FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ
CURSO DE BACHARELADO EM RELAÇÕES INTERNACIONAIS

PETRUS DANIEL LEAL BELMONTE

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

Recife
(2022)

PETRUS DANIEL LEAL BELMONTE

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

Trabalho de conclusão de curso como exigência parcial para graduação no curso de Relações Internacionais, sob orientação do Prof. Dr. Antônio Henrique Lucena Silva

Recife
(2022)

Catalogação na fonte
Bibliotecário Ricardo Luiz Lopes CRB-4/2116

Belmonte, Petrus Daniel Leal.
B451o Osint e relações internacionais: o caso dos militares russos em Donbas entre 2014 e 2021 / Petrus Daniel Leal Belmonte. – Recife, 2022.
77 f. : il. Color.

Orientador: Prof. Dr. Antônio Henrique Lucena Silva.
Trabalho de Conclusão de Curso (Monografia – Relações Internacionais) – Faculdade Damas da Instrução Cristã, 2022.
Inclui bibliografia.

1. Estudos estratégicos. 2. Inteligência. 3. Fontes abertas. 4. OSINT. 5. Zonas cinzentas. 6. Invasão. 7. Forças ambíguas. 8. Rússia. 9. Ucrânia. 10. Donbas. I. Silva, Antônio Henrique Lucena. II. Faculdade Damas da Instrução Cristã. III. Título.

327 CDU (22. ed) FADIC (2022.2-030)

PETRUS DANIEL LEAL BELMONTE

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

Trabalho de conclusão de curso como exigência parcial para graduação no curso de Relações Internacionais, sob orientação do Prof. Dr. Antônio Henrique Lucena Silva

Aprovada em:____ de _____ de 2022.

BANCA EXAMINADORA

_____

Avaliador interno, Prof. Me. Bianor da Silva Teodósio Neto

_____

Avaliadora externa, Prof. Me. Maria Eduarda Buonafina Franco Dourado

_____

Orientador, Prof. Dr. Antônio Henrique Lucena Silva

Recife
(2022)

DEDICATÓRIA

Dedico este trabalho especialmente a meu pai, que me ensinou a virtude da inteligência, no trabalho e na vida pessoal. A todos os amigos; “os casas”, e colegas analistas independentes empenhados na arte da investigação.

AGRADECIMENTOS

Agradeço primeiramente a Deus, o Senhor dos Exércitos, pelo dom da vida. Agradeço à minha família, pela paciência, pelo apoio, e pelo imensurável amor. Agradeço ao meu orientador, Antônio Lucena, pela dedicação e atenção, pela sua disposição infinita em direcionar e observar o potencial acadêmico e racional dos seus alunos. A todos os meus amigos de infância, que me acompanharam e incentivaram durante todo esse caminho, nos tempos difíceis e nos tempos de alegria.

EPÍGRAFE

“We live in the world that your propaganda made
But where you think you are strong you are weak
Your lies tell us the truth we will use against you
Your secrecy shows us where we will strike
Your weapons reveal your fear for all to see
From Cairo to Quito a new world is forming
The power of people armed with the truth.”

Calle 13 & Julian Assange – Multi_viral

RESUMO

Focado em Estudos Estratégicos, o presente trabalho aborda as oportunidades que a Inteligência em Fontes Abertas (OSINT) apresentam nas relações internacionais. Busca demonstrar como o OSINT pode ser utilizado contra as Zonas Cinzentas; a área de enfrentamento entre guerra e paz, utilizada pelos grandes poderes para competir entre si. Neste sentido, o uso de forças ambíguas na invasão russa no leste ucraniano de 2014 a 2021, é utilizado como exemplo de táticas nas Zonas Cinzentas. Investigações OSINT, realizadas para evidenciar a presença russa na Ucrânia, são então utilizadas para demonstrar como essa doutrina auxilia no processo de tomada de decisões contra essas Zonas, na esfera política, legal e estratégica. Para isso, foi imperativa a construção de um detalhado arcabouço teórico. Primeiro, foram apresentados o significado Inteligência nas Relações Internacionais, as demais doutrinas na produção de inteligência, e o conceito de OSINT; suas vantagens, desvantagens, versões e versatilidade. Depois, foi apresentado um rápido panorama do plano internacional pós-Guerra Fria. Conciliando neorrealismo e neoliberalismo, foi demonstrado como este cenário propiciou a ascensão das Zonas Cinzentas, bem como sua definição e suas táticas mais comuns. Com este arcabouço teórico, o último capítulo se debruça sobre o contexto ucraniano contemporâneo; sua localização, os antecedentes e as táticas da invasão russa de 2014, para então apresentar detalhadamente algumas investigações OSINT que foram utilizadas para expor a presença russa, e suas repercussões internacionais em diversos setores.

Palavras-Chave: Estudos Estratégicos; inteligência; fontes abertas; OSINT; Zonas Cinzentas; invasão; forças ambíguas; Rússia; Ucrânia; Donbas.

ABSTRACT

Focused on Strategic Studies, this paper examines the opportunities that Open Source Intelligence (OSINT) presents in international relations. It aims to demonstrate how OSINT can be used against Gray Zones; the area of confrontation between war and peace, used by great powers to compete with each other. In this regard, the use of ambiguous forces in the Russian invasion of eastern Ukraine from 2014 to 2021, serves as an example of tactics in the Gray Zones. OSINT investigations conducted to highlight the Russian presence, are then used to demonstrate how this doctrine assists in the decision-making process against these Zones, in the political, legal, and strategic spheres. To this end, the construction of a theoretical framework was imperative. First, the meaning of Intelligence in International Relations, the other doctrines in intelligence production, and the concept of OSINT; its advantages, disadvantages, versions, and versatility were presented. Then, a brief overview of the post-Cold War international plane was presented. Reconciling neo-realism and neo-liberalism, it was shown how this scenario favored the rise of the Gray Zones, as well as their definition and most common tactics. With this theoretical framework, the last chapter delves into the contemporary Ukrainian context; its location, the background and tactics of the 2014 Russian invasion, to then present in detail some OSINT investigations that were used to expose the Russian presence, and its international repercussions in various sectors.

Keywords: Strategic Studies; open source; intelligence; OSINT; Gray Zones; invasion, ambiguous forces; Russia; Ukraine; Donbas.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

CIA	Central Intelligence Agency
COMINT	Communications Intelligence
CSIS	Center for Strategic and International Studies
DDoS	Distributed Denial of Service
DPR	Donetsk Peoples Republic
ECHR	European Court of Human Rights
EHRAC	European Human Rights Advocacy Centre
ELINT	Electronics Intelligence
GEOINT	Geointelligence
GSM	Global System for Mobile communication
HUMINT	Human Intelligence
IMINT	Image Intelligence
OSCE	Organization for Security and Co-operation in Europe
OSINT	Open Source Intelligence
LPR	Lugansk Peoples Republic
NATO PA	North Atlantic Treaty Organization Parliamentary Assembly
MI6	Military Intelligence, Section 6
SMM	Special Monitoring Mission
TECHINT	Technical Intelligence
TRADOC	Training and Doctrine Command
USASOC	U.S. Army Special Operations Command
SBU	Sluzhba Bezpeky Ukrayiny

SUMÁRIO

1. INTRODUÇÃO

O presente trabalho explora, através de exemplos práticos, as amplas oportunidades de estudo e aplicação que a doutrina de Inteligência digital em fontes abertas oferece para as Relações Internacionais, especialmente na área de Estudos Estratégicos. Para tal, o trabalho também demonstrará como a ascensão da Internet propiciou estas oportunidades, e o contexto internacional contemporâneo, caracterizado por conflitos indiretos.

Ocupando o cargo de maior revolução tecnológica do final do século XX, ao longo do seu desenvolvimento, a internet trouxe à humanidade um novo palco para interações humanas; o mundo digital. Segundo a Intert World Status (2022) 5 bilhões de pessoas interagem neste mundo digital, sem as fronteiras informacionais comuns a outros meios de comunicação; o espaço, tempo, a linguagem. Essas barreiras foram implacavelmente destruídas ou mitigadas, à medida que ele se espalhava por todos os continentes. Embora o resultado atual desta revolução esteja mais claro na economia e na cultura, com transações financeiras e mensagens trocadas de forma instantânea, a política e, consequentemente, as relações internacionais, foram profundamente modificadas pela internet.

O início do século XXI demonstra o impacto da Internet e do mundo digital na Segurança Internacional. Não apenas novas ameaças, mas novas oportunidades de revisar os métodos utilizados pelos setores de inteligência dos Estados. Enquanto alguns métodos tiveram sua aplicação reduzida, outros foram impulsionados pela capacidade inovadora da internet. Destaca-se, neste caso, a Inteligência em Fontes Abertas (OSINT). Trata-se do processo investigativo cujo método é a coleta e análise de dados acessíveis em fontes publicamente disponíveis. Os dados são processados, instrumentalizados, em um contexto de inteligência e tomada de decisão em diversas áreas. Embora governos possam utilizar OSINT para diversas outras áreas, como economia, indústria, etc, aplicações na área de Segurança Internacional são cada vez mais comuns (CSIS, 2021).

Junto à ascensão da internet e do OSINT, outra inovação marca o início do século XXI nas RI; a Zona Cinzenta, uma nova forma de enfrentamento entre Estados, principalmente grandes potências, que utilizam ferramentas dispostas no limiar da paz e da guerra direta, para combater adversários e conquistar objetivos a longo prazo. O conflito no leste da Ucrânia, iniciado pela invasão russa em Abril de 2014, é um dos principais exemplos desta nova forma de enfrentamento. Antes de 2022, a Rússia negou qualquer envolvimento militar na região, mas vários atores internacionais, estatais e não-estatais, aplicaram técnicas

OSINT para identificar e expor várias unidades e equipamentos russos presentes no leste ucraniano. Técnicas OSINT, então, podem ser apontadas como uma das principais medidas contra as Zonas Cinzentas.

O presente trabalho parte da conciliação de conceitos de teorias neorrealistas e neoliberais das Relações Internacionais. Apresentam-se as interpretações neorrealistas sobre Poder, Anarquia Internacional e Hegemonia, de John Mearsheimer, bem como a interpretação atualizada de Robert Jervis sobre o Dilema de Segurança. A conciliação com a teoria neoliberal vem da contribuição de Joseph Nye sobre atores não-estatais e as camadas onde o Poder está distribuído, no plano, e especialmente as formas como atores estatais e não estatais utilizam-no, elencando principalmente o conceito de Smart Power. Por fim, estes conceitos serão, relacionados ao OSINT e às Zonas Cinzentas, e como ambas estão galgando mais espaço no campo de inteligência e segurança internacional. Como consequência, o trabalho pretende demonstrar a importância do aprendizado de tais técnicas para os diversos atores internacionais, num mundo cada vez mais digital e transparente, mas dominado pelo enfrentamento entre Estados nas Zonas Cinzentas.

Para alcançar tais objetivos, serão apresentados três capítulos. No primeiro capítulo, será definida a noção de Inteligência nas Relações Internacionais, as doutrinas mais comuns, suas vantagens e desvantagens e, por último, o que é OSINT e como pode responder aos desafios apresentados pelas doutrinas tradicionais. No segundo capítulo, será abordado o plano internacional pós-Guerra Fria, como o Poder foi redistribuído, e como sua noção foi profundamente modificada, após a ascensão de novos atores. Neste panorama, serão apresentadas as Zonas Cinzentas, suas técnicas, exemplos, e como desafiou formas convencionais de inteligência e respostas do governo. No terceiro capítulo, será apresentado um pano de fundo da Ucrânia; sua formação histórica e divisões internas, e como a Rússia utilizou as Zonas Cinzentas no conflito em 2014. Com este contexto, será exposto como a OSINT foi utilizada para responder às Zonas Cinzentas, suas repercussões internacionais e conquistas relacionadas ao conflito.

Dado os objetos e objetivos do trabalho, é observável que sua metodologia é qualitativa, descritiva. A sua abordagem é majoritariamente, indutiva; primeiro descreve os objetos mais específicos e depois os aplica, exemplifica, avalia em um cenário mais amplo, já no campo da realidade. No caso das investigações, apresentadas e datalhadas no terceiro capítulo, todas utilizaram métodos qualitativos.

2. CAPÍTULO I: DOUTRINAS DE INTELIGÊNCIA

Inteligência é um tema universal, e seu uso por diversos atores, para propósitos variados, cria definições distintas, específicas para cada aplicação. Além disso, para o público, informação e inteligência têm o mesmo significado. Em consequência, torna-se necessário não apenas definir Inteligência no campo internacional, mas diferenciá-la do significado de informação. Numa definição geral, aplicável a todos os propósitos, Shulsky e Schmitt (2002) entendem que inteligência é fruto da coleção de informações, sendo então avaliadas, analisadas e interpretadas para necessidades específicas de um consumidor final. Informação, então, é qualquer dado que pode ser conhecido, independente da forma que é descoberta, coletada.

Informações, no entanto, são inúteis se não forem analisadas e avaliadas. Além disso, elas podem servir vários propósitos, que lhes conferem valores diferentes, a depender das necessidades de quem as demandam. Por isso, torna-se necessário o processo de interpretação; para demonstrar como essas informações impactam os objetivos e necessidades de quem a consome. Em outras palavras, inteligência é o processo que coleta e traduz as informações para um consumidor, que deseja aplicá-las para alcançar um propósito definido.

No campo internacional, o conhecido Dilema de Segurança não gera apenas hostilidades armadas, mas ações de espionagem em uma miríade de temas. A inteligência só existe porque governos tentam esconder suas próprias informações, enquanto tentam descobrir as de seus pares (LOWENTHAL, 2011). Ao desconhecimento geral, causado por essa atitude, dá-se o nome de *Fog of War*, isto é; a incerteza sobre a distribuição física e econômica de capacidades, equipamentos e atividades que potenciais adversários exercem em determinado espaço. Assim, nas Relações Internacionais, inteligência significa a coleta e interpretação de informações que os governos julgam necessárias para a formulação e implementação de políticas, seja para promover seus interesses, nacionais e internacionais, ou para lidar com ameaças de [potenciais] adversários, mitigando a incerteza.

Vale ressaltar, no entanto, que o termo “adversário” não se refere necessariamente a um inimigo militar. Um governo aliado, amigável, pode ser adversário de outro no contexto de negociação econômica; um lado estará sempre tentando alavancar os seus ganhos em relação ao outro (SHULSKY & SCHIMTT, 2002), e exatamente por isso implementa técnicas de inteligência, descobrindo fragilidades que podem ser exploradas, ou desvantagens que devem ser evitadas.

Qualquer que seja seu objetivo, as categorias de produto de inteligência se organizam seguindo quatro formas: coleção, análise, ação encoberta e contrainteligência. Prezando pela objetividade do trabalho, serão apresentadas apenas as categorias de coleção.

Coleção é o ajuntamento de dados brutos, por vários métodos, que variam de espionagem, meios técnicos, até fontes abertas. A esses meios de coleta, dá-se o nome de Doutrinas de Inteligência, e embora haja grande discordância entre analistas e acadêmicos, em como as elas são organizadas, as formas são precisamente as mesmas. Schuslky e Schimtt (2002) as organizam em três categorias: inteligência humana (HUMINT), inteligência técnica TECHINT), e ação aberta (OSINT). Serão apresentadas suas características, utilidades, vantagens e desvantagens, respectivamente.

2.1. HUMINT: Espiões e informantes

Trata-se da mais conhecida forma de inteligência, onde habita a imagem popular do espião. Sua definição pode ser encontrada no Comando de Treinamento e Doutrina do Exército dos Estados Unidos (TRADOC). O TRADOC (2004, 2010), define HUMINT como a coleta de informações de pessoas, por um coletor de inteligência humana treinado. A inteligência angariada pode ser aplicada para alcançar objetivos ou confundir e impedir adversários.

As fontes do HUMINT são pessoas de todas as categorias, intituladas Fontes Humanas. Habitantes locais, forças aliadas, membros de governo aliado ou adversário, refugiados, desabrigados, prisioneiros de guerra e outros, todas podem possuir informações de primeira ou segunda mão, então são consideradas fontes válidas. A depender do nível de cooperação das fontes, de totalmente cooperativas a totalmente antagonísticas, diferentes estratégias são aplicadas para a extração de informações; de simples entrevistas até interrogatórios.

Outra forma de HUMINT são as operações mais invasivas e hostis, conhecidas como HUMINT clandestino. Apesar do nome, continuam sendo reguladas pelos respectivos países, com regras de engajamento e limites legais. As operações incluem infiltração em território ou organização inimiga, instalação de escutas e outros aparelhos de vigilância, campanas, roubo de documentos e sabotagem. Embora sejam controversas e caminhem no limiar da ilegalidade internacional, ainda são consideradas formas válidas de coleção de informações.

O TRADOC (2004, 2010) avalia que o HUMINT serve para complementar produtos de inteligência produzidos por outras doutrinas, negando ou confirmando as informações

coletadas anteriormente. Essa forma de inteligência, como qualquer outra, sofre com inúmeras limitações. Grande parte delas é fruto da própria natureza dessas operações (SHULSKY & SCHIMTT, 2002).

Em primeiro lugar, operações de HUMINT precisam de muito tempo para se desenvolver. É esperado que o coletor opere com o mínimo de equipamentos, em todos os tipos de ambientes. Logo, o sucesso da operação depende inteiramente das capacidades interpessoais subjetivas do coletor, em vez de habilidades técnicas. Além disso, enquanto um coletor de HUMINT pode dispor de um intérprete em algumas situações, a ausência de habilidades em outras línguas pode atrasar e prejudicar ainda mais o processo de entrevista ou interrogatório, ou operações de maior segredo.

Outros problemas surgem da natureza das fontes e próprios agentes. Há a possibilidade de agentes desertarem ou servirem de agentes duplos. De fato, como já exposto, a polêmica internacional da deserção do espião soviético Igor Gouzenko, três dias após o fim da Segunda Guerra, quando trabalhava disfarçado de diplomata no Canadá, é considerada por estudiosos da inteligência como Knight (2008) como o início oficial da Guerra Fria. Fontes, por sua vez, podem fabricar uma informação, ou fazê-la parecer importante, por qualquer motivo. Shulsky e Schmitt (2002), por exemplo, mencionam os casos dos “Moinhos de Papel”; termo da guerra fria criado para se referir ao processo de falsificação, semelhante à grilagem, que imigrantes e refugiados de governos soviéticos usavam para subsistir. Os documentos eram vendidos com informações falsas, sob a afirmativa de que vinham de conhecidos que ganharam cargos de confiança nos governos recém-formados.

Por último, HUMINT é uma atividade arriscada, em geral. Aid e Wiebes (2001) expõem que a CIA, MI6 e outras agências do bloco capitalista perderam mais de 300 agentes em seis anos (1949 - 1955), em operações de infiltração na Rússia Soviética. Centenas de outros foram perdidos tentando estabelecer redes de informantes no Leste Europeu durante toda a década de 50. No final da Guerra Fria, apenas entre 1984 e 1985, dezenas de redes de espiões do bloco soviético foram presos em território americano, muitos deles agentes duplos do próprio governo (WISE, 2015). Nesse sentido, a TECHINT é integrada ao processo de inteligência para mitigar estes riscos.

2.2. TECHINT: Utilizando tecnologias

Essa doutrina abriga o grupo de técnicas que utiliza de equipamentos e tecnologia, em vez de exclusivamente agentes humanos. Desta forma, seus limites são apenas as leis da física e o desenvolvimento tecnológico (SHULSKY & SCHIMTT, 2002). Em sua maioria, as técnicas envolvem a coleta, análise e interpretação de ondas eletromagnéticas e imagens de longa distância. As principais técnicas são: inteligência de Sinais (SIGINT), Inteligência Geoespacial ou Geointeligência (GEOINT) e Inteligência de Imagem (IMINT), que podem interagir com e complementar, umas às outras.

2.2.1 SIGINT: Informações nos sinais

Refere-se à técnica de produção inteligência a partir da interceptação de ondas eletromagnéticas, geralmente chamadas pelo nome de "sinais" (TRADOC, 2004, 2010.). Há dois subgrupos de SIGINT: COMINT (Inteligência de Comunicação) e ELINT (Inteligência Eletrônica)

COMINT é a interceptação de sinais de comunicação estrangeira, como mensagens de rádio, conversas telefônicas, código morse e outras formas de comunicação entre humanos. ELINT é a técnica que intercepta radiação eletromagnética e de telemetria que emanam de aparelhos eletrônicos, como aeronaves, radares, sistemas antiaéreos, sensores instalados em veículos terrestres, e outros equipamentos.

Operações de Inteligência de Sinais coletam informações de alvos que estão há milhares de quilômetros de distância, evitando a necessidade de criação de estruturas próximas dos alvos. Desta forma, essa doutrina raramente envolve risco físico ou político. Aid e Wiebes (2001), demonstram que, durante toda a Guerra Fria, cerca de 140 operadores da NSA foram mortos em cumprimento do dever; 60 no Vietnã. Um contraste enorme se comparado à quantidade de agentes de HUMINT mortos ou capturados. SIGINT fornece informações importantes de inteligência, e são geralmente utilizadas para direcionar outras técnicas a possíveis alvos de interesse. Pode ser aplicado, por exemplo, para sugerir a presença de estruturas e equipamentos em uma determinada área, para qual a GEOINT será utilizada, para confirmar ou negar essa atividade. Historicamente, a interceptação e quebra de mensagens criptografadas, através do COMINT, foi atividade essencial para a vitória aliada na Segunda Guerra (AID & WIEBES, 2001).

No entanto, há desafios em cada um dos subgrupos do SIGINT. Em primeiro lugar, dependendo das capacidades tecnológicas do governo investigado, as comunicações entre

alvos humanos podem ser realizadas numa grade estrutura de criptografias. Embora não seja impossível quebrar estas criptografias, sistemas de aviso e contrainteligência podem alertar a quebra de segurança e introduzir novos sistemas de criptografia, ou novos canais de comunicação. Além disso, com avanços tecnológicos das últimas décadas, como a ascensão da internet e do mundo digital, serviços de comunicação com criptografia de ponta a ponta tornaram-se mais acessíveis para atores não-estatais, dificultando ainda mais o uso de COMINT em alvos de todos os níveis. Já no ELINT, o uso de Contramedidas Eletrônicas, como *jammers* e emissores de sinais falsos, podem limitar e confundir os equipamentos.

2.2.2. GEOINT: Informações na Terra

Essa doutrina é definida pela coleta e análise de Imagens e Informações Geoespaciais, usadas para descrever e interpretar visualmente características físicas, e atividades que acontecem na Terra. Tais informações vão desde complexos registros de radiação ultravioleta, sensores de emissão de calor instalados em satélites, até informações derivadas de fotos aéreas, pelas mais diversas aeronaves. (TRADOC, 2004, 2010).

Imagens não são necessariamente fotos, mas representações ou semelhanças, como imagens de calor, relevo e outras representações gráficas que facilitem a visualização do terreno, sempre incluindo a posição exata ou aproximada do que se deseja representar. Informações Geoespaciais são os dados que identificam a localização e as características, naturais ou construídas, de um espaço específico da Terra. São informações sobre a topografia do lugar; elevação do terreno, vegetação, construções, estradas e outros detalhes considerados importantes. Essas duas informações são então mescladas num produto final, que é a GEOINT, como demonstra a figura abaixo.

Figura 1 – Organograma da GEOINT

Colagem do autor, baseada em TRADOC (2011)

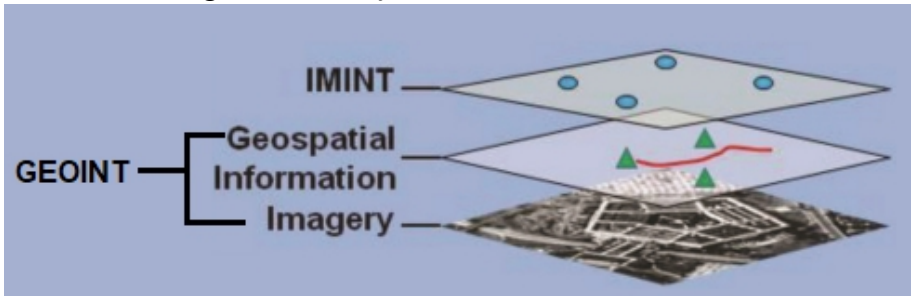
Durante a Guerra do Golfo, a Geointeligência foi primordial no desenvolvimento de sistemas de mísseis guiados, garantindo ataques devastadores, mas precisos. Recentemente, a GEOINT foi indispensável no descobrimento da existência de campos de reeducação destinados a minorias étnicas na China (SADAT E SINCLAIR, 2021). Diversos outros abusos de direitos humanos e crimes de guerra puderam ser avaliados através da Geointeligência, tornando-a importante, também, em diversas outras áreas da política internacional.

Uma das maiores limitações atuais da GEOINT em governos vem, paradoxalmente, da rápida evolução na tecnologia de dados, contrastada com a lenta evolução na estrutura de armazenamento e gerenciamento. Bancos de dados atuais, e a maneira que são gerenciados, não acompanham o volume maior e mais frequentes de dados, vindos de sensores novos instalados nos satélites, como demonstra o estudo do Conselho Nacional de Pesquisa dos EUA (2006), e da empresa de big data e geografia Better (2020). Como dito, informações são inúteis se não forem analisadas, avaliadas e interpretadas, não importa sua quantidade. Ausência de filtro de informações, levando a uma sobrecarga delas, pode ser tão prejudicial quanto a falta delas.

2.2.3 IMINT: Informações em imagens

IMINT é a produção de inteligência a partir da interpretação e análise de imagens e materiais relacionados (TRADOC, 2004). Análise de imagens é a prática de converter informações extraídas de imagens em inteligência sobre atividades, objetos, instalações e/ou áreas de interesse. De certa forma, IMINT é bastante ligado a GEOINT, pois interpreta o valor estratégico que construções, objetos e atividades, humanas e naturais, representam para a investigação. Militarmente, considerando que construções podem ser utilizadas improvisadamente como cativeiros, quarteis generais ou armazéns, o IMINT surge como uma interpretação direta e humana sobre a utilização de estruturas e equipamentos. A figura abaixo ilustra a estruturação do IMINT e sua relação com a GEOINT.

Figura 2 – Relação entre GEOINT e IMINT



Colagem do autor, baseada em TRADOC (2010)

Desta forma, é possível observar a OSINT como uma camada acima da IMINT. No entanto, embora seja uma das principais formas de complementar a inteligência gerada pela GEOINT, sua utilidade não se refere apenas a imagens espaciais. Num contexto econômico, espionagem industrial pode ser realizada com fotografias de dentro de uma fábrica, de equipamentos e maquinário, ou outros objetos de interesse. Num contexto militar, fotos obtidas de coletores de HUMINT podem ser analisadas, e informações pertinentes angariadas e interpretadas a partir delas.

2.2.4. Limitações

Como observado, ainda que a TECHINT ofereça diversas vantagens na produção de inteligência, investir nela implica em uma custosa estrutura. A necessidade da produção e compra de tecnologias, a construção de prédios, produção de equipamentos com as tecnologias angariadas e treinamento de engenheiros para manutenção, são algumas das exigências básicas, que permeiam todas as formas de TECHINT.

A aquisição de grandes estruturas para TECHINT também implica novas vulnerabilidades, principalmente a vazamento de dados e ciberataques, gerando novos custos

para prevenir e diminuir os danos relacionados. Por outro lado, a dependência de estruturas fornecidas por aliados, na maioria das vezes grandes potências — que futuramente podem se tornar adversárias, limita os governos na procura pelos próprios objetivos, subordinando-os ainda mais às potências regionais. O cenário piora se analisado do ponto de vista de atores não-estatais, como ONGs, que não têm sequer território para implementação dessa forma de inteligência, e, financeiramente dispõem de frações em relação aos recursos financeiros dos governos. Além disso, suas relações com os Estados geralmente são, no mínimo, instáveis. Nesta conjuntura, o OSINT surge como saída viável para vários governos e atores que buscam elevar suas capacidades de tomada de decisão.

2.3. OSINT: Informações públicas

Fontes abertas possuem muitas das informações necessárias para entender os fatores, naturais e humanos, dos ambientes nos quais operações de inteligência podem ser realizadas. Assim, OSINT se refere justamente à exploração dessa capacidade de informação nas fontes abertas, através de todas as categorias de dados que estão publicamente disponíveis. Embora historicamente as fontes abertas se refiram a documentos físicos e mídias de massa, o mundo digital impactou essa doutrina de inteligência de tamanha forma, que atualmente é possível dividi-la em duas categorias; clássica e digital, tornando necessário diferenciá-las.

O OSINT clássico pode ser facilmente observado em antigos manuais de inteligência dos EUA, como o Manual de Campo 2–29, do TRADOC (2004), e o Manual de OSINT da OTAN (2002). Nestas primeiras décadas do Século XXI, a maioria das fontes consideradas se referiam à mídia tradicional de massa, como rádio, jornais impressos, televisão, revistas e diários do governo. De fato, as vantagens destas informações públicas já eram evidentes.

Em primeiro lugar, oferecem menos risco político e legal: o uso de informações publicamente disponíveis para coletar informações não apresenta riscos em comparação à TECHINT, especialmente se o alvo estiver localizado em um país militarmente hostil (HASSAN & RIJAZI, 2018). Como já exposto, o custo muito é menor: coletar OSINT geralmente é mais barato em comparação com as doutrinas da TECHINT. Pequenas organizações, com orçamentos de inteligência limitados podem explorar fontes OSINT com custos mínimos, utilizando apenas os materiais mencionados.

No entanto, o OSINT clássico se deparava com vários desafios. Seus métodos de coleta se limitavam à pura e simples absorção das informações, sem a capacidade de

implementar técnicas de análise e ligação entre as fontes de informação. Analisar sua legitimidade dependia quase completamente de horas a fio em longas pesquisas documentais, alongando desnecessariamente as operações por meses (TRADOC, 2004, 2010)

Já o OSINT digital pode ser observado na metade final da década de 2000 e 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:

> "Inteligência de código aberto (OSINT) é a inteligência produzida a partir de informações publicamente disponíveis e coletada, explorada e disseminada em tempo hábil para um público apropriado com o objetivo de atender a um requisito específico de inteligência. Com a Revolução da Informação, a quantidade, importância e acessibilidade da informação de código aberto se expandiu significativamente, mas a comunidade de inteligência não expandiu seus esforços de exploração e sistemas para produzir inteligência de código aberto. A produção de inteligência de código aberto é uma valiosa disciplina de inteligência que deve ser integrada às tarefas, coleta, processamento, exploração e disseminação de inteligência para garantir que os formuladores de políticas dos Estados Unidos sejam total e completamente informados" (109th US CONGRESS, 2006, tradução nossa[1])

Neste sentido, suas técnicas e métodos não se referem mais apenas à simples absorção de informações, mas a diversas formas de comprová-las, verificar seus impactos e quais caminhos elas trilharam, localizando tanto o primeiro quanto o último a publicá-la, em um curto espaço de tempo. Embora livros, enciclopédias e documentos públicos continuem sendo utilizados, é no mundo digital que a maioria das oportunidades de operações acontecem. Não apenas blogues, redes sociais e arquivos digitais, mas os seus metadados, webcams e câmeras wi-fi de rua, desprotegidas, endereço IP e falhas de segurança apontadas publicamente podem ser consideradas fontes abertas.

A história do HUMINT demonstra que, embora livros, revistas e jornais mencionem grandes eventos moldados por grandes atores, informações importantes podem estar nas mãos de meros subalternos. A diferença reside no fato de que, enquanto o coletor de HUMINT precisa entrar em contato direto com o possível informante, ou espioná-lo por escutas, arriscando ser capturado e elevando tensões, o coletor de OSINT pode verificar suas

1 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

informações em redes sociais.

Pessoas têm mais chances de relevar informações preciosas de forma espontânea, quando não têm consciência de estarem sendo vigiadas, ou se encontram em zonas de conforto. Redes sociais, de todas as categorias, são a principal zona de conforto no mundo digital, e são cuidadosamente desenhadas para incentivar a exposição exagerada e impensada de detalhes da vida e do trabalho. Nesse sentido, a capacidade de coleta é ainda maior.

Toler (2018), por exemplo, demonstrou como o Strava, um aplicativo social de rastreamento de atividades físicas, que funciona em *smartphones* e *smartwatches*, havia exposto dezenas de quartéis generais e bases operacionais na África e na Ásia. No aplicativo, o usuário pode observar e compartilhar informações sobre o caminho, o tempo e a frequência em que realiza os exercícios físicos. Para isso, no entanto, é necessário compartilhar os dados de GPS e outras formas de localização com o servidor do aplicativo, junto a outros milhões de usuários.

Como parte do seu esforço publicitário, em 2017, o Strava lançou um mapa interativo de calor, mostrando estatísticas para mais de 700 milhões de usuários, que contava com 5 Terabytes de dados. Entre usuários todos os usuários, estavam militares, desde soldados a oficiais em serviço, trabalhando em bases americanas no exterior. Suas atividades também apareceram no mapa interativo de calor, como demonstra a imagem abaixo.

Figura 3 – Base militar americana em Helmand, Afeganistão

fonte: The Guardian (2018)

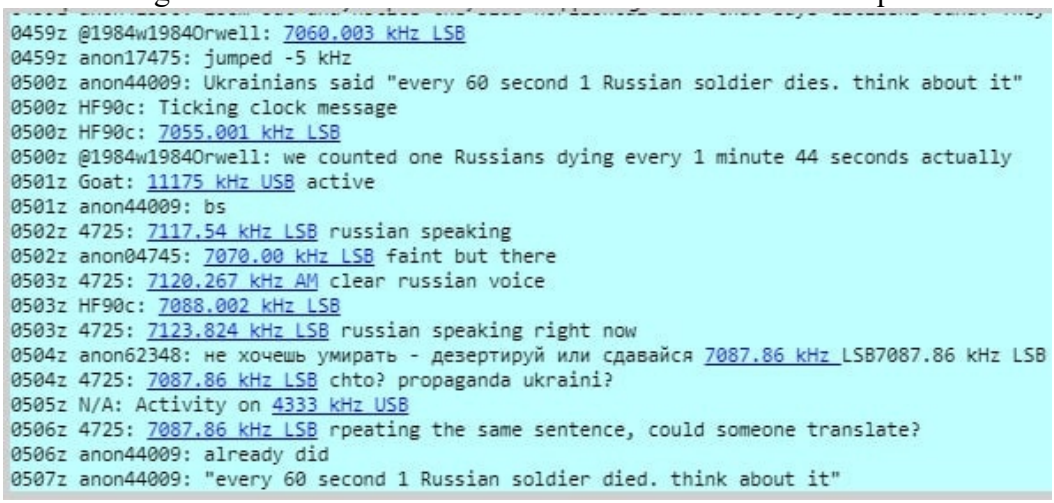
Embora as bases sejam normalmente visíveis por satélite, a trilha de calor, que expõe por onde os usuários percorrem, revela detalhes de dentro das bases, além de potenciais falhas na segurança delas; por onde andam as patrulhas, e quais lugares ficam desprotegidos em tempos específicos (TOLER, 2018).

O caso também demonstra outra das grandes vantagens do OSINT digital; a implementação de outras doutrinas de inteligência através da terceirização de serviços. IMINT e GEOINT podem ser realizados através de dados fornecidos por ferramentas e serviços sob demanda, gratuitos ou não. Segundo a Grand View Research (2020), em 2019 o mercado de imagens de satélite, liderado por empresas privadas como a Maxar, atingiu o valor de US$ 5.3 bilhões. Com um mercado crescente, os preços abaixam e permitem que qualquer indivíduo ou organização possa adquirir imagens. O satélite Geoeye-1, vende imagens e informações geográficas que variam de 17 a 25 dólares por quilômetro quadrado capturado (APOLLO MAPPING, 2022), dependendo principalmente de quão recente é a imagem. Versões gratuitas, mas com imagens de qualidade menor, e mais antigas, também estão disponíveis. Além da mais óbvia alternativa, com Google Earth e Yandex Maps, imagens vindas diretamente dos satélites americanos Sentinel-1 e 2, contando com versões arquivadas, 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. Soldados russos, após invadir abertamente a Ucrânia em Fevereiro 2022, precisaram recorrer a rádios de ondas curtas, após a queda de sinal GSM na região. As frequências foram interceptadas por ferramentas on-line, transcritas e documentadas, como mostram Bandouil e Hall (2022). Ativistas também bombardearam-nas com interferências e propagandas pró-Ucrânia. A imagem abaixo ilustra a conversação entre de radioamadores no site de WebSDR da Universidade de Twente, Holanda.

Figura 4 – Radioamadores e ativistas conversam sobre frequência russa



Fonte: captura de tela do autor (2022)

Limitações e desafios também atingem o OSINT. Sobrecarga de informações, principalmente sem qualidade, ou investigações que estagnam por ausência de outras pistas, podem prejudicar o andamento da inteligência. Conhecer ciberespaço e sua cultura; fóruns, sites, grupos e salas de conversa que possíveis alvos utilizam, e seus comportamentos, é primordial e requer imersão. Além disso, não há um conjunto bem definido de métodos OSINT, deixando o coletor à mercê da sua própria criatividade. No entanto, tais problemas diminuem à medida que o coletor sobe a curva de aprendizado e consome as diversas matérias e estudos de caso.

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, descentralizados e auto-organizados, mas que interagem localmente. Governos podem explorar esta capacidade e apoio destas comunidades, não só aumentando o escopo da sua produção de inteligência, mas exercendo Soft Power nestes grupos. Grande parte das investigações que serão apresentadas nos capítulos seguintes foram, inclusive, produzidas por grupos voluntários de inteligência.

Para compreender a importância desta doutrina, é necessário evidenciar os desafios que o mundo pós-guerra fria impôs aos setores de segurança internacional, dada a nova forma que o poder passou a ser distribuído, e as novas formas que os atores estatais encontraram, para competir com seus adversários. Este é o objetivo do próximo capítulo, que abordará as Zonas Cinzentas.

3. CAPÍTULO II: CONFLITO NAS ZONAS CINZENTAS

Apresentadas a natureza, necessidade e atualidade da produção de Inteligência nas relações internacionais, torna-se necessário entender em qual contexto internacional ela atualmente se desenvolve e funciona. Para isso, será necessário compreender a forma como o Poder é distribuído no cenário internacional, e como essa distribuição influencia a competição entre as grandes potências, gerando as chamadas Zonas Cinzentas. Aqui, é importante compreender o Poder não só como a capacidade de convencimento e ação através de diversas ferramentas, ou como o controle sobre resultados de eventos a nível internacional, mas como um objetivo final dos Estados.

3.1. Poder pós-Guerra Fria

Como demonstrado por Mearsheimer (2001), embora a sobrevivência seja preocupação dos Estados a curto prazo, todos os estados são revisionistas, buscando alterar a balança de poder no cenário internacional a seu favor. Desta forma, uma vez satisfeitas tais necessidades primárias de sobrevivência, objetivos secundários são perseguidos, como a busca pela hegemonia total. Esse controle global, no entanto, é virtualmente impossível de ser alcançado, devido a limitações de inúmeras naturezas; militares, econômicas, políticas e geográficas.

Esse contexto condena o plano internacional a uma competição perpétua pela mudança “final” na balança de poder, em busca da hegemonia global, que, por via de regra, sempre se limitará a hegemonias regionais. Desta forma, mesmo quando grandes poderes alcançam poderio militar e político superior na região, eles aglutinando poder, dado que nunca alcançarão, ou terão noção de qual é a “quantia apropriada” dele. (MEARSHEIMER, 2001, p. 45-55)

Tal visão permaneceu imaculada até poucos anos após o colapso da União Soviética. Neste período, para muitos teóricos, a conclusão havia chegado; aquela era a confirmação da hegemonia ideológica, econômica e militar dos Estados Unidos. Uma leitura mais atenta do cenário internacional demonstra que esta é uma interpretação equivocada. Houve não apenas a reformulação da competição, mas o surgimento de uma versão mais profunda, com noções modificadas de poder, sua distribuição e sua forma de enfrentamento.

Jordán (2019) aponta que não se trata de uma nova Guerra Fria, pois não há o confronto entre dois grandes blocos econômicos, nem um contexto de bipolaridade. Há, no caso, uma crescente rivalidade entre várias grandes potências, que vêm, ao longo das décadas,

se sedimentando em diversas frentes, e se preparando para eventual conflito num futuro próximo. Neste mundo multipolar, com hegemonias regionais, diversas em ideologias, identidades e objetivos principais, as grandes potências, apesar de perceberem o mundo sob diferentes lentes, estão temporariamente ligadas e aliadas, sob a força da conveniência a um objetivo primário em comum; um embate contra a larga influência remanescente dos Estados Unidos[2].

Estas transformações na distribuição do Poder internacional também modificaram, lentamente, como ele é percebido e utilizado pelos Estados contemporâneos. Para ilustrar melhor estas modificações, é preciso compreender que o Poder existe em três grandes camadas. A primeira e mais aparente delas é a militar, seguida da econômica e, por último, a camada das relações transnacionais (NYE, 2011). Sua distribuição é, quase sempre, assimétrica, como será demonstrado a seguir.

Na camada militar, diretamente ligada à atuação dos Estados e ao Hard Power; a coerção e a força militar, o poder permaneceu nas mãos dos EUA durante e após o fim da União Soviética. O triunfo militar da operação *Desert Storm,* realizada em solo iraquiano, diante de uma União Soviética bastante enfraquecida internacionalmente, foi importante demonstração internacional deste domínio militar, e da capacidade de mobilização mundial dos EUA.

A segunda camada, dominada pelos processos econômicos e financeiros, é difusa, com ligeiras variações ao longo dos anos. Nela, os EUA, China e União Europeia compartilham grande parte do domínio, enquanto outros países se alinham aos maiores poderes e/ou tentam conquistar outros setores desta camada. É nela que reside parte significante da ideia de Soft Power; a influência de terceiros também pode ser realizada através de empreendimento econômico.

Na terceira e última camada; a das relações transnacionais não-governamentais, o poder é distribuído de forma ainda mais difusa, dividida entre os mais diversos atores não-estatais, até então fora do controle dos Estados e suas fronteiras. Tais atores não-estatais variam de banqueiros, investidores internacionais comuns, personalidades influenciadoras e ONGs, até grupos hackers, terroristas e traficantes de armas. Ao longo das décadas, esta terceira camada tem ganhado cada vez mais protagonismo, ajudando na difusão de poder entre os mais variados tipos de atores.

2 Seria o equivalente multipolar de “Balancing” ou “Aliança Defensiva”, descrito por Mearsheimer (2001, p. 160), visto que tais grandes poderes observam os Estados Unidos como uma ameaça, sendo a destruição de seu poder um ato de autodefesa.

Os novos adversários dos EUA, surgidos após a queda da URSS e o fim da Guerra Fria, florescem justamente neste contexto mais difuso de distribuição do Poder. Tais adversários não são necessariamente novos Estados, mas os mesmos Estados sob novos governos, com novas doutrinas instauradas que preencheram o espaço da competição internacional. Irã, China e a própria Federação Russa — geograficamente menor e sem acesso aos *buffer states* que antes exercia controle, são os principais atores aqui tratados como novos adversários. Durante o fim do último conflito, estes atores puderam observar em primeira mão as importantes lições oferecidas, adaptando-as para aplicar e competir no novo mundo multipolar, embora os Estados Unidos também tenham se apropriado de tais técnicas, como será abordado neste capítulo. É possível sintetizar os aprendizados do fim da Guerra Fria em duas grandes lições:

Em primeiro lugar, a atuação internacional contemporânea foge do sentido puramente militar, territorial e coercivo, típico do Hard Power, e caminha para uma noção crescente de que a sobrevivência e o domínio também dependem de quem carrega a melhor, mais atraente narrativa. Nye (2011) também expõe que isso não se trata de uma mudança total para o Soft Power, pois a ideia de convencimento apenas através diplomacia, exportação cultural e assistência econômica é infundada. Portanto, é necessária uma nova forma de utilizar ambos os poderes, sincronizadamente, sempre correspondente às necessidades e capacidades disponíveis para os atores. Em outras palavras, trata-se do uso do Smart Power.

Pode-se contra-argumentar que o financiamento de guerrilhas e governos autoritários, por parte dos governos soviéticos e americanos na Guerra Fria, para conflitos proxy[3], era uma forma efetiva de sincronizar Soft e Hard Power. No entanto, o mero fornecimento financeiro e militar não significa a utilização inteligente destes poderes, e não constrói uma narrativa atraente a longo prazo. Exemplo perfeito está na mudança radical do posicionamento de Osama Bin Laden e outros líderes de guerrilha, financiados pela CIA e aliados, para combater a intervenção soviética no Afeganistão. De grandes parceiros *mujahideen*[4] contra o "ateísmo soviético" (ARMSTRONG, 2016), tornaram-se a face do inimigo internacional, na Guerra Global ao Terror, após o atentado às Torres Gêmeas em 2001.

3 É o envolvimento de grandes poderes em um conflito de terceiros. Desejam influenciar o resultado deste conflito através do financiamento, treinamento e suporte político às forças terceiras, de modo a alcançar objetivos estratégicos na região; a remoção da influência de um adversário, que financia o lado oposto.

4 Termo árabe que se refere às pessoas que se envolvem em jihad, geralmente armadas. Foi utilizado de forma amigável pelo governo e cultura americana, a exemplo do uso por Ronald Reagan, ou em filmes como Rambo 3.

Em segundo lugar, a construção de uma narrativa convincente, superior à estabelecida pelo adversário, é um trabalho que demanda grande e detalhado planejamento, tratando-se de um objetivo a longo prazo. Conflitos proxy, que como dito, permearam toda a Guerra Fria, são indiretos por natureza, e visam o lento, mas contínuo enfraquecimento de uma força maior. Logo, seu potencial foi retirado do sentido estritamente militar e aplicado a todos os âmbitos do conflito internacional, mas temporalmente estendido; por sair do âmbito tático e ascender ao estratégico. A contínua corrosão das capacidades do adversário, sejam elas econômicas, militares ou políticas, aparece como principal estratégia das grandes potências. O caráter indireto ajuda a evitar um conflito total contra a capacidade militar e política de um adversário, enquanto garante uma vantagem futura (HICKS et al., 2019), num conflito direto contra um inimigo desgastado. Além disso, a melhor forma de um Estado legitimar uma nova narrativa é fazer parecer que não parte dele, mas de outros atores independentes, fortalecendo o teor indireto.

3.2. Definindo as Zonas Cinzentas

É a partir destes aprendizados, adaptações gerais e experiências no campo internacional que, ao longo dos anos, foi formado o conjunto de táticas e estratégias definidas como Conflito em Zonas Cinzentas. Dado o seu caráter extremamente ambíguo e indireto, ainda existem grandes discussões sobre seus mecanismos específicos, e até mesmo da validade do seu termo, mas é possível coletar características comuns a todas as definições (CHAMBERS, 2016; DOBS et al., 2020; HICKS, 2019). Uma definição que abarca de forma geral a natureza e ferramentas das Zonas Cinzentas pode ser apresentada da seguinte 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,)

Existe, então, um grupo de atividades que são mais ameaçadoras do que a política comum, mas não que envolve combate militar direto entre as grandes potências. Localizando-se entre a paz e o conflito, as Zonas Cinzentas representam perfeitamente o balanço que a noção de Smart Power promove entre Soft e Hard Power, embora apresente um caráter muito mais agressivo do que o aconselhado por Joseph Nye.

Os atores estatais passam não só a interagir mais com a terceira camada do Poder,

como disfarçar-se de atores não-estatais típicos desta camada, como influenciadores, grupos guerrilheiros e empresas. O ator estatal que usa ferramentas das Zonas Cinzentas pode ter como objetivo acumular ganhos lentamente, aglutinando posições aprimoradas, que antes eram adquiridas apenas em batalha; algo que, na atualidade, estará sempre no limiar da destruição nuclear mútua. De fato, o ator ainda pode se envolver em violência, mas na maioria das vezes, ela é mitigada por ser realizada por atores quase-estatais (HICKS et al., 2019).

É possível sintetizar as ferramentas utilizadas pelos atores estatais em seis categorias, embora muitas vezes sejam utilizadas combinadamente, para conquistar efeitos diferentes, conforme as capacidades e necessidades dos atores. São as Operações de Informação; Operações Cibernéticas; o uso de Forças Ambíguas; Coerção Política, a Coerção Econômica e, por último, Operações Espaciais. A bem da objetividade do trabalho, apenas o uso das Operações de Informação, Operações Cibernéticas e Forças Ambíguas serão explorados de maneira detalhada, vista suas implicações no conflito ucraniano.

3.2.1. Operações de Informação

Operações de Informação se referem ao uso de mídias sociais e outros meios de comunicação tradicionais, para reforçar a narrativa do ator que a usa, através da semeação de dúvidas, dissidências e informações errôneas no país adversário (CHAMBERS, 2016). Elas não criam dúvidas ou divisões na sociedade do adversário, mas se aproveitam de um contexto já existente, para aprofundar e radicalizar oposições políticas. Nem sempre essas operações se alinham a uma posição específica, preferindo disseminar desinformação em nome de várias posições políticas. As narrativas são espalhadas por atores estatais disfarçados de indivíduos não-afiliados, geralmente através de vários perfis interligados nas redes sociais, com seguidores comprados, para aumentar a aparência de legitimidade. EUA, Rússia e China são os principais utilizadores destas operações, que podem ser observadas desde os anos 2000, ainda de forma bastante rudimentar.

Nesta década, observa-se que a China se destacou por utilizar a rede do “Partido dos 50 centavos”[5]. Era uma grande rede de comentaristas contratados pelo governo chinês para vasculhar a internet em busca de notícias negativas sobre sua política interna e externa, e depois negá-las ou atacá-las. (BRISTOW, 2008). Dada a ausência de redes sociais mundialmente conhecidas no período, as postagens eram publicadas nas seções de comentários em sites e fóruns. Ao longo da

5 Nome dado pela imprensa ocidental aos funcionários do governo chinês, que trabalhavam nesta rede. Supostamente, eles ganhavam US$ 0.50 pelo serviço (BRISTOW, 2008)

evolução da rede, a China conseguiu contratar mais de 2 milhões de comentadores, gerando 450 milhões de publicações (STEINFIELD, 2018).

Já em 2011, o então diretor da CIA defendeu abertamente a realização de operações psicológicas, para combater "propagandas e ideologias extremistas". No mesmo ano, o Comando Central dos Estados Unidos havia anunciado a contratação de uma desenvolvedora de software, que garantiria que agentes de inteligência americanos assumissem o comando de dezenas de *Sockpuppets*[6] espalhados em todo o mundo (FIELDING & COBAIN, 2011). Embora a reação pública tenha sido majoritariamente negativa, é impossível saber se o projeto foi abandonado, embora aparente ter evoluído para outros métodos. Atualmente, no Facebook e no Twitter, a China e os EUA competem acirradamente em operações de informação.

De setembro de 2019 até o início de 2021, a China empreendeu uma operação apelidada de "Spamouflage", onde utilizava bancos de imagens e ferramentas de conversão de texto em voz, em inglês. As peças criticavam os protestos de Hong Kong, dissidentes políticos da China e a personalidade do então presidente Donald Trump e atuação dos EUA no Mar do Sul da China. Nos meses finais da operação, aproveitaram-se dos protestos do *Black Lives Matter* para insuflar a divisão racial americana e a presidência de Joe Biden. As publicações eram realizadas através de perfis comprados na Deep Web, geralmente em pacotes, consistidos de contas abandonadas ou hackeadas (GRAPHIKA, 2019, 2020, 2021b). Em agosto de 2022, as redes sociais do Meta e o Twitter removeram das suas plataformas centenas de perfis ligados a uma longa operação de informação dos Estados Unidos. A empreitada durou quase cinco anos, e funcionava similarmente às operações chinesas. Nelas, os agentes utilizavam identidades falsas para, através de publicações e comentários, espalhar visões, valores e objetivos dos EUA enquanto atacava os interesses da Rússia, China e Irã. Os idiomas eram variados, e pareciam evitar o inglês, preferindo russo, árabe e urdu. O diferencial dessas operações é a ampla utilização de falsas agências de notícias independentes, que elogiavam a atuação americana no Oriente Médio, África e Ásia. (GRAPHIKA, 2022)

A Rússia detém grande domínio destas operações, com teóricos russos se destacando nesta área de estudo. Importante exemplo é o trabalho de Igor Panarin. Desde o final dos anos 90, sua carreira é quase completamente dedicada ao estudo e implementação de Operações de Informações, com mais de 15 obras na área, variando de aplicações em guerra e eleições. Sua influência não se limita à academia civil, já que com seu doutorado em Ciência Política e

6

Psicologia, ele exerce o cargo de professor na Academia de Diplomacia do Ministério das Relações Exteriores da Rússia (USASOC, 2015). Neste sentido, o impacto de suas teorias, que defendem o uso generalizado de Operações de Informações, são evidentes.

Panarin argumenta as revoluções na Europa oriental da década de 2000, como a Revolução Laranja, e as revoluções da Primavera Árabe na década de 2010, foram orquestradas por operações de informações dos EUA. Partindo deste entendimento, ele defendeu a ideia da Rússia criar uma campanha de guerra de informação usando sincronizadamente aparatos de propaganda, inteligência, análise, agências secretas, manipulação da mídia e operações especiais selecionadas para influenciar as massas e os políticos. Similarmente, o teórico Alexandr Dugin, famoso pela Quarta Teoria Política, defende a criação de uma grande rede "eurasiática", onde nacionalistas russos se organizam e tomam o domínio das mídias sociais a serviço do Estado. Esta organização deve combater liberalismo pró-Ocidente através da criação de polêmicas e difamações, categorizando liberais russos como lacaios dos americanos.

Neste sentido, as Operações de Informação da Rússia, apesar de também utilizar canais de televisão e meios tradicionais de informação, tem como foco as redes sociais e aplicativos regionais, como VK, OK e Telegram. Observa-se que há o objetivo de fortalecer a própria narrativa internamente, através da criação de câmaras de eco e controle legal sobre as plataformas, permitindo a ascensão da dita "rede eurasiática". Isto não significa, no entanto, que não busquem desestabilizar seus oponentes, como os EUA (GRAPHIKA, 2021a). De fato, a Rússia foi grande ameaça nas eleições presidenciais dos Estados Unidos, em 2016, embora sua atuação nessa região tenha sido combatida vorazmente pelo governo americano (HICKS et al., 2019).

3.2.2. Operações Cibernéticas

Trata-se do uso de hackers, vírus ou outros métodos para causar danos físicos e financeiros, interromper ou atrapalhar processos políticos, punir concorrentes econômicos ou cometer outros atos maliciosos no ciberespaço (HICKS et al., 2019). Vale relembrar que, nas Zonas Cinzentas, a interação dos atores estatais com a terceira camada do Poder é mais comum, resultando em grande ambiguidade. Neste caso, a maioria dos ataques hackers não é diretamente promovida por organizações governamentais, mas por atores não-estatais contratados, ou atores estatais utilizando a aparência de grupos criminosos. Grupos hacker ativistas também atuam em simultâneo, dificultando ainda mais a apuração.

De qualquer forma, os grupos, malwares e vírus que atuam nestas operações são

categorizados como Agentes de Ameaça (PISCITELLO, 2015), e já estão estabelecidos na internet. Outro adendo é que nem sempre os alvos são estruturas e atividades do governo adversário, mas importantes empresas, personalidades e até mesmo estruturas civis, como hospitais. Além disso, concatenar a história destas operações nas relações internacionais é um trabalho difícil, mas é possível apontar alguns ataques que demonstram a variedade e crescimento destas técnicas.

Durante toda revolução na Ucrânia, em 2014, e o processo de anexação da Crimeia, no mesmo ano, operações cibernéticas tomaram o espaço da Rússia e Ucrânia. Com a fuga do então presidente Viktor Yanukovych e, depois, à medida que a anexação da Crimeia se desenvolvia, a Rússia intensificava suas operações, variando desde simples ataques DDOS[7] até ataques à estrutura de telefonia de toda a região. No dia 13 de março de 2014, três dias antes do referendo sobre o status da Crimeia, a Rússia lançou um ataque DDoS de oito minutos, visando desestabilizar as comunicações ucranianas e desviar a atenção do público da presença de tropas russas na Crimeia. (PAGANINI, 2014; EUROPARL, 2022).

Embora estas táticas sejam amplamente utilizadas no Conflito nas Zonas Cinzentas, a mais aparente e próxima do limiar da guerra é a utilização de forças ambíguas e proxies, para a conquista de objetivos. A seguir, será descrita esta forma de conflito e, no caso do leste ucraniano, como desafiou as formas tradicionais de inteligência.

3.2.3. O uso de Forças Proxy e Forças Ambíguas

Nas Zonas Cinzentas, operações utilizando forças proxy e uso de forças ambíguas buscam promover a intimidação, ou controle de território para exercer influência e alcançar resultados políticos e de segurança específicos dos estados que a utilizam (HICKS et al., 2019). Alguns teóricos tendem a definir forças proxy e forças ambíguas como equivalentes, mas existem diferenças fundamentais.

Forças proxy são grupos de um determinado estado ou região, financiados por um estado terceiro, geralmente mais fraco política, militar e economicamente. Perfeito exemplo do uso de forças proxy estão nos conflitos da Guerra Fria. Naquele período, governos menores, sem autonomia frente à bipolaridade do cenário internacional, serviam de proxy de um Estado mais forte, em troca de auxílio financeiro, econômico ou militar. O mesmo acontecia com grupos políticos opositores ou guerrilhas, cooptados pelo Estado rival. Desta forma, um Estado financiava, treinava e defendia publicamente o governo, enquanto outro o

7 Ataque de negação de serviço; a tentativa de derrubar sites e servidores através do seu congestionamento

fazia em relação a grupos armados opositores. Em outras palavras, os Estados e atores beneficiados tinham necessariamente um relacionamento, ideológico e econômico, com o governo que o apoiava; naquele caso, EUA ou URSS (HUGHES, 2014; MUMFORD, 2013), levando ao apoio aberto, público, do Estado. O caráter indireto se apresentava apenas no setor militar, onde guerrilhas e ditaduras lutavam entre si, em nome dos dois blocos.

Forças ambíguas, por outro lado, são forças armadas utilizadas pelo estado, que flutuam entre a categoria de proxy e de forças regulares do estado. Desta forma, não argumentam necessariamente serem grupos não-estatais, enquanto negam que estejam obedecendo ordens de algum terceiro envolvido. Como dito anteriormente, no mundo contemporâneo, os atores estatais não apenas interagem com terceira camada de poder, como se misturam e se "disfarçam" de atores não-estatais. Esta ambiguidade foi bastante aparente 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). Este mesmo comportamento está, por exemplo, nas embarcações civis utilizadas pela Marinha da China, no Mar do Sul da China. Apesar de ter a maior força naval do mundo, a marinha chinesa transporta equipamentos de vigilância em embarcações civis, no Mar do Sul da China, e com eles realizam treinamentos e operações de patrulha (DAWSON, 2022; TOKMAK, 2022). Forças ambíguas são frutos da enorme ambiguidade da contemporaneidade, permitindo que a Negação Plausível seja usada prolongadamente, em relação ao envolvimento do Estado com o conflito que se desenvolve em outro país ou região.

Outra vantagem do uso de forças ambíguas vem da capacidade de intensificar ou retardar a escalada de violência conforme planejado. Isto evita chamar atenção internacional, reduz o custo humano com baixas, auxilia na construção da narrativa e o consequente apoio popular, que seria afetado caso a situação saísse do controle. Isto coincide com as considerações de Valeri Gerasimov (2013), ao observar a política externa americana na Primavera Árabe. Ele argumenta que a linha entre guerra e paz se tornou tênue, ambígua, onde insurreições e protestos democráticos liberais no Oriente Médio podem não parecer uma guerra típica, mas geralmente resultam em intervenção militar e destruição civil. Esta escalada, de protesto para violência, segundo Gerasimov, demonstra uma capacidade do ocidente em unir ações cinéticas e não-cinéticas, para manipular a evolução do conflito entre militar e civil. Como num roteiro, o Estado tem possibilidade de justificar atividades

cinéticas, o apoio a determinados grupos e, finalmente, solidificar a própria narrativa na região (GERASIMOV, 2013; USASOC, 2015). Tal maleabilidade não seria possível através de um proxy, que, apesar de "submissa" ao Estado que o financia, tem ideologias e cadeia de comando próprias, eventualmente discordando ou se tornando inimigo, como no já mencionado caso da Al-Qaeda.

Em casos como no leste da Ucrânia, o uso de atores não-estatais foi diluído na presença de soldados regulares russos sem insígnias, permitindo que a Rússia pudesse continuar a negar qualquer envolvimento, político ou militar, com o conflito ou aumento de tensões. É válido ressaltar que forças, no entanto, forças ambíguas não excluem o uso de proxy; as duas técnicas podem ser utilizadas num mesmo conflito. No leste ucraniano, apesar de soldados russos regulares participarem e comandarem soldados e separatistas voluntários no conflito, grupos proxy da Rússia, conhecidos internacionalmente, como a companhia militar privada Wagner, participavam de combates (ASSYMETRIC WARFARE GROUP STUDY, 2020; KAPUSTA, 2015).

Como dito anteriormente, esta ambiguidade atrasa e prejudica qualquer reação dos Estados atingidos, geralmente de menor poder político e militar no plano internacional. Estes se se veem incapazes de revidar utilizando aparelhos oficiais de inteligência. Ora, além de não terem grande capacidade de inteligência à sua disposição, estes aparelhos foram desenhados e evoluídos para competir contra estados ou atores não-estatais, não com atores de natureza desconhecida. Além disso, mesmo sabendo a quem pertence o ator na Zona Cinzenta, o uso de HUMINT, por exemplo, para investigar os responsáveis é arriscado. O fracasso em provar algo, devido à ambiguidade, ou a chance de traição, podem levar a tensões irreversíveis.

Softwares de espionagem também podem gerar abusos e reações negativas da própria população, e mal-estar diplomático, caso descoberto pelo Estado-alvo, ou mal utilizado; o que pode ser aproveitado na narrativa de inimigos. Além disso, para Estados democráticos que desejam seguir a lei internacional, competir contra estratégias das Zonas Cinzentas, utilizando-se delas, é uma decisão arriscada, de efeito limitado. Como já mencionado, o fruto destas táticas se apresenta a longo prazo, sendo necessária uma grande continuidade nas relações internacionais de um país; algo um tanto difícil em democracias. Democracias contam com o poder descentralizado, sendo difícil mobilizar diversos instrumentos de poder simultaneamente. Este quesito explica porque as Zonas Cinzentas são utilizadas mais livremente por Estados autocráticos, que gozam de unidade de comando e singularidade no

poder (KAPUSTA, 2015), e a dificuldade de respondê-las utilizando as formas tradicionais de política e inteligência.

Pode-se argumentar que a GEOINT da OTAN foi utilizada para identificar o agrupamento de soldados russos na fronteira com a Ucrânia em 2014. Embora essa informação seja verdadeira, não há registros [públicos] do uso de GEOINT evidenciando o movimento das tropas para dentro do território ucraniano, efetivamente invadindo o país, o que provaria antecipadamente a invasão. Como será exposto no capítulo seguinte, uma das técnicas utilizadas pelo governo russo foi a diluição e o lento transporte de equipamentos e pessoal, para o leste ucraniano. Enquanto a GEOINT é capaz de identificar grandes colunas militares e estruturas, é incapaz frente a movimentos dosados e diluídos entre fronteiras, principalmente em conflitos não assumidos. Isto pode explicar porque, durante os primeiros meses do início oficial da agressão da Rússia em Donbas experienciou um vácuo de informações (PROMETHEUS, 2017)

Esta mesma ambiguidade das Zonas Cinzentas, que incapacita respostas diretas, é a mesma que permite o uso de aparatos abaixo do limiar da espionagem, usados legalmente e não limitado aos Estados. Este é o papel do OSINT, o principal entre os vários métodos utilizados pela comunidade independente de inteligência e investigadores privados.

Como demonstrado no capítulo anterior, sua versatilidade permite a livre produção e compartilhamento de informações legalmente angariadas entre aliados. O OSINT também fornece aos Estados e outros atores afetados pelas estratégias das Zonas Cinzentas, a capacidade de produzir provas para legitimar o uso de suas tecnologias formais, evitar a evolução do conflito, ou engajar-se legalmente contra o Estado perpetrador. No capítulo seguinte, será apresentado um breve histórico do conflito no leste da Ucrania, de 2014 a 2021. Partindo desta introdução, será abordado como foram realizadas as investigações que expuseram a participação direta da Rússia, e a utilização destas evidências em cortes e eventos.

4. CAPÍTULO III: OSINT NO CONFLITO EM DONBAS

Tendo definidos os conceitos de Zonas Cinzentas, e as táticas de enfrentamento que se utilizam delas, será oferecido um panorama sobre a Ucrânia, sua contradição interna, e como estas táticas foram utilizadas na invasão russa que começou em março de 2014. Desta forma, será possível demonstrar as investigações e evidências construtivamente. Logo após, será possível demonstrar suas repercussões.

4.1. Ucrânia, Donbas e o conflito de 2014

Localizada na Europa Oriental, a Ucrânia é o segundo maior país do continente. Seus 603 mil quilômetros quadrados fazem fronteiras com sete países. Ao sul e sudeste estão acessos ao Mar negro e Mar de Azov, como visto no mapa 1. Sua extensão territorial e localização na Grande Planície Europeia[8], também o transformam no principal meio de transporte de energia da Rússia para a Europa, através de gasodutos. Em suma, a Ucrânia é um estado de fronteira por excelência, algo diretamente inscrito em seu nome; *Okraina*, em russo, significa "arredores", "bordas". Está estrategicamente localizado entre países a Rússia, seus aliados e a União Europeia, separando duas hegemonias regionais em disputa. (FRIEDMAN, 2013)

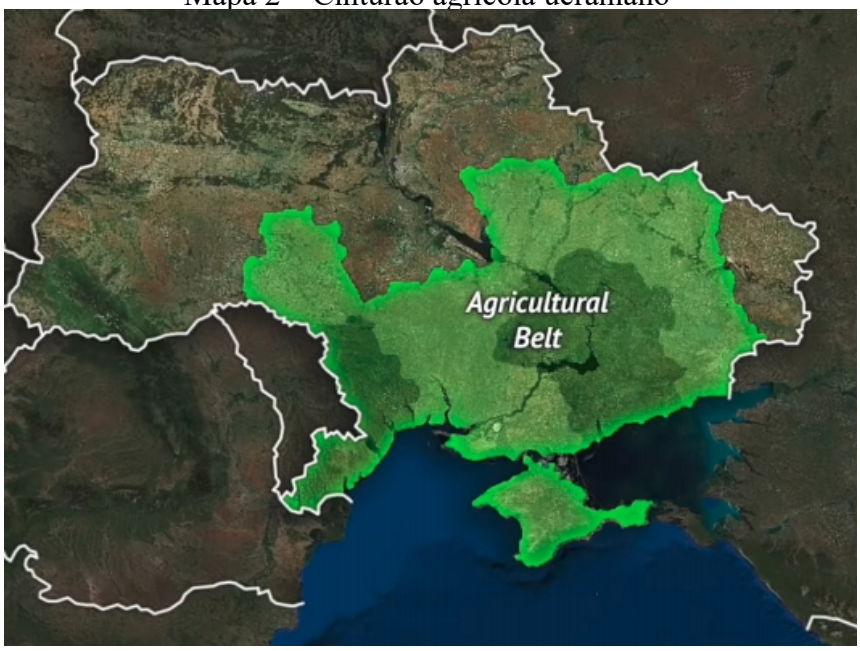
Mapa 1 – Ucrânia

Fonte: CIA (2017)

8 A Grande Planície Europeia é uma das principais características topográficas do continente, sendo a maior forma de relevo plano, livre de montanhas, da Europa. Com exceção dos Montes Cárpatos, na parte ocidental, a Ucrânia é basicamente uma planície.

Cerca de dois terços do terreno ucraniano é constituído de chernossolo[9], tornando-o abundante em recursos minerais e agrícolas. Ao longo da história ucraniana, quatro núcleos populacionais se formaram. A capital Kyiv, no centro, e L'viv, no oeste, foram fortemente influenciadas pela Europa Ocidental, desde a Idade Média, principalmente através da dominação polonesa. Donetsk e Lugansk, por outro lado, localizados no cinturão agrícola, como visto no Mapa 2, e mineral no leste do país, foram historicamente ligados ao Império Russo, União Soviética e, após 1991, à Federação Russa.

Mapa 2 – Cinturão agrícola ucraniano



Fonte: STRATFOR (2014)

Donetsk e Lugansk têm muitas características em comum, costumando ser unidas sob o nome "Donbas", correspondendo a 9% do território do país, com a área mais densamente povoada e urbanizada. A região tem área de mais de 60 mil km², e uma fronteira terrestre de 923 km² com a Federação Russa Como já exposto nas figuras 6 e 7, a maioria da produção agrícola também vem de Donbas, assim como grande atividade extração de carvão, exposto no Mapa 3. As fronteiras administrativas da região, criadas já na década de 20, sob domínio soviético, foram especialmente construídas para unir as cidades industriais sob uma administração (PROMETHEUS, 2017).

Após a Segunda Guerra, Nikita Khrushchov ordenou a transferência de milhões russos para a Ucrânia, acelerando o processo de industrialização, transformando a região no motor econômico da URSS, além de torná-la permanentemente a região do país com maior

9 Chernossolo, ou Chernozem, é um solo mineral de aparência escura, extremamente fértil e agriculturável.

concentração de russos étnicos e russófonos. Apesar da tentativa de russificação, movimentos de independência e nacionalistas continuaram fortes durante todo o século XX (USASOC, 2015).

Mapa 3 – Indústria de carvão no leste ucraniano

Fonte: Prometheus (2017)

Estes fatores evidenciam que a Ucrânia, mais que um mero buffer state, é uma zona perpétua de conflitos entre o Ocidente e Oriente, cuja política interna reflete seus desdobramentos. Desta forma, o país está submetido a um cabo de guerra cultural, econômico, político e, inevitavelmente, militar entre as duas potências. Ao longo das décadas, estas tensões externas inflamaram as divisões internas da Ucrânia, oferecendo à Europa e Rússia a oportunidade de construir suas narrativas que justificassem suas influências ou coerções na região. Na próxima seção, serão abordados os antecedentes contemporâneos que resultaram no ciclo de tensões que eclodiram no conflito indireto de Março de 2014 e, mais tarde, na invasão direta de Fevereiro de 2022.

4.1.1. Prelúdio da invasão

Desde a sua independência em 1991, a Ucrânia passava por um longo e conturbado processo de aproximação com a União Europeia. Mesmo Leonid Kuchma, amplamente apoiado pelo leste, defendia uma atitude pragmática e independente. Durante seus dois mandatos, de 1994 a 2004, promoveu a aproximação com a UE, mas um contínuo diálogo com a Rússia.

Diferenças políticas regionais se acentuaram significativamente apenas nas eleições presidenciais de 2004, quando o país foi palco de grandes manifestações (USASOC, 2015, p.

23). A eleição foi disputada entre dois Viktors; Yanukovych e Yushchenko, ambos com experiência política, tendo ocupado o cargo de primeiro-ministro nos governos de Kuchma. Yanukovych, nascido em Donetsk, era mais favorável à integração com a Rússia, por isso bastante apoiado no Leste do país. Yushchenko, nascido no nordeste ucraniano, tinha grande apoio da bancada pró-ocidente (YORK, MERRIMAN ZIMMERMAN & BOAZ, 2010; WOMACK, 2004).

Durante a acirrada campanha, Yushchenko sofreu uma tentativa de assassinato por envenenamento, levando à suspeição de tentativas de interferência russa na eleição. Além disso, a inteligência ucraniana (SBU) e observadores internacionais apresentaram diversas evidências de irregularidades e crimes eleitorais a favor de Yanukovych. Manifestações em massa, greves e desobediência civil logo tomaram o país. O movimento, que mais tarde foi nomeado de Revolução Laranja, alcançou o objetivo de recontagem judicial, o que garantiu a vitória de Yushchenko (KUZIO, 2007; PRAVDA, 2004; BOAZ et al., 2010).

A presidência de Yushchenko foi exatamente o que a Rússia temia; uma grande guinada da Ucrânia em direção ao ocidente (PACE, 2005). Além de continuar o processo de integração à União Europeia, iniciado por Kuchma, Yushchenko endossou a entrada da Ucrânia à OTAN, sinalizando a possibilidade de uma emenda constitucional para remover sua declaração de neutralidade (INTERFAX, 2009). Naquele mesmo ano, diversos ex-membros da URSS haviam seguido o mesmo caminho. Mais de sete países haviam entrado para a OTAN. Três deles; Letônia, Estônia e Lituânia, em contato direto com a Rússia e Bielorrússia (NATO, 2018)

Principalmente durante a Guerra Fria, parte integral da estratégia russa sempre foi o cultivo de um grande escudo de estados satélite, compensando a ausência de barreiras geográficas contra possíveis ataques. Abdicar da influência sobre a Ucrânia, além de perder o potencial acesso ao Mar Negro, seria grande ameaça estratégica e existencial para a Rússia (USASOC, 2015). A qualidade das relações entre os dois países, inevitavelmente, diminuiu.

Os receios russos foram brevemente cessados após a eleição de Yanukovych, em 2010. Embora seu governo tenha expressado o retorno de uma política pragmática, mantendo a neutralidade e cultivando boas relações, os últimos anos do governo Yanukovych foram marcados pela preferência à integração econômica com a Rússia, em detrimento do prosseguimento de relações com a UE, gerando diversas críticas no Parlamento unicameral e grande instabilidade política (PROMETHEUS, 2017).

Na noite de 21 de Novembro de 2013, um dia após realizar uma reunião com o então primeiro-ministro da Rússia, Dmitri Medvedev, Yanukovych suspendeu o acordo de associação à UE, que marcaria um importante passo para o processo estabelecido nas décadas anteriores. Em vez disso, manifestou interesse na União Aduaneira da Eurásia. A abrupta suspensão levou imediatamente a protestos na Praça da Independência, em Kyiv, exigindo o prosseguimento do acordo (USASOC, 2015, p. 28). As manifestações, organizadas por redes sociais, continuaram ao longo nove dias, com um ápice de 20 mil pessoas na praça.

O movimento ganhou um tom violento na madrugada de 30 de Novembro, quando os policiais da Berkut dispersaram violentamente todos os manifestantes e outras pessoas da Praça da Independência. Segundo a Humans Right Watch (2013), 35 pessoas foram feridas. A repressão gerou mais aderência civil e uma rápida escalada de violência tomou as ruas, com o ministro do Interior autorizando as forças policiais a usar armas de fogo para reprimir os distúrbios. No dia 21 de Fevereiro, cerca de 100 civis foram mortos por atiradores desconhecidos em menos de uma semana. Em meio à troca de acusações entre manifestantes e autoridades, Yanukovych e inúmeros membros do Partido das Regiões fugiram para a Rússia. A fuga, e a organização de um governo provisório serviram como sinal para o começo da invasão russa à Ucrânia, começando pela Crimeia (ROTH, 2019; SCHWARTZ, 2018; USASOC, 2015).

4.1.2. Início da invasão

Na Crimeia, o processo de invasão foi completamente baseado no uso sincronizado de três táticas nas Zonas Cinzentas; forças ambíguas, operações cibernéticas e operações de informações. As operações cibernéticas suprimiam a circulação de informações entre veículos de informação, cidadãos e militares ucranianos, enquanto forças especiais da Rússia, sem insígnia, organizavam a tomada da região junto a cidadãos pró-Rússia. Além do uso de ataques *DDoS* e *jamming* de sinais de satélite de TV e sabotagem no sistema de fibra óptica foram realizados. As operações de informações, realizadas por jornais governamentais como TASS e Ria Novosty, direcionadas à população russa e residentes da Crimeia, legitimavam a tomada dos órgãos governamentais, e se referiam aos soldados sem insígnia como “milícias de autodefesa”, além de alimentar tensões étnicas entre ucranianos e russos. (EUROPARL, 2022; JAITNER & MATTSON, 2015; KOFMMAN et al., 2017)

Movimentos de militares russos começaram no dia 20 de Fevereiro, um dia antes da fuga de Yanukovych, com o reposicionamento de suas unidades para o Estreito de Kerch

(PROMETHEUS, 2017). Quatro dias depois, várias unidades da 810.ª Infantaria Naval chegaram à praça central da cidade, violando as regras que regiam as divisões territoriais na Crimeia[10]. No dia 27, cerca de cinquenta operadores de forças especiais, sob o disfarce de "milícias de autodefesa", tomaram o Parlamento da Crimeia e subiram a bandeira da Rússia no telhado. Outras supostas milícias de "autodefesa" tomaram vários prédios do governo, bases aéreas, instalações militares. O governo interino de Kyiv, com problemas na cadeia de comando e comunicação, no entanto, ordenou que suas forças militares não resistissem (KOFMMAN et al., 2017; USASOC, 2015).

Neste período, a agência TASS e outros meios estatais russos de comunicação alegavam que centenas de russos étnicos estavam fugindo da Ucrânia e buscando proteção na Rússia, como resultado de supostas violências do governo interino contra a população. As fotos e vídeos utilizados nas peças de reportagem, no entanto, eram da fronteira da Ucrânia com a Polônia (JAITNER & MATTSON, 2015, p. 42). As matérias foram publicadas dias antes do Parlamento Russo autorizar oficialmente o uso de militares regulares para "proteger russos na Crimeia e normalizar a situação" (LALLY, ENGLUND; BOOTH, 2014).

Durante a primeira quinzena de Março, foi organizado o processo do referendo de anexação da Crimeia, embora Putin publicamente negasse qualquer intenção de anexar a região, ou da existência de soldados regulares envolvidas no processo político da Crimeia (JAITNER & MATTSON, 2015). O referendo, realizado em 16 de Março de 2014 e considerado legalmente nulo internacionalmente, foi permeado de irregularidades, mas legitimou e finalizou com sucesso a narrativa que sustentava o processo de tomada da Crimeia. Em pouco tempo, a Rússia anexou a região sem baixas diretas, com apenas seis mortes ligadas ao processo, incluindo conflitos entre grupos civis opostos.

Paralela à anexação da Crimeia, o governo russo também tentava tomar Donbas. Enquanto a utilização sincronizada de táticas nas Zonas Cinzentas foi relativamente pacífica na Crimeia, sua implementação em Donetsk e Lugansk levou a um longo e violento conflito armado em Abril, que se estenderia até a invasão direta de 2022. Dada as diferenças geográficas e étnicas entre as duas regiões (KOFMMAN et al., 2017, p. 17), além do caráter ambíguo das próprias táticas, é impossível estabelecer se a escalada de violência foi imprevista, ou uma adaptação do já mencionado modelo proposto por Gerasimov.

Por um lado, observa-se que na Crimeia, a etnia predominante é russa. Qualquer

10 Estabelecidos desde 1997, os tratados de partição do Mar Negro, entre Rússia e Ucrânia, definiam as condições a criação da Frota Russa do Mar Negro na Crimeia. Entre elas, quantidade e categorias de unidades militares, além de proibir a movimentação sem aviso e acordo prévio entre as duas partes.

postura de resistência vinda de Kiyv, que levasse a confrontos armados, diminuiria significativamente o apoio da população local ao governo ucraniano. Apelo à etnia e a disseminação de um suposto conflito étnico foi tática amplamente utilizada pela Rússia em suas operações de informação (USASOC, 2015, p. 48-49). Uma postura passiva levou o governo interino a ser rapidamente cercado, suas forças foram ordenadas a não reagir, perdendo rapidamente estruturas militares e governamentais. Tudo foi ainda mais facilitado pela autonomia política da Crimeia, com unidade política distinta do governo de Kyiv (KOFMMAN et al., 2017, xi)

Por outro lado, em Donbas, como dito, embora a quantidade de russos étnicos seja significativa, ucranianos ainda constituem maioria, fazendo também parte da mesma unidade política de Kyiv. Uma postura ativa e apoiada pelo governo interino foi possível. Em março, a inteligência ucraniana (SBU) pôde repelir várias tentativas iniciais de tomar estruturas governamentais e militares, como o prédio da Administração Estatal Regional de Donetsk (USASOC, 2015). De qualquer forma, a Rússia precisou, ou antecipou a necessidade de deixar as operações cibernéticas e de informação em segundo plano, e priorizar o uso de forças ambíguas. Neste sentido, em Abril houve um aumento radical de soldados e o uso de operações cinéticas (PROMETHEUS, 2017).

No dia 7 de Abril, militares e manifestantes em Donetsk declararam a República Popular de Donetsk (DPR). 12 de Abril, Igor Girkin, ex-agente da FSB e veterano de diversas invasões russas, que também havia organizado milícias na Crimeia, liderou um time armado na tomada de diversos prédios governamentais em Slkoviansk, oblast de Donetsk. Assim como na Crimeia, seu grupo se dizia formado de cidadãos locais e exigia um referendo semelhante ao da península. Neste período, ônibus civis foram vistos saindo dos oblasts russos de Rostov e Belgorod, assim como da região da Transnístria, para manifestações e tentativas de tomar outras estruturas (PROMETHEUS, 2017; USASOC, 2015).

Diferente do desenrolar na Crimeia, o governo interino anunciou a ofensiva contra as forças ocupantes no leste da Ucrânia, no dia 14 de Abril, criando uma “Zona de Operação Anti-Terrorista” (ATO). Os militares russos continuaram seus esforços apesar das medidas, e anunciaram a República Popular de Lugansk (LPR) no dia 27, realizando um referendo conjunto pela independência dos dois oblasts no início de Maio. Além disso, a guerra permaneceu estática e com pequenas altercações até Setembro, quando as batalhas mais violentas e decisivas aconteceram. Naquele mês, os encarregados pela ATO precisaram

reconhecer oficialmente a participação direta de militares e equipamentos russos em Donbas (PROMETHEUS, 2017; USASOC, 2015).

Deve-se compreender que, embora atualmente milhares evidências demonstrem a ampla atuação e planejamento russo no conflito, o seu período inicial foi obscuro. Como exposto no capítulo anterior, mesmo as agências de inteligência do ocidente permaneceram relativamente silenciosas durante os primeiros meses. Além disso, a parte ocidental da Ucrânia acabava de sair de meses de tumulto e violência política, contribuindo ainda mais para a incerteza e desconcerto.

Somando estes fatores à assimetria de informações, típica de conflitos militares, o atraso nesse reconhecimento é compreensível. A desconfiança e acusações políticas haviam sido feitas em relação à Rússia, mas detalhes e evidências de sua participação precisariam ser documentadas durante um longo período, para formar um compilado conciso de provas cabais.

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

Durante os oito anos de conflito indireto, e principalmente durante o "blackout" de informações dos primeiros meses, indivíduos e comunidades dedicadas ao OSINT digital preencheram esse vazio informacional. Nesta seção, serão abordadas as evidências em fontes abertas que foram cruciais para o desmonte da narrativa russa diante do cenário internacional. No entanto, as investigações não serão dispostas em ordem cronológica, mas em categorias.

Primeiro, serão apresentadas investigações sobre unidades de infantaria; sua camuflagem, identidade e armamentos únicos. Em segundo lugar, serão apresentados casos sobre veículos de guerra exclusivos da Rússia, presentes em solo ucraniano. Apresentadas estas investigações, será abordado como várias destas evidências foram utilizadas por organizações governamentais internacionais nas suas tomadas de decisões.

4.2.1. Soldados russos em Donbas

Desde o primeiro dia da invasão à Crimeia, centenas de fotos e vídeos, capturados por jornalistas civis, publicadas na TV, sites de notícia na internet e nas redes sociais, mostravam a chegada dos largos comboios de soldados na península da Crimeia. Essa extensa base de dados abertos é suficiente para analisar os soldados.

A partir destas mídias, é possível identificar e checar a origem de equipamentos, armamentos de infantaria e camuflagem, comparando as imagens com bases de dados e repositórios especializados em militaria. Entre eles, é possível utilizar principalmente os sites

CamoPedia, Deagel e Weapons Systems. Estes dados ganham mais credibilidade se comparados com peças jornalísticas dos setores militares, que oferecem dados sobre a produção e distribuição destes equipamentos.

Observa-se que, 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 "homenzinhos verdes"[11] está na Figura 5.

Figura 5 – 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 6, abaixo.

Figura 6 – Primeira versão da Camuflagem EMR

11 Termo dado pela imprensa e movimentos civis pró-Ocidente aos soldados sem insígnias. É oposto ao termo dado por Alexandr Dugin, chamando-os "homens gentis", dada sua postura não combativa na Crimeia (USASOC, 2014, p. 47)

Fonte: Voyennoye Obozreniye (2010)

Segundo notícia publicada pelo próprio Ministério de Defesa da Rússia (2011), a camuflagem foi criada em 2008, mas adotada oficialmente pelas Forças Armadas Russas apenas em 2011 (CAMOPEDIA, 2022). Bielorrússia e Rússia são os únicos países da região utilizando esta camuflagem, enquanto regiões parcialmente reconhecidas internacionalmente, ocupadas por forças russas, começaram a usá-las em 2016, como abertamente observado na Transnístria e Ossétia do Sul (FULLER, 2017; ORYX, 2020).

O colete tático modular utilizado é o 6SH117, demonstrado na Figura 7. É parte do programa Ratnik-2, criado também em 2008 pelo Ministério de Defesa da Rússia (MDR), para modernizar os equipamentos de infantaria. Segundo o jornal RIA Novosty (2012), o equipamento foi exposto em público pela primeira vez em 2011. No entanto, sites de notícia oficiais da Rússia mostram que o equipamento foi adotado em outubro de 2014, mas usado em larga escala apenas em 2015 (DEAGEL, 2022; GRAVRILOV, 2015; SPUTNIK, 2014).

Figura 7 – 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[12], 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 exibido na próxima seção.

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[13], ou a localização embutida nos metadados de fotos, para marcar automaticamente a localização da publicação. Esse descuido também apresenta

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

13 A opção de localização deve estar ligada com antecedência, para ser utilizada na publicação. Entretanto, é notável que aplicativos de redes sociais pedem permissão de acesso à localização no seu primeiro uso, e a partir daí, ligadas automaticamente quando o aplicativo está em operação. Dado que a maioria destas redes eram usadas pelos soldados antes mesmo da invasão, é provável que não tenham prestado atenção neste detalhe, ou sequer tenham compreendido as implicações de segurança.

oportunidades de investigação. Como será observado, 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.

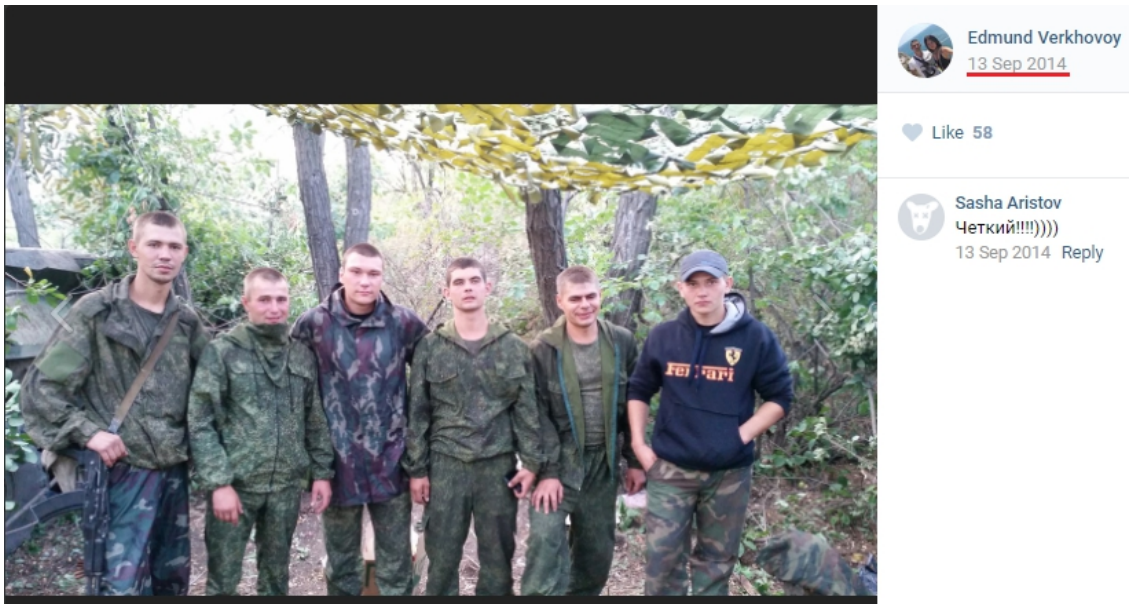
A comunidade foi idealizada pelo especialista militar georgiano Irakli Komaxidze e pelo jornalista ucraniano Roman Burko, semanas após a anexação da península em março (INFORMNAPALM, 2014a). Contando com investigações cooperativas com outros grupos voluntários de todo o mundo, o site conta com versões 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[14], 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 8, 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.

14 Criada em 2005, é uma formação de infantaria mecanizada, parte da Unidade Militar 22223 (2.º Exército de Armas Combinadas) localizada no Distrito Militar Central da Rússia. Essa formação é composta por militares de contrato, em vez de conscrição, e dedicada a operações de *Peacekeeping* sob auspícios da ONU, participando em 2020 da missão em Nagorno-Karabakh. No entanto, participou da Invasão à Geórgia, em 2008, e em 2022 esteve nos esforços militares russos no Leste da Ucrânia. (COHEN & HAMILTON, 2011; KOMMERSANT, 2004; CHERNICHKIN & PONOMARENKO, 2022; MDR, 2015; TASS, 2020)

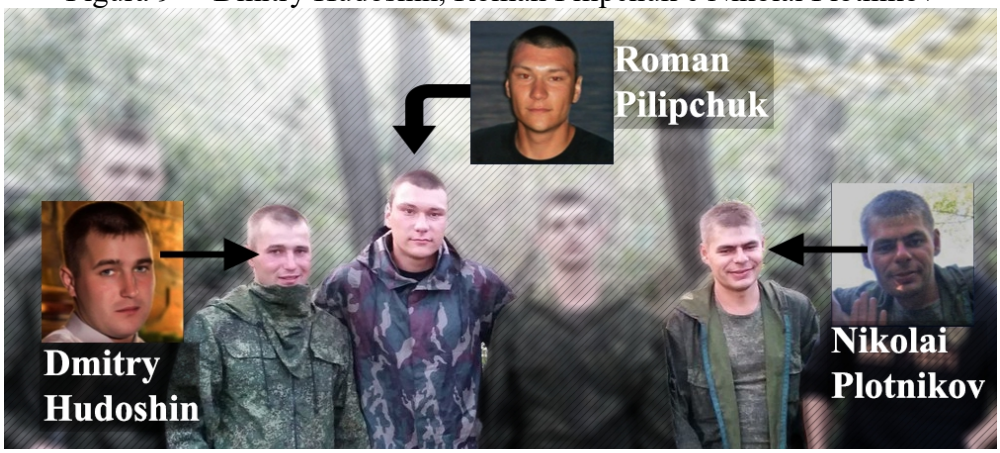
Figura 8 – Publicação de Vitaly Perfilov



Fonte: INFORMNAPALM (2017)

Das cinco identificações, três foram as mais importantes: Dmitry Hudoshin, Roman Pilipchuk e Nikolai Plotnikov. Destacados na Figura 9, eles são donos, e relativos de donos 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.

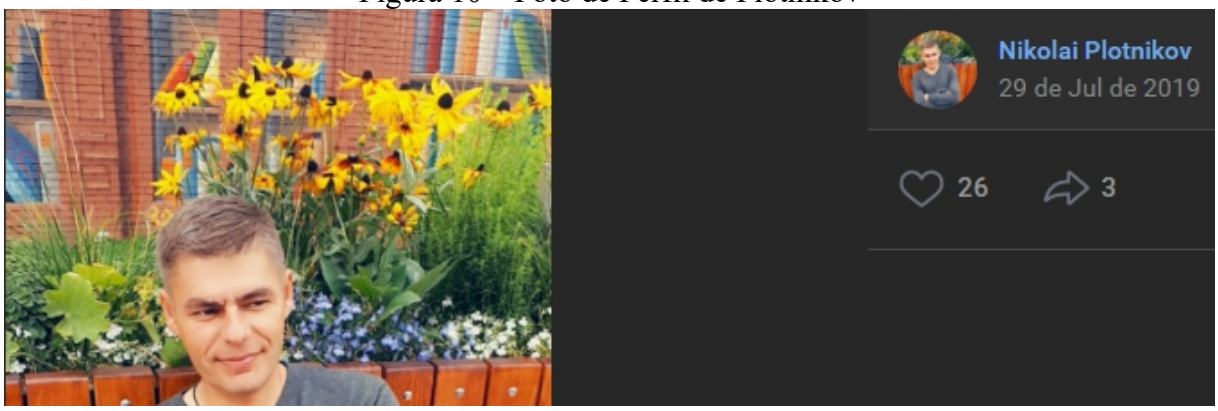
Figura 9 – Dmitry Hudoshin, Roman Pilipchuk e Nikolai Plotnikov



Fonte: Colagem do autor (2020)

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 10) mostra o rosto de forma bastante nítida.

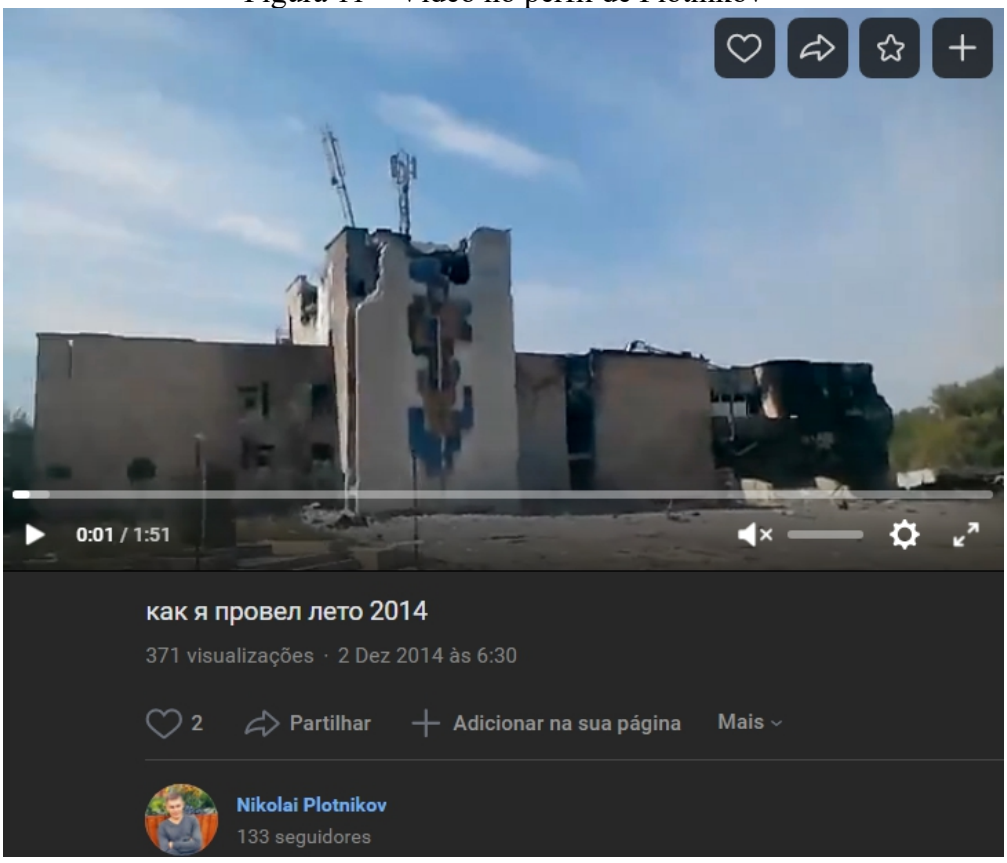
Figura 10 – Foto de Perfil de Plotnikov



Fonte: Captura de tela do autor no site VK (2022)

Também na sua conta, há um vídeo publicado em dezembro de 2014 (PLOTNIKOV, 2014), entitulado "Como passei o verão de 2014" (Figura 11). Com quase dois minutos de duração, o vídeo mostra um comboio de APCs passando por prédios destruídos, veículos e campos incendiados.

Figura 11 – Vídeo no perfil de Plotnikov

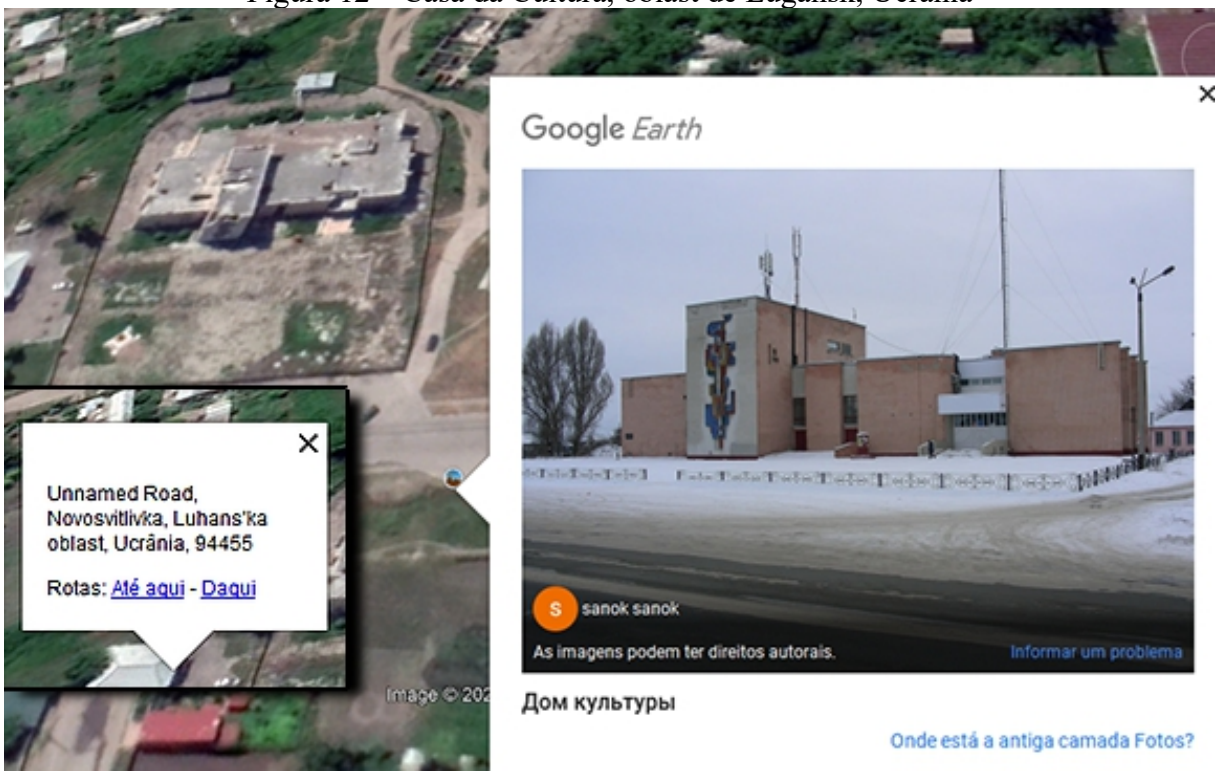


Fonte: Captura de tela do autor no site VK (2022)

Já nos dois primeiros frames, é visível uma construção governamental, exposto na Figura 11. 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 12).

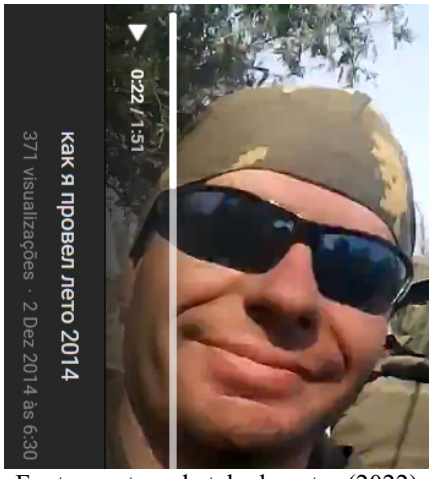
Figura 12 – Casa da Cultura, oblast de Lugansk, Ucrânia



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, como expõe a Figura 13. Trata-se de uma evidência da presença de Nikolai em Lugansk durante o início conflito, dada a destruição do local.

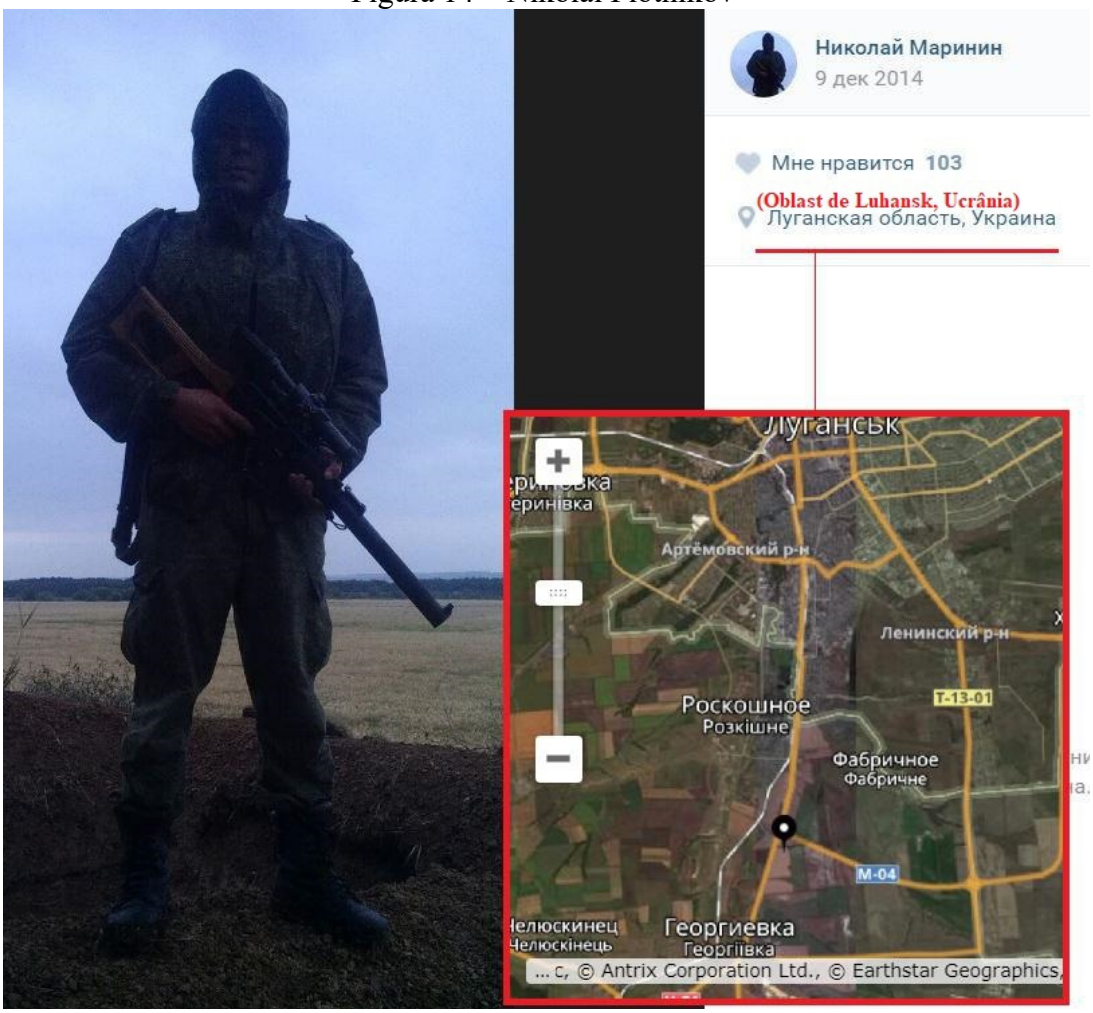
Figura 13 – Rosto de Nikolai Plotnikov



Fonte: captura de tela do autor (2022)

A geolocalização do vídeo coincide com uma foto publicada por ele, em 9 de dezembro de 2014 (Figura 14), onde posava portando um fuzil de precisão. Por descuido ou imprudência, ele deixou ativa a localização no VK, antes de publicar a foto, localizando-a em Lugansk, Ucrânia[15].

Figura 14 – Nikolai Plotnikov



Fonte: InformNapalm (2017)

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 países terceiros é bastante limitada (MILITARY FACTORY, 2022; MITROFANOV, 2019).

15 Em 2022, Nikolai removeu a marcação, mas a versão original da publicação, arquivada pelo Informnapalm (2017), permanece disponível.

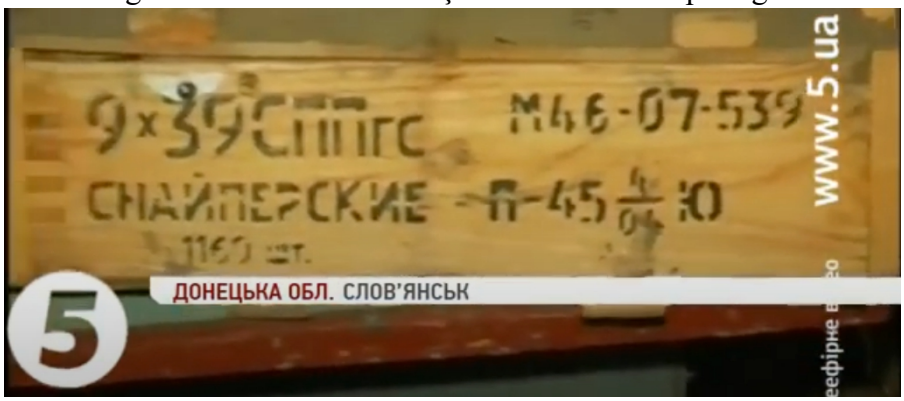
Por fim, outra evidência da participação de Plotnikov como soldado russo está na medalha entregue pelo MDR como recompensa pela participação na tomada da Crimeia. Plotnikov publicou uma foto segurando esta medalha (Figura 15) em maio de 2015.

Figura 15 – Plotnikov segura medalha Pelo Retorno da Crimeia

Fonte: captura de tela do autor (2022)

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 foças 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 16), várias caixas de munição 39x9mm são vistas.

Figura 16 – Caixa de munição em frame de reportagem



Fonte: Captura de tela do autor (2022)

Observa-se a marcação "9x39СПП", significando a variante SPP[16] do calibre 3x39mm. Também é observável 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; TSETSKOVA, 2016).

Ainda assim, como dito, a negação constante é característica das técnicas nas Zonas Cinzentas, para proteger a narrativa construída. Nos casos da infantaria, é relativamente fácil negar que eles estivessem sob suas ordens, afirmando 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. É possível e aconselhável, no caso, utilizar investigações e evidências sobre estes equipamentos em zonas de guerra que não os produzem, nem os importam.

4.2.2. Veículos militares russos em Donbas

A operação russa não se limitou ao envio de oficiais de inteligência para a formação de grupos separatistas, e nem ao envio de infantaria e seus veículos de suporte. Nos primeiros anos do conflito, Donbas esteve saturada com equipamento militar russo, principalmente[17]

16 Do russo "*Snaiperskiy, Povishennaya Probivaemos*", significando "Atirador de elite, penetração aumentada"
17 Excluindo veículos de transporte de infantaria.

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 boa evidência é o RB-341V Leer-3; um sistema de Guerra Eletrônica baseado em drones. Esse sistema é baseado no caminhão militar russo KamAZ, com a traseira modificada para transportar a cabine de operação, oferecendo mobilidade. O operador permanece no caminhão, enquanto um drone Orlan-10 é lançado, localizando fontes de sinais e sinais que se encaixem no padrão GSM[18]. A partir da localização, o sistema pode interferir nesse sinal, inviabilizando várias formas de comunicação, ou imitar sinais GSM, confundindo os sistemas de SIGINT do adversário, ou enviando informações falsas para seus receptores decodificarem. (DEAGEL, 2015; OE DATA INTEGRATION NETWORK, 2021)

Segundo as próprias fontes pró-Rússia, como a revista de conteúdo militar Military Review (2015), o Leer-3, visto na Figura 17, foi mostrado ao público pela primeira vez no início de outubro de 2015, na exposição do Dia da Inovação, que acontece no Distrito Militar do Sul. Segundo os especialistas da unidade de EW do Distrito Militar do Oeste, eles foram os primeiros a efetivamente usar o Leer-3, para tarefas de treinamento em outubro de 2015.

Figura 17 – 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, implicando que a Rússia conduziu os testes desse equipamento em condições reais de batalha, na Ucrânia. A evidência vem do líder do Esquadrão Viking, parte do primeiro Batalhão de Fuzileiros

18 O sistema 2G comumente usado pelos celulares e outros equipamentos móveis de comunicação.

Motorizados da DPR, Gennadiy Dubovoy (2015). Publicado no Youtube em 10 de maio de 2015, o vídeo (Figura 18) mostra soldados do esquadrão operando em Donetsk, e na marca dos 53 segundos é possível ver o Leer-3 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 18 – Vídeo propagandístico no YouTube

Fonte: Captura de Tela do autor (2020); Gennadiy Dubovoy (2015)

Este avistamento é somado a outros três, também documentados pelo InformNapalm (2016b) sobre o avistamento do Leer 3 em Donetsk. Como dito anteriormente, sistemas de Guerra Eletrônica são alguns dos veículos mais comuns no esforço russo de guerra indireta entre 2014 e 2021. Tratando-se de equipamentos recentes, não sendo produzidos em outros países, nem vendidos à Ucrânia, tornando-se úteis para demonstrar a participação russa no conflito. No entanto, é válido relembrar que equipamentos mais letais também foram utilizados na região, sendo necessário dedicar esforços de inteligência para identificá-los. 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 Ilovaysk.

Após uma série de vitórias retomadas de cidades no início da ATO, as forças ucranianas decidiram retomar a cidade de Ilovaysk, em Donetsk, começando em 7 de agosto de 2014. Após meses de violentas altercações, os separatistas e russos saíram vitoriosos em setembro de 2014, levando o governo ucraniano a mudar para uma estratégia defensiva na região. A derrota foi importante fator no processo de impasse do conflito, que solidificou as fronteiras, permanecendo relativamente inalteradas durante oito anos. Sua importância, no

entanto, vai além de provocar a mudança estratégica; foi vital no ponto de vista investigativo. (KORRESPONDENT, 2014)

Como dito, foi no período de setembro que os responsáveis pela ATO precisaram reconhecer a participação russa ativa em combates, dada sua presença crescente na região. Grande parte do crédito pela vitória separatista em Ilovaysk se deu exatamente pela participação de brigadas de tanques exclusivos da Rússia, como o T-90A e T-72B3, cercando os soldados ucranianos. 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; WALKER, 2019)

Sediada na Universidade de Londres, a FA é uma agência investigativa que integra o uso de arquitetura, modelagem 3D, inteligência artificial e fontes abertas nos seus estudos. Ela investiga violações de direitos humanos em vários aspectos; violência por forças policiais, militares e mesmo corporações (FA, 2010). Os investigadores atuam em parceria com equipes jurídicas, ONGs internacionais e organizações de mídia, 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 Ilovaysk apresentado em agosto de 2019, a FA aplicou princípios de Machine Learning[19] e Visão Computacional[20] a uma base de dados de fotos e vídeos capturados por agências de notícias cobrindo o conflito (incluindo agências russas), investigadores independentes e outras mídias em fontes abertas. Cerca de 300 veículos militares russos nas cidades de Ilovaysk e Lugansk foram identificados. As evidências e o processo investigativo foram publicados num site com um mapa interativo. No mapa, vários ícones apontam a geolocalização das fotos e vídeos da base de dados, e um filtro é disponibilizado, permitindo visualizar casos onde apenas infantarias russas foram vistas, apenas os veículos, ou os dois juntos. Também são oferecidos vídeos que expõem como foi determinado o modelo do veículo captado pelas câmeras, além de sua geolocalização (FA, 2019)

Grande exemplo oferecido pela FA é a identificação de um tanque de batalha

19 Segundo a IBM (2021) “machine learning é um ramo da inteligência artificial (IA) e da ciência da computação que se concentra no uso de dados e algoritmos para imitar a maneira como os humanos aprendem, melhorando gradualmente sua precisão.”

20 A IBM (2022) define Visão Computacional como uma área da IA “que permite que computadores e sistemas obtenham informações significativas a partir de imagens digitais, vídeos e outras entradas visuais (…) Se a IA permite que os computadores pensem, o Computer Vision permite que eles vejam, observem e compreendam.”

principal (MBT) diferente dos produzidos na Ucrânia. Trata-se do 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 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[21] (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, em agosto e setembro de 2014.

Identificar o tanque é relativamente fácil. O sistema OE Data Integration Network (ODIN), do Exército dos Estados Unidos (2022) demonstra que a nova versão buscava as vantagens do T-72, enquanto atualizou e adicionou componentes mais tecnológicos, como o Sosna-U e a blindagem Kontakt-5. O Sosna-U é um aparelho de visão panorâmica termal e diurna, adicionado ao lado do casco, num formato de caixa, enquanto o Kontakt-5 é uma armadura reativa explosiva, que “cobre” o casco do MBT com pequenos blocos, parecendo tijolos. Estes dois componentes se destacam bastante, como visto na Figura 19, tornando o 72B3 distinto do seu antecessor soviético.

Figura 19 – T-72B3 em exposição

Fonte: colagem pelo autor (2022) baseado em fotos de Kuzmin (2017)

21 É uma competição de tanques, parte dos Jogos Internacionais do Exército, um evento esportivo militar que o MDR promove entre parceiros e utilizadores de tanques russos, como Bielorrússia, Armênia e Kuwait. Os tanques passam por uma série de desafios de estabilidade, agilidade e acurácia.

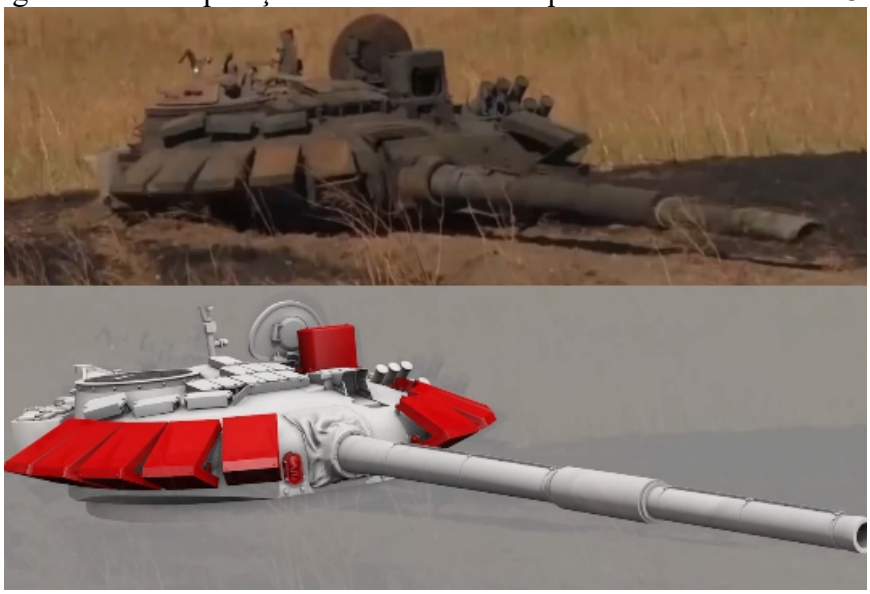
Contando com todas as fotos e vídeos em exposições e exercícios, a FA pôde desenvolver um modelo 3D para compará-lo com fotos do campo de batalha em Ilovainsk onde o tanque foi avistado. Utilizando qualquer software 3D, é possível posicionar câmeras virtuais no mesmo ângulo da foto, posicionando o MBT similarmente e comparando seus detalhes, para comprovar sua presença. Como demonstrado na Figura 20, a foto de um dos tanques capturados em Ilovainsk é comparada com o modelo 3D.

Figura 20 – Comparação entre foto em campo de batalha e modelo 3D

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

Destroços de tanques, 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 21 abaixo.

Figura 21 – 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. Ela coincide com as conclusões de Toler e Aksai (2015a, 2015b) no BellingCat, e duas outras investigações do InformNapalm (2015a, 2015b).

4.3. Repercussões internacionais

Tamanhas investigações e evidências seriam inúteis se não fossem direcionadas para organizações capazes de utilizá-las na tomada de decisões, sejam elas no âmbito legal, político ou estratégico. Por isso, serão apresentadas a presença destas investigações em diversas ocasiões. Destacam-se as diversas contribuições do InformNapalm no cenário internacional.

No dia 19 novembro de 2016, após atingir a marca de 75 unidades militares russas identificadas em Donbas, a comunidade 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. O material, que selecionou 165 incidentes, foi utilizado por delegados do Parlamento Ucraniano, numa apresentação na Assembleia Parlamentar da OTAN (NATO PA)[22]. (INFORMNAPALM, 2016c, UNIAN, 2016b). A apresentação das

22 Existente desde 1955, a AP é composta por 269 delegados dos 30 países membros da OTAN e de mais 11 países associados, incluindo a Ucrânia, Geórgia e países do Oriente Médio. Embora seja institucionalmente separada da organização, ela serve como um elo essencial entre ela e os parlamentos internos dos seus membros. É nela onde os membros especializados dos países trocam informações, discutem e decidem sobre os próximos passos da organização frente a problemas de segurança (NATO PA, [s.d]).

evidências, que ocorreu em Istambul, levou à seguinte conclusão da AP:

> "Está evidente que atualmente não existem condições para uma relação melhorada; que as prioridades da política externa da Rússia e os valores subjacentes a essas prioridades permanecem em conflito fundamental com os da OTAN. (…) Por meio de suas ações e retórica, a Rússia continua a desestabilizar o ambiente de segurança europeu e a minar a estabilidade da qual depende a segurança da Aliança." (NATO PA, 2016, tradução nossa) [23]

Os delegados da AP também afirmaram que, dada a permanência da Rússia no leste da Ucrânia, as sanções já aplicadas deveriam ser reforçadas e reafirmadas, numa forte e coletiva mensagem a Vladimir Putin (NATO PA, 2016). As investigações foram importantes para demonstrar à Europa que, mesmo com o relativo congelamento do conflito após as batalhas de 2014, a presença russa não diminuiu. De fato, ela continuava aumentando; um número crescente de sistemas tecnológicos, ofensivos e de suporte, eram transportados, pouco a pouco, dificultando as chances de retomada do território. Em conclusão, serviram para o fortalecimento de sanções e renovação da atenção da OTAN ao conflito.

Em relação à capacidade de identificar e reportar a presença destes equipamentos, o InformNapalm foi importante contribuinte para a Organização para Segurança e Cooperação na Europa (OSCE). Considerada a maior organização intergovernamental orientada para a segurança regional, e um dos parceiros mais próximos às Nações Unidas, a OSCE conta 57 membros da Europa, Ásia e América do Norte, incluindo competidores no contexto da Segurança Internacional, como Armênia e Azerbaijão, Rússia, Bielorrússia, Ucrânia e Turquia (OSCE, 2014, 2017). Em suas missões, ela aconselha e observa membros em questões como controle de armas, promoção dos direitos humanos, liberdade de imprensa e observação de eleições livres e justas (OSCE, [s.d]). Uma das missões mais importantes da organização na região europeia é a Missão Especial de Monitoramento na Ucrânia (SMM).

Uma SMM é uma missão internacional de observadores civis cujo objetivo é ajuda na desescalada de tensões e promoção de paz em zonas de conflito. Para isso, os observadores, contratados de vários países membros, são enviados para prédios administrativos no local, e realizam patrulhas na região, a pé ou utilizando equipamentos como drones, outros veículos ou câmeras estáticas. Para desescalar o conflito, a missão estabelece contato com o governo local, as partes envolvidas no conflito, grupos religiosos, étnicos ou civis, além de organizar encontros com os diferentes lados do conflito, para firmar

23 "It is clear that conditions for an improved relationship currently do not exist; that Russia's foreign policy priorities and the values underpinning these priorities remain in fundamental conflict with those of NATO. (…) Through its actions and rhetoric, Russia continues to unsettle the European security environment and undermine the stability upon which Alliance security depends"

acordos. Na Ucrânia, a SMM foi implantada em Donbas após um pedido do governo da Ucrânia à OSCE, seguida de uma decisão consensual dos membros, durando exatos 8 anos; começando em março de 2014, e terminando com a invasão em larga escala, em março de 2022. Os mais de 700 observadores se dedicavam principalmente à documentação dos equipamentos russos e ucranianos, as violações de cessar-fogo de ambos os lados, e ocasionais altercações utilizando armamento proibido por acordos ou leis internacionais, em relatórios diários.

Vários dos equipamentos russos observados pela SMM haviam sido identificados pela InformNapalm anteriormente, e serviram de fonte para a missão da Ucrânia na OSCE. De forma recíproca, várias das documentações do SMM foram analisadas pela InformNapalm, validando a identificação dos equipamentos. Há, por exemplo, a identificação do 51U6 Kasta-2E1; veículo de SIGINT e ELINT russo projetado especificamente para detectar alvos no ar, incluindo drones (INFORMNAPALM, 2021; OSCE, 2021). A identificação pela SMM foi seguida de uma análise e geoloalização pela InformNapalm, que então serviu de base para denúncias formais ucranianas (UKRINFORM, 2021). Há também o caso da já mencionada identificação do Leer-3 em Donetsk, pelo InformNapalm, em 2015 e 2016. Três anos depois, ela foi confirmada pela SMM, em duas observações diferentes, também em Donetsk (OSCE, 2019a, 2019b).

Outra importante contribuição internacional do OSINT, desta vez no aspecto legal, vem da FA. Em setembro de 2018, o Centro Europeu de Advocacia pelos Direitos Humanos (EHRAC) comissionou a agência para ajudar no seu caso. O EHRAC estava representando representar 25 combatentes voluntários do Batalhão Donbas, da Ucrânia. Eles participaram da batalha de Ilovaisk, e foram detidos por soldados russos em agosto de 2014. Até serem soltos, como parte de troca de prisioneiros em dezembro de 2014, eles sofreram violência física, verbal e psicológica, como ameaças de execução; uma violação do Artigo 3.º da Convenção Europeia de Direitos Humanos (EHRAC, 2018). Dado que os “separatistas” não carregavam insígnias, não eram ucranianos e a Rússia negava qualquer envolvimento, era difícil atribuir a responsabilidade pelos atos a um mandante maior, impossibilitando a execução da justiça. A Ucrânia, por outro lado, era incapaz de representar seus soldados ou promover qualquer reparação após os danos (EHRAC, 2019).

Para resolver este dilema e atestar a responsabilidade das partes, o EHRAC contratou a FA para reunir e apresentar evidências da presença militar russa em Ilovaisk e seus

arredores, entre agosto e setembro de 2014, provando a responsabilidade da russa pelas violações cometidas pelos seus soldados regulares. 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 (ECHR, 2017).

Muito embora o caso pareça estar “congelado”, o procedimento é de fato longo e burocrático, o uso de fontes abertas para a coleta de evidências significa um grande passo na sua rapidez. Sua utilização, como reiterado diversas vezes, evita um processo moroso de investigações e coletas presenciais de evidências e testemunhas que, dado o tempo corrido, provavelmente não são mais acessíveis. Neste caso, a investigação da FA em 2019 foi importante para o reconhecimento legal das evidências em fontes abertas.

A maior conquista do uso de OSINT nas relações internacionais, no entanto, está no veredito expedido pelo tribunal distrital de Haia[24], em novembro de 2022 (RANKIN, 2022, CASERT & CORDER, 2022). Trata-se da sentença de três acusados pelo assassinato das 298 pessoas a bordo do voo MH17. O avião civil, que saía da Holanda em direção à Malásia, foi abatido por um sistema antiaéreo BUK M1 pertencente à Rússia, quando sobrevoava o território controlado pela DPR, em 17 de julho de 2014. As investigações começaram logo após, com cerca de 200 investigadores de todo o mundo. O julgamento começou em março de 2020, e após dois anos, o veredito condenou à prisão perpétua o separatista ucraniano Leonid Kharchenko, e dois russos; Sergey Dubinskiy e Igor Girkin, comandante da DPR que liderou a tomada de Sloviansk em 2014, já mencionado neste trabalho.

Entre os esforços forenses, parte significativa na definição de que sistema antiaéreo foi utilizado, e quais pessoas estavam envolvidas na derrubada do avião foi a utilização de OSINT. O trabalho dos investigadores do BellingCat (2017, 2019) se destaca. Fundado pelo jornalista investigativo Eliot Higins, a agência utiliza fontes abertas para investigar abusos contra direitos humanos e participação de governos em conflitos no exterior, tendo investigações na Síria, Iêmen, Ucrânia, Armênia, Azerbaijão e outros. A agência aglutinou evidências da presença do sistema BUK M1 nas imediações do incidente, o número de série do sistema antiaéreo, a identidade e fotos de vários membros da DPR envolvidos na pilhagem dos corpos e destroços do avião.

5. CONSIDERAÇÕES FINAIS

24 Não confundir com o Tribunal Penal Internacional ou com a Corte Internacional de Justiça. Embora não seja um tribunal penal permanente, o tribunal distrital de Haia também tem experiência com casos internacionais relacionados a violações de Direitos Humanos e leis de guerra.

Embora a Rússia não reconheça a jurisdição da corte holandesa sobre cidadãos russos, assim como não reconheceu relatórios da OSCE, que escancaravam sua participação em Donbas, sua capacidade de negar responsabilidade está ameaçada. Como dito no capítulo anterior, 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.

É observável que a literatura contemporânea no tema de OSINT em relações internacionais, especialmente na área de defesa, é extensivamente abordado nos Estados Unidos. Não é um espanto pois, como exposto no primeiro capítulo, embora os EUA tenham considerável domínio nas capacidades tradicionais, deixou de lado a atenção aos desdobramentos tecnológicos do OSINT, como demonstra o Center for Strategic and International Studies (2021). Este tópico também parece não ter chamado a atenção da literatura de outros países, e dos autores de Relações Internacionais, embora seja um desdobramento relevante para área.

Cabe ressaltar que o uso de OSINT não se limita à área de Estudos Estratégicos. Embora este seja o foco do trabalho, o uso de OSINT é cada vez mais presente em Organizações Internacionais, governamentais ou não, dedicadas à proteção de Direitos Humanos. Esta tendência se verifica principalmente em conferências recentes da ECHR (2021). Na introdução do evento, demonstra-se que, nos últimos anos, houve um crescimento de casos de pedidos interestatais sobre violações dos Direitos Humanos. O aumento foi um grande desafio em relação à determinação dos fatos, de complexas noções jurídicas, que esbarram em legislações internas e internacionais, o que torna ainda mais fatigante um processo naturalmente moroso.

Relatando as experiências, no entanto, a ECHR demonstra a habilidade do OSINT em coletar evidências para a determinação de fatos, sem esbarrar em problemas de jurisdição, reduzindo a lentidão do processo e oferecendo uma coleção mais imparcial de dados. Como exemplo, o ECHR avalia o uso de investigações do BellingCat em casos de violações dos

Direitos Humanos no Oriente Médio. Além disso, outros temas que tangem as relações internacionais, como questões climáticas e históricas podem ser explorados (BALLINGER & ZWIJNENBURG, 2021; FA, 2022; POSTMA, 2021). 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.

AID, M. M.; WIEBES, C. **Introduction on The Importance of Signals Intelligence in the Cold War.** Intelligence and National Security, v. 16, n. 1, p. 1–26, mar. 2001.

ARMSTRONG, K. **Campos de sangue**. [S.l.]: Editora Companhia das Letras, 2016.

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.

ASSYMETRIC WARFARE GROUP STUDY. **Russian Private Military Companies**. [S.l.]: [s.n.], 2020. Disponível em: https://info.publicintelligence.net/AWG-RussianPrivateMilitaryCompanies.pdf. Acesso em: nov. 2022.

BALLINGER, O.; ZWIJNENBURG, W. What Oil, Satellite Technology and Iraq Can Tell Us about Pollution. **BellingCat**, 15 abr. 2021. Disponível em: https://www.bellingcat.com/resources/2021/04/15/what-oil-satellite-technology-and-iraq-can-tell-us-about-pollution/.

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: 1º 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.

BELLINGCAT. MH17 - the Open Source Investigation, Three Years Later. **BellingCat**, 17 jul. 2017. Disponível em: https://www.bellingcat.com/news/uk-and-europe/2017/07/17/mh17-open-source-investigation-three-years-later/.

_____. Identifying the Separatists Linked to the Downing of MH17 - Bellingcat. **BellingCat**, 19 jun. 2019. Disponível em: https://www.bellingcat.com/news/uk-and-europe/2019/06/19/identifying-the-separatists-linked-to-the-downing-of-mh17/.

BOAZ, C. *et al.* **Study Guide**. [S.l.]: [s.n.], 2010. Disponível em: https://www.nonviolent-conflict.org/wp-content/uploads/2016/02/Orange-Revolution-Study-Guide-2.pdf.

BRISTOW, M. China's internet "spin doctors". **news.bbc.co.uk**, [S.l.], 16 dez. 2008. Disponível em: http://news.bbc.co.uk/2/hi/asia-pacific/7783640.stm.
CAMOPEDIA. Russia. **CamoPedia**, 2022. Disponível em: https://www.camopedia.org/index.php/Russia.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. **Maintaining The Intelligence Edge**: Reimagining and Reinventing Intelligence through Innovation. [S.l.]: [s.n.], 2021. Disponível em: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf.

CENTRAL INTELLIGENCE AGENCY. Ukraine - The World Factbook. **Central Intelligence Agency**, 2022. Disponível em: https://www.cia.gov/the-world-factbook/countries/ukraine/. Acesso em: 1º dez. 2022.

CHAMBERS, J. **An Analysis of Russia's "New Generation Warfare" and Implications for the US Army:** countering gray-zone hybrid threats. [S.l.]: [s.n.], 2016. Disponível em: https://mwi.usma.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf. Acesso em: 1º dez. 2022.

COHEN, A.; HAMILTON, R. **The Russian military and the Georgia war:** lessons and implications. Carlisle, Pa: Strategic Studies Institute, U.S. Army War College, 2011.

CORDER, M.; CASERT, R. 3 Convicted in 2014 Downing of Malaysian Jet over Ukraine. **AP News**, 17 nov. 2022. Disponível em: https://apnews.com/article/russia-ukraine-business-kuala-lumpur-malaysia-netherlands-099084a82b49b77b116878e24fc63a18. Acesso em: 20 nov. 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.

DAWSON, B. China is using a stealth fleet of fishing boats and ferries to boost its naval power, say military experts. **Business Insider**, 2022. Disponível em: https://www.businessinsider.com/china-stealth-fleet-fishing-boats-ferries-boost-sea-power-experts-2022-9. Acesso em: 1º dez. 2022.

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

_____. Ratnik. **Deagel**, 2022. Disponível em: https://www.deagel.com/Cannons%20&%20Gear/Ratnik/a002427. Acesso em: 1º dez. 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.

ECHR. Yosyp Vasylyovych PONOMARENKO against Ukraine and Russia and 19 Other Applications. **HUDOC Database**, 28 ago. 2017. Disponível em: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%2260372/14%22],%22itemid%22:[%22001-177144%22]}.

EUROPARL. Russia's war on Ukraine: Timeline of cyber-attacks | Think Tank | European Parliament. **www.europarl.europa.eu**, 21 jun. 2022. Disponível em: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549. Acesso em: dez. 2022.

EUROPEAN HUMAN RIGHTS ADVOCACY CENTRE. EHRAC Instructs Forensic Architecture in Case concerning Conflict in Eastern Ukraine. **EHRAC**, 1 set. 2018. Disponível em: https://ehrac.org.uk/en_gb/ehrac-new-project-forensic-architecture-conflict-eastern-ukraine/. Acesso em: nov. 2022.

_____. 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.

FIELDING, N.; COBAIN, I. Revealed: US spy operation that manipulates social media. **The Guardian**, [S.l.], 17 mar. 2011. Disponível em: https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks. Acesso em: 1º dez. 2022.

FIRST Il-76 planes with Russian peacekeepers depart for Karabakh. **TASS**, [S.l.], 10 nov. 2020. Disponível em: https://tass.com/defense/1221795. Acesso em: 2 dez. 2022.

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.

FRIEDMAN, G. Ukraine: on the Edge of Empires. **Stratfor**, 17 dez. 2013. Disponível em: https://worldview.stratfor.com/article/ukraine-edge-empires. Acesso em: 1º 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.

GEOEYE-1 satellite. **Apollo Mapping**. 2002. Disponível em: https://apollomapping.com/geoeye-1-satellite-imagery. Acesso em: 20 set. 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.

GRAND VIEW RESEARCH. **Satellite Data Services Market Size, Industry Report, 2020-2027.** 2020. Disponível em: https://www.grandviewresearch.com/industry-analysis/satellite-data-services-market Acesso em: 11 out. 2022

GRAPHIKA. **Cross-Platform Spam Network Targeted Hong Kong Protests**. [S.l.]: [s.n.], 2019. Disponível em: https://public-assets.graphika.com/reports/graphika_report_spamouflage.pdf. Acesso em: 2022.

_____. **Return of the (Spamouflage) Dragon**. **Graphika**. [S.l.]: [s.n.], 2020. Disponível em: https://public-assets.graphika.com/reports/Graphika_Report_Spamouflage_Returns.pdf. Acesso em: 2022.

_____. **Spamouflage Breakout Chinese Spam Network Finally Starts to Gain Some Traction**. [S.l.]: [s.n.], 2021a. Disponível em: https://public-assets.graphika.com/reports/graphika_report_spamouflage_breakout.pdf. Acesso em: 2022.

_____. Posing as Patriots. **Graphika**, 7 jun. 2021b. Disponível em: https://public-assets.graphika.com/reports/graphika_report_posing_as_patriots.pdf. Acesso em: 2022.

_____. **UNHEARD VOICE Evaluating five years of pro-Western covert influence operations**. [S.l.]: [s.n.], 2022. Disponível em: https://public-assets.graphika.com/reports/graphika_stanford_internet_observatory_report_unheard_voice.pdf. Acesso em: nov. 2022.

GREENWALD, G. The NSA's mass and indiscriminate spying on Brazilians. **The Guardian**. 2013. Disponível em: https://www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying. Acesso em: 10 mar. 2020

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

HERN, Alex. Fitness tracking app Strava gives away location of secret US army bases. **The Guardian**, 2018. Disponível em: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases. Acesso em: 15 ago. 2020

HICKS, K. *et al.* **CAMPAIGNING IN THE GRAY ZONE**. [S.l.]: [s.n.], 2019. Disponível em: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_GrayZone_interior_v4_FULL_WEB_0.pdf. Acesso em: ago. 2022.

HUGHES, G. **My enemy's enemy : proxy warfare in international politics**. Brighton ; Portland: Sussex Academic Press, 2014.

HUMANS RIGHT WATCH. Ukraine: Excessive Force Against Protesters. **Human Rights Watch**, 3 dez. 2013. Disponível em: https://www.hrw.org/news/2013/12/03/ukraine-excessive-force-against-protesters.

INFORMNAPALM. International Volunteer Community InformNapalm. **INFORMNAPALM**, 2014. Disponível em: https://informnapalm.rocks/. Acesso em: nov. 2022.

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

_____. "Tank Biathlon 2014" of the Russia's 6th Tank Brigade in Donbas. **InformNapalm**, 18 ago. 2015b. Disponível em: https://informnapalm.org/en/tank-biathlon-2014-of-the-russia-s-6th-tank-brigade-in-donbas/. Acesso em: 2 dez. 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.

_____. InformNapalm's proofs of Russian military aggression presented during NATO PA. **InformNapalm**, 19 nov. 2016c. Disponível em: https://informnapalm.org/en/75-russian-military-units-fight-donbas/. Acesso em: nov. 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.

INTERFAX-UKRAINE. Yushchenko: Ukraine has every chances to be European Union member - Oct. 16, 2009. **Kyiv Post**, 16 out. 2009. Disponível em: https://www.kyivpost.com/article/content/ukraine-politics/yushchenko-ukraine-has-every-chances-to-be-europea-50824.html.

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

INTRODUCTION to Open Source Intelligence (OSINT) Gathering, **Sec Juice,** 2018. Disponível em: https://www.secjuice.com/introduction-to-open-source-intelligence-osint/ Acesso em: 02 ago. 2020

JAITNER, M.; MATTSSON, P. A. Russian Information Warfare of 2014. *In*: **7TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT, 2015,** . Anais..., 2015. p. 39–48.

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.

KNIGHT, A. W. **How the Cold War began:** the Igor Gouzenko Affair and the hunt for Soviet spies. Nova York: Publishers Group West, 2005.

KOFMAN, M. *et al.* **Lessons from Russia's Operations in Crimea and Eastern Ukraine**. [S.l.]: RAND Corporation, 2017.

KOMMERSANT. Pervuyu mirotvorcheskuyu brigadu poselyat pod Samaroy. **Kommersant.RU**, 23 out. 2004. Disponível em: https://www.kommersant.ru/doc/518875.

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.

KUZIO, T. Oligarchs, Tapes and Oranges: "Kuchmagate" to the Orange Revolution. **Journal of Communist Studies and Transition Politics**, mar. 2007. v. 23, n. 1, p. 30–56.

KUZMIN, V. T-72B3 main battle tank walkaround. **Vitalykuzmin**, 2017. Disponível em: https://www.vitalykuzmin.net/Military/T-72B3-walkaround/i-gn2BRbS/A. Acesso em: nov. 2022.

LALLY, K.; ENGLUND, W.; BOOTH, W. Russian Parliament Approves Use of Troops in Ukraine. **Washington Post**, [S.l.], 1 mar. 2014. Disponível em: https://www.washingtonpost.com/world/europe/russian-parliament-approves-use-of-troops-in-crimea/2014/03/01/d1775f70-a151-11e3-a050-dc3322a94fa7_story.html.

LEACH, P. Enhancing Fact-finding in Inter-State Cases. *In*: INTER-STATE CASES UNDER

THE EUROPEAN CONVENTION ON HUMAN RIGHTS, 2021, Berlim. **Anais**... Berlim: [s.n.], 2021. p. 75–78.

LOWENTHAL, M. M. **Intelligence: from Secrets to Policy**. Washington, Dc: Cq Press, 2011.

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.

MUMFORD, A. **Proxy warfare:** war and conflict in the modern world. Cambridge: Polity Press, 2013.

NATIONAL RESEARCH COUNCIL. **Priorities for GEOINT Research at the National Geospatial-Intelligence Agency**. Washington, D.C.: National Academies Press, 2006.
NATO. **NATO OSINT Handbook**. [S.l.]: NATO, 2002.

_____. Member countries. **NATO**, 2018. Disponível em: https://www.nato.int/cps/en/natohq/topics_52044.htm.

NATO PA. NATO PA Urges United Stance on Russia, Support for Ukraine. **NATO PA**, 19

nov. 2016. Disponível em: https://www.nato-pa.int/news/nato-pa-urges-united-stance-russia-support-ukraine. Acesso em: nov. 2022.

_____. How We Work. **NATO PA**, [s.d.]. Disponível em: https://www.nato-pa.int/content/how-we-work. Acesso em: 2 dez. 2022.

NOGUEIRA, J. P.; MESSARI, N. **Teoria das relaçoes internacionais**. 1. ed. Rio de Janeiro: Elsevier, 2005.

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

O QUE é Computer Vision? **IBM**, 2022. Disponível em: https://www.ibm.com/br-pt/topics/computer-vision. Acesso em: nov. 2022.

O QUE é machine learning? **IBM**, 2021. Disponível em: https://www.ibm.com/br-pt/cloud/learn/machine-learning. Acesso em: nov. 2022.

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.

ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE. Where we are. **OSCE**, 21 mar. 2014. Disponível em: https://www.osce.org/where-we-are.

_____. What Is the OSCE? **YouTube**, 14 nov. 2017. Disponível em: https://www.youtube.com/watch?v=KRYMwpQ44X0. Acesso em: ago. 2020.

_____. Latest from the OSCE Special Monitoring Mission to Ukraine (SMM), Based on Information Received as of 19:30, 3 April 2019. **OSCE**, 4 abr. 2018. Disponível em: https://www.osce.org/special-monitoring-mission-to-ukraine/416273. Acesso em: 2 dez. 2022.

_____. Latest from the OSCE Special Monitoring Mission to Ukraine (SMM), Based on Information Received as of 19:30, 4 April 2019. **OSCE**, 5 abr. 2019. Disponível em: https://www.osce.org/ru/special-monitoring-mission-to-ukraine/416450. Acesso em: 2 dez. 2022.

_____. OSCE Special Monitoring Mission to Ukraine (closed). **OSCE**, [s.d.]. Disponível em: https://www.osce.org/special-monitoring-mission-to-ukraine-closed.

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.

PACE. Viktor Yuschenko Speech Made to the Assembly. **Parliamentary Assembly of the Council of Europe**, 25 jan. 2005. Disponível em: http://www.assembly.coe.int/nw/xml/Speeches/Speech-XML2HTML-EN.asp?SpeechID=253. Acesso em: nov. 2022.

PAGANINI, P. Crimea – The Russian Cyber Strategy to Hit Ukraine. **Infosec Resources**, 24 mar. 2014. Disponível em: https://resources.infosecinstitute.com/topic/crimea-russian-cyber-strategy-hit-ukraine/. Acesso em: nov. 2022.

PLOTNIKOV, Nikolai. Kak ya provel leto 2014. **VKontakte**. 2014. Disponível em: https://vk.com/video241882719_ 170716755. Acesso em: 23 nov 2022.

PLOTNIKOV, N. Perfil. **VKontakte.** 2022. Disponível em: https://vk.com/nikolay1562. Acesso em: 20 nov. 2022.

PONOMARENKO, I.; CHERNICHKIN, K. "Welcome to hell": Ukrainian Airborne Fighting Russia in Donbas Woods. **The Kyiv Independent**, [S.l.], 27 maio. 2022. Disponível em: https://kyivindependent.com/national/welcome-to-hell-ukrainian-airborne-fighting-russia-in-donbas-woods. Acesso em: 2 dez. 2022.

POSTMA, F. How Instagram Celebrities Promote Dubai's Underground Animal Trade. **BellingCat**, 8 fev. 2021. Disponível em: https://www.bellingcat.com/news/mena/2021/02/08/how-instagram-celebrities-promote-dubais-underground-animal-trade/

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

RANKIN, J. Three Men Found Guilty of Murdering 298 People in Shooting down of MH17. **The Guardian**, 17 nov. 2022. Disponível em: https://www.theguardian.com/world/2022/nov/17/three-men-found-guilty-of-murdering-298-people-in-flight-mh17-bombing. Acesso em: 20 nov. 2022.

ROTH, A. Ukraine's ex-president Viktor Yanukovych Found Guilty of Treason. **The Guardian**, 25 jan. 2019. Disponível em: https://www.theguardian.com/world/2019/jan/25/ukraine-ex-president-viktor-yanukovych-found-guilty-of-treason.

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/.

SCHWARTZ, M. Who Killed the Kyiv Protesters? A 3-D Model Holds the Clues. **The New York Times**, 30 maio. 2018. Disponível em: https://www.nytimes.com/2018/05/30/magazine/ukraine-protest-video.html.

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/new-atlanticist/todays-wars-are-fought-in-the-gray-zone-heres-everything-you-need-to-know-about-it/.

STEINFELD, J. The new "civil service" trolls who aim to distract: The government in China is using its civil servants to act as internet trolls. It's a hard management task generating 450 million social media posts a year. **Index on Censorship**, dez. 2018. v. 47, n. 4, p. 102–104.

TOKMAK, E. China's Naval Fusion Strategy: Civilian Ships. **ANKASAM | Ankara Kriz ve Siyaset Araştırmaları Merkezi**, 3 out. 2022. Disponível em: https://www.ankasam.org/chinas-naval-fusion-strategy-civilian-ships/?lang=en. Acesso em: 1º dez. 2022.

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.
TRADOC. **FM 2-0: Intelligence**. [S.l.]: US Army, 2002.

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

_____. **TC 2-22.7: Geospatial Intelligence Handbook**. [S.l.]: Us Army, 2011.

TSVETKOVA, M. Special Report: Russian fighters, Caught in Ukraine, Cast Adrift by Moscow. **Reuters**, 18 abr. 2016. Disponível em: https://www.reuters.com/article/us-ukraine-crisis-captured-specialreport-idUSKBN0OE0YE20150529. Acesso em: nov. 2022.

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

UKRAINSKA PRAVDA. How Yanukovich Forged the Elections. **Ukrainska Pravda**, 24 nov. 2004. Disponível em: https://web.archive.org/web/20051223004354/http://www2.pravda.com.ua/en/archive/2004/november/24/4.shtml. Acesso em: ago. 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.

_____. New Evidence Emerges of Russian Role in Ukraine Conflict. **The Guardian**, 18 ago. 2019. Disponível em: https://www.theguardian.com/world/2019/aug/18/new-video-evidence-of-russian-tanks-in-ukraine-european-court-human-rights?CMP=twt_a-world_b-gdnworld. Acesso em: nov. 2022.

WISE, D. Thirty Years Later, We Still Don't Truly Know Who Betrayed These Spies. **Smithsonian**, 21 out. 2015. Disponível em: https://www.smithsonianmag.com/history/still-unexplained-cold-war-fbi-cia-180956969/.

WOMACK, H. One election, Two Viktors. Will Ukrainians Accept results? **Christian Science Monitor**, 23 nov. 2004. Disponível em: https://www.csmonitor.com/2004/1123/p05s01-woeu.html. Acesso em: 2 dez. 2022.

YOULA. Zhilet Razgruzochnyy YEMR 6sh117 Starshiy Strelok. **Youla.Ru**, 2020. Disponível em: https://youla.ru/all/sport-otdyh/ohota-rybalka/zhiliet-razghruzochnyi-6sh117-starshii-strielok-5e8dbca4aaab287f0c4468b3. Acesso em: nov. 2022.