Investigações e Inteligência Digital na Guerra na Ucrânia

Kevin Limonier

Professor de geografia e estudos eslavos no Institut Français de Géopolitique (Université Paris 8). Especialidade(s): Rússia, ciberespaço de língua russa, ciência e tecnologia na ex-URSS, cartografia, OSINT

Marie-Gabrielle Bertran

Doutoranda noInstitut Français de Géopolitique (Université Paris 8), especialista em desenvolvimento de software na Rússia. Mestre em Geopolítica (Institut Français de Géopolitique, Université Paris 8) e em Filosofia (Paris IV - Sorbonne).

Tradução de Carolina Salomão

Em junho de 2022, o jornalista belga Brecht Castel publicou no jornal flamengo Knack uma extensa investigação para explicar como, dois meses antes, o exército russo teria sido capaz de atingir um alvo estratégico ucraniano graças a uma "investigação OSINT"[1]. Segundo ele, o exército russo teria conseguido localizar, a partir de imagens de uma reportagem de televisão, uma oficina ucraniana de reparação de tanques capturados. Mais do que a própria investigação, são os métodos de sua realização que chamam a atenção. A análise cruzada dos dados e das imagens não teria sido realizada pelo serviço de inteligência militar russo, mas por indivíduos anônimos reunidos em um canal do Telegram chamado *Rybar* ("pescador", em russo), do qual falaremos mais adiante. O trabalho de investigação parece ter sido conduzido fora das estruturas do Estado, em uma rede social, por pessoas não identificadas, em um ambiente que parece ser participativo. Este modelo, aliás, não é exclusivo dos russos. Do lado ucraniano, existem numerosas iniciativas participativas e de código aberto para, por exemplo, relatar movimentos de tropas ou reunir evidências de massacres de civis para futuros julgamentos perante a justiça internacional.

Muito mais do que uma ruptura, essa nova forma de coletar informações sobre a guerra é o resultado de um processo que começou no início dos anos 2010, quando o desenvolvimento simultâneo das redes sociais, por um lado, e da internet móvel, por outro, multiplicou os sensores que permitem registrar, na forma de pegadas digitais, instantâneos do que está ocorrendo no ambiente direto do dispositivo e do seu usuário. Os conjuntos de dados gerados por esses sensores cada vez mais numerosos rapidamente permitiram revelar algumas informações ocultas, muitas vezes por simples processos de coleta, análise e cruzamento de pegadas disponíveis em fontes abertas. Esta abordagem investigativa, que reúne um conjunto heterogêneo de práticas de contornos difusos, rapidamente foi designada pelo nome de OSINT, acrônimo para *Open Source Inteligence*, ou inteligência de código aberto.

[1] www.knack.be/nieuws/wereld/hoe-oekraiense-journalisten-onbedoeld-een-russische-raketaanval-hielpen-lanceren

A zona pós-soviética (e mais especificamente a Rússia) se mostrou desde cedo um terreno particularmente propício para tais abordagens. Elas foram inicialmente utilizadas por diversos coletivos e ativistas para denunciar a corrupção e o autoritarismo. Assim, desde os anos 2000, surgiram bases de dados online que permitem aos cidadãos investigarem por si próprios casos de nepotismo[2] ou denunciarem de forma participativa crimes como fraudes eleitorais. Em 2014, a Revolução Maidan, a anexação da Crimeia e o início da guerra civil no Donbass permitiram que essas práticas invadissem o campo da geopolítica externa e dos conflitos internacionais. Assim, diversas investigações demonstraram, através da análise de fotos postadas nas redes sociais, o envolvimento direto do exército russo com os separatistas do Donbass, ao contrário das afirmações de Moscou[3]. Muito mais espetacular, a investigação que provou a culpabilidade da Rússia na destruição do avião MH17 marcou uma virada, pois permitiu que o OSINT emergisse como uma abordagem investigativa capaz de influenciar as relações de poder internacionais e desmascarar os relatos propagados por uma grande potência[4]. Desde então, as investigações e contra-investigações se multiplicaram na Rússia, onde os requisitos legais de retenção de dados e a corrupção na administração levam a disponibilizar muitos bancos de dados no mercado negro[5]. Foi assim que, através de manifestos de voo[6] obtidos na *dark web,* o círculo próximo de Alexei Navalny conseguiu identificar seus envenenadores do FSB, notando que os mesmos três nomes apareciam

[2] Um exemplo é o site antikompromat.ru, que reunia milhares de artigos e diversos recursos sobre corrupção e clientelismo em todos os níveis do poder russo. Este site foi fundado pelo politólogo e ativista Vladimir Pribylovski, que foi encontrado morto em sua casa em 2016.

[3] Paul Szoldra, "Sem perceber, soldados russos estão provando que Vladimir Putin está mentindo sobre o leste da Ucrânia", Business Insider, 1 de agosto de 2014, www.businessinsider.com/russian-soldiers-social-ukraine-2014-7?r=US&IR=T

[4] Consulte o site do Conselho de Segurança Holandês, responsável pela investigação: www.onderzoeksraad.nl/en/page/3546/mh17-crash-17-juli-2014

[5] Consulte o site https://fsb.dossier.center/report

[6] Uma lista de todos os passageiros que se acredita estarem a bordo de um avião no momento da decolagem, excluindo os membros da tripulação. Esta lista inclui os números dos bilhetes dos passageiros e informações sobre suas identidades.

constantemente nas listas de passageiros de todos os voos que ele havia feito durante dois anos[7].

Mais do que uma ruptura, a guerra na Ucrânia iniciou uma mudança de escala no uso de investigações digitais. O volume de investigações empreendidas, tanto por jornalistas experientes quanto por anônimos nas redes sociais, explodiu. Isso se deve em parte ao fato de que a guerra que atualmente assola a Ucrânia é o primeiro conflito de alta intensidade que ocorre em uma área com uma alta taxa de penetração da internet (67,6% em 2021[8]), onde as infraestruturas digitais foram em grande parte poupadas pelos beligerantes - exceto nos locais sitiados como Mariupol. Portanto, a Ucrânia constitui um teatro de operações "conectado" no sentido em que as manobras, ataques e atrocidades são documentados quase em tempo real, fornecendo aos beligerantes um volume considerável de dados passíveis de serem analisados, cruzados e interpretados para otimizar as estratégias de controle territorial em tempos de guerra.

OSINT como técnica de inteligência de guerra

O OSINT emerge hoje na Rússia como uma nova ferramenta de inteligência a serviço das forças armadas russas. Ele é implementado por diversos atores aparentemente independentes, que se autodenominam patriotas e parecem apoiar voluntariamente a realização de certas manobras militares russas, incluindo até mesmo ataques de mísseis tão destrutivos. O trabalho desses "*OSINTers*", que se organizam em comunidades na internet para realizar suas pesquisas a partir de dados publicamente disponíveis online, pode permitir que os serviços de inteligência terceirizem investigações e obtenham diretamente os resultados alcançados. A integração e o uso explícito desses resultados pelas forças armadas russas representam uma economia de tempo para os serviços de inteligência e uma economia financeira para as autoridades que se beneficiam das informações fornecidas voluntariamente pelos investigadores. Seguindo essa nova

[7] Aric Toler, "Caçando os caçadores: como identificamos os perseguidores do FSB de Navalny", Bellingcat, 14 de dezembro de 2020, www.bellingcat.com/resources/2020/12/14/navalny-fsb-methodology

[8]

dinâmica, as comunidades de pesquisadores em OSINT começam a ganhar importância e acabam se tornando parte integrante do aparato de inteligência civil e militar na Rússia.

O caso do ator independente Russian OSINT (@Russian_OSINT no Twitter desde setembro de 2019) é a ilustração perfeita disso. Este investigador russo inicialmente publicou ferramentas disponíveis em código aberto e métodos de investigação para os internautas no Twitter, antes de anunciar sua saída da plataforma americana em 11 de março de 2022 e convidar seus seguidores a segui-lo na plataforma russa Telegram[9]. Desde sua saída do Twitter, ele faz parte dos criadores de conteúdo no Telegram que foram reconhecidos pelo KILLNET, um grupo de hackers que defende os interesses do Estado russo[10], como um apoio ao esforço de guerra[11]. Parece que o anúncio da guerra na Ucrânia levou este ator a empregar suas habilidades em OSINT a serviço das autoridades russas no contexto do conflito.

Além dos atores que surgiram nos anos que antecederam a guerra, novos grupos de investigadores russos se formaram diretamente relacionados ao conflito, como o grupo por trás do canal Telegram *Rybar*. Este grupo conduz investigações a partir de imagens de satélite e dados disponíveis em fontes abertas, GEOINT (Inteligência Geoespacial[12]), para permitir que o exército russo alveje infraestruturas estratégicas para o exército ucraniano. Inicialmente apresentados como atores independentes, os colaboradores do canal Telegram *Rybar* são suspeitos por jornalistas poloneses de serem financiados pelas estruturas de Evgueni Prigozhine, um empresário próximo do Kremlin[13], conhecido por

[9] Veja a publicação do grupo no Twitter no seguinte link: https://twitter.com/Russian_OSINT/status/1502299203107762179?cxt=HHwWhsC5uc3KntkpAAAA

[10] Um grupo de hacktivistas que realiza ataques cibernéticos no exterior para apoiar a política externa do governo russo. KILLNET atacou especialmente a Itália e a Lituânia, após disputas comerciais entre a Rússia e esses países sobre gás e transporte ferroviário de carga, https://factuel.afp.com/doc.afp.com.32D34R9

[11] Consulte a conta do Telegram do KILLNET: https[://]t[.]me/s/killnet_reservs?q=Russian_OSINT

[12] A prática de OSINT se desdobra em uma multiplicidade de domínios, incluindo a GEOINT e a inteligência a partir das redes sociais (Social Media Intelligence, SOCMINT).

[13] "Putin Chef's Kisses of Death: Russia's Shadow Army's State-Run Structure Exposed", Bellingcat, 14 de agosto de 2020, www.bellingcat.com/news/uk-and-europe/2020/08/14/pmc-structure-exposed. Sobre os possíveis vínculos entre as estruturas de Evgueni Prigozhine e o canal Telegram *Rybar*, cf. Anna Mierzyńska "Um canal Telegram indica ao exército russo o que bombardear. A guerra informativa

financiar as famosas "fábricas de trolls" que teriam apoiado a campanha de Donald Trump nos Estados Unidos em 2016, em consonância com os interesses russos[14]. Ele também seria o financiador da empresa paramilitar Wagner, que fornece mercenários a vários governos na África e no Oriente Médio e atualmente apoia as forças armadas russas na Ucrânia[15]. Embora suas atividades sejam apresentadas como independentes dos interesses do Kremlin pelas autoridades russas[16], assim como as do grupo Wagner, Evgueni Prigozhine reivindica uma postura de empreendedor patriota[17], que pressupõe que suas atividades visam defender, se não promover, os interesses russos. Essa postura também lhe permite obter muitos contratos públicos na Rússia, tornando-o um empreendedor a serviço do Estado[18]. Se o canal Telegram *Rybar* foi de fato criado com seu apoio, é possível deduzir que as autoridades russas realmente consideram o OSINT como um trunfo para a inteligência militar.

Diante dos usos ofensivos do OSINT pelas autoridades russas, desenvolvedores ucranianos criaram aplicativos destinados a proteger os dados de seus compatriotas. Entre esses aplicativos, destaca-se especialmente o aplicativo móvel *Diïa* (Дія). Ele permite a identificação em outro serviço online cujo objetivo é geolocalizar e descrever os movimentos das tropas russas no solo ucraniano[19]. Em relação a este aplicativo e seu papel na guerra, Anastasia Kryvetska, autora de uma dissertação de pesquisa no Instituto

assassina do Kremlin", 18 de junho de 2022, https://oko.press/sobota-kanal-na-telegramie-wskazuje-co-ma-zbombardowac-rosyjska-armia-zabojcza-wojna-informacyjna-kremla/

[14] Colin Gérard, "Usines à trolls russes: de l'association patriotique locale à l'entreprise globale", INA, 20 de junho de 2019, https://larevuedesmedias.ina.fr/usines-trolls-russes-de-lassociation-patriotique-locale-lentreprise-globale

[15] "Le groupe Wagner déployé dans l'est de l'Ukraine, selon Londres", Le Monde, 29 de março de 2022, www.lemonde.fr/international/article/2022/03/29/guerre-en-ukraine-le-groupe-paramilitaire-prive-wagner-deploye-dans-l-est-du-pays_6119562_3210.html

[16] Nadejda Mullen, "Wagner: l'armée secrète de Poutine", Amnesty International, 1º de setembro de 2021, www.amnesty.fr/justice-internationale-et-impunite/actualites/wagner-armee-secrete-poutine

[17] Élie Guckert, "Evgueni Prigojine: l'industriel de la désinformation russe", 14 de setembro de 2020, www.conspiracywatch.info/evgueni-prigojine-lindustriel-de-la-desinformation-russe.html

[18] Consulte o artigo de Kevin Limonier e Marlène Laruelle, "Além da 'Guerra Híbrida': Uma Exploração Digital dos Empresários de Influência da Rússia", Post-Soviet Affairs, vol. 37, nº 4, 17 de julho de 2021, www.tandfonline.com/doi/full/10.1080/1060586X.2021.1936409

[19] Anastasia Kryvetska, Dissertação de Mestrado no Instituto Francês de Geopolítica (IFG), "O Desenvolvimento do Ciberespaço Ucraniano desde a Guerra com a Rússia (2014-2022)", sob a orientação de Louis Pétiniaud, p. 96, https://omeka.geopolitique.net/items/show/542

Francês de Geopolítica (IFG), escreve: "Desde o início da guerra, o exército ucraniano tem uma vantagem particular: o conhecimento do terreno e uma colaboração maciça dos cidadãos. Fala-se de uma espécie de 'cibermobilidade' de que hoje as forças armadas ucranianas se beneficiam. Essas informações têm como objetivo final a inteligência e, portanto, servem para conhecer os movimentos das tropas e realizar ataques aéreos ou de artilharia, bem como organizar ações militares de infantaria ou cavalaria[20]." Neste sentido, o *Diïa* desempenha um papel semelhante, do lado ucraniano, ao canal Telegram *Rybar* do lado russo, com a diferença de que as informações fornecidas no *Diïa* vêm diretamente do terreno, enquanto os contribuintes do *Rybar* se baseiam principalmente em dados coletados remotamente por meio de fontes digitais (imagens de satélite, fotografias postadas nas redes sociais por ucranianos, etc.). No entanto, a produção de investigações em OSINT não se destina apenas a informar. Pelo contrário, também se tornou um novo modo de desinformação e influência no contexto da guerra.

A OSINT como uma ferramenta de comunicação e desinformação

A guerra na Ucrânia mostra que o controle da *disseminação* da informação é mais central do que nunca como um meio de comunicação para os beligerantes. A imagem das diferentes partes envolvidas no conflito tornou-se fundamental, pois favorece ou desfavorece a adesão das opiniões públicas à causa que elas afirmam defender e aos seus objetivos[21]. Uma percepção *positiva* dos beligerantes pode favorecer o recrutamento de novos combatentes ou o voluntariado em diferentes áreas, como evidenciado pela formação de grupos de investigadores em OSINT e hackers que se envolvem na guerra ao oferecer sua ajuda a uma ou outra parte[22].

Para influenciar as opiniões públicas, alguns sites russos dedicados à OSINT chegam até mesmo a disseminar informações falsas. Um exemplo disso é o

[20] Ibid

[21] Sobre este assunto, consulte o capítulo IV "Mobilização e Hacktivismo" do livro de Bertrand Boyer Guérilla 2.0., Guerras Irregulares no Ciberespaço, Edições da École De Guerre, coleção "Ligne De Front", 2020.

[22] Emma Vail, "Rússia ou Ucrânia: grupos de hackers tomam partido", The Record, 25 de fevereiro de 2022, https://therecord.media/russia-or-ukraine-hacking-groups-take-sides

WarOnFakes[23], que, sob o pretexto de expor operações de desinformação anti-russas, na realidade produz investigações falsas[24]. O *WarOnFakes*, por exemplo, publicou um artigo explicando que as tropas russas não planejavam usar o local da usina nuclear de Zaporizhzhia como uma base militar avançada no território ucraniano[25], enquanto essa informação estava sendo relatada por diferentes veículos de mídia[26]. No entanto, a usina foi de fato convertida em uma base militar e utilizada pelas tropas russas para lançar ataques balísticos uma semana após a publicação do artigo[27].

Do lado ucraniano, a valorização das pegadas digitais geradas pela guerra, assim como as investigações realizadas a partir dessas pegadas, constituem um poderoso vetor de influência para capturar a atenção das opiniões públicas ocidentais e de seus líderes. Entre todas as mudanças que ela simboliza, a guerra na Ucrânia marca, de fato, uma verdadeira virada em nossa maneira de acompanhar, mas também de viver, um conflito de alta intensidade. Passada a consternação dos primeiros momentos, a cobertura midiática do conflito se desenvolveu inicialmente ao ritmo das inúmeras fotos, vídeos ou testemunhos provenientes das profundezas das redes sociais. Imagens de colunas de tanques russos carbonizados ou sendo rebocados por tratores, vídeos de helicópteros ou aviões de combate abatidos, testemunhos de desertores russos chorando... Um fluxo contínuo de informações permitiu acompanhar de hora em hora, ou mesmo de minuto em minuto, os fracassos de um exército russo do qual muitos pensavam que estaria em

---

[23] . https[://]waronfakes[.]com/fr, cujo nome de domínio foi oficialmente registrado em 1º de março de 2022. Veja www.whois.com/whois/waronfakes.com

[24] Veja Nicholas De Rosa, "Falsas verificações de fatos sobre a invasão têm grande sucesso na Rússia", Radio-Canada, 23 de março de 2022, https://ici.radio-canada.ca/nouvelle/1870981/faux-fact-check-ukraine-war-on-fakes-russie e a investigação de Craig Silverman e Jeff Kao para a ProPublica, "Na Conflito da Ucrânia, Falsas Verificações de Fatos estão Sendo Usadas para Disseminar Desinformação", 8 de março de 2022, www.propublica.org/article/in-the-ukraine-conflict-fake-fact-checks-are-being-used-to-spread-disinformation

[25] A infotox: As forças armadas russas querem transformar a usina nuclear de Zaporojia em uma base militar", WarOnFakes, 8 de julho de 2022, https[://]waronfakes[.]com/fr/information-generale/linfox-les-forces-armees-russes-veulent-tourner-la-centrale-nucleaire-de-zaporojie-en-une-base

[26] "Rússia rejeita afirmações de Blinken sobre o uso da Zaporozhye NPP como base militar - missão para a ONU", TASS (agência de notícias estatal russa), 2 de agosto de 2022, https://tass.com/politics/1487763

[27] "Guerra na Ucrânia: mísseis russos lançados da usina nuclear de Zaporijjia", Le Figaro, 16 de julho de 2022, www.lefigaro.fr/flash-actu/guerre-en-ukraine-des-missiles-russes-tires-depuis-la-centrale-nucleaire-de-zaporijjia-20220716

Kiev em 48 horas. Essas imagens permitiram capturar instantâneos do conflito com uma granularidade cada vez maior. Pode-se dizer hoje que as inúmeras contas que relatam a guerra em tempo real nas redes sociais, do ponto de vista daqueles que a vivem, substituíram a transmissão ao vivo da guerra apresentada pelos jornalistas na televisão[28]. Além disso, as imagens que essas contas produzem e disseminam moldam imediatamente[29] a maneira como diferentes públicos e partes envolvidas no conflito percebem a guerra, desde o cidadão até o tomador de decisões. O papel dos usuários da internet e das redes sociais nessa nova maneira de construir a imagem da guerra e dos beligerantes, e, consequentemente, de participar nos fronts cibernético e informacional, é sem dúvida tão novo quanto foi a introdução da transmissão ao vivo pela televisão na cobertura de conflitos.

A coleta, análise, cruzamento e valorização dos dados gerados pela invasão russa da Ucrânia estão redesenhando nossa maneira de ver e entender a guerra. Se isso é resultado de um processo iniciado há mais de uma década, a irrupção de um conflito de alta intensidade às portas da Europa, em um espaço altamente conectado, resultou na explosão do número de pegadas digitais disponíveis, assim como na quantidade de investigadores capazes de analisá-las. Se essas investigações estão sendo usadas para atingir alvos, influenciar opiniões públicas ou disseminar informações falsas, parece que o primeiro grande conflito militar do século XXI na Europa também é, sem dúvida, a primeira guerra de alta intensidade "*open source*".

[28] A cobertura mediática da operação Desert Fox (Iraque) em 1991 também constituiu uma ruptura no campo da informação, devido ao papel desempenhado pela transmissão ao vivo da CNN. Essa ruptura no uso jornalístico da televisão pela CNN foi tão significativa que foi posteriormente estudada através do conceito de "efeito CNN". Veja o artigo do professor Eytan Gilboa, "O Efeito CNN: A Busca por uma Teoria da Comunicação das Relações Internacionais", Comunicação Política, vol. 22, nº 1, 24 de fevereiro de 2007, p. 27-44, www.tandfonline.com/doi/abs/10.1080/10584600590908429

[29] Ou seja, sem a mediação do discurso jornalístico.