OSINT E RELAÇÕES INTERNACIONAIS: O CASO DOS MILITARES RUSSOS EM DONBAS ENTRE 2014 E 2021.

Antônio Henrique Lucena Silva[1] e Petrus Daniel Leal Belmonte[2]

RESUMO – O presente artigo pretende analisar detalhadamente as oportunidades oferecidas pela doutrina de Inteligência digital em fontes abertas (OSINT) e suas aplicações nos Estudos Estratégicos. Para atingir estes objetivos, apresenta exemplos práticos e demonstra como a ascensão da internet propiciou amplas oportunidades de estudo e aplicação da OSINT, frente à ascensão de uma nova forma de conflito no pós-Guerra Fria; a Zona Cinzenta. Para demonstrar o que é esta forma de conflito, e suas ferramentas, o caso dos militares russos em Donbas entre 2014 e 2021 é utilizado como exemplo. Logo após, é exposto detalhadamente como a OSINT foi utilizada para combater as táticas da Zona Cinzenta, e suas repercussões no campo legal e político internacional, além de suas outras aplicações.
Palavras-chave: inteligência; fontes abertas; Zona Cinzenta; forças ambíguas; Rússia; Ucrânia; Donbas.

ABSTRACT – This article aims to thoroughly analyze the opportunities offered by the doctrine of digital Open-Source Intelligence (OSINT) and its applications in Strategic Studies. To achieve this goals, it presents practical examples and demonstrates how the rise of the internet has provided extensive opportunities for the study and application of OSINT, in response to the emergence of a new form of post-Cold War conflict known as the Gray Zone. To illustrate this form of conflict and its tools, the case of Russian forces in Donbas between 2014 and 2021 is used as an example. Subsequently, it is detailed how OSINT has been used to counter the tactics of the Gray Zone and its implications in the legal and international political arena, as well as its other applications.
Key words: Intelligence, open source; Gray Zone; Ambiguous Forces; Russia; Ukraine; Donbas

INTRODUÇÃO

Considerada a maior inovação tecnológica do final do século XX, a Internet trouxe à humanidade um novo palco para as interações sociais: o mundo digital. Segundo a Internet World Stats (2022), é neste mundo onde mais de 5 bilhões de pessoas interagem, onde as fronteiras informacionais comuns a outros meios de comunicação; o espaço, tempo e a linguagem, já não existem. Embora as consequências desta troca instantânea e ilimitada de informações estejam mais claras

[1] Professor de Ciência Política da Universidade Católica de Pernambuco e de Relações Internacionais da Faculdade Damas da Instrução Cristã.
[2] Graduado em Relações Internacionais pela Faculdade Damas da Instrução Cristã.

na economia e na cultura, as relações internacionais também foram profundamente modificadas pela Internet, especialmente no tópico da Segurança Internacional. O mundo digital apresentou novas ameaças, como ataques cibernéticos e operações de desinformação, levando à necessidade de revisar os métodos tradicionais utilizados pelos setores de inteligência dos Estados.

Enquanto alguns métodos tiveram aplicação reduzida frente aos novos desafios, outros foram impulsionados pela Internet. Destaca-se, neste caso, a Inteligência em Fontes Abertas (OSINT): o processo investigativo cujo método é inteiramente baseado na coleta e análise de dados acessíveis em fontes publicamente disponíveis, e cada vez mais explorado em setores dos Estados. Perfeita oportunidade para demonstrar as potencialidades da OSINT está na sua capacidade de solucionar outra grande inovação do século XXI: o conflito na Zona Cinzenta. Trata-se de uma nova forma de enfrentamento entre Estados, que se utiliza de ferramentas criadas a partir da experiência de conflitos proxy na Guerra Fria.

De natureza extremamente ambígua, estas ferramentas estão no limiar da paz e da guerra declarada, permitindo que Estados combatam forças maiores de forma indireta, evitando ações cinéticas contra um adversário econômica e militarmente superior. O conflito no leste da Ucrânia, iniciado pela invasão russa em abril de 2014, serve de exemplo. Protegida pela grande ambiguidade das forças participantes da invasão, durante oito anos, a Rússia pôde negar oficialmente qualquer envolvimento militar na região, até iniciar oficialmente uma operação militar, em fevereiro de 2022. Ao iniciar a operação direta, já tomados nos anos anteriores foram consolidados, restando apenas expandi-los. Embora o sucesso da operação atual seja debatível, o conflito na Zona Cinzenta se demonstrou eficaz contra as formas tradicionais de inteligência.

Neste contexto de desafio às doutrinas de inteligência, a OSINT surgiu como resposta, tendo o conflito como principal campo de testes. Como será exposto, nos primeiros meses da invasão de 2014, várias unidades e equipamentos russos presentes no leste ucraniano foram expostos através de dados abertos, por uma miríade de atores internacionais, principalmente não-estatais. Desta forma, através de exemplos práticos, extraídos da primeira fase do conflito no leste ucraniano, de 2014 a 2021, este artigo pretende demonstrar as oportunidades de estudo e aplicação que a doutrina de OSINT, em sua versão digital, oferece para os Estudos Estratégicos, num mundo cada vez mais digital e transparente, mas dominado pelo enfrentamento na Zona Cinzenta.

O artigo se desenvolve a partir da definição do conceito de OSINT, e como responde às limitações das doutrinas tradicionais. Depois, é abordada a Zona Cinzenta, explorando seu surgimento pós-Guerra Fria, suas principais ferramentas.

Isto permitirá compreender o conflito no leste ucraniano como um conflito na Zona Cinzenta e como a OSINT foi utilizada para respondê-la, bem como suas repercussões.

1. Doutrinas de inteligência

Inteligência é um tema universal, e seu uso por diversos atores, para propósitos variados, tornando-se necessária uma definição geral. Shuslky e Schmitt (2002) definem inteligência como a coleção, avaliação e análise de informações, traduzidas para necessidades específicas de um consumidor final. Nas Relações Internacionais, diversos atores são consumidores de inteligência, principalmente o Estado, graças ao Dilema de Segurança. Este dilema não gera apenas corridas e hostilidades armadas, mas ações de espionagem em uma infinidade de temas. Desta forma, nas Relações Internacionais, inteligência significa é a coleta e interpretação de informações que os governos julgam necessárias para a formulação e implementação de políticas, para promover seus interesses e lidar com ameaças de [potenciais] adversários, em temas econômicos, militares e políticos, enquanto se empenham para esconder suas informações vitais.

Qualquer que seja o objetivo da inteligência, a coleção de informações é parte indispensável. Coleção é o ajuntamento de dados brutos, através de várias técnicas, chamadas Doutrinas de Inteligência. Schuslky e Schmitt (2002) as organizam em três categorias: inteligência humana (HUMINT), inteligência técnica (TECHINT), e ação aberta (OSINT), que será abordada.

1.1 OSINT: informações em fontes abertas

Numa definição sucinta, OSINT é a coleta e análise de informações vindas de fontes abertas; todos os lugares onde as informações estão publicamente disponíveis, dispensando invasões, ilegalidades ou violação de segredos. Estas fontes possuem grande parte dos dados indispensáveis para a produção de inteligência, e além de reduzirem o risco político, especialmente se o alvo estiver localizado em um país hostil (HASSAN & RIJAZI, 2018), pode ser coletada gratuitamente, ou com serviços sob demanda, refletindo um baixo custo operacional. O impacto da internet na noção de fontes abertas tornou necessário dividir a OSINT em duas versões: clássica e digital.

Sua versão clássica é observada em antigos manuais de inteligência dos EUA, como o Manual de Campo 2–29, do TRADOC (2010), publicados antes da explosão de dados na internet. Neles, “fontes abertas” ainda se referiam a mídias analógicas; rádios, jornais impressos, televisão e diários oficiais. Ao se referirem a sites, se limitavam a diários eletrônicos, micro blogs ou sites oficiais. Assim, a versão

clássica se deparava com desafios. Seus métodos de coleta se limitavam à simples absorção das informações, sem a capacidade de implementar técnicas de análise e ligação entre as fontes de informação. Analisar sua legitimidade dependia de longas pesquisas documentais, prolongando o período de operações.

A OSINT digital pode ser observada principalmente no início da década de 2010. Neste período, a noção de ciberespaço e mundo digital amadureceram, com a ascensão de redes sociais, machine learning e Big Data (ÜNVER, 2018.). O fato do Centésimo Nono Congresso dos Estados Unidos abordar sua definição e importância, oferece uma primeira visão sobre o impacto da OSINT na era da informação:

> Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. With the Information Revolution, the amount, significance, and accessibility of open-source information has expanded significantly, but the intelligence community has not expanded its exploitation efforts and systems to produce open- source intelligence. The production of open-source intelligence is a valuable intelligence discipline that must be integrated into intelligence tasking, collection, processing, exploitation, and dissemination to ensure that United States policymakers are fully and completely informed (109th US CONGRESS, 2006).

Assim, suas técnicas e métodos não se referem à simples absorção de informações, mas a diversas formas de comprová-las, verificar seus impactos e quais caminhos elas trilharam, do primeiro ao último a publicá-la, em um curto espaço de tempo. Embora livros, enciclopédias e documentos analógicos continuem sendo utilizados, é no mundo digital que reside a maioria das oportunidades. Não só nas redes sociais e arquivos digitais, mas nos seus metadados, webcams e câmeras wi-fi de rua, desprotegidas, falhas humanas e vazamentos apontados publicamente.

IMINT e GEOINT podem ser realizados através de dados fornecidos por ferramentas e serviços sob demanda, gratuitos ou não.

Imagens de satélite, por exemplo, são acessíveis. O satélite Geoeye-1 vende imagens e informações geográficas que variam de 17 a 25 dólares por quilômetro quadrado capturado, dependendo principalmente de quão recente é a imagem (APOLLO MAPPING, 2022). Versões gratuitas, mas de qualidade menor e mais antigas, também estão disponíveis. Além do Google Earth, imagens vindas diretamente de satélites famosos, como os Sentinel-1 e 2, estão disponíveis em sites como SentinelHub. Outras ferramentas gratuitas, como sites que fornecem transmissões de rádio de ondas curtas, chamadas WebSDR, auxiliam na produção de

SIGINT, caso o alvo da investigação se comunique sem criptografia. Após a invasão russa em fevereiro de 2022, por exemplo, soldados russos precisaram recorrer a rádios de ondas curtas, graças à queda de sinal GSM na região. As frequências, não encriptadas, foram interceptadas por ferramentas on-line, transcritas e documentadas, como mostram Bandouil e Hall (2022).

Limitações, claro, também atingem a OSINT. Conhecer o ciberespaço e sua cultura; fóruns, sites e redes sociais que alvos utilizam, e seus comportamentos, é primordial e requer tempo. Além disso, não há um conjunto bem definido de métodos OSINT, deixando o coletor à mercê da sua própria criatividade. Tais problemas diminuem à medida que a curva de aprendizado é conquistada, além da leitura de estudos de caso e interação com outros investigadores.

Este último fato leva à última vantagem; a ascensão dessa forma de inteligência criou uma grande comunidade, que compartilha técnicas, ferramentas e experiências com impactos reais e compartilhamento descentralizado de informações. Governos podem explorar esta capacidade e apoio destas comunidades, não só aumentando capacidade de inteligência, mas exercendo Soft Power. Grande parte das investigações que serão apresentadas, por exemplo, foram produzidas por grupos voluntários de inteligência. Antes de explorar as aplicações desta doutrina, no entanto, é necessário evidenciar os desafios que a Zona Cinzenta impôs no mundo pós-guerra fria, e como a OSINT pôde ser utilizada.

1.2. A Zona Cinzenta

Dado seu caráter extremamente ambíguo, a ideia de Zona Cinzenta ainda é bastante discutida, e abriga diversas definições sobre sua natureza. Todas elas, no entanto, descrevem atividades muitíssimo reais no cenário internacional contemporâneo, definidas desta forma:

> (...) a set of activities that occur between peace (or cooperation) and war (or armed conflict). A multitude of activities fall into this murky in-between — from nefarious economic activities, influence operations, and cyberattacks to mercenary operations, assassinations, and disinformation campaigns. Generally, gray-zone activities are considered gradualist campaigns by state and non-state actors that combine non-military and quasi-military tools and fall below the threshold of armed conflict. They aim to thwart, destabilize, weaken, or attack an adversary, and they are often tailored toward the vulnerabilities of the target state. (STARLING et al., 2022, n. P,)

Em outras palavras, a Zona Cinzenta é um grupo de atividades que são mais ameaçadoras do que a política comum e menos ameaçadoras que o combate militar direto entre as grandes potências, e visa vantagens essencialmente no longo prazo. É uma adaptação de uma grande lição aprendida na Guerra Fria: o Poder existe em três, não duas, grandes camadas (NYE, 2011). Além das camadas tradicionais, de poder militar e econômico, há a camada das relações transnacionais não-estatais. Nela, o poder é difuso e compartilhado por diversos atores não-estatais, como banqueiros, influenciadores, ONGs, guerrilheiros e grupos terroristas. Na Guerra Fria as potências financiavam membros desta terceira camada, através de conflitos proxys. Isto é, financiavam grupos armados não-estatais para a tomada de poder em curto prazo, e o enfraquecimento do bloco inimigo a longo prazo (HUGHES, 2014). Tratava-se de um propósito mais operacional e tático do que estratégico.

A Zona Cinzenta adapta este conceito em dois pontos. Em primeiro lugar, os Estados passam não só a interagir mais com a terceira camada, como a se disfarçar de atores não-estatais típicos dela; influenciadores, grupos guerrilheiros ou empresas. Esta interação mais profunda e disfarce geram o segundo ponto; evolução da camada operacional e tática, para a estratégica, visando essencialmente acumular ganhos a longo prazo. De fato, o Estado ainda pode se envolver em violência, mas na maioria das vezes, ela é mitigada por ser realizada por forças ambíguas; estados disfarçados de atores não-estatais (DOBBS et al., 2020; HICKS et al., 2019)

Desta forma, a Zona Cinzenta se divide em seis ferramentas. Tratam-se das Operações de Informação; Operações Cibernéticas; o uso de Forças Ambíguas; Coerção Política, a Coerção Econômica e, por último, Operações Espaciais. Apenas o uso de Forças Ambíguas será explorado, visto suas implicações no conflito ucraniano.

2.1 Forças Ambíguas e seu uso na Ucrânia

Nas Zonas Cinzentas, operações utilizando forças ambíguas promovem a intimidação, ou o controle de território para exercer influência política, econômica ou militar a longo prazo (HICKS et al., 2019). Diferente de forças proxy, forças ambíguas são forças armadas utilizadas pelo estado, mas que flutuam entre a categoria de forças independentes, proxy e forças regulares do estado. Seus responsáveis não argumentam necessariamente serem grupos não-estatais, mas negam que estejam obedecendo ordens de algum governo ou que sejam financiados por ele. Como dito anteriormente, os atores estatais não apenas interagem com terceira camada de poder; se misturam e se “disfarçam” de atores não-estatais.

Esta ambiguidade foi evidente nas forças ambíguas empregadas nos primeiros meses de anexação da Crimeia, em 2014. Inicialmente, os soldados não

apresentavam postura combativa e, nas raras vezes que se comunicavam com terceiros, respondiam de maneira lacônica e evasiva (USASOC, 2015).

Além de permitir que o artifício da negação seja usado prolongadamente, o uso de forças ambíguas permite que o Estado intensifique ou retarde a escalada de violência conforme planejado, sem maiores repercussões internas ou externas. Também mitiga a atenção internacional, reduz o custo humano com baixas, auxilia na construção da narrativa e o consequente apoio popular, que outrora seria afetado.

Essa perspectiva coincide com as considerações de Valeri Gerasimov (2013) ao analisar a política externa dos Estados Unidos durante a Primavera Árabe. Argumentando que a linha entre guerra e paz se tornou tênue e ambígua, ele argumenta que o Ocidente pôde combinar ações cinéticas e não-cinéticas para influenciar a evolução do conflito entre o âmbito militar e civil, à medida que desejar. Essa estratégia permite ao Estado justificar atividades cinéticas, apoiar certos grupos e, por fim, solidificar sua própria narrativa na região (GERASIMOV, 2013; USASOC, 2015), até que seja suficiente para um ataque final, como se pretendia demonstrar na operação russa de 2022.

É válido ressaltar que o uso de forças ambíguas não exclui o de proxy. No leste da Ucrânia, o uso de proxys e voluntários foi diluído na presença de soldados regulares russos sem insígnias. Além disso, apesar de soldados russos regulares participarem e comandarem soldados e separatistas voluntários no conflito, grupos mercenários como a Wagner participaram de combates (KAPUSTA, 2015). O uso combinado de proxy e força ambígua permite um controle ainda maior do proxy. Ora, apesar de ser “submisso” ao Estado que o financia, um proxy possui suas próprias ideologias e cadeia de comando, podendo eventualmente discordar ou se tornar um inimigo[3].

Em 24 de Fevereiro de 2014, após a conclusão do Euromaidan, soldados russos da 810.ª Infantaria Naval chegaram à praça central da cidade, violando as regras que regiam as divisões territoriais na Crimeia. Em menos de três dias, estes soldados, sob o disfarce de “milícias de autodefesa” e juntos a manifestantes pró-Rússia, tomaram o Parlamento da Crimeia (PROMETHEUS, 2017). Isto permitiu que a Rússia pudesse continuar a negar qualquer envolvimento, enquanto aumentava a manobrabilidade destas forças e alimentava sua retórica. O golpe final foi realizado em 16 de Março de 2014. quando um referendo pela anexação, considerado legalmente nulo internacionalmente, legitimou e finalizou com sucesso a narrativa que sustentava o processo de tomada da Crimeia, sem baixas e altercações militares.

[3] Exemplo recente deste erro está na própria Rússia, após o lançamento oficial da invasão, em 2022. Começando a depender mais da companhia Wagner do que das forças ambíguas pré-estabelecidas, a empresa pôde, em Junho de 2023, se rebelar temporariamente contra o alto comando do Ministério da Defesa da Rússia, e sair praticamente ilesa.

Paralela à anexação da Crimeia, a Rússia também tentava tomar Donbass: o Leste ucraniano. Enquanto a utilização sincronizada de táticas nas Zonas Cinzentas foi relativamente pacífica na península, sua implementação em Donbass desencadeou um violento conflito armado. Dadas as circunstâncias étnicas e políticas da região, a inteligência ucraniana (SBU) pôde repelir várias tentativas iniciais de tomar estruturas governamentais e militares. Embora seja impossível definir se esta escalada era planejada ou esperada, é verificável que a Rússia aumentou o número de soldados e operações cinética como resposta (PROMETHEUS, 2017; USASOC, 2015).

No dia 14 de Abril de 2014, o governo ucraniano anunciou uma contra ofensiva, criando uma “Zona de Operação Anti-Terrorista” (ATO). Militares russos continuaram seus esforços apesar das medidas, anunciando a República Popular de Lugansk (LPR) no dia 27, realizando um referendo conjunto pela independência de Lugansk e Donetsk, no início de Maio, além de estabelecer oficialmente a República Popular de Donetsk. Em setembro de 2014, o conflito se intensificou e, por fim, estagnou novamente. (PROMETHEUS, 2017; USASOC, 2015)

Embora atualmente milhares evidências demonstrem a ampla atuação e planejamento russo no conflito, o seu período inicial foi obscuro. Como exposto, mesmo as agências de inteligência do ocidente, com acesso a imagens de satélite permaneceram relativamente silenciosas durante os primeiros meses; o uso de forças diluídas e formações não convencionais dificultou o reconhecimento da infiltração destes soldados em forças voluntárias no leste ucraniano. Além disso, a Ucrânia acabara de sair de meses de tumulto e violência política, contribuindo ainda mais para a incerteza e desconcerto. De qualquer forma, o “blackout” de informações destes primeiros meses foi clareado por indivíduos e comunidades dedicadas ao OSINT digital, preenchendo este vazio informacional com resultados louváveis.

3. Investigações OSINT e a utilização de evidências no plano internacional

Nesta seção, serão abordadas as investigações OSINT cruciais para o desmonte da narrativa russa diante do cenário internacional. Primeiro, serão apresentadas investigações sobre unidades de infantaria; sua camuflagem, identidade e armamentos únicos. Logo após, serão apresentados casos sobre veículos de guerra exclusivos da Rússia, presentes em solo ucraniano. Depois, será abordado como várias destas evidências foram utilizadas por organizações governamentais internacionais nas suas tomadas de decisões.

3.1. Soldados russos em Donbass

Desde o primeiro dia da invasão à Ucrânia, centenas de fotos e vídeos, capturados por jornalistas civis, publicadas na TV, sites na internet ou redes sociais, mostravam a chegada dos comboios de soldados no país. Essa extensa base de dados abertos é suficiente para analisar os soldados. A partir destas mídias, verificamos e checamos a origem dos equipamentos, comparando as imagens com bases de dados especializadas em militaria. Estes dados ganham mais credibilidade se comparados com peças jornalísticas dos setores militares, que oferecem dados sobre a produção e distribuição destes equipamentos. Principalmente na Crimeia, os soldados utilizavam o mesmo conjunto de equipamentos, com pouca variação. Utilizando uma camuflagem digital verde, eles não carregavam insígnias, e seus rostos eram cobertos por balaclavas. Evitavam se comunicar com a população local e com jornalistas, assim. Um bom exemplo da aparência e do equipamento usado por estes soldados está na Figura 1, abaixo.

Figura 1 – Soldado sem insígnia em Simferopol

Fonte: Arrott (2014)

O uniforme e o colete tático do soldado chamam a atenção. No uniforme, tanto o esquema de cores quanto o padrão digital da camuflagem são o padrão EMR, também chamado Tsifra, exemplificado Figura 3, abaixo. Segundo o Ministério de Defesa da Rússia (MDR), a camuflagem foi criada em 2008, mas adotada oficialmente pelo exército em 2011 (CAMOPEDIA, 2022; MDR, 2011). Bielorrússia e Rússia são os únicos países da região utilizando esta camuflagem, enquanto ocupadas por forças russas, começaram a usá-las em 2016, como abertamente observado na Transnístria e Ossétia do Sul (FULLER, 2017; ORYX, 2020).

Figura 2 – Primeira versão da Camuflagem EMR

Fonte: Voyennoye Obozreniye (2010)

O colete modular utilizado é o 6SH117, demonstrado na Figura 4. É parte do programa Ratnik-2, criado também em 2008 pelo MDR, para modernizar os equipamentos de infantaria. Segundo o jornal RIA Novosty (2012), o equipamento foi exposto em público pela primeira vez em 2011. Sites de notícias oficiais da Rússia mostram que o equipamento foi adotado em outubro de 2014, mas usado em larga escala apenas em 2015 (GRAVRILOV, 2015; SPUTNIK, 2014).

Figura 3 – Colete 6SH117 com estojos inclusos, camuflagem EMR

Fonte: YOULA (2017)

Destaca-se o fato da camuflagem do colete na Figura 5 ainda ser a versão Flora[4], tratando-se provavelmente de um protótipo, exclusivo da Rússia. Em outras palavras, é improvável que grupos civis tenham conseguido estes equipamentos em lojas de artigos militares, durante o período da invasão, já que seu excedente não estava à venda. A presença antecipada deste equipamento também demonstra o uso da Ucrânia como campo de testes de equipamentos, de infantaria até de veículos, como será exposto.

[4] Camuflagem anterior à EMR, lançada em 1998, usada amplamente pelas unidades convencionais das Forças Armadas Russas (CAMOPEDIA, 2022)

Embora fontes jornalísticas, publicitárias e governamentais sejam bastante úteis, a maioria das evidências cruciais partem dos próprios soldados, em suas redes sociais. Como já dito, a mesma sensação de anonimato que permite que os soldados exponham toda sua vida privada na internet, se tornam oportunidades de investigação.

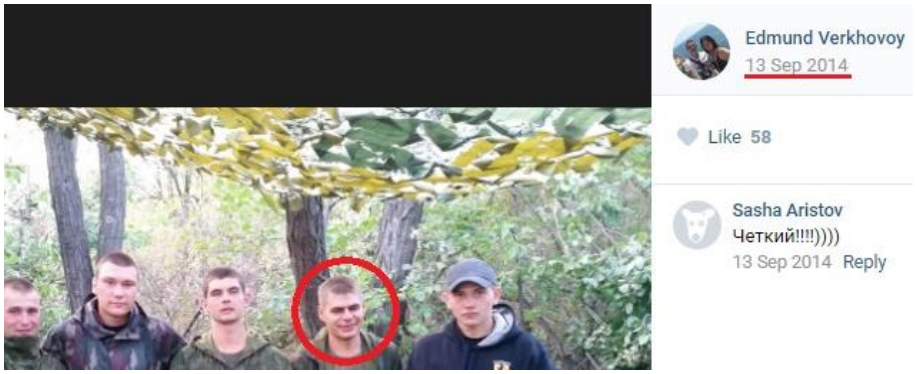
Ferramentas das próprias redes sociais, que delimitam a pesquisa de pessoas por categorias como local, cargos e grupos, e pesquisa de publicações por local, data e palavras-chave, são pontos de partida interessantes. Além disso, como no Facebook, a versão móvel do VK pode utilizar o GPS do Smartphone, ou a localização embutida nos metadados de fotos, para marcar automaticamente a localização da publicação. Isto também representa oportunidades de investigação. A descoberta de um perfil leva à de outros, na rede de amigos, sendo o descuido de apenas um soldado o suficiente para a exposição de toda a unidade. Uma das comunidades de OSINT com maior destaque neste princípio investigativo é o InformNapalm.

Contando com investigações cooperativas com outros grupos voluntários de todo o mundo, o site conta com versões em 31 idiomas e permanece ativo mesmo após a invasão de fevereiro de 2022. Apenas entre 2014 e 2016, a comunidade identificou mais de 70 unidades militares russas atuando em Donbas. Embora várias técnicas OSINT sejam utilizadas, o seu destaque está nas redes sociais. De 195 investigações conduzidas ou documentadas pelo grupo no período de 2 anos, 134 partiram das redes sociais regionais VK e OK (INFORMNAPALM, 2016a, 2016b)

Importante exemplo desta investigação vem de uma das várias exposições da participação de soldados da 15.ª Brigada de Fuzileiros de Guardas Separados Alexandria, das forças terrestres russas, na guerra em Donbas e na Crimeia. As evidências desta investigação específica, referente a Donbas, foram publicadas em novembro de 2017, tendo como ponto de partida o descuido de um dos membros; Nikolai Plotnikov.

Ele aparece numa foto, visto na Figura 5, publicada em setembro de 2014, no perfil do VK de um de seus colegas, chamado Vitaly Perfilov (codinome Edmund Verkhovoy). Da foto, 5 dos 6 sujeitos presentes foram precisamente identificados, partindo da identificação de Plotnikov. Além disso, evidências adicionais foram encontradas nos perfis de mídia social desses militares, publicadas em 2014, e geolocalizadas em Lugansk.

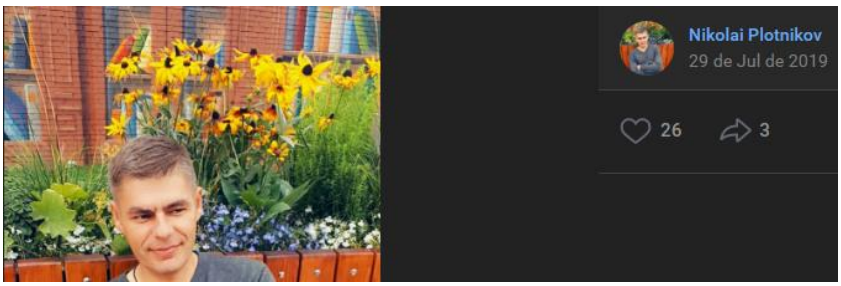
Figura 4 – Publicação de Vitaly Perfilov



Fonte: INFORMNAPALM (2017)

Das cinco identificações, a de Nikolai Plotnikov, circulado na Figura 4 foi a mais importante. Ele é dono de perfis nas redes sociais, de onde foram extraídas informações mais pertinentes. Para manter o trabalho conciso, apenas a investigação acerca de Plotnikov será abordada, concedendo espaço para abordar outras categorias de investigações. Segundo o perfil de Plotnikov (2022), que no ano da investigação usava o codinome “Nikolai Marinin”, ele nasceu em Yoshkar-Ola, na república étnica de Mari El, Rússia. Sua mais recente foto de perfil (Figura 7) mostra o rosto de forma bastante nítida.

Figura 5 – Foto de Perfil de Plotnikov



Fonte: Captura de tela do autor (2022)

Também na sua conta, há um vídeo publicado em dezembro de 2014 (PLOTNIKOV, 2014), intitulado “Como passei o verão de 2014” (Figura 8). Com quase dois minutos de duração, o vídeo mostra um comboio de APCs passando por prédios destruídos, veículos e campos incendiados. Já nos dois primeiros frames, é visível uma construção governamental, exposta na Figura 6, abaixo.

Figura 6 – Vídeo no perfil de Plotnikov

Fonte: Captura de tela do autor (2022)

Extraindo os frames e cruzando com imagens da ferramenta de fotos do Google Earth, chega-se à conclusão de que a construção é um centro comunitário chamado Casa da Cultura, no vilarejo de Novosvitlivka, localizado no oblast de Lugansk, Ucrânia (Figura 7).

Figura 7 – Casa da Cultura, oblast de Lugansk, Ucrânia

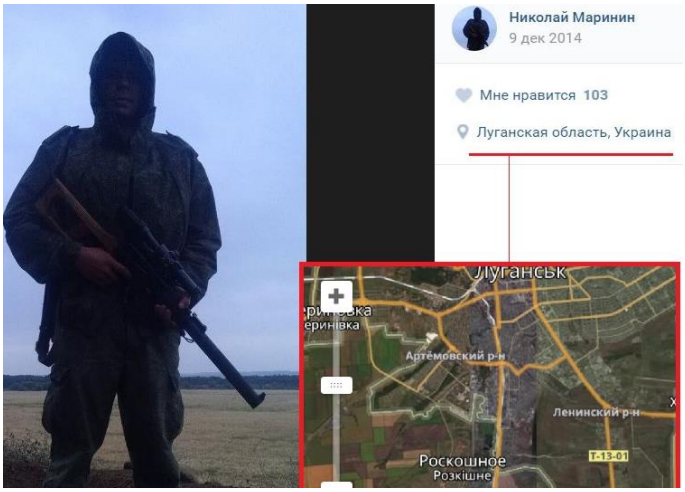
Fonte: Colagem do autor no software Google Earth PRO (2020)

Aos 22 segundos do vídeo, o celular vira e filma o rosto de Nikolai, evidenciando que o vídeo foi gravado por ele. Trata-se de uma evidência da presença de Nikolai em Lugansk já durante o conflito, dada a destruição do local. A geolocalização do vídeo coincide com uma foto publicada por ele, em 9 de dezembro de 2014 (Figura 8), portando um fuzil de precisão. Ele deixou ativa a localização no VK, antes de publicar a foto, localizando-a em Lugansk, Ucrânia.

Ele segura o VSS Vintorez, um fuzil de precisão com silenciador integrado. Concebido nos anos 80, também pela TsNIITochMash, o VSS é uma arma bastante particular. Sua munição subsônica é de calibre único, de 9x39mm, criado para as

armas soviéticas e russas com silenciador integrado, especialmente da família VSS, como a As Val e VKS. Desta forma, embora a SBU tenha acesso a esse rifle, ele é escasso, sendo sua distribuição a outros países, é limitada (MITROFANOV, 2019).

Figura 8 – Plotnikov em Lugansk



Fonte: InformNnapalm (2017)

Outras evidências de participação direta de infantaria russa estão nas munições e equipamentos apreendidos e avistados. A já mencionada VSS é um bom exemplo. Plotnikov não foi o único observado utilizando este armamento. Em julho de 2014, quando as forças ucranianas retomaram Sloviansk do controle dos soldados de Igor Girkin, vários veículos de mídia realizaram reportagens. Muitas caixas de munições russas podem ser vistas. Ótimo exemplo está na notícia transmitida pelo Kanal 5 (2014). Em um dos seus frames (Figura 9), várias caixas de munição 39x9mm são vistas.

Figura 9 – Caixa de munição em frame de reportagem

Fonte: Captura de tela do autor (2022)

A marcação “9x39СПП” expõe se tratar da variante SPP[5] do calibre 3x39mm. Observa-se o código “M46-07-539” na caixa. Segundo Ezell e Stevens (2001) e a Small Arms Survey (2018), estas marcações representam, respectivamente, o lote: M46, ano: 2007, e código da fábrica: 539. Segundo a International Ammunition Association (2022), o código de fábrica 539 é referente à Planta de Cartuchos de Tula. Verificando o site da planta, é possível ver que este cartucho está no seu catálogo. Já em maio de 2015, dois membros das forças especiais russas foram capturados pelo exército da Ucrânia, também em Lugansk, utilizando o mesmo fuzil. Fato esse admitido pelo próprio MDR, que argumentou que os dois soldados foram descomissionados do exército russo, antes de serem presos na Ucrânia (BBC, 2015).

Nos casos da infantaria, ainda é relativamente fácil negar que eles estivessem sob ordens da Rússia, argumentando que foram afastados do exército anteriormente, ou que cruzaram a fronteira “por acidente”, ainda que seus equipamentos sejam impossíveis de obter individualmente (WALKER, 2014). Já em relação a veículos e outras armas de guerra exclusivas da Rússia, esta negação é desafiada, como será exposto a seguir.

3.1.2. Veículos militares russos em Donbas

Nos primeiros anos do conflito, Donbass estava saturada com equipamento militar russo, principalmente tanques, artilharia e unidades de guerra eletrônica (PROMETHEUS, 2017, p. 73). Alguns não haviam sido adotados oficialmente pela Rússia no período, fortalecendo a já mencionada ideia de que a Ucrânia foi usada como campo de testes.

Uma evidência é o RB-341V Leer-3; sistema de Guerra Eletrônica baseado em drones. Ele é transportado no caminhão militar russo KamAZ. O operador permanece no caminhão, enquanto um drone Orlan-10 é lançado, localizando fontes de sinais GSM. O sistema interfere nesse sinal, inviabilizando várias formas de comunicação, ou imitar confundindo os sistemas de SIGINT do adversário, ou enviando informações falsas para seus receptores decodificarem (DEAGEL, 2015; OE DATA INTEGRATION NETWORK, 2021).

Segundo fontes da Rússia, como a revista de conteúdo militar Military Review (2015), o Leer-3, visto na Figura 10, foi mostrado ao público pela primeira vez no início de outubro de 2015, na exposição do Dia da Inovação, em Rostov. Segundo especialistas do Distrito Militar do Oeste, eles foram os primeiros a usar o sistema, para tarefas de treinamento, em outubro de 2015.

[5] Do russo “Snaiperskiy, Povishennaya Probivaemos”, significando “Atirador de elite, penetração aumentada”

Figura 10 – Leer 3 e drone Orlan-10 exibidos em outubro de 2015

Fonte: Military Review (2015)

No entanto, em maio de 2015, o Leer-3 foi avistado em Donbas. A evidência vem do líder do Esquadrão Viking, parte do primeiro Batalhão de Fuzileiros Motorizados da DPR, Gennadiy Dubovoy (2015). Publicado no Youtube em 10 de maio de 2015, o vídeo (Figura 11) mostra soldados do esquadrão operando em Donetsk. Aos 53 segundos é possível ver o caminhão estacionado, no canto superior esquerdo da tela. No dia 11 de maio de 2015, o vídeo foi publicado na página oficial do esquadrão, no VKontakte.

Figura 11 – Vídeo propagandístico no YouTube

Fonte: Gennadiy Dubovoy (2015)

Além de sistemas de guerra eletrônica, equipamentos mais letais também foram utilizados na região. Estes equipamentos foram responsáveis por inúmeras baixas nas mais importantes batalhas do conflito em 2014, sendo o principal fator de violência. Um dos eventos que servem a esse exemplo é a Batalha de Ilovaisk.

No início do conflito, as forças ucranianas obtiveram uma série de vitórias na retomada de alguns territórios. Aproveitando o “momentum”, as forças planejavam

retomar a cidade de Ilovaisk, em Donetsk. As operações começaram em 7 de agosto de 2014, mas pós meses de violentas altercações, os separatistas russos saíram vitoriosos, em setembro de 2014. A derrota foi importante fator no processo de impasse do conflito, que solidificou as fronteiras, permanecendo relativamente inalteradas durante oito anos. Trata-se também de uma importante batalha do ponto de vista investigativo (KORRESPONDENT, 2014). Grande parte do crédito pela vitória separatista em Ilovaisk se deu exatamente pela participação de tanques exclusivos da Rússia. Vários grupos OSINT se debruçaram sobre as evidências nesta batalha, com destaque do trabalho realizado pela Forensic Architecture (FA) e seus colaboradores (MOORE, 2018; UNIAN, 2016a).

A FA é uma agência investigativa londrina que integra o uso de arquitetura, modelagem 3D e inteligência artificial às fontes abertas. Seus investigadores atuam em parceria com equipes jurídicas e ONGs internacionais, realizando as investigações em nome das comunidades e indivíduos afetados diretamente por conflitos e abusos de autoridade (E-FLUX, 2017). Para o caso da Batalha de Ilovaisk, apresentado em agosto de 2019, a FA aplicou princípios de inteligência artificial a uma base de dados de fotos e vídeos capturados em fontes abertas, como agências de notícias de todo o mundo, que reportavam o conflito in loco.

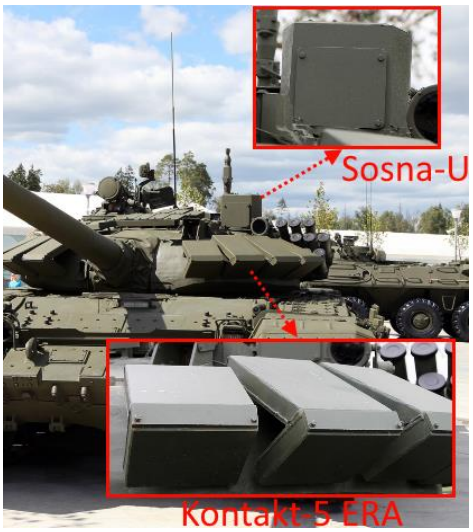
Com estas fontes, cerca de 300 veículos militares russos nas cidades de Ilovaisk e Lugansk foram identificados. As evidências e o processo investigativo foram publicados num site com um mapa interativo. Também são oferecidos vídeos que expõem como foi determinado o modelo do veículo captado pelas câmeras, além de sua geolocalização (FA, 2019). Uma das principais identificações foi o T-72B3 que, segundo a revista pró-Rússia Military Review e o site Deagel, foi desenvolvido pela Rússia a partir de 2010, numa empreitada para modernizar o tanque soviético T-72. Enquanto o T-72 foi largamente vendido e produzido em países parceiros e membros da URSS, incluindo a Ucrânia, o T-72B3 não foi exportado para a Ucrânia, estando em produção na Rússia desde 2012 (FA, 2019).

A primeira grande exibição pública pode ser verificada no Biatlo do Tanque de 2014 (LUHN, 2014). Já em relação ao seu uso militar, segundo o Tank Encyclopedia (2014), a primeira distribuição para o exército russo ocorreu apenas em outubro de 2014. Neste sentido, o tanque, assim como outros equipamentos, parece ter sido testado em combate na Ucrânia, entre agosto e setembro de 2014.

O sistema OE Data Integration Network (ODIN), do Exército dos Estados Unidos (2022) expõe que a nova versão buscava as vantagens do T-72, enquanto adicionou componentes como o Sosna-U e a blindagem Kontakt-5. O primeiro é um aparelho de visão panorâmica termal e diurna, num formato de caixa, enquanto o segundo é uma armadura reativa explosiva, que cobre o tanque. Estes dois

componentes se destacam bastante, como visto na Figura 12, abaixo,

Figura 12 – T-72B3 em exposição



Fonte: colagem do autor (2022)

Através das várias fotos e vídeos em exposições e exercícios, a FA pôde desenvolver um modelo 3D e compará-lo com fotos do campo de batalha em Ilovaisk, onde o tanque foi avistado. Posicionando o tanque similarmente e comparando seus detalhes, é possível comprovar sua presença, como demonstrado na Figura 13, abaixo.

Figura 13 – Comparação entre foto em campo de batalha e modelo 3D

Fonte: colagem do autor (2022), baseada na apresentação da FA (2019)

Destroços encontrados no campo de batalha e filmados por correspondentes de vários noticiários, incluindo o jornal pró-Rússia Russia Today, também foram geolocalizados e utilizados para a comparação com o modelo 3D, como demonstra a Figura 14, abaixo.

Figura 14 – Comparação entre casco de tanque destruído e modelo 3D

Fonte: colagem do autor (2022), baseada na apresentação da FA (2019)

Através de outras formas de comparação e análise, a FA chega à conclusão da ampla participação de brigadas de tanques russos na batalha, coincidindo com outras investigações de Toler e Aksai (2015a, 2015b) e da InformNapalm (2015).

3.3. Repercussões internacionais

Várias destas investigações e grupos obtiveram relativos sucessos no cenário internacional. Destaca-se o grupo InformNapalm. No dia 19 novembro de 2016, após atingir a marca de 75 unidades militares russas identificadas em Donbass, a o grupo desenvolveu uma base de dados, publicada junto a um vídeo com duração de seis minutos e legendas disponíveis em cinco idiomas, sobre as investigações e provas coletadas. Com 165 incidentes selecionados, o material foi utilizado por delegados do Parlamento Ucraniano, numa apresentação na Assembleia Parlamentar da OTAN (NATO PA). (INFORMNAPALM, 2016c, UNIAN, 2016b). A apresentação das evidências levou à conclusão de que através de suas ações e retórica, a Rússia tentava desestabilizar o ambiente de segurança europeu e minar as atividades da OTAN, levando à necessidade de mais sanções (NATOPA, 2016). Demonstrou-se à Europa que, mesmo com o congelamento do conflito, a presença russa não havia diminuído. Ao contrário; mais sistemas tecnológicos russos, ofensivos e de suporte, eram transportados. Em conclusão, elas serviram para o fortalecimento de sanções à Rússia.

Outra importante repercussão veio do apoio da Forensic Architecture ao Centro Europeu de Advocacia pelos Direitos Humanos (EHRAC) num caso relacionado à batalha de Ilovaisk. A EHRAC representava 25 combatentes voluntários do Batalhão Donbass, da Ucrânia, que foram detidos por soldados russos em agosto

de 2014. A FA foi contratada para expor evidências da presença russa em Ilovaisk e arredores, comprovando a responsabilidade russa pelas violações ao Artigo 3.º da Convenção Europeia, cometidas por seus soldados. O caso foi apresentado na Corte Europeia de Direitos Humanos (ECHR), sob a aplicação número 60372/14, de nome "Ponomarenko V. Ukraine and Russia and 19 other applications". Atualmente, ainda é considerado um Caso Comunicado; os governos acusados no litígio foram comunicados do pedido (EHRAC, 2017, 2018, 2019).

CONCLUSÃO

Embora a Rússia não reconheça a jurisdição da corte holandesa sobre cidadãos russos, assim como não reconheceu os relatórios oficiais que escancaram sua participação em Donbas, sua capacidade de negar responsabilidade está ameaçada. Como dito, grande parte das táticas das Zonas Cinzentas são dedicadas ao objetivo de construir uma narrativa a longo prazo, que valide ações ofensivas no campo internacional e resulte num ganho mais estável de poder.

O uso de OSINT digital, com softwares de códigos abertos, sem ligações com informações privilegiadas ou malwares, destroem esta tática argumentativa, que afirma que agências de inteligência de países oponentes estão utilizando sua autoridade para modelar acusações e evidências falsas. Neste caso, o OSINT corrói a narrativa que sustenta as ações ofensivas do governo, especialmente nas Zonas Cinzentas. Estas potencialidades devem ser melhor exploradas pelos estudiosos das Relações Internacionais, caso desejem permanecer atentos aos desdobramentos desse complexo mundo digital.

REFERÊNCIAS

109TH U.S CONGRESS. **NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2006,** 2006. Disponível em: https://www.govinfo.gov/content/pkg/PLAW- 109publ163/html/PLAW-109publ163.htm Acesso em: 5 set. 2020.

5. KANAL Terorysty U Slov'yans'ku Buly Osnashcheni Suchasnoyu Rosiys'koyu Zbroyeyu. **YouTube**, 7 jul. 2014. Disponível em: https://www.youtube.com/watch?v=lvQgIZNHEkM. Acesso em: nov. 2022.

APOLLO MAPPING. **GEOEYE-1 satellite**. 2002. Disponível em: https://apollomapping.com/geoeye-1-satellite-imagery. Acesso em: 20 set. 2022

ARROTT, E. On the Scene: Crimea Divided. **VOA News**, 28 fev. 2014. Disponível em: https://www.voanews.com/a/on-the-scene-voas-elizabeth-arrott-in-crimea-/1861242.html. Acesso em: nov. 2022.

BANDOUIL, K.; HALL, R. Online sleuths are intercepting Russian radios and revealing potential war crimes. **The Independent**, 3 mar. 2022. Disponível em: https://www.independent.co.uk/world/ukraine-russia-putin-radio-civilians-b2027256.html. Acesso em: 1 dez. 2022.

BBC. Ukraine to prosecute captured “Russian soldiers”. **BBC News**, [S.l.], 18 maio. 2015. Disponível em: https://www.bbc.co.uk/news/world-europe-32788413. Acesso em: 2 dez. 2022.

DAVID. T-72. Tank Encyclopedia, 23 nov. 2014. Disponível em: https://tanks-encyclopedia.com/coldwar/ussr/soviet_t-72.php. Acesso em: nov. 2022.

DEAGEL. Leer-3 (RB-341V). **Deagel**, 2015. Disponível em: https://www.deagel.com/Tactical%20Vehicles/Leer-3/a003204. Acesso em: nov. 2022.

_____. T-72. **Deagel**, [s.d.]. Disponível em: https://www.deagel.com/Armored%20Vehicles/T-72/a000770. Acesso em: nov. 2022.

DOBBS, D, *et al.* Grey Zone. **The Forge.** 2020. Disponível em: https://theforge.defence.gov.au/sites/default/files/2020-10/Grey%20Zone_0.pdf Acesso Em: 30 fev 2022.

DUBOVOY, G. Vikingi. Ucheniya. Bronya krepka i tanki nashi bystry. **YouTube**, 10 maio. 2015. Disponível em: https://www.youtube.com/watch?v=V5LjhrPFH9c. Acesso em: ago. 2020.

EUROPEAN HUMAN RIGHTS ADVOCACY CENTRE. Ponomarenko and others v Ukraine and Russia. **EHRAC**, 19 ago. 2019. Disponível em: https://ehrac.org.uk/en_gb/key-ehrac-cases/ponomarenko-and-others-v-ukraine-and-russia/. Acesso em: ago. 2022.

EZELL, E. C.; STEVENS, B. **Kalashnikov, the arms and the man : a revised and expanded edition of the AK47 story**. Cobourg, Ont.: Collector Grade Publications, 2001.

FORENSIC ARCHITECTURE. Agency. **Forensic Architecture**, 2010. Disponível em: https://forensic-architecture.org/about/agency.

_____. The Battle of Ilovaisk. **Forensic Architecture**, 2019. Disponível em: https://ilovaisk.forensic-architecture.org/. Acesso em: nov. 2022.

FORENSIC Architecture: Towards an Investigative Aesthetics. **E-Flux**, 15 out. 2017. Disponível em: https://www.e-flux.com/announcements/93328/forensic-architecturetowards-an-investigative-aesthetics/. Acesso em: 2 dez. 2022.

FULLER, L. Caucasus Report: Putin Green Lights South Ossetian Units In Russian Army. **RadioFreeEurope/RadioLiberty**, 20 mar. 2017. Disponível em: https://www.rferl.org/a/russia-south-ossetia-army-incorportation/28379998.html. Acesso em: 2 dez. 2022.

GAVRILOV, Y. Okolo 80 Tysyach Voyennykh Poluchili Ekipirovku “Ratnik” V 2015 Godu. **Rossiyskaya Gazeta**, 9 jan. 2016. Disponível em: https://rg.ru/2016/01/09/ratnik-site.html. Acesso em: 2 dez. 2022.

GEOSPATIAL Intelligence. **BETTER**, 2020. Disponível em: https://www.ec-better.eu/pages/geospatial-intelligence. Acesso em: 1º dez. 2022.

GERASIMOV, V. Tsennost' Nauki V Predvidenii. **VPK**, [S.l.], 2013. Disponível em: https://archive.ph/gHt9q. Acesso em: 1º dez. 2022.

HASSAN, N. A.; HIJAZI, R. **Open Source Intelligence Methods and Tools.** Nova York: Apress Media LLC, 2018.

_____. A Unit of the 6th Tank Brigade Transferred to Rostov Oblast. **InformNapalm**, 7 jul. 2015. Disponível em: https://informnapalm.org/en/a-unit-of-the-6th-tank-brigade-transferred-to-rostov-oblast/. Acesso em: nov. 2022.

_____. [EN] Russian Presence. Incidents and Unit Numbers. **Google Docs**, 2016a. Disponível em: https://docs.google.com/spreadsheets/d/159jVqzSfz5gR-0YwsdnbeQMsNNEOwnhjJswkvqQNqm8/edit#gid=941406428. Acesso em: nov. 2022.

_____. Russian Leer-3 EW system revealed in Donbas. **InformNapalm**, 23 set. 2016b. Disponível em: https://informnapalm.org/en/russian-leer-3wf-donbas/. Acesso em: 2 dez. 2022.

_____.75 Russian military units that fight in Donbas [EN, UA, DE, RU subs]. **YouTube**, Disponível em: https://www.youtube.com/watch?v=xfaxifCx94o. Acesso em: ago. 2020.

_____. Identified: 5 Soldiers from the 15th MRB Who Tried to Hide Their Participation in the Aggression. **InformNapalm**, 28 nov. 2017. Disponível em: https://informnapalm.org/en/identified-5-soldiers-from-the-15th-mrb-who-tried-to-hide-their-participation-in-the-aggression/. Acesso em: 2 dez. 2022.

INTERNATIONAL AMMUNITION ASSOCIATION. Headstamp Codes. **IAA**, [s.d.]. Disponível em: https://www.cartridgecollectors.org/headstampcodes. Acesso em: nov. 2022

INTERNET WORLD STATS. World Internet Users Statistics and 2019 World Population Stats. **Internetworldstats.com**, 2022. Disponível em: https://www.internetworldstats.com/stats.htm. Acesso em: ago. 2022

JORDÁN, J. It is not a new Cold War: they are 'gray zone' conflicts. **Global Strategy.** Disponível em: https://global-strategy.org/it-is-not-a-new-cold-war-they-are-gray-zone-conflicts/. Acesso em: 12 jun. 2022.

KAPUSTA, P. **The Gray Zone.** Special Warfare, p. 18–25, dez. 2015. Disponível em: https://www.soc.mil/swcs/ProjectGray/Gray%20Zones%20-%20USSOCOM%20White%20Paper%209%20Sep%202015.pdf Acesso em: 20 abr. 2022.

KORRESPONDENT. Viys'kovi U stanovyshchi. Yak Zminylasya Sytuatsiya Na Donbasi. **Korrespondent** 28 ago. 2014. Disponível em: https://ua.korrespondent.net/ukraine/politics/3411523-viiskovi-u-stanovyschi-yak-zminylasia-sytuatsiia-na-donbasi. Acesso em: nov. 2022.

LUHN, A. Russia's tank biathlon world championship kicks off outside Moscow. **The Guardian**, 4 ago. 2014. Disponível em: https://www.theguardian.com/world/2014/aug/04/russia-tank-biathlon-world-championship-moscow. Acesso em: nov. 2022.

MEARSHEIMER, J. J. **The Tragedy of Great Power Politics**. New York: W.W. Norton & Company, 2001.

MILITARY REVIEW. Sevastopol: Russian Military Dress up in Digital Form. **Military Review**, 13 dez. 2010. Disponível em: https://en.topwar.ru/2685-sevastopol-rossijskix-voennyx-pereodevayut-v-cifrovuyu-formu.html. Acesso em: nov. 2022.

_____. T-72B3... What Is This beast? **Military Review**, 9 nov. 2013. Disponível em: https://en.topwar.ru/35631-t-72b3chto-eto-za-zver-chast-1.html.

_____. Innovation Day of South-Eastern Military District: EW RB-341B Complex “Leer-3”. **Military Review**, 16 out. 2015. Disponível em: https://en.topwar.ru/84386-den-innovaciy-yuvo-kompleks-reb-rb-341v-leer-3.html. Acesso em: nov. 2022.

MINISTERSTVO OBORONY. Soobshcheniye Upravleniya press-sluzhby I Informatsii Ministerstva Oborony Rossiyskoy Federatsii. **Ministerstvo Oborony Rossiyskoy Federatsii**, 5 mar. 2011. Disponível em: https://archive.is/313fH. Acesso em: nov. 2022.

_____. Yedinstvennaya V Rossii Motostrelkovaya Mirotvorcheskaya Brigada Otmechayet 10-letniy Yubiley. **Ministerstvo Oborony Rossiyskoy Federatsii**, 1 fev. 2015. Disponível em: https://function.mil.ru/news_page/country/more.htm?id=12006837. Acesso em: 10 nov. 2022

MITROFANOV, A. О боеприпасах, армейских пистолетах и пистолетах-пулемётах в ВС РФ. **Military Review**, 24 set. 2019. Disponível em: https://en.topwar.ru/162774-o-boepripasah-armejskih-pistoletah-i-pistoletah-pulemetah-v-vs-rf.html. Acesso em: nov. 2022.

NYE, J. S. **The Future of Power**. New York: Public Affairs, 2011.

OE DATA INTEGRATION NETWORK. Leer-3 Russian 6x6 Mobile Drone-Based Electronic Warfare (EW) System. **OE Data Integration Network**, 2021. Disponível em: https://odin.tradoc.army.mil/mediawiki/index.php?title=Leer-3_Russian_6x6_Mobile_Drone-Based_Electronic_Warfare_(EW)_System&printable=yes. Acesso em: nov. 2022.

_____. T-72B3 Russian Main Battle Tank (MBT). **OE Data Integration Network**, 2022. Disponível em: https://odin.tradoc.army.mil/WEG/Asset/T-72B3_Russian_Main_Battle_Tank_(MBT). Acesso em: nov. 2022.

ORYX. The Victory Day Parade That Everyone Forgot. **Oryx**, 30 nov. 2020. Disponível em: https://www.oryxspioenkop.com/2020/09/transnistria-shows-off-military.html. Acesso em: 2 dez. 2022.

PLOTNIKOV, N. Kak ya provel leto 2014. **VKontakte**. 2014. Disponível em: https://vk.com/video241882719_ 170716755. Acesso em: 23 nov 2022.
_____. Perfil. **VKontakte.** 2022. Disponível em: https://vk.com/nikolay1562. Acesso em: 20 nov. 2022.

PROMETHEUS Center; Informnapalm **Donbas in flames:** A Guide to the Warzone, Prometheus Center, 2017.

ROWAN MOORE. Forensic Architecture: the Detail behind the Devilry. **The Guardian**, 25 fev. 2018. Disponível em: https://www.theguardian.com/artanddesign/2018/feb/25/forensic-architects-eyal-weizman.

SADAT, M.; SINCLAIR, M. The not-so-secret value of sharing commercial geospatial and open-source information. **Brookings**, 31 mar. 2021. Disponível em: https://www.brookings.edu/blog/order-from-chaos/2021/03/31/the-not-so-secret-value-of-sharing-commercial-geospatial-and-open-source-information/.

SHULSKY, A. N.; SCHMITT, G. J. **Silent Warfare**. 3. ed. [S.l.]: Potomac Books Incorporated, 2002.

SMALL ARMS SURVEY. Weapons Identification: Small-calibre Ammunition. *In*: JENZEN-JONES, N. R.; SCHROEDER, M. (Org.). **An Introductory Guide to the Identification of Small Arms, Light Weapons, and Associated Ammunition**. [S.l.]: Small Arms Survey, 2018, p. 132–166.

SPUTNIK. Russia's Army to Get "Future Soldier" Gear in October: Defense Ministry. **Sputnik**, 2014. Disponível em: https://sputniknews.com/20140805/Russias-Army-to-Get-Future-Soldier-Gear-in-October--Defense-191731713.html. Acesso em: 2 dez. 2022.

STARLING, C. G.; IYER, A.; GIESLER, R. J. Today's Wars Are Fought in the "gray zone". **Atlantic Council**, 23 fev. 2022. Disponível em: https://www.atlanticcouncil.org/blogs/newatlanticist/todays-wars-are-fought-in-the-gray-zone-heres-everything-you-need-to-knowabout-it/

TOLER, A. How to Use and Interpret Data from Strava's Activity Map. **BellingCat**, 29 jan. 2018. Disponível em: https://www.bellingcat.com/resources/how-tos/2018/01/29/strava-interpretation-guide/. Acesso em: 15. ago. 2020

_____; AKSAI. Russia's 6th Tank Brigade: the Dead, the Captured, and the Destroyed Tanks (Pt. 1). **BellingCat**, 22 set. 2015a. Disponível em: https://www.bellingcat.com/news/uk-and-europe/2015/09/22/russias-6th-tank-brigade/. Acesso em: nov. 2022.

_____; _____. Russia's 6th Tank Brigade: the Dead, the Captured, and the Destroyed Tanks (Pt.2). **BellingCat**, 29 set. 2015b. Disponível em: https://www.bellingcat.com/news/uk-and-europe/2015/09/29/russias-6th-tank-brigade-pt-2/. Acesso em: 2 dez. 2022.

_____. **FM 2-0: Intelligence**. [S.l.]: US Army, 2010.

ÜNVER, A. **Digital Open Source Intelligence and International Security:** A Primer. Disponível em: https://www.jstor.org/stable/resrep21048. Acesso em: 17 mar. 2020.

WALKER, S. Russia Admits Its Soldiers Have Been Caught in Ukraine. **The Guardian**, 26 ago. 2014. Disponível em: https://www.theguardian.com/world/2014/aug/26/russia-admits-soldiers-in-ukraine. Acesso em: nov. 2022.