OS RISCOS DAS REDES SOCIAIS NO CAMPO DE BATALHA: OSINT E O TIKTOK NA GUERRA ENTRE A RÚSSIA E UCRÂNIA

THE RISKS OF SOCIAL NETWORKS ON THE BATTLEFIELD: OSINT AND TIKTOK IN THE WAR BETWEEN RUSSIA AND UKRAINE

Jheimis Santos, FATEC Americana, jheimis.silva@fatec.sp.gov.br,
Matheus Antonietto, FATEC Americana, matheus.antonietto@hotmail.com,
Henri Alves, FATEC Americana, henri.godoy@fatec.sp.gov.br

Resumo

Nos conflitos atuais a interação dos soldados nas redes sociais caracteriza um novo comportamento social levado para a guerra, alertando para os riscos do uso delas nesse contexto. Este artigo tem por objetivo trazer um exemplo prático sobre o modo com que o compartilhamento de informações em plataformas de redes sociais representa um risco e pode ser explorado pela Inteligência de Fontes Abertas (Open Source Intelligence - OSINT), tendo como base o conflito entre Rússia e Ucrânia. Além disso, serão abordados elementos cruciais para a compreensão desse tema, como a definição de OSINT e a origem da guerra entre Rússia e Ucrânia. Os resultados indicam que é arriscado o compartilhamento de informações nas redes sociais no contexto da guerra e que o TikTok é uma fonte para produzir inteligência.

Palavras-chave: OSINT, TikTok, Segurança da Informação.

Abstract

This meta-paper describes the style to be used in articles and short papers for Fatec Information Security Congress - FatecSeg. For papers in English, you should add just an abstract while for the papers in Portuguese, we also ask for an abstract in Portuguese ("resumo"). In both cases, abstracts should not have more than 10 lines or according to ABNT 6028 – 150 to 250 words, both of which must be on the first page of the article. The abstract text must be in a single paragraph, single spaced between lines, Times New Roman font, font size 12, justified and no indentation on the first line. The abstract must present the objectives, methodological approach, results and conclusions. The use of bibliographic citations should be avoided in the abstract.

Keywords: *OSINT, TikTok, Information Security.*

1. Introdução

Segundo Hassan (2018), desde o final da Guerra Fria, a transformação digital tornou o mundo menor e mais conectado, trouxe um aumento na produção e compartilhamento de informação, além de trazer grandes benefícios para a sociedade. Contudo, essa rápida

transformação também trouxe consigo diferentes tipos de ameaças. As informações compartilhadas de modo público podem ser exploradas com o objetivo de produzir conhecimento ou inteligência, e muitas dessas informações podem ser consideradas sensíveis, principalmente em um contexto de conflitos militares deflagrados (JOTA, 2022).

De acordo com Manual de Fundamentos EB20-MF 10.107 - Inteligência Militar Terrestre (2015), no contexto militar, a atividade de inteligência é o ciclo de coleta, processamento e análise de dados e informações com o objetivo de produzir conhecimento ou inteligência sobre o inimigo. Existem diferentes maneiras que a Atividade de Inteligência pode coletar informações para analisar e produzir conhecimento. Elas se diferem de acordo com a "natureza da fonte ou do órgão de obtenção que a explora" (Manual de Fundamentos EB20-MF 10.107- Inteligência Militar Terrestre, 2015). A Inteligência de Fontes Abertas (Open Source Intelligence - OSINT), é a inteligência baseada em informações coletadas de fontes disponíveis de modo público, tais como: meios de comunicação (rádio, televisão e jornais) ou Internet (plataformas de redes sociais - Facebook, Twitter e TikTok).

Segundo Aparecido (2022), no dia 24 de fevereiro de 2022, Vladimir Putin autorizou uma "operação militar especial" na Ucrânia, o segundo maior país da Europa, dando início ao maior conflito naquele continente, desde a II Guerra Mundial. Silva e Silva (2022) considera que nos conflitos atuais, não se pode desconsiderar a atuação do indivíduo no campo de batalha e nas mídias sociais. Os relatos "Este vídeo [que circulou em canais do Telegram] denunciou a presença de um depósito russo de armas em Nova Khakovka, destruído ontem pela Ucrânia" (MILITAR, 2022), "Forças Armadas da Ucrânia líquida um grupo de Kadyrovites graças a um vídeo no Tiktok" - Traduzido por Google Tradutor - ("Загримировались[...]", 2022) ou "Obsessão de soldado por selfies pode provar operações da Rússia na Ucrânia", caracterizam esse novo comportamento social levado para a guerra (SILVA; SILVA GOMES FILHO, 2022). Portanto, esse comportamento pode prejudicar as operações, favorecer o inimigo e consequentemente, colocar vidas em risco, alertando para os riscos do uso das redes sociais na guerra.

Dessa forma, o objetivo desse artigo é trazer um exemplo prático sobre o modo com que o compartilhamento de informações em plataformas de redes sociais pode ser explorado pela OSINT e colocar em vantagem operacional em relação ao seu oponente, tendo como base o conflito entre Rússia e Ucrânia. Neste trabalho, primeiro será abordado a definição de OSINT,

depois uma contextualização da origem da guerra entre Rússia e Ucrânia. Por fim, será realizado um estudo prático para demonstrar que é possível explorar e produzir conhecimento ou inteligência baseado em informações compartilhadas no TikTok.

2. Segurança da Informação

No contexto atual, o compartilhamento e o armazenamento de informações já fazem parte do dia-a-dia das pessoas devido ao aumento da informatização, do uso maciço da tecnologia de redes, dos computadores e da internet, que facilitaram a troca de informações. No entanto, as informações estão sujeitas às ameaças externas e internas. Com isso, a segurança da informação se mostra fundamental para proteger as informações (GAMARA SAÚ, 2020).

Apesar da ideia de que a segurança da informação se tornou popular devido ao aumento da informatização, a história do desenvolvimento da segurança da informação mostra que a busca por meios para garantir a necessidade de prevenir o uso ou acesso não autorizado da informação existe há muito tempo. Nesse sentido, podemos citar como exemplo a decifragem da máquina Enigma durante o período da Segunda Guerra Mundial. Essa máquina era usada pela Alemanha nazista para codificação e decodificação das comunicações. Ela utilizava um algoritmo de codificação muito complicado para a época e a sua decifragem representou um papel importante no curso da guerra (IBRAHIMOVA,. 2020). Logo, tais aspectos mostram que a necessidade de segurança da informação não é recente, mas algo que sempre foi almejado.

A ISO/IEC 27001 (2006) define a Segurança da Informação como a preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade.

A confidencialidade, integridade e disponibilidade da informação são propriedades consideradas como princípios fundamentais da segurança. Esses princípios são conhecidos como o triângulo CIA (HINTZBERGEN et al., 2018). Portanto, vale a pena destacar uma definição mais aprofundada deles, de acordo com a ISO/IEC 27001 (2006):

- Confidencialidade: é a propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.
- Integridade: é a propriedade de salvaguarda da exatidão e completeza de ativos.
- Disponibilidade: é a propriedade de estar acessível e utilizável sob demanda por

uma entidade autorizada.

Todos os controles de segurança, mecanismos e proteções são implementados para prover um ou mais desses princípios, e todos os riscos, ameaças e vulnerabilidades são medidos pela sua capacidade potencial de comprometer um ou todos os princípios do triângulo (HINTZBERGEN et al., 2018).

3. Inteligência de Fontes Abertas (Open-Source Intelligence - OSINT)

De acordo com Manual de Fundamentos EB20-MF 10.107- Inteligência Militar Terrestre (2015), no contexto militar, a Atividade de Inteligência é o ciclo de coleta, processamento e análise de dados e informações com o objetivo de produzir conhecimento ou inteligência sobre o inimigo. O resultado desse processo é essencial para os comandantes que planejam e executam operações militares, em diferentes níveis de utilização - estratégico, operacional e tático. Existem diferentes maneiras que a atividade de inteligência pode coletar informações para analisar e produzir conhecimento. Elas são divididas de acordo com a "natureza da fonte ou do órgão de obtenção que a explora" (Manual de Fundamentos EB20-MF 10.107- Inteligência Militar Terrestre, 2015).

Segundo Manual de Fundamentos EB20-MF 10.107- Inteligência Militar Terrestre (2015), a comunidade de inteligência sempre coletou informações em fontes abertas para produção de conhecimento. A Inteligência de Fontes Abertas (Open-Source Intelligence - OSINT) é definida como: a Inteligência baseada em informações coletadas de fontes de caráter público, tais como os meios de comunicação (rádio, televisão e jornais), propaganda de estado, periódicos técnicos, Internet, manuais técnicos e livros (Manual de Fundamentos EB20-MF 10.107- Inteligência Militar Terrestre, 2015).

Igualmente, Hassen (2018), define OSINT como: uma inteligência que é produzida a partir de informações disponíveis publicamente e é coletada, explorada e disseminada em tempo hábil para um público apropriado com a finalidade de atender a um requisito específico de inteligência (HASSEN, 2018).

Considerando que a OSINT inclui todas as informações disponíveis em fontes de caráter público, convém mencionar que as informações compartilhadas em plataformas de redes sociais - Facebook, Twitter, TikTok - também estão sob o domínio da OSINT, ou seja, de acordo com Haasen (2018), podem ser exploradas para produzir inteligência, embora existam discussões

entre especialistas sobre a necessidade de cadastrar-se na plataforma para poder ter o acesso completo ao conteúdo disponível.

Por fim, vale a pena destacar algumas vantagens da OSINT, como:

- Questões legais. A legislação sobre o acesso à informação produzida por fontes abertas possibilita a obtenção de dados e informações sensíveis (Manual de Fundamentos EB20-MF 10.107- Inteligência Militar Terrestre, 2015) e (HASSEN, 2018).
- Baixo custo. Coletar informações de fontes abertas é mais barato comparado a outras fontes para obtenção de informações e produzir inteligência (JOTA, 2022).
- Facilidade de acesso. A Internet facilitou o acesso à informação. (Manual de Fundamentos EB20-MF 10.107- Inteligência Militar Terrestre, 2015).

4. A guerra entre a Rússia e Ucrânia

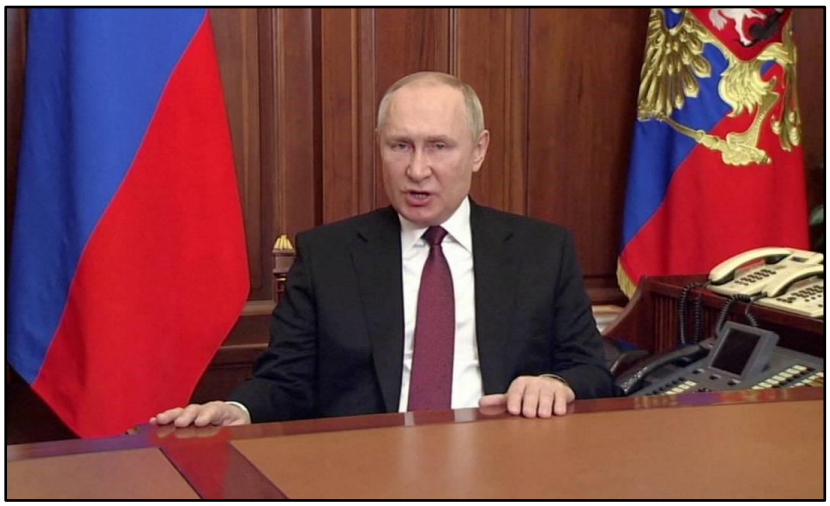
Segundo Aparecido (2022), em 21 fevereiro de 2022, Putin reconheceu as regiões separatistas de Donetsk e Luhansk como repúblicas independentes. No dia 24 de fevereiro de 2022, o presidente da Rússia autorizou uma “operação militar especial” no Donbass, leste da Ucrânia, o segundo maior país da Europa, alegando ataques e opressões por parte de Kiev, e apontou que o objetivo era “desmilitarizar e desnazificar a Ucrânia”, dando início ao maior conflito naquele continente, conforme figura 1. O conflito na região se estende até os dias de hoje.

Para Aparecido (2022), a origem desse conflito tem como fundamento as divergências entre o nacionalismo dos dois países; isto é, o nacionalismo ucraniano é pro-ocidental e deseja que a Ucrânia seja um país independente. Em contraste, o nacionalismo russo opõe-se ao Ocidente e, além disso, acredita que a Ucrânia faz parte da Rússia, visto que os russos apoiam a ideia de que apenas os ucranianos do oeste do país de fato são ucranianos e tem proximidade com o Ocidente, mas o Leste, em sua maior parte, se identifica com a Rússia e é leal a ela por afinidades históricas e etnoculturais. Dessa forma, a aproximação da Ucrânia com o Ocidente prejudica os interesses russo de influência regional, por outro lado, a submissão da Ucrânia em aceitar a influência russa acaba por prejudicar a capacidade de adotar os seus próprios interesses

globalmente.

Entretanto, pode-se apontar antecedentes históricos, políticos e econômicos que são importantes para entender esse conflito. Por isso, a explicação de Aparecido (2022), não significa esgotar o assunto. O conflito envolve uma disputa de narrativas, por um lado, disseminada pela Rússia, por outro, disseminada pelo Ocidente; portanto, de acordo com Silva (2022), é necessário levar em conta a Guerra Informacional que engloba o evento para compreender essa guerra.

Figura 1 - "Vladimir Putin fez discurso televisionado nacionalmente comunicando operação militar contra a Ucrânia Foto: RUSSIAN POOL / via REUTERS"



Fonte: O GLOBO, 2022

5. Metodologia

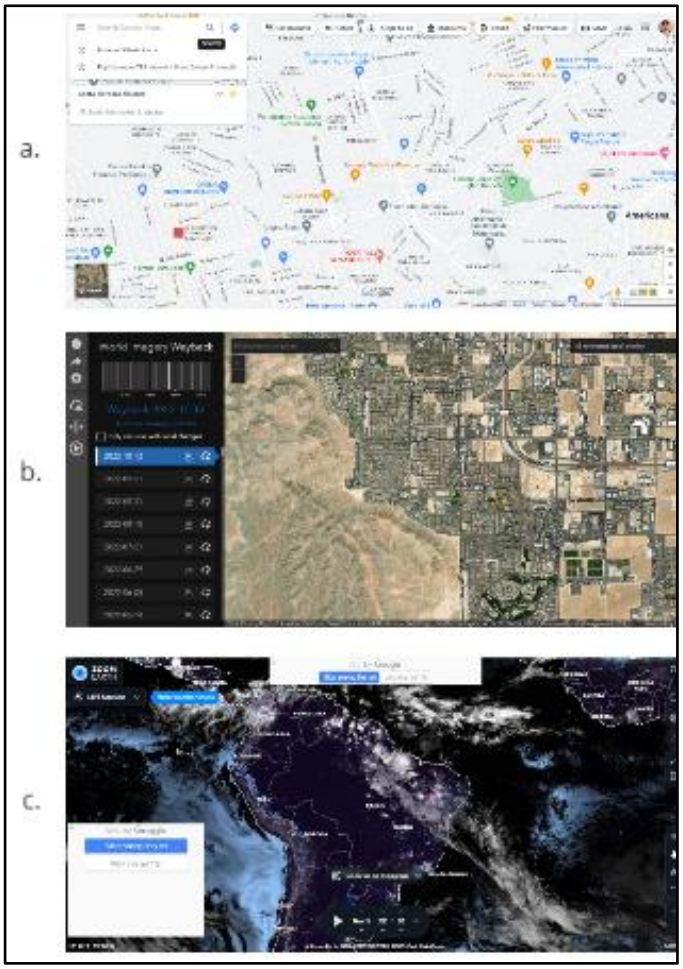
O método utilizado neste trabalho foi a pesquisa empírica para comprovação prática de que técnicas e ferramentas OSINT podem explorar Fontes Abertas e apoiar a Atividade de Inteligência a produzir conhecimento ou inteligência sobre o inimigo, no contexto da guerra. Além disso, foi realizada uma revisão bibliográfica para definição dos principais conceitos e ideias sobre o tema, bem como para confrontar algumas referências encontradas com os resultados alcançados.

As ferramentas utilizadas foram as seguintes: Google Maps, World Imagery Wayback e Zoom Earth. Essas ferramentas disponibilizam mapas e imagens obtidas por satélites de forma

gratuita. A figura 2 ilustra a interface de cada ferramenta. Além do mais, o Google Search (ferramenta de search engine do Google) também foi utilizado.

A Fonte Aberta escolhida para exploração foi a plataforma de mídia social Tik Tok. Hoje o Tik Tok é uma das redes sociais mais utilizadas no mundo, com milhões de usuários interagindo na plataforma todos os dias. Segundo o site da empresa, o TikTok é o principal destino do compartilhamento de vídeos no formato curto, produzidos com celular.

Figura 2 - Interface de cada ferramenta, respectivamente: Google Maps (a), World Imagery Wayback (b) e Zoom Earth (c)



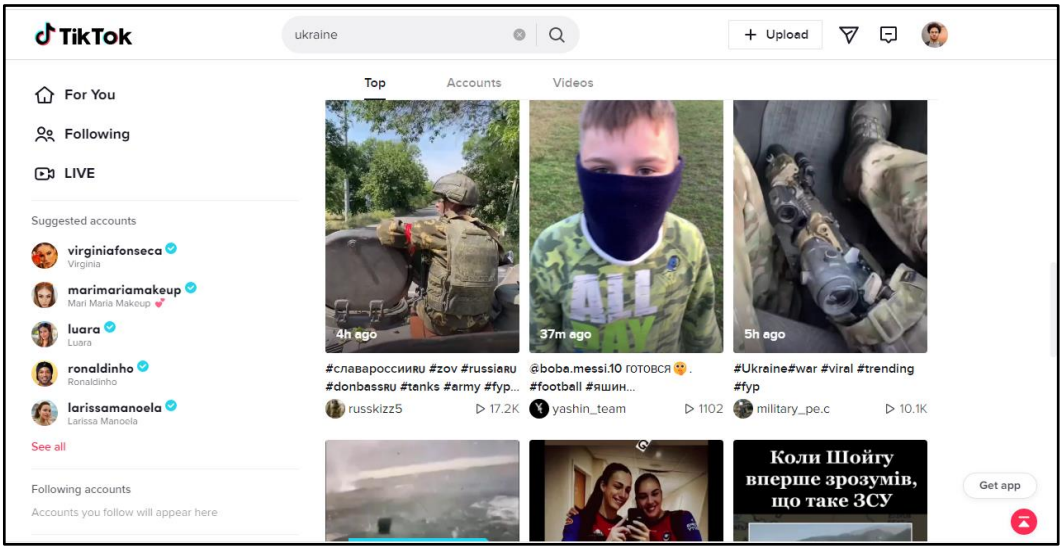
Fonte: Google Maps, World Imagery Wayback, Zoom Earth – Elaborado pelo autor

6. Análise e Interpretação dos Resultados

6.1. Resultado de busca por assuntos relacionados a guerra

A plataforma de mídia social TikTok permitiu encontrar muitas informações relacionadas à guerra entre a Rússia e a Ucrânia. Foi realizada uma busca por termos que envolvessem o conflito, em inglês e ucraniano - e para a tradução dos termos foi utilizado a ferramenta Google Translate. Utilizou a funcionalidade search bar, que permite ao usuário explorar e buscar por vídeos, hashtags e contas de usuários, de acordo com o termo buscado, conforme figura 3. Foi possível obter inúmeros vídeos que revelavam as peculiaridades da rotina dos soldados na guerra, como por exemplo: momentos na linha de frente, instantes antes e durante ofensivas, períodos de descanso e descontração. Além disso, outros eventos podem ser observados, como o deslocamento de equipamentos militares e o resultado da destruição, pelos ataques do exército russo, de vilas e infraestruturas ucranianas. Jota (2022), encontrou informações semelhantes nos relatórios sobre o conflito produzidos por entidades não estatais que utilizam Fontes Abertas.

Figura 3 - Resultado de busca pelo termo “ukraine” (Ucrânia, em Inglês) no TikTok



Fonte: TikTok

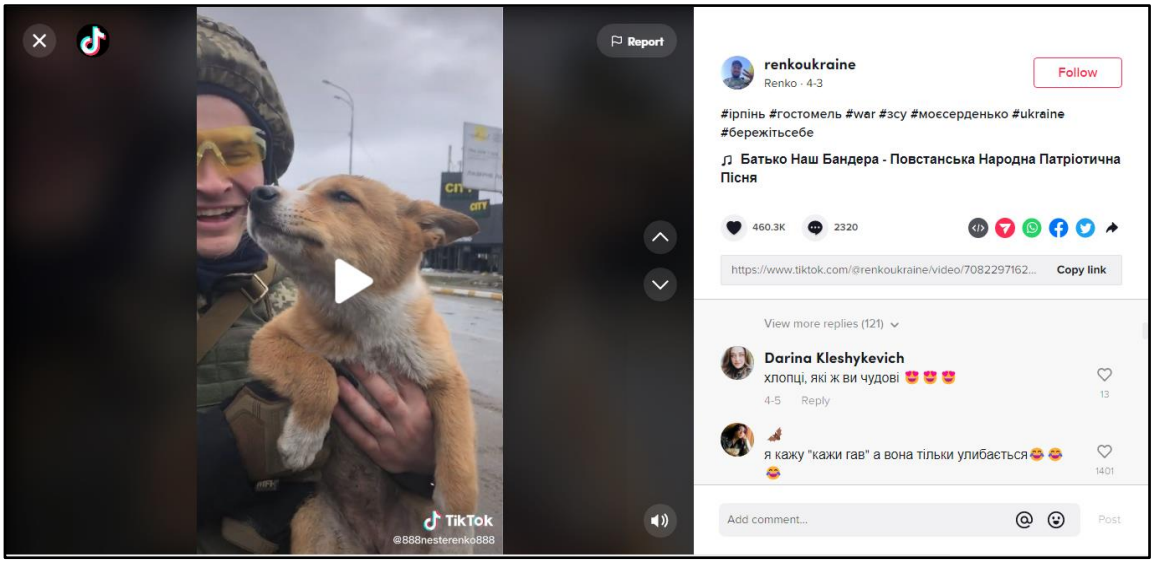
As funcionalidades disponíveis na plataforma podem ser uma ferramenta útil na etapa de exploração e coleta. O aproveitamento desses recursos possibilitou maior precisão e facilidade para encontrar vídeos ou contas de soldados que participavam do conflito. As buscas por palavras chaves em inglês e ucraniano exibiram resultados interessantes, principalmente em

idioma ucraniano. Segundo Hassen (2018), o uso de palavras chaves na etapa de busca é essencial para que o analista encontre melhores resultados (HASSEN, 2018). De acordo com Nascimento (2019), os mecanismos de buscas são a principal ferramenta que o pessoal em atividade OSINT usa para coletar informações em Fontes Abertas.

6.2. Informações sobre localização em vídeos compartilhados

Os vídeos compartilhados no TikTok podem revelar informações importantes. Após a busca por vídeos relacionados à guerra, foi escolhido um vídeo com o interesse de coletar informações sobre a localização do lugar onde foi filmado o vídeo . Para isso, combinou algumas técnicas OSINT e ferramentas de mapas virtuais e imagens de satélites, bem como e um motor de busca para pesquisar. O vídeo escolhido foi o vídeo compartilhado pelo usuário “Renko” (@renkoukraine). A figura 4 mostra o vídeo escolhido.

Figura 4 - Vídeo compartilhado por “Renko”



Fonte: TikTok

Durante a análise foi possível determinar a provável localização de “Renko”. No vídeo em que o soldado segura um cachorro, seu entorno revela informações importantes. Essas informações podem ser consideradas como pontos de referência para pesquisas em outras ferramentas de Fontes Abertas, a fim de determinar o local exato. Por exemplo, foi possível observar que eles estão próximos a um mercado, CITY MARKET. Buscando pelo termo “CITY MARKET ukraine” no Google, foi possível localizar o endereço do mercado. Verificando essa

informação em outras ferramentas, foi possível confirmar o lugar onde eles estavam.

Os resultados apontam que, naquele momento, eles estavam em Sviato-Pokrovska St, 22, Hostomel', Kyivs'ka oblast, Ucrânia, próximo a um supermercado. A figura 5 mostra alguns pontos de referência como evidências de que este local era onde os soldados estavam. A informação da localização deles poderia trazer consequências graves, pois ela denuncia a presença de tropas ucranianas naquele região, e o inimigo poderia realizar um ataque ali ou tomar vantagem de alguma outra forma sob posse desse conhecimento. Portanto, essa informação pode fornecer vantagem ao inimigo, principalmente em um contexto de conflito deflagrado. Além do mais, podemos considerar esse comportamento como uma violação da preservação do princípio da confidencialidade da informação.

Figura 5 - Pontos de referência que evidenciam o local onde “Renko” estava no momento do vídeo

Fonte: Zoom Earth e TikTok

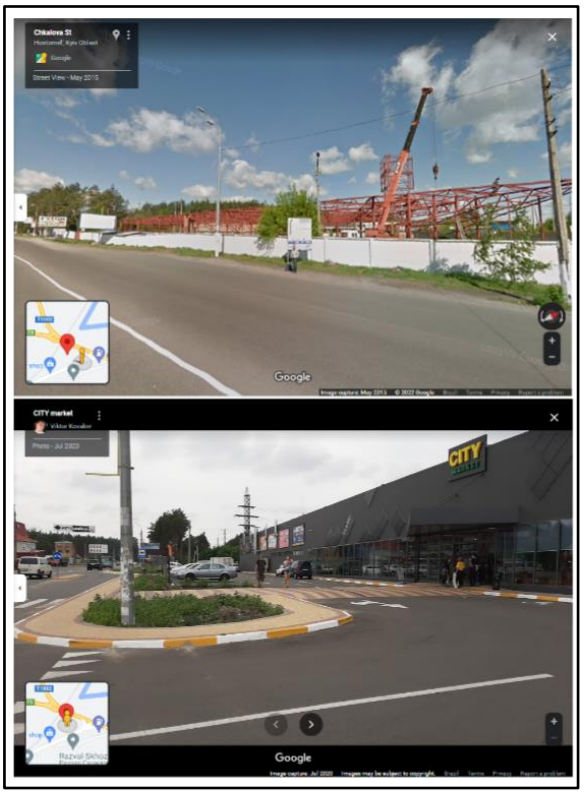
O “conhecimento de Inteligência deve ser produzido em tempo oportuno para basear a tomada de decisão de forma adequada” (Manual de Fundamentos EB20-MF 10.107 - Inteligência Militar Terrestre, 2015). Dessa forma, é importante informar que o critério para escolha do vídeo não levou em consideração a data em que o vídeo foi compartilhado, pois a ideia principal dessa atividade foi exemplificar a possibilidade de identificar a posição de um soldado através de um vídeo compartilhado em uma rede social e chamar a atenção sobre o risco desse comportamento.

6.3. Dificuldades encontradas sobre as ferramentas

Durante a investigação da localização dos soldados, foram observados problemas que são importantes comentar: as informações em fontes abertas nem sempre estão atualizadas ou completas, podendo levar a conclusões errôneas ou não incrementar a atividade de Inteligência. “A produção do conhecimento de Inteligência deve valer-se de dados oriundos de todas as fontes, favorecendo a geração de produtos precisos e completos.” (Manual de Fundamentos EB20-MF 10.107 - Inteligência Militar Terrestre, 2015).

Em outras palavras, as imagens do Street View no Google Maps estavam desatualizadas, mesmo que as fotos compartilhadas por outros usuários e a imagem de satélite disponível na mesma ferramenta fossem mais recentes, conforme figura 6.

Figura 6 - Imagens desatualizadas no Google Street View



Fonte: Google Maps e Street View - Elaborado pelo autor

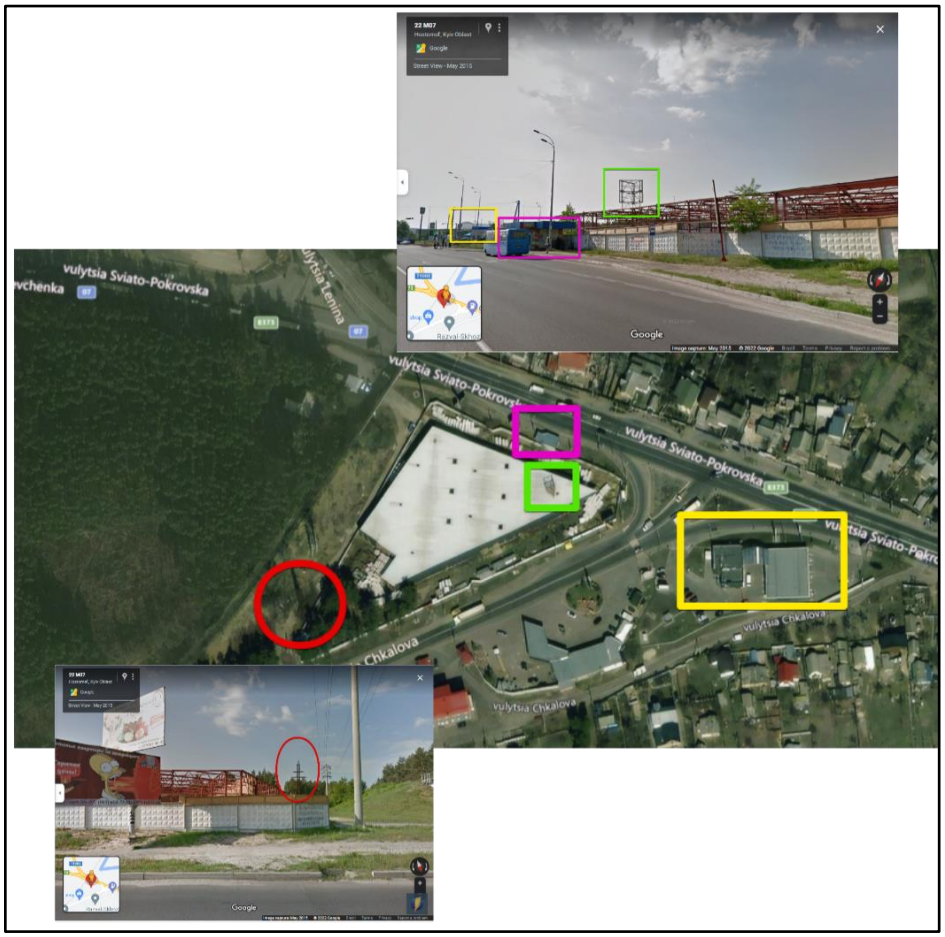
Na ferramenta World Imagery Wayback, a data das imagens de satélite não seguia uma cronologia exata de acordo com a marcação da data de criação das imagens de satélite, comparado com as imagens das outras fontes, conforme figura 7.

Figura 7 - Imagens de satélite não acompanham a data correta, comparado com as imagens das outras fontes

Fonte: World Imagery Wayback - Elaborado pelo autor

Com a soma dos pontos de referência em comum, infere-se que se tratava do mesmo lugar, conforme figura 8.

Figura 8 - Pontos de referência em comum entre as fontes



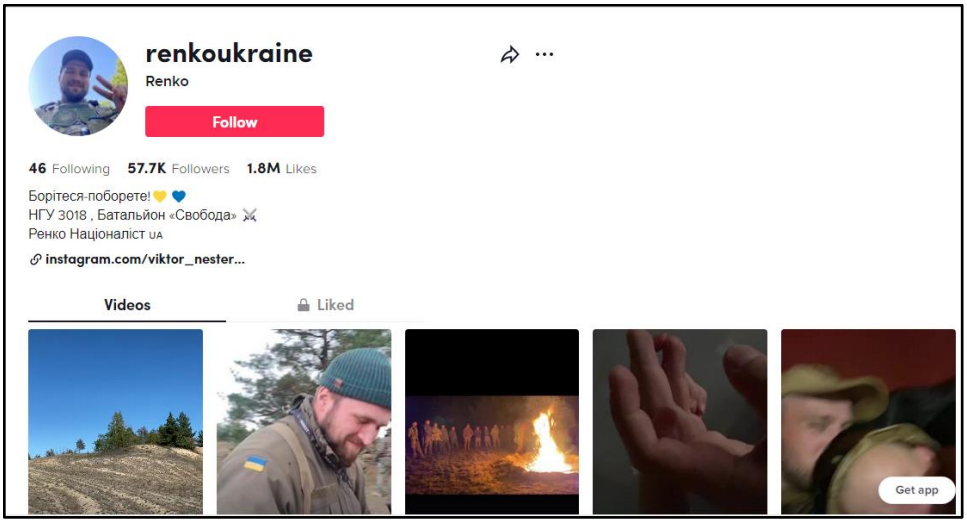
Fonte: Zoom Earth e Google Maps - Elaborado pelo autor

6.4. Informações encontradas no perfil de soldados

O perfil de soldados no TikTok pode revelar dados relevantes. Foi realizado um levantamento de informações e dados no perfil de “Renko”. Foi capaz de encontrar a sua conta do Instagram, o que permitiu saber um pouco mais sobre ele, em particular, o nome do militar: “Viktor Nesterenko”. Além do mais, foi possível saber que Viktor faz parte do “НГУ 3018 , Батальйон «Свобода»” (NSU 3018, Batalhão "Liberdade", em portugues), conforme figura 9. Esse batalhão é uma formação da Guarda Nacional da Ucrânia, unidade militar 3018 , que faz parte da 4ª brigada de missão operacional e atuaram em Kiev, Lukyanivka, Staritsa, Lukashi, Irpin , Bucha, Gostomel (УЧАСНИКИ ПРОЕКТІВ ВІКІМЕДІА, 2016). O inimigo de posse dessas informações poderia utilizá-las para o planejamento de ações de Engenharia Social (NASCIMENTO, 2019). “Perfis Pessoais onde se é postado, voluntariamente nossos dados e

informações importantes é onde mais devemos nos preocupar em aplicar a segurança da informação" (BARROS, 2021).

Figura 9 - Imagens desatualizadas no Google Street View



Fonte: TikTok

Em suma, esta atividade buscou demonstrar o risco do uso das redes sociais no campo de batalha e que as informações compartilhadas nessas plataformas podem ser exploradas pela OSINT. Além disso, cabe destacar que durante a pesquisa foram encontrados outros vídeos e contas de militares que trouxeram informações e resultados diferentes, por exemplo, foi realizada a tentativa de descobrir a posição de militares em um outro vídeo, porém não obteve sucesso, mas outras informações foram encontradas.

7. Conclusões

Este artigo buscou trazer um exemplo prático sobre o modo com que o compartilhamento de informações em plataformas de redes sociais pode ser explorado pela OSINT, tendo como base o conflito entre Rússia e Ucrânia.

Foi possível observar que: as redes sociais aumentaram a superfície para coleta de informação para a Atividade de Inteligência; Fontes Abertas, como bancos de imagens de satélite, mapas virtuais e redes sociais, podem ser aproveitadas para produzir conhecimento ou inteligência; o perfil de militares no TikTok e vídeos compartilhamentos na plataforma pode

revelar informações importantes.

Portanto, ficou evidente que a interação de militares participantes de um conflito deflagrado, nas redes sociais, é uma vulnerabilidade que revela informações que deveriam ser protegidas e que podem ser exploradas para produzir conhecimento e conferir vantagem ao oponente. Os militares devem ser orientados e educados sobre esses riscos. Além disso, mecanismos de contrainteligência e segurança da informação devem ser adotados.

Por fim, como proposta de trabalhos futuros e continuidade da pesquisa, recomenda-se: um estudo a fim de saber se os soldados no conflito entre Rússia e Ucrânia estão recebendo orientações sobre o uso de redes sociais no campo de batalha. Se sim, quais recomendações estão sendo empregadas e qual a adesão dos soldados a essas recomendações.

Referências

Antes de atacar Ucrânia, Putin prometeu "consequências nunca antes vistas na História" em caso de interferências. Disponível em: <https://oglobo.globo.com/mundo/epoca/antes-de-atacar-ucrania-putin-prometeu-consequencias-nunca-antes-vistas-na-historia-em-caso-de-interferencias-25407874>. Acesso em: 24 nov. 2022.

NASCIMENTO, Marcelo Antonio do. Uso de open source intelligence no contexto da guerra Cibernética: exposição de dados sensíveis sobre a infraestrutura de tecnologia da informação e comunicações do Exército através das fontes abertas. Orientador: Maj QCO Infor Marcelo Antonio do Nacimento. 2019. Trabalho de Conclusão de Curso (Especialização em Ciências Militares – Curso de Aperfeiçoamento Militar) - Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais, [S. l.], 2019. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/4863/1/CAM_QC_2019_CAP_ABNER.pdf. Acesso em: 23 nov. 2022.

APARECIDO, Julia Mori; AGUILAR, Sérgio Luiz Cruz. A Guerra entre a Rússia e a Ucrânia. In AGUILAR, Sérgio Luiz Cruz (Ed.). Série Conflitos Internacionais, v. 9, n. 1. Marília: OCI, 2022. Disponível em: https://www.marilia.unesp.br/Home/Extensao/observatoriodeconflitosinternacionais/v.-9-n.-1fev.-2022.pdf. Acesso em: 8 jun. 2022.

BARROS, A. P.; MACEDO, V. DOS S. A segurança da informação nas redes sociais. Revista Processando o Saber, v. 13, p. 252-266, 14 jun. 2021.

GAMARA SAÚ, C. S. A segurança da informação e sua importância na proteção dos sistemas informatizados em uso nas organizações militares do Exército brasileiro. A Defesa Nacional, v. 88, n. 794, 30 jul. 2020. Disponível em: http://ebrevistas.eb.mil.br/index.php/ADN/article/view/5867. Acesso em: 8 jun. 2022.

HASSAN, Nihad. Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence. 1. ed. [S. l.]: Apress, 2018. 354 p. ISBN 978-1484232125.

HINTZBERGEN, Jule et al. Ver todas as 2 imagens Fundamentos de Segurança da Informação: com Base na ISO 27001 e na ISO 27002Fu. 1. ed. Rio de Janeiro: Brasport, 2018. 256 p. ISBN 978-8574528601.

IBRAHIMOVA, Aytakin. (2020). The defintions of information and security; history of information security development. Vilnius University Open Series. 48-57. 10.15388/OS.LAW.2020.5. Disponível em: https://www.researchgate.net/publication/349154997_The_defintions_of_information_and_security_history_of_information_security_development. Acesso em: 8 jun. 2022.

JOTA, Lucas. A INFORMAÇÃO COMO ELEMENTO DE DIFUSÃO DE PODER NO ESPAÇO CIBERNÉTICO: O USO DE INTELIGÊNCIA DE FONTES ABERTAS (OSINT) NO CONFLITO ENTRE RÚSSIA E UCR NIA. Orientador: Graciela de Conti Pagliari. 2022. Trabalho de Conclusão de Curso (Bacharel em Relações Internacionais) - Universidade Federal de Santa Catarina, Florianópolis, 2022. Disponível em: https://repositorio.ufsc.br/handle/123456789/237465. Acesso em: 16 nov. 2022.

Manual de Fundamentos EB20-MF 10.107- Inteligência Militar Terrestre. 2. ed. Brasília, DF, 2015c. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/95/1/EB20-MF-10.107.pdf Acesso em: 8 jun. 2022.

MILITAR, Hoje no Mundo. Este vídeo denunciou a presença de um depósito russo de armas em Nova Khakovka, destruído ontem pela Ucrânia. Circulou apenas em canais Telegram [...]., 13 de jul. 2022. Twitter: @hoje_no. Disponível em: https://twitter.com/hoje_no/status/1547314871548739584. Acesso em: 16 nov. 2022.

Referência Bibliográfica ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. ABNT, 2006.

SILVA, Sylvio Pessoa; SILVA GOMES FILHO, Paulo Roberto. GUERRA INFORMACIONAL NO CAMPO DE BATALHA. Centro De Estudos Estratégicos Do Exército (Ceeex), [s. l.], ano 2022, v. 24, n. 2, p. 45 - 56, 2022. Disponível em: http://ebrevistas.eb.mil.br/CEEExAE/article/view/9526/8113. Acesso em: 8 jun. 2022.

“Загримировались ради нового ролика”: ВСУ “закобзонили” группу кадыровцев благодаря видео в Тиктоке (видео). Disponível em: <https://tsn.ua/ru/ukrayina/zagrimirovalis-radi-novogo-rolika-vsu-zakobzonili-gruppu-kadyrovcev-blagodarya-video-v-tiktoke-video-2187121.html>. Acesso em: 16 nov. 2022..

УЧАСНИКИ ПРОЕКТІВ ВІКІМЕДІА. 4-та бригада оперативного призначення НГ (Україна). Disponível em: <https://uk.wikipedia.org/wiki/4-та_бригада_оперативного_призначення_НГ_(Україна) >. Acesso em: 23 nov. 2022.