ISSN: 2525-457X
Análise Estratégica
Vol 28 (1) Dez/Fev 2023

GUERRA RUSSO-UCRANIANA: GRANDE LABORATÓRIO PARA ENSAIOS DESTRUTIVOS E NÃO DESTRUTIVOS DE TECNOLOGIAS EMERGENTES E DISRUPTIVAS

RUSSIAN-UKRAINIAN WAR: LARGE LABORATORY FOR DESTRUCTIVE AND NON-DESTRUCTIVE TESTING OF EMERGING AND DISRUPTIVE TECHNOLOGIES

FERNANDA DAS GRAÇAS CORRÊA

RESUMO

Neste terceiro ensaio da linha de pesquisa Tecnologia, Inovação e Emprego Militar, serão apresentadas tecnologias reconvertidas, desenvolvidas *in loco* para pronto-emprego do exército ucraniano contra as tropas russas. Processos de reconversão tecnológica conduzidos por organizações de financiamento e aceleradoras locais, também, despontam como inovadores nos teatros de operações. Além disso, serão apresentadas e detalhadas tecnologias emergentes e disruptivas, como drones, cibertecnologias, sistemas de gerenciamento de campo de batalha, o sistema de lançamento múltiplo de foguetes *Himars* e a rede *Starlink* da empresa *SpaceX*. Juntas, essas tecnologias emergentes e disruptivas têm transformado a Ucrânia em um grande laboratório para ensaios destrutivos e não destrutivos.

PALAVRAS-CHAVE

Guerra russo-ucraniana; tecnologias emergentes e disruptivas; rede Starlink

ABSTRACT

In this third essay of the Technology, Innovation and Military Employment research line, reconverted technologies developed in loco for ready use by the Ukrainian Army against the Russians will be presented. Technological reconversion processes led by funding organizations and local accelerators are also emerging as innovators in theaters of operations. Emerging and disruptive technologies will also be presented and detailed, such as drones, cybertechnologies, battlefield management systems, the US Himars multiple rocket launch system and the Starlink network of the US company SpaceX. Together these emerging and disruptive technologies have transformed Ukraine into a great laboratory for destructive and non-destructive testing.

KEY WORDS

Russo-Ukrainian War; emerging and disruptive technologies; starlink network

A AUTORA

Coordenadora de Prospecção Tecnológica e Gestão do Conhecimento no Departamento de Ciência, Tecnologia e Inovação (DECTI) da Secretaria de Produtos de Defesa (SEPROD)/ Ministério da Defesa. Pós-doutoranda em Modelagem de Sistemas Complexos (EACH/USP). Pós-Doutora em Ciências Militares (ECEME). Doutora em Ciência Política na Área de Concentração Estudos Estratégicos (UFF). Pesquisadora na linha Tecnologia, Inovação & Emprego Militar (2022-2023) do Centro de Estudos Estratégicos do Exército (CEEEx).

SUMÁRIO EXECUTIVO

O século XXI foi inaugurado com diversas vertentes conceituais, tais como novas ameaças, multidomínio, guerra assimétrica, guerra informacional, guerra híbrida etc, como contraponto às guerras simétricas ou convencionais. Nesse sentido, em especial, devido às tecnologias de quarta geração, como cibernética e energia dirigida, muito se espera, na comunidade internacional, sobre o emprego de inovações disruptivas nos atuais teatros de operações (TO) militares.

Com ênfase na disrupção, a linha de pesquisa Tecnologia, Inovação & Emprego Militar tem por atribuição, neste terceiro ensaio, identificar demandas tecnológicas emergentes e disruptivas para o Exército Brasileiro, selecionando o TO ucraniano, no contexto atual de guerra, como objeto de estudo. No entanto, a atual guerra na Ucrânia tem exigido um olhar diferenciado com a intervenção de múltiplos atores, incluindo, empresas e órgãos de financiamento internacional. Diversas tecnologias têm sido desenvolvidas para dar pronta-resposta ao Exército ucraniano na guerra contra a Rússia; porém, a maioria delas não possui caráter de inovação emergente ou disruptiva. Em geral, são tecnologias civis, usadas em guerras recentes, reconvertidas para emprego militar. São apresentadas, neste estudo, tecnologias de Veículos Aéreos Não Tripulados (VANT), como o octocóptero *R18*, o drone *PC-1* dobrável e drones *Bayraktar TB2* de ataque e reconhecimento. Ainda, é abordado o emprego de tecnologias cibernéticas, como conexão ao servidor C&C, ataque de força bruta, ataque a aplicativos *web, malwares* e *DDoS*. Essas cibertecnologias, em especial, são empregadas por russos em território ucraniano, desde 2014, quando a Crimeia foi anexada à Rússia.

Por meio de processos inovadores, entidades civis têm apoiado o Exército ucraniano para desenvolver e/ou financiar o desenvolvimento de tecnologias emergentes, como o Sistema de Gerenciamento de Campo de Batalha (ComBat), para aumentar a consciência situacional e reduzir os incidentes de fogo amigo nos TO. Uma das maiores inovações no TO ucraniano é a rede de banda larga de *Internet Starlink*. Como será abordado, a doação de terminais de banda larga de internet *Starlink*, da *Space X*, está muito mais associada a uma disputa mercadológica da empresa por contratos com setores de Defesa do governo estadunidense do que com seu interesse em acabar com a guerra.

Os processos conduzidos, na guerra, pela Ucrânia, para garantir prontidão tecnológica contra as ofensivas russas, como o *Aerorozvidka* e o *Projeto Gente*, são também considerados neste estudo como inovadores.

A Ucrânia também tem recebido tecnologias militares de outros países, como o sistema *HIMARS*. Embora esse sistema não seja considerado inovador, seu emprego conjunto com mísseis e drones de ataque e reconhecimento têm proporcionado à Ucrânia maior resistência em batalha.

Se, por um lado, todo esse apoio e pressão internacional tem aumentado as chances de a Ucrânia obter concessões russas na guerra, por outro, tem causado uma escalada militar na Eurásia que pode chegar a uma guerra nuclear. Daí a estratégia ucraniana de tentar envolver os Estados Unidos da América (EUA) e a Organização do Tratado do Atlântico Norte (OTAN) no conflito contra a Rússia ser melhor dimensionada pelas autoridades locais, regionais e internacionais. Independente das especulações de fraudes nos referendos e do não reconhecimento da Secretaria-Geral da Organização das Nações Unidas (ONU), a Rússia está seguindo as regras da Carta da ONU a fim de tentar legitimar a anexação de territórios ucraniano e é membro do Conselho de Segurança daquela organização. Considerando que a China tende a se posicionar favorável às decisões político-militares da Rússia nas Assembleias-Gerais do Conselho de Segurança da ONU, qualquer decisão de intervenção militar de outros países ou organizações na Ucrânia poderá resultar no emprego de armas nucleares táticas russas para defender o direito desses povos recém-anexados de existirem.

1. Reconversão e prontidão tecnológica na Guerra da Ucrânia

Um mês após o referendo que tornou a Crimeia e Sevastopol regiões anexas à Rússia, em abril de 2014, a República Popular de Donetsk e a República Popular de Lugansk, ambas regiões ucranianas, solicitam o reconhecimento internacional como Estados soberanos. Embora não tenham obtido o reconhecimento da ONU, essas regiões passaram a ser entidades estatais com limitada aceitação à medida que países como Rússia[1] , Coreia do Norte e Síria. Após o *impeachment* sofrido por Yanukovytch, a Ucrânia foi governada, de forma interina, por Olexandr Turtchynov (2014) e, por eleição democrática, por Petro Poroshenko (2014-2019).

Desde 2014, forças militares ucranianas vêm combatendo com o apoio intensificado de VANT[2], forças militares e simpatizantes russos, nas regiões que se tornaram independentes da Ucrânia, em especial, em Donetsk. Em função dos atrasos nas entregas de VANT solicitadas pelo governo ucraniano ao governo estadunidense, os ucranianos desmontaram, converteram e reconfiguraram drones basicamente recreativos para realizar missões de inteligência nas fronteiras. Assim, nasceu a *Aerorozvidka*, equipe que promove a criação e a implementação de capacidades militares netcêntricas e robóticas com a missão de *ajudar as forças de segurança e defesa da Ucrânia a derrotar os agressores russos*[3]. Um dos VANT desenvolvido pela *Aerorozvidka* é o *R18*[4], octocóptero capaz de lançar granadas anticarro cumulativas de uma altura de 100 a 300 metros pairando sobre o alvo e equipado com um termovisor. Desde que foi criada, a equipe da *Aerorozvidka* saltou para mais de 20 pessoas e, em 2015, contava com "uma unidade tática equipada com vans blindadas e 16 drones operados com dois dos sistemas operacionais mais conhecidos – o NAZA ou o *Pixhawk*, desenvolvido pela *3D Robotics* (agora mantida pela Fundação Linux)" (TUCKER, 2015, p.2).

> O VANT mais sofisticado no lado ucraniano desde o começo do conflito é chamado PD-1, do inventor Igor Korolenko. O veículo tem envergadura de 3 metros e autonomia para até cinco horas de voo, além de carregar sensores eletro-óticos e infravermelhos, bem como uma câmera de vídeo para transmissão em um canal criptografado de 128 bits. O componente mais importante no drone é o software de piloto automático que lhe permite retornar à base caso o sistema de posicionamento global seja comprometido ou perdido.(TUCKER, 2015, p.2-3).

Até mesmo as missões de coleta de dados não tornam a assinatura eletrônica dos VANT imune aos radares inimigos. Além disso, o custo humano a quem opera esses VANT, em bases terrestres, pode ser muito alto às forças militares. Há necessidade de que tanto os VANT tenham sistemas de assinatura eletrônica e criptografia cada vez mais seguras, quanto seus operadores sigam determinadas medidas de segurança que exigem, por exemplo, a troca frequente de localização, deslocamento das antenas e operações baseadas dentro de abrigos. Entre 2014 e 2018, quatro drones russos modelo Forpost *ISR*[5] e um VANT russo modelo UAV *OrlAn*-10 foram abatidos em regiões estratégicas por forças militares ucranianas, em território ucraniano. Em 2014, as forças armadas russas abateram as seguintes aeronaves ucranianas:

[1] Em 21 de fevereiro de 2022, a Rússia reconheceu a República Popular de Donetsk e a República Popular de Lugansk como entidades estatais.

[2] VANT são controladas à distância por meios eletrônicos e computacionais sob a supervisão humana ou sem intervenção humana por meio de Controladores Lógicos Programáveis (CLP).

[3] Para conhecer mais sobre a *Aerorozvidka*, acesse: <https://aerorozvidka.xyz/about/>

[4] Trata-se de um octocóptero de decolagem e aterrissagem vertical, que possui oito parafusos de içamento e pode transportar vários quilos de carga útil.

[5] VANT de Inteligência, Vigilância e Reconhecimento (*ISR*, sigla em inglês) israelense produzido pela empresa IAI na década de 1980 e vendido sob licença pela Rússia.

quatro helicópteros modelo *Mil Mi–8*, três helicópteros modelos *Mil Mi–24*, um avião de aerofotogrametria Antonov Na-30, um avião de transporte Ilyushin Il–76, dois caças Sukhoi Su-24, quatro caças Sukhoi Su-25, um avião de transporte *Antonov Na-26* e dois caças modelo *Mikoyan MiG-29*. Outra inovação surgida no TO é o *Projeto Gente*, cujo funcionamento se assemelha ao de uma incubadora de *startups*; porém, com modelo de negócios baseado em financiamento voluntário, coletivo e solidário de projetos, para apoiar civis e militares, na área de saúde, que estejam na linha de frente da guerra contra os russos[6]. Um dos projetos para o qual essa organização solicita apoio financeiro é o quadricóptero *PC-1* dobrável, unidade de inteligência móvel para exploração de área, detecção e rastreio a curta distância. A **figura 1** ilustra o drone PC-1 dobrável.

Os fundos arrecadados pelo *Projeto Gente* deverão ser gastos na produção de sete quadricópteros com alcance de até cinco mil metros e autonomia de 40 minutos, desenvolvidos pela empresa *Ukrspec Systems*[7] para uso pelos militares ucranianos contra invasores russos.

Figura 1: PC-1 dobrável

Fonte: Projeto Gente

2. Emprego de tecnologias emergentes na Guerra da Ucrânia

Outro projeto para o qual a organização solicitou apoio financeiro foi o do Sistema de Gerenciamento de Campo de Batalha (ComBat) com a finalidade de aumentar a consciência situacional e reduzir os incidentes de fogo amigo nos TO. Embora a organização não tenha anunciado publicamente os desenvolvedores, informou que o ComBat foi 100% concluído e desempenhará "as mesmas funções das versões estrangeiras, com custo técnico relativamente baixo"[8]. A **figura 2** ilustra o ComBat.

Em maio de 2019, Volodymyr Zelensky foi eleito democraticamente como presidente da Ucrânia, comprometido em buscar maior diálogo com Putin e encerrar a presença russa em regiões estratégicas ucranianas. Contudo, Zelensky intensificou as tensões políticas e militares com a Rússia.

Diversas agências do governo e bancos ucranianos se tornaram alvos de ataques cibernéticos, tais como conexão ao servidor C&C, ataque de força bruta, ataque a aplicativos *web, malwares* etc. De acordo com o Serviço de Segurança da Ucrânia (SSU), desde janeiro de 2022, o Centro de Situação de Segurança Cibernética/SSU parou e conteve 121 ciberataques contra sistemas de informação de instituições estatais[9]. O governo ucraniano, em sua página oficial no *Twitter*, conforme **figura 3**, além da guerra de narrativas, declarou que o País estava sendo ameaçado por uma onda de guerra híbrida.

A SSU reagiu neutralizando ataques cibernéticos, desmantelando diversas redes de

[6] Para conhecer mais o Projeto Gente, acesse <https://www.peoplesproject.com/en/projects/>

[7] Para conhecer mais sobre a empresa Ukrspec Systems, acesse <https://ukrspecsystems.com/drones/pc-1>

[8] Para obter mais informações sobre o projeto ComBat, acesse <https://www.peoplesproject.com/en/battlefield-management-system/>

[9] Para ler a matéria da SSU, acesse <https://ssu.gov.ua/en/novyny/u-sichni-2022-roku-sbu-zablokuvala-ponad-120-kiberatak-na-ukrainski-orhany-vlady>

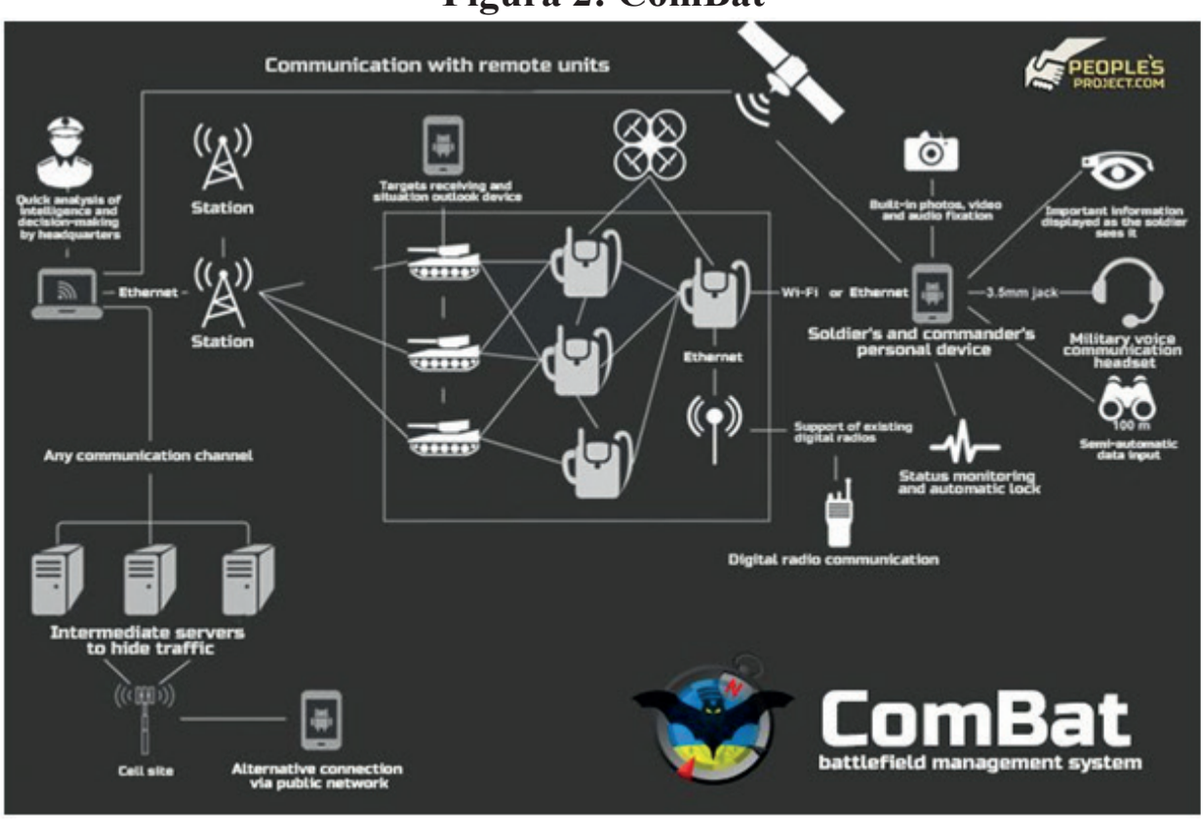
bots farms, expondo redes de agentes de serviços de inteligência hostis e prevenindo sabotagem e ataques terroristas. A Microsoft confirmou, em quatro de fevereiro de 2022, que um grupo russo de *hackers*, conhecido como Gamaredon, estava por trás de uma série de e-mails de *spear phishing*, direcionados às entidades e às organizações ucranianas desde outubro de 2021 e que, desde 2013, esse mesmo grupo ataca organizações ucranianas.

> Pesquisadores de segurança e ameaças do *Microsoft ThreatIntelligence Center* (MSTIC) e da *Microsoft Digital Security Unit* (DSU) disseram hoje que a campanha de espionagem cibernética da Gamaredon está sendo coordenada fora da Crimeia, confirmando a avaliação da SSU de que os *hackers* da Gamaredon são oficiais do FSB [Serviço Federal de Segurança da Rússia] da Crimeia, que se aliou à Rússia durante a ocupação de 2014. (GATLAN, 2022, p. 2-3).

Diversas organizações e bancos ucranianos passaram a ser alvos também de ataques distribuídos de negação de serviço (*DDoS*, sigla em inglês). *DDoS* é um tipo de ataque de rede de hosts infectados, mais conhecidos como *bots*, que tem por finalidade interromper e indisponibilizar o funcionamento de servidores e redes.

> Pesquisadores de segurança e ameaças do *Microsoft ThreatIntelligence Center* (MSTIC) e da *Microsoft Digital Security Unit* (DSU) disseram hoje que a campanha de espionagem cibernética da Gamaredon está sendo coordenada fora da Crimeia, confirmando a avaliação da SSU de que os *hackers* da Gamaredon são oficiais do FSB [Serviço Federal de Segurança da Rússia] da Crimeia, que se aliou à Rússia durante a ocupação de 2014. (GATLAN, 2022, p. 2-3).

Figura 2: ComBat



Fonte: Projeto Gente

Figura 3: Declaração do governo ucraniano de que o País é alvo de onda de guerra híbrida

Fonte: <https://mobile.twitter.com/mfa_ukraine/status/1488545980815446017>

De acordo com o *Computer Emergency Response Team of Ukraine* (*CERT-UA*), os invasores realizaram os ataques *DDoS* usando plataformas *DDoS-as-a-Service* e diversas redes de *bots*, como Mirai e Meris. A informação foi confirmada pelo Centro Nacional de Segurança Cibernética do Reino Unido, acusando a Direção Principal de Inteligência Russa (*GRU*, sigla em inglês) de estar envolvida nos ataques *DDoS*, em 15 e 16 de fevereiro de 2022, na Ucrânia.

Em 21 de fevereiro de 2022, a Rússia reconheceu Donetsk e Lugansk como entidades estatais e, no dia 24 de fevereiro, foi iniciada a invasão militar russa em larga escala sobre o território ucraniano.

Em 25 de março de 2022, em relatório oficialreproduzido pela Agência Brasil, o Ministério da Defesa da Ucrânia afirmou:

> a Força Aérea da Ucrânia ontem atingiu 6 alvos aéreos inimigos: 1 avião, 1 VANT e 4 mísseis de cruzeiro. A força aérea patrulhou o espaço aéreo, destruiu as tropas e instalações e disparou contra os veículos blindados de transporte de pessoal, centros de logística e agrupamentos de tropas inimigas. O agrupamento das Forças de Defesa continua realizando uma operação de defesa nas direções Leste, Sudeste e Nordeste. (AGÊNCIA BRASIL, 2022, p.1).

As operações militares ucranianas estavam concentradas nas áreas de Donetsk, Slobozhansky

e Tavriya.

A fim de desacelerar e bloquear o avanço da artilharia russa, a Ucrânia passou a empregar drones turcos modelo *Bayraktar TB2,* fabricado pela empresa *Baykar Makina Sanayive Ticaret A.S. (Baykar)*. Esse drone pode realizar ataques, atinge média altitude e longa duração e é capaz de fazer operações de voo autônomas ou controladas remotamente, a partir de estação de controle de solo. Na **figura 4**, é possível visualizar uma estação de controle de solo do *Bayraktar TB2* em uma plataforma móvel.

O Exército russo emprega esse modelo de drone, mas a fabricante turca desenvolveu uma versão comercial para exportação. Embora esteja em uso pelos militares turcos no Curdistão, no Iraque e na Síria desde 2014, o *Bayraktar TB2* tem sido um dos modelos de drones mais empregados pela Ucrânia contra a artilharia russa. Em virtude de suas alianças geoestratégicas e econômicas com a Rússia, a Turquia tem se declarado neutra na guerra. No entanto, *experts* em aquisições tecnológicas de defesa têm rastreado os drones *TB2* desde a linha de produção até o recebimento, levantando suspeitas de que novas encomendas privadas desses drones à *Baykar* estejam sendo recebidas pela artilharia do Exército ucraniano. (VALDUGA, 2022, p. 2-3). No sítio eletrônico da *Oryx*, está disponibilizada uma lista atualizada sobre aeronaves, helicópteros e VANT destruídos, danificados e capturados, tanto do lado ucraniano quanto do lado russo no ano de 2022. De acordo com esse sítio eletrônico, catorze (14) *Bayraktar TB2* e um (1) mini drone de reconhecimento *Bayraktar* foram destruídos na guerra[10].

Figura 4: Estação de controle de solo de Bayraktar em uma plataforma móvel

Fonte: Baykar Makina Sanayi ve Ticaret A.Ş.

[10] Para conhecer a lista, acesse <https://www.oryxspioenkop.com/2022/03/list-of-aircraft-losses-during-2022.html>

3. Emprego de tecnologias disruptivas na Guerra da Ucrânia

Desde que a Rússia declarou guerra e invadiu militarmente o território ucraniano, a Ucrânia vem recebendo apoio de diversas empresas estrangeiras. Uma delas é a estadunidense *SpaceX*. Atendendo prontamente à solicitação de Mykhailo Fedorov, Ministro da Transformação Digital e Vice-Primeiro-Ministro da Ucrânia, no final de fevereiro de 2022, ElonMusk, fundador e CEO da *SpaceX*, utilizou a Agência dos Estados Unidos para o Desenvolvimento Internacional (*USAID*, sigla em inglês) para viabilizar o transporte de cinco mil terminais de internet de banda larga, modelo *Starlink*, para a Ucrânia. Diferente do que tem sido noticiado pela grande mídia internacional, os drones militares ucranianos não se conectam diretamente aos Satélites de Baixa Órbita (*LEO*, sigla em inglês) *Starlink*. A tecnologia *LEO Starlink* conecta a internet às equipes do Exército ucraniano que controlam os drones nas estações de controle de solo, nas plataformas móveis.

> O Exército estadunidense tem manifestado publicamente profundas preocupações com relação às incoerências intencionais de Guerra Eletrônica na emissão de sinais a receptores *GPS* militares e tem focado na aquisição/ desenvolvimento de satélites menores e de baixa órbita terrestre (LEO, sigla em inglês). (CORRÊA, 2021, p.67).

Estudos prospectivos têm sido suscitados, na Academia, para oferecer soluções tecnológicas ao Exército estadunidense que substituam o emprego do Sistema de Posicionamento Global (*GPS*, sigla em inglês) na guerra do futuro. Peter Iannucci e Todd Humphreys, ambos pesquisadores do Laboratório de Radionavegação da Universidade do Texas, em Austin, publicaram artigo intitulado *Fused Low-Earth-Orbit GNSS*, no qual concluíram que o *GPS* pode ser substituído pelos satélites *Starlink*, rede de satélite em órbita terrestre com baixo custo de aquisição que fornece serviços de navegação altamente precisos e quase invulneráveis (IANNUCCI e HUMPHREVS, 2020, p.14).

Embora a *SpaceX* tenha conseguido comprovar que as ondas de rádio da *Starlink* apresentam muito menos latência e que a transmissão de sinais seja muito mais rápida do que a do *GPS*, o Exército estadunidense tem manifestado preocupações em relação à prestação de serviços rápidos de banda larga. (CORRÊA, 2021, p.67). No *Twitter* e em sua página oficial, Mykhailo Fedorov publicou foto da rede *Starlink* a bordo de uma estação móvel, agradecendo a doação de ElonMusk[11].

Figura 5: Rede Starlink a bordo de uma estação móvel

Fonte: Mykhailo Fedorov

A guerra da Ucrânia se tornou oportunidade ímpar para que a *SpaceX* teste e comprove a eficiência da barda larga de internet da rede *Starlink* em áreas remotas de teatros de operações militares. A *Aerorozvidka* tem empregado a rede *Starlink* para monitorar e coordenar ações de drones militares ucranianos que estão no TO, bombardeando a artilharia e blindados russos. Importante destacar que a rede *Starlink* tem sido empregada pelo

[11]Para ler a mensagem no Twitter do ministro ucraniano, acesse: <https://twitter.com/fedorovmykhailo/status/1498392515262746630>

governo para restabelecer a comunicação em todo território ucraniano, inclusive, por meio de redes móveis de telefonia.

Atendendo aos insistentes pedidos de apoio de material militar, os EUA anunciaram que enviariam plataformas móveis lançadoras de mísseis balísticos táticos tipo *M142 High Mobility Artillery Rocket System* (*HIMARS*), em maio de 2022, para o Exército ucraniano. Esse sistema é considerado lançador múltiplo porque pode ser usado tanto como lançador de foguetes quanto como lançador de mísseis táticos. O *M142 HIMARS* é uma versão leve do *M270 Multiple Launch Rocket System* e pode ser transportado a bordo de um avião como o C-130 (Hércules). O chassi do *HIMARS* foi produzido pela empresa *BAE Systems* e o sistema de lançamento dos foguetes foi desenvolvido pela empresa *Lockheed Martin*. O *M142 HIMARS* está em operação no Exército dos EUA desde 2010. O primeiro sistema *HIMARS* desembarcou em território ucraniano em junho desse mesmo ano. Nesse mesmo mês, houve o anúncio ucraniano do sucesso do emprego do sistema, lançando míssil *ATACMS* contra uma base militar russa em Izyum, no Donbass. Inicialmente, o *HIMARS* começou a ser empregado pela artilharia do Exército ucraniano contra o avanço de tropas russas em Donetsk e em Lugansk. Graças ao emprego bem-sucedido contra alvos russos, a artilharia ucraniana passou a empregá-lo contra alvos em outras regiões do país que estavam sob domínio da Rússia, como Kherson. Dentre as vantagens do emprego desse sistema, encontram-se: artilharia de alta precisão, capacidade de voo baixo em velocidade e alta mobilidade, o que torna o *M142 HIMARS* mais difícil de ser rastreado e destruído pelas tropas russas.

A ponte de Antonivskyi, localizada na cidade Antonivka, província de Kherson do sul da Ucrânia, foi construída sobre o rio Dniepre. Ela liga duas cidades ucrânias e tem sido utilizada como travessia de tropas e veículos militares russos desde a Crimeia até o centro da Ucrânia. Os russos sofreram diversas baixas de tropas e veículos sobre a ponte de Antonivskyi, desde fevereiro de 2022, no entanto, foi o emprego de mísseis e foguetes a partir do sistema *HIMARS*, em agosto de 2022, pelo Exército ucraniano, bombardeando e destruindo a ponte de Antonivskyi, que isolou as tropas russas.

Figura 6: HIMARS

Fonte: Estado-Maiors das Forças Armadas da Ucrânia

Apesar dos esforços do Exército ucraniano, além de Donetsk e de Lugansk, outros referendos realizados na Ucrânia aprovaram a anexação russa de Kherson e de Zaporíjia, em 27 de setembro de 2022.

4. Ucrânia como laboratório de ensaios destrutivos e não destrutivos de tecnologias emergentes e disruptivas estrangeiras

O teatro de operações ucraniano, como ocorre na maior parte das guerras contemporâneas, tem sido utilizado como laboratório para testar tecnologias estrangeiras por meio de ensaios destrutivos e não destrutivos. Conceitualmente,

Ensaios Destrutivos (ED) são técnicas empregadas para analisar o comportamento dos materiais quando sujeitos a esforços mecânicos em condições específicas, semelhantes às de operação. Na maioria das vezes, esses ensaios promovem a ruptura ou a inutilização da amostra analisada, haja vista que algumas propriedades físicas somente são observadas por meio de testes que causam danos no material. (MOL DA SILVA, 2022, p.1).

Os observadores internacionais têm

analisado a capacidade de velocidade de tecnologias cibernéticas e o potencial de danos às empresas, bancos e ao governo ucraniano,o potencial dissuasório dos drones turcos de ataque *Bayraktar TB2* e a precisão do sistema *HIMARS* para causar danos em drones e em blindados russos e para inutilizar infraestruturas críticas ucranianas, como a ponte de Antonivskyi, isolando tropas russas.

Conceitualmente, ensaios não destrutivos "são ensaios praticados a um material ou equipamento, que não altere de forma permanente suas propriedades físicas, químicas, mecânicas ou dimensionais". (SGS, 2018, p.3). Não há interesse da *SpaceX* de que seus satélites sejam alvos de ataques russos. A empresa estadunidense não tem por objetivo causar danos materiais nem aos seus satélites nem aos seus terminais *Starlink*, mas sim, comprovar a eficiência do fornecimento de banda larga de internet em áreas hostis. Embora a iniciativa de doar terminais *Starlink* tenha partido da própria empresa, há desconfiança por parte do governo russo de que os EUA estejam apoiando de forma sigilosa o financiamento militar para a Ucrânia por meio da *SpaceX*. Os russos alegam que podem retaliar militarmente os satélites civis da *SpaceX* à medida que tanto a empresa quanto, se comprovado, o governo estadunidense, estariam violando o Tratado sobre os Princípios que Regem as Atividades dos Estados na Exploração e Uso do Espaço Exterior, incluindo a Lua e Outros Corpos Celestiais. (OLHAR DIGITAL, 2022, p.2) Países europeus também têm apoiado Zelensky, por meio de doações de tecnologias militares,na resistência contra a invasão militar russa em território ucraniano. De acordo com o Twitterdo canal *Ukraine Weapons Tracker*, veículos blindados M113A1/A2 doados por Portugal ao Exército ucraniano, estão em operação em Kherson. O M113 é uma família de Veículos Blindados de Transporte de Pessoal (VBTP) fabricada desde a década de 1960 pela empresa estadunidense *FMC Corporation*. De acordo com informações da ONU, até setembro de 2022, foram confirmadas 14.059 vítimas civis, das quais 5.767 estão mortas e 8.292 estão feridas[12]. A ofensiva militar pode promover uma escalada militar na Eurásia, à medida que os milhões de refugiados da guerra interferem diretamente na política e na economia dos países da região. Assim, cada vez mais, países europeus, independentemente de seus alinhamentos estratégicos com organizações militares europeias, como a OTAN, mobilizam meios militares para apoiar a Ucrânia na guerra contra a Rússia.

Em 30 de setembro de 2022, o Presidente russo Vladimir Putin assinou documento oficial que anexou quatro territórios ucranianos à Rússia: Kherson, Donetsk, Luhansk, Zaporizhia, conforme ilustrado pela AFP, na **figura 7**.

Em virtude do posicionamento público de Putin, referente às áreas ucranianas anexadas à Rússia, ao aumento das tensões e ao risco iminente de escalada militar na Eurásia, diversos debates internacionais têm ocorrido sobre o emprego de armas nucleares táticas russas contra a Ucrânia. Apesar de a ONU contestar a credibilidade do plebiscito russo, Putin exalta o Princípio de Autodeterminação dos Povos da Carta das Nações Unidas e resgata o nacionalismo soviético para justificar os laços que unem os povos das regiões anexadas à Rússia. O Princípio de Autodeterminação dos Povos somente pode ser aplicado a um povo mediante a vontade popular, como um referendo. Esse princípio confere aos povos o direito de autogoverno, o poder de decidir livremente a situação política e o direito de os Estados defenderem a sua existência. Seguindo o Princípio de Autodeterminação dos Povos da Carta da ONU, ao anexar quatro territórios do país vizinho, a Rússia garante o direito de autogoverno, o poder de decidir livremente a situação política e o direito de usar os meios tecnológicos necessários para defender seus territórios e criar um mecanismo jurídico, na própria ONU, de manipular a comunidade internacional a reconhecer politicamente esses territórios como russos.

[12] Para acessar os dados da ONU, <https://news.un.org/en/story/2022/09/1126391>

Figura 7: Novos territórios ucranianos anexados à Rússia

5. Conclusão

Em virtude das diversas vertentes conceituais que têm surgido nos últimos anos, a saber, multidomínio, guerra assimétrica, guerra informacional e guerra híbrida, como contraponto às guerras simétrica ou convencionais, muito se espera, na comunidade internacional, sobre o emprego de tecnologias inovadoras nos TO. No entanto, esse não tem sido o caso da atual guerra na Ucrânia. Diversas tecnologias têm sido desenvolvidas para dar pronta-resposta ao Exército ucraniano na guerra contra seu oponente. Contudo, a maioria delas não possui um caráter inovador. Em geral, são tecnologias civis reconvertidas para emprego militar, como o octocóptero *R18* e o drone *PC-1* dobrável, e tecnologias emergentes que já foram empregadas em guerras recentes, como *DDoS*, drones *Bayraktar TB2* e o sistema *HIMARS*. Pouquíssima informação foi divulgada sobre o *ComBat*, mas, de fato, apresenta tecnologias emergentes, em especial de sensores, capaz de gerar maior consciência situacional no TO.

Independente do que tem sido repercutido na mídia sobre o emprego da *SpaceX* na defesa dos direitos humanos ucranianos contra ofensivas de tropas russas, Elon Musk está realizando ensaios destrutivos e ensaios não destrutivos de terminais de banda larga de *Internet Starlink*, para, entre outras razões, comprovar a eficiência da sua rede como substituta do *GPS*, em novas guerras das quais os EUA participem futuramente. A doação de terminais de banda larga de *Internet Starlink* está muito mais associada a uma disputa mercadológica da *SpaceX* por contratos com o Exército estadunidense.

Também, é possível destacar como inovação os processos conduzidos na guerra para garantir prontidão tecnológica. Por essa razão, foram apontadas as ações promovidas pela *Aerorozvidka* e pelo *Projeto Gente* como sistemas inovadores capazes de garantir pronta resposta em tempo hábil.

Na "artilharia anticarro", o sistema *HIMARS* com apoio de drones tem sido bem-sucedido no bombardeamento de alvos controlados por tropas russa; porém, é preciso que o Exército ucraniano invista também na aquisição de tecnologias antiaéreas. Essas tecnologias emergentes e disruptivas juntas têm transformado a Ucrânia em um grande laboratório para ensaios destrutivos e não destrutivos.

Com a anexação e se respaldando no Princípio da Autodeterminação dos Povos, qualquer ato militar de qualquer país, nesses novos territórios, pode ser estrategicamente interpretado

pela Rússia como uma inviolabilidade territorial e, portanto, declaração de guerra. Independente das especulações de fraudes nos referendos e do não reconhecimento da Secretaria-Geral da ONU, a Rússia está seguindo as regras da Carta da ONU, a fim de tentar legitimar a anexação de territórios ucranianos, sendo membro do Conselho de Segurança dessa organização. A China tende a se posicionar favorável às decisões político-militares da Rússia nas Assembleias-Gerais do Conselho de Segurança da ONU. Logo, qualquer decisão de intervenção militar na Ucrânia não partirá desse Conselho. Embora a OTAN considere publicamente a anexação de territórios ucranianos pela Rússia como ilegal e ilegítima, ainda não se decidiu por intervir militarmente. Mas, alguns países que integram a organização, como Portugal, estão interferindo militarmente. Essas tensões políticas e a escalada de um possível conflito a nível regional ou internacional são variáveis que precisam estar no radar dos principais decisores da política internacional. Assim, o emprego de armas nucleares táticas russas para defender esses territórios tem que ser tratado com seriedade tanto pelos países e empresas estrangeiras quanto por organizações militares que, eventualmente, decidirem mobilizar meios tecnológicos para apoiar militarmente a Ucrânia.

Referências

CORRÊA, Fernanda das Graças. Sistemas de Navegação por Satélite e a Guerra do Futuro: uma abordagem prospectiva. Revista Análise Estratégica. v. 19 n. 1, 2021. Disponível em <http://ebrevistas.eb.mil.br/CEEExAE/article/view/7732>. Acesso em: 16 de janeiro de 2023.

Equipe Técnica SGS. Ensaios não destrutivos – o que é preciso saber? Função - Industrial, SGS. Abril de 2018. Disponível em <https://www.sgsgroup.com.br/mwg-internal/de5fs23hu73ds/progress?id=Y1sdyShx4Qvp7h_38xijLXnbVKqY2_owFnVly44OYl0,&dl>. Acesso em: 16 de janeiro de 2023.

FERREIRA, Arthur E. G. NOGUEIRA, Michele. Identificando Botnets Geradoras de Ataques *DDoS* Volumétricos por Processamento de Sinais em Grafos. *In Anais do XXIII Workshop* de Gerência e Operação de Redes e Serviços, maio 06, 2018, Campos do Jordão, Brasil. SBC, Porto Alegre, Brasil.

GATLAN, Sergiu. *Microsoft: Russian FSB hackers hitting Ukrainesince October. Bleeping Computer*, quatro de fevereiro de 2022. Disponível em <https://www.bleepingcomputer.com/news/microsoft/microsoft-russian-fsb-hackers-hitting-ukraine-since-october/>. Acesso em: 16 de janeiro de 2023.

IANNUCCI, Peter A. HUMPHREVS, Todd E Fused Low-Earth-Orbit GNSS. arXiv:2009.12334v1 [eess.SP] 25 September 2020. Disponível em <https://arxiv.org/pdf/2009.12334.pdf>. Acesso em: 16 de janeiro de 2023.

MOL DA SILVA, Gisele. Ensaios Destrutivos – 162. Departamento de Engenharia de Materiais (DEMAT), CEFET-MG, Belo Horizonte, 23 de junho de 2022. Disponível em <https://www.demat.cefetmg.br/ensaios-destrutivos-162/>. Acesso em: 16 de janeiro de 2023.

Satélites *Starlink* na Ucrânia podem ser derrubados pela Rússia. Olha Digital, 22 de setembro de 2022. Disponível em <https://olhardigital.com.br/2022/09/20/ciencia-e-espaco/satelites-Starlink-na-ucrania-podem-ser-derrubados-pela-russia/>. Acesso em: 16 de janeiro de 2023.

TUCKER, Patrick. Ucrânia – A guerra de drones do amanhã acontece hoje. DefesaNet, 11 de março de 2015. Disponível em <https://www.defesanet.com.br/vant/noticia/18387/UcraniaA-guerra-de-drones-do-amanha-acontece-hoje/>. Acesso em: 16 de janeiro de 2023.

Ucrânia afirma ter matado 200 soldados russos em um único dia. Agência Brasil, 25 de março de 2022. Disponível em <https://agenciabrasil.ebc.com.br/internacional/noticia/2022-03/ucrania-afirma-ter-matado-200-soldados-russos-em-um-unico-dia>. Acesso em: 16 de janeiro de 2023.

VALDUGA, Fernando. Parece que a Ucrânia continua recebendo novos drones turcos *Bayraktar*. Cavok, 12 de maio de 2022. Disponível em <https://www.cavok.com.br/parece-que-a-ucrania-continua-recebendo-novos-drones-turcos-bayraktar>. Acesso em: 16 de janeiro de 2023.