TARGETS ON TWITTER: OPEN-SOURCE INTELLIGENCE SUPPORT TO TACTICAL TARGETING

by Mrs. Shelly L. Bailey &
Chief Warrant Officer 4 (Retired) Jay Gack

Disclaimer: The views expressed in this article are the author's alone and do not necessarily reflect the opinion of Science Applications International Corporation or any U.S. Army organization.

Introduction

Open-source intelligence (OSINT) is likely the world's oldest intelligence discipline. Exercised by Viking explorers, Roman Legionnaires, and Silk Road traders,[1] OSINT was the dominant form of intelligence gathering through much of recorded history. From Hannibal's knowledge of Gallic separatist aspirations in northern Italy,[2] to William the Conqueror's use of local terrain knowledge in his defeat of the Ely Rebellion,[3] decision makers have historically relied on publicly available information (PAI) to inform strategy and military tactics.

Despite performing admirably through the major wars of the 20th century, OSINT fell out of vogue after World War II in favor of more technical and clandestine collection capabilities. Signal intercepts and space-based satellite imagery were simply better suited for Cold War intelligence missions targeting the insular authoritarian regime behind the Iron Curtain.[4] While it remained a source of foundational intelligence, OSINT was unable to substantially contribute to the Nation's foremost intelligence challenges, such as the readiness of Soviet troops, because the information available to OSINT collectors originated almost exclusively from the adversary's own media sources. This trend began to reverse when the Berlin Wall fell, helping to foster the information revolution and global network integration. As social networks and mobile computing technologies gained global popularity, the OSINT collector suddenly gained access to billions of sources, who—through the course of their daily activities—shared a staggering amount of intelligence data.

The value of PAI's resurgence is demonstrated nowhere better than in Ukraine. Since Russia's invasion in February 2022, social media platforms such as Facebook, TikTok, and Telegram have become primary sources for current information on the Russia-Ukraine conflict. In the West, both government intelligence agencies and private OSINT enthusiasts are using social media and other online sources to collect, correlate, and verify Russian military activities. Ukraine's government has gone further by soliciting public observations and receiving tens of thousands of crowd-sourced reports every day on Russian maneuvers.[5] As suggested in ATP 2-22.9, *Open-Source Intelligence*, "Circumstances have never been more favorable for using open-source information . . . The exponential increase in the number of publicly available information (PAI) sources worldwide provides an unprecedented opportunity for the intelligence warfighting function to support command and control."[6]

Since the buildup of forces along the Russian-Ukraine border in 2021, PAI has provided consistent, timely, and accurate insights into the preparation and prosecution of Russia's invasion. This includes the staging of forces in Belarus, the initial attack targeting the Donbas region and Kyiv, the siege of Mariupol, and evidence of various alleged Russian atrocities.[7] Despite Russian attempts to disrupt internet and phone services in occupied areas, local citizens continue to collect and share tactical combat information via social media and other web-based repositories.[8]

OSINT's utility during the Russia-Ukraine conflict presents a compelling case for the Army intelligence enterprise to employ the discipline more broadly. OSINT is already widely acknowledged as a critical enabler for nonlethal target development, nonlethal effects assessment,[9] and cyber-enabled intelligence.[10] Recent global conflicts—and Ukraine in particular—demonstrate OSINT's ability to enable tactical intelligence as well, including target intelligence and battle damage assessment (BDA).

Open-Source Intelligence and Tactical Intelligence

OSINT has enjoyed consistent success in recent conflicts. For example, after Russia's 2014 occupation of eastern Ukrainian provinces, a team of Ukrainian military and private OSINT enthusiasts successfully verified the presence of Russian military forces—a fact long denied by Moscow—through online photographs and personal social media accounts.[11] Around the same time, the Defense Intelligence Agency was tracking Yemeni Houthi SCUD missile launches via Twitter,[12] and other United States intelligence agencies leveraged social media to identify and target ISIS locations in Syria.[13] Government and press reports since 2015 list dozens of examples of PAI informing force protection,[14] providing warning, [15] tracking enemy force projection,[16] informing counterinfluence activities,[17] and providing decisive input to tactical targeting efforts.

The 2022 National Defense Strategy discusses the critical nature of "mutually-beneficial Alliances and partnerships" and the need for a "whole-of-government" approach to strategic competition.[18] This type of partnering requires the sharing of intelligence under a structured foreign disclosure plan. Of course, rigorous sanitization and disclosure review takes time; a limited resource in tactical environments. Raw publicly available data and information, on the other hand, is highly shareable. This makes OSINT an optimal choice for intelligence sharing, whether independently generated or corroborated with more traditional collection capabilities.

Open-Source Intelligence in Tactical Target Development

OSINT's value on the modern tactical battlefield extends well beyond its ability to enable intelligence sharing and includes target development, BDA, and other direct support to military operations. A 2019 Chairman of the Joint Chiefs of Staff Instruction defines targeting as "the process of selecting and prioritizing targets and matching the appropriate response to them."[19] From a target selection standpoint, OSINT has much to offer. Public information provides dynamic notification of high-value or high-payoff target identification, supporting dynamic targeting operations. This was demonstrated repeatedly during counter-ISIS operations in Syria and Iraq, as previously mentioned. It is also a common fixture in the conflict in Ukraine. For example, in mid-August 2022, Ukraine's Armed Forces struck a Wagner mercenary headquarters in Popasna destroying the facility and killing an unverified number of Russian mercenary fighters. According to statements from Ukraine's Ministry of Defense, military forces identified the headquarters building after a Russian propagandist posted photos of the location on his Telegram page.[20]

Public information also holds vast amounts of geospatial, structural, and cultural information to help “characterize the function, criticality, and vulnerabilities” of potential targets, supporting deliberate target development.[21] Most often, this includes foundational intelligence information, such as the function of structures surrounding a military target, or the population’s composition and sympathies in an operating area. Sometimes, however, OSINT can be used to identify specific target locations for deliberate strikes. For example, the April 16, 2022, Russian missile strike on eastern Kyiv. The target—a workshop used to convert captured Russian equipment for Ukrainian use—was struck by multiple missiles after Ukraine’s 1+1 News network ran a story on the operation. After the story’s release, Rybar (a pro-Russian OSINT consortium) analyzed images from the video and published a report on VKontakte (a Russian social media platform) identifying the exact location of the workshop. Russia struck the site two days later destroying the factory and multiple captured military vehicles. Additionally, three Ukrainian civilians were reported killed in the strike.[22]

Open-Source Intelligence in Tactical Combat Assessment

The 2019 Chairman of the Joint Chiefs of Staff Instruction lists combat assessment, which includes the intelligence task of BDA, as another key component of the targeting process.[23] Here too, OSINT is providing regular and discrete contributions. After Ukraine’s mid-August 2022 strikes on Russia’s Saki airbase in Crimea, a combination of commercial imagery and social media videos verified the destruction of at least 10 Russian aircraft. Notably, a Russian Su-24, which was destroyed on the far west end of the airfield, did not appear on satellite imagery; however, separate ground-level social media videos verified its location and status despite apparent quick recovery by Russian forces.[24]

> “The wide use of smartphones among Ukraine’s population effectively means millions of civilians are armed with sensors, something extremely hard for the Russian army to prevent.[28]”

Commercial and private OSINT elements have also been surprisingly effective at cataloging combat losses. The resulting BDA registries rival the detail of public-sector intelligence agencies. Social media users like “OSINTtechnical” and “The Kyiv Independent”[25] catalog daily strikes and individual equipment losses, often including ground-level imagery from local witnesses. Analytics and conflict-tracking firms, such as the Turkish firm Oryx, catalog daily strikes and individual equipment losses from a host of secondary sources. They provide verification of the dates, locations, and equipment types destroyed by Ukrainian strikes. Many of these sources also provide BDA data at no charge and to the public, exposing the resident data to further scrutiny, and improving its reliability.[26]

Challenges and Vulnerabilities of Open-Source Intelligence Derived Targeting

While the previous examples demonstrate OSINT’s practical applicability to the tactical targeting process, timeliness and reliability remain challenges. This is a result of the volume of PAI available to an OSINT collector. The information available online, on almost any topic, is so expansive that finding precise information on an issue may be prohibitively time-consuming. For example, an early October 2022 search for Twitter posts related to artillery or airstrikes in Ukraine returned more than 1.5 million results. If each post took 10 seconds to review, an OSINT collector could review Twitter posts continuously for 6 months without reading the same post twice.[27] Of course, Twitter is just one of a multitude of online repositories capturing statements, claims, and observations regarding the Ukraine conflict. While automation and commercial data analytic tools mitigate some of the information overload, the problem is likely to persist as online networks continue to grow and diversify.

The reliability of online data is also a persistent challenge. America’s competitors are notorious for saturating online platforms with fake news, fraudulent personas, and biased content.[29] When applied deliberately and in a concerted manner, disinformation campaigns can overwhelm legitimate voices and create a corroboration challenge for OSINT collectors. One of the most noteworthy examples of this phenomenon was Russia’s attempt to use false flag incidents to justify the invasion of Ukraine. Fortunately, Ukrainian leaders effectively countered Russia’s propaganda campaign by using PAI to disprove Russia’s claims. Ukraine even turned the tables on Russia by using PAI to catalog the atrocities incited by Russian aggressors on the people and infrastructure of Ukraine, helping Ukrainian leaders garner and maintain international support.[30]

Conclusion

Russia’s 2022 invasion of Ukraine not only affirms the intelligence value of public data; it identifies several tactical applications for OSINT in a combat operations environment. OSINT offers a competitive advantage by tipping and cueing other intelligence disciplines, observing activity in denied locations, and delivering a releasable product to our allies and partners.[31] Like other intelligence disciplines, OSINT remains vulnerable to adversarial deception. However, the Russia-Ukraine conflict demonstrates that crowd-sourced PAI can be applied to target intelligence and BDA functions at the tactical level with significant effect. Moreover, repeated failed attempts by the Russians to disrupt the information environment in eastern Ukraine demonstrates the resiliency of modern communication networks, implying that high-volume public information will likely be available for exploitation in a large-scale combat operations environment.

Endnotes

[1] Chris Westcott, "Open source intelligence: academic research, journalism, or spying?" chap. 28 in *Routledge International Handbook of Universities, Security and Intelligence Studies* ed. Liam Francis Gearon (New York: Routledge, 2020).

[2] Jona Lendering, "Hannibal Barca," Articles on ancient history, Livius, last modified September 8, 2020, https://www.livius.org/articles/person/hannibal-3-barca/.

[3] Mark Cartwright, "William the Conqueror & the Ely Rebellion," *World History Encyclopedia*, last modified January 21, 2019, https://www.worldhistory.org/article/1321/william-the-conqueror--the-ely-rebellion/.

[4] Cameron Colquhoun, "A Brief History of Open Source Intelligence," OSINT, Bell¿ngcat, July 14, 2016, https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/.

[5] Pranshu Verma, "The rise of the Twitter spies," Technology, *Washington Post*, March 23, 2022, https://www.washingtonpost.com/technology/2022/03/23/twitter-open-source-intelligence-ukraine/.

[6] Department of the Army, Army Techniques Publication (ATP) 2-22.9, *Open-Source Intelligence* (Washington, DC: Government Publishing Office [GPO], 15 August 2019), VII.

[7] Daryna Krasnolutska, Arne Delfs, Alberto Nardelli, Aliaksandr Kudrytski, Aine Quinn, John Follain, and Kateryna Choursina, "A Visual Guide to the Russian Invasion of Ukraine," Bloomberg, https://www.bloomberg.com/graphics/2022-ukraine-russia-us-nato-conflict/.

[8] The Kyiv Independent news desk, "General Staff: Russia blocks Ukrainian mobile network operators, internet in nearly all occupied territories," Kyiv Independent, June 1, 2022, https://kyivindependent.com/uncategorized/general-staff-russia-blocks-ukrainian-mobile-network-operators-internet-in-nearly-all-occupied-territories.

[9] Miles O'Brien and Will Toubman, "Open source intelligence combats disinformation on Russia's war against Ukraine," anchored by Judy Woodruff, aired April 13, 2022, on *PBS News Hour*, https://www.pbs.org/newshour/show/open-source-intelligence-combats-disinformation-on-russias-war-against-ukraine.

[10] Dmytro V. Lande and Ellina V. Shnurko-Tabakova, "OSINT as a part of cyber defense system," *Theoretical and Applied Cyber Security* 1, no. 1 (2019): 104–108, http://tacs.ipt.kpi.ua/issue/view/10154.

[11] "OSINT group identifies more Russian war criminals in Donbas," War, Unian Press, April 27, 2017 https://www.unian.info/war/1897309-osint-group-identifies-more-russian-war-criminals-in-donbas.html; and Eliot Higgins, "Ukraine's Dnipro Battalion Combines Drone Footage with Open Source Intelligence," Ukraine, Bell¿ngcat, July 25, 2015, https://www.bellingcat.com/news/uk-and-europe/2015/07/25/ukraines-dnipro-battalion-combines-drone-footage-with-open-source-intelligence/.

[12] Sean D. Naylor, "Top Pentagon Intel Officer: Iraq 'May Not Come Back as an Intact State'," *Foreign Policy Magazine*, July 31, 2015, https://foreignpolicy.com/2015/07/31/top-pentagon-intel-officer-iraq-may-not-come-back-as-an-intact-state/.

[13] Brian Everstine, "Carlisle: Air Force intel uses ISIS 'moron's' social media posts to target airstrikes," Your Air Force, *Air Force Times*, June 4, 2015, https://www.airforcetimes.com/news/your-air-force/2015/06/04/carlisle-air-force-intel-uses-isis-moron-s-social-media-posts-to-target-airstrikes/.

[14] Adéla Klečková, "Open Source Intelligence and Terrorism" (Alumni Brief–1, Prague Security Studies Institute, Prague, Czech Republic, Feb 2021), https://www.pssi.cz/download/docs/8539_pssi-alumni-brief-01-osint-4.pdf.

[15] Christian Haimet and Thomas Bullock, "Russia/Ukraine - Coming of Age for OSINT?," interview by Harry Kemsley and Sean Corbett, The World of Intelligence Podcast, *Janes*, February 24, 2022, https://podcast.janes.com/public/68/The-World-of-Intelligence-50487d09/0fd51eaa.

[16] Pierre Vaux, "Putin in Syria," The Interpreter, September 17, 2015, https://www.interpretermag.com/putin-in-syria/.

[17] Houda Abadi, *Countering Daesh Propaganda: Action-Oriented Research for Practical Policy Outcomes* (Atlanta, GA: Carter Center, 2016), https://www.cartercenter.org/resources/pdfs/peace/conflict_resolution/countering-isis/counteringdaeshpropaganda-feb2016.pdf.

[18] U.S. Department of Defense, *2022 National Defense Strategy of The United States of America* (Washington, DC, October 27, 2022), 2.

[19] Office of the Chairman of the Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff Instruction 3162.02, *Methodology for Combat Assessment* (Washington, DC: The Joint Staff, 8 March 2019), B-1.

[20] Matt Burgess, "Their Photos Were Posted Online. Then They Were Bombed," Security, *Wired*, August 26, 2022, https://www.wired.co.uk/article/wagner-group-osint-russia-ukraine.

[21] Department of the Army, ATP 3-60, *Targeting* (Washington, DC: GPO, 7 May 2015), 2-8.

[22] Amra Dorjbayar, Archit Mehta, Ben Heubl, Brecht Castel, Kalim Ahmed, Alberto Olivieri, and the volunteers of GeoConfirmed, "Killer Coordinates: How a Russian missile hit Kyiv with the help of online sleuths," *Eyes on Russia* (blog), *Center for Information Resilience*, June 15, 2022, https://www.info-res.org/post/killer-coordinates-how-a-russian-missile-hit-kyiv-with-the-help-of-online-sleuths.

[23] Office of the Chairman of the Joint Chiefs of Staff, *Methodology for Combat Assessment*, B-1.

[24] HARM [pseud], "Operation Cigarette Butt: Ukraine's Covert Strike on Saki Air Base," T-Intelligence, August 15, 2022, https://t-intell.com/2022/08/15/operation-cigarette-butt-ukraines-covert-strike-on-saki-air-base/.

[25] OSINTtechnical (@Osinttechnical), "Ukrainian forces destroy a Russian T-80V and BREM-1 ARV with drone dropped munitions and artillery fire," Twitter, September 12, 2022, 5:24 p.m., https://twitter.com/Osinttechnical/status/1569481999743688704; and The Kyiv Independent (@KyivIndependent), "Ukraine's military destroys Russian equipment in southern Ukraine," Twitter, September 30, 2022, 6:34 p.m., https://twitter.com/KyivIndependent/status/1576022716934602752.

26. Stijn Mitzer and Jakub Janovsky, "Attack On Europe: Documenting Russian Equipment Losses During The 2022 Russian Invasion Of Ukraine," in collaboration with Joost Oliemans, Kemal, Dan, and naalsio26, Oryx, February 24, 2022, https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html.

27. Web search via Google API using search criteria: "site:twitter.com "Ukraine" AND (destroy OR airstrike OR bomb OR artillery)," October 3, 2022.

28. Magdalene Karalis, "Open-source intelligence in Ukraine: Asset or liability?" Russia and Eurasia Programme, Chatham House, 16 December 2022, https://www.chathamhouse.org/2022/12/open-source-intelligence-ukraine-asset-or-liability.

29. Sherry Ricchiardi, "How to use open source intelligence data to debunk Russian disinformation," Combating Mis- and Disinformation, International Journalists' Network, September 14, 2022, https://ijnet.org/en/story/how-use-open-source-intelligence-data-debunk-russian-disinformation.

30. Vanessa Smith-Boyle, "How OSINT Has Shaped the War in Ukraine," American Security Project, June 22, 2022, https://www.americansecurityproject.org/osint-in-ukraine/.

31. Department of the Army, ATP 2-22.9, *Open-Source Intelligence*, 1-4; and Department of the Army, ATP 3-60, *Targeting*, 1-1.

Mrs. Shelly L. Bailey is the Acting Director of the Army Open Source Center. She has over 28 years of intelligence experience as a counterintelligence agent, analyst, collection manager, and open-source manager. She has a master's degree in strategic intelligence from American Military University and has over 6 years of staff officer experience.

CW4 (retired) Jay Gack recently retired from the Army after 23 years of service and is currently a senior open-source advisor with Science Applications International Corporation. He previously managed the Army's main open-source intelligence (OSINT) pilot at the 513th Military Intelligence Brigade (Theater). Jay has a master's degree in strategic intelligence from National Intelligence University. He has contributed to myriad studies on technology and intelligence, including a 2019 Rand study on the military application of OSINT.