — Personagem “1T Mariana”
Fonte: Própria Autora, 2020.

ANEXO — FIGURAS

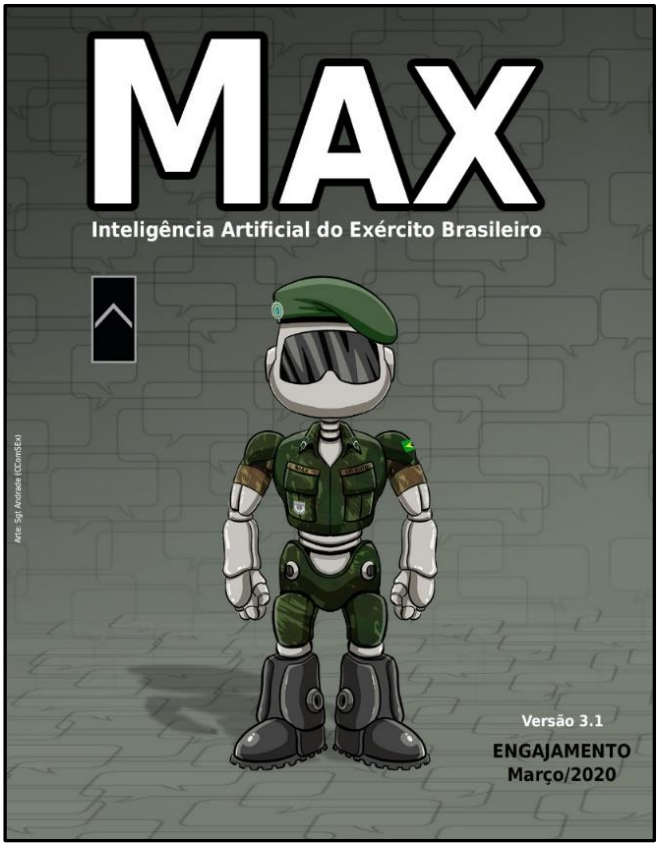

FIGURA 1 — Personagem soldado Max
Fonte: CComSEx.

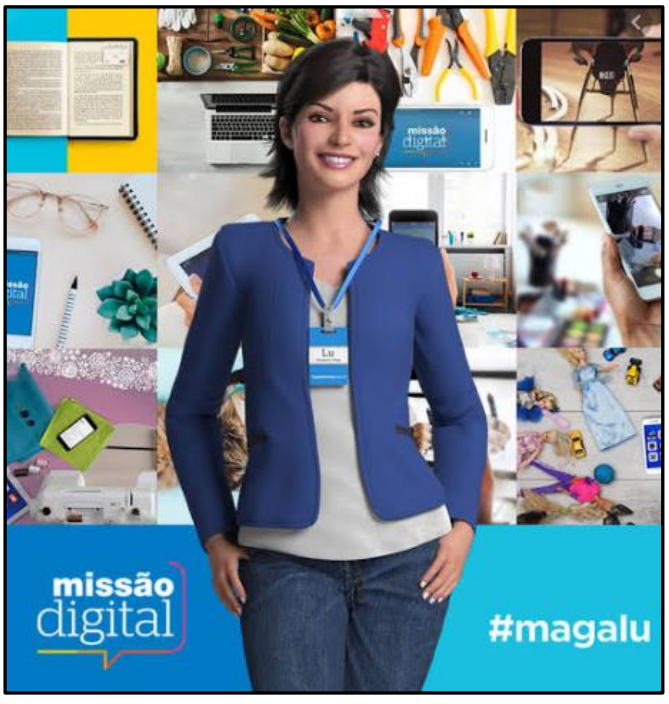

FIGURA 2 — Personagem “Lu” da Magalu
Fonte: Magalu.