Security Journal
https://doi.org/10.1057/s41284-024-00446-0

ORIGINAL ARTICLE

Open-source intelligence and great-power competition under mediatization

Jiaxi Zhou[1]

Accepted: 21 August 2024

Abstract

With the rise of mediatization, open-source intelligence (OSINT) has evolved into a decentralized form of intelligence gathering, influenced by both political and commercial logic. This transformation has positioned social media as a primary source of OSINT, enhancing the capabilities of non-state actors and significantly impacting international politics, particularly in the realm of great-power competition. Through an analysis spanning individual, state, and systemic levels, this article examines OSINT's role in shaping contemporary international politics. By exploring case studies such as the Russo-Ukrainian War, Israel-Hamas War, and strategic competition between China and the United States, this article illuminates how OSINT influences decision-making processes and global power struggles and contributes to a deeper understanding of the evolving landscape of intelligence and its implications for statecraft.

Keywords Open-source intelligence · Great-power competition · Mediatization · Social media · Social media intelligence

Introduction

Open-source intelligence (OSINT) has a historical foundation dating back to pivotal developments such as the establishment of the BBC Monitoring Service in Britain in 1939 and the Foreign Broadcast Monitoring Service (FBMS) in the United States in 1941 (Baker 2023, 6; Block 2023, 4). OSINT has undergone profound changes in the past few decades, evolving from initial small-scale sharing to a form of intelligence that has a broad impact globally. Mediatization has accelerated the spread and sharing of information, providing valuable knowledge resources for individuals and collectives around the world. OSINT plays a new role in the era of mediatization,

✉ Jiaxi Zhou
zhoujiaxi@sass.org.cn

[1] Institute of International Relations, Shanghai Academy of Social Sciences, Room 126, No.7, Lane 622, Middle Huaihai Road, Shanghai 200020, China

Published online: 12 September 2024

and its influence on international politics is increasingly significant. Both state actors and non-state actors can obtain strategic information through OSINT (Stoddart 2022, 380–83).

However, the influence of OSINT comes with certain risks and challenges. Open sharing of information may lead to leakage of sensitive data, which poses threats to national security and personal privacy. The credibility and authenticity of information may be questioned, thereby affecting the accuracy and reliability of decisions. Additionally, OSINT has become part of great-power competition; not only does OSINT itself affect great-power relations, but the great powers also use OSINT gathering and analysis capabilities to dramatize threats. This article aims to summarize and encapsulate the changes and characteristics of OSINT under mediatization. Subsequently, cases at three levels—the individual, the state, and the state system—are analyzed to elaborate on the role of OSINT in international politics.

Literature review

OSINT holds a significant position in the U.S. intelligence community (IC). In 2006, the U.S. National Intelligence Agency defined OSINT as intelligence generated from publicly available information that is collected, exploited, and disseminated to appropriate audiences promptly to meet specific intelligence needs (U.S. Congress 2006). The former U.S. director of National Intelligence, Mike McConnell, referred to OSINT as the starting point for collection, in other words, finding the required intelligence first in open sources and then assigning classified collection sources (either technical or human) (Lowenthal 2012, 111).

In addition, there has been considerable discussion on the concept of OSINT. The amount of information collected by countries is referred to as Intelligence, Surveillance, and Reconnaissance (ISR), and the collection methods are divided into three types: OSINT, human intelligence (HUMINT), and technical intelligence (TECHINT) (Hwang et al. 2022, 1). According to RAND's research findings, OSINT has progressed into what they term its "third generation," signaling significant advancements in its methodologies and capabilities. Compared to the first two generations, its distinguishing feature is that it is based on machine learning and automated reasoning techniques. It has adopted a counter-strategy to the commonly adopted denial-of-access encryption while focusing on the collection and dissemination of information (Williams and Blum 2018, 40). As a result, significant progress has been made in third-generation OSINT, enabling more effective gathering, analysis, and dissemination of intelligence with the help of technologies such as machine learning and automated reasoning.

The core of OSINT is the ability to navigate an extraordinarily rich, complex information landscape (Glassman and Kang 2012, 674). Based on the use of data from open sources that emerged in an intelligence context, Block (2023, 1–3) defined OSINT as the methodical collection and exploitation of information from publicly available sources to fulfill intelligence requirements. OSINT, a collection discipline that does not include analysis and dissemination and does not perceive OSINT as a finalized product, is a systematic method of purposefully collecting and

utilizing information from open sources to meet intelligence requirements. However, the concept of OSINT involves not only the availability of open information but also challenges in language, expertise, and difficulty in obtaining information (Hatfield 2024, 400).

Mediatization denotes a period characterized by the pervasive influence of mass communication and digital platforms on societal, cultural, and institutional dynamics. It entails the increasing role of media in shaping social structures, political discourse, economic practices, and everyday communication processes, blending media logic seamlessly into various facets of human activity (Hjarvard 2008, 106–10; Couldry and Hepp 2013, 191–92; Kortti 2017, 117–20). The OSINT gathering in the era of mediatization has shifted from traditional channels such as letters, newspapers, radio, and television to predominantly internet-based media such as Web 2.0 and even Web 3.0 (Chauhan 2015, 16; Akhgar et al. 2016, 5; Jarmon 2019, 275; Evangelista et al. 2021, 2).

In the realm of international politics, the competition among great powers for intelligence gathering has intensified significantly. The advent of media logic has marked a significant turning point in international politics, intensifying the rivalry among leading nations for intelligence dominance, which has given rise to OSINT. Generally, great-power competition is not only a descriptor of a competitive mindset between great powers in their bilateral relationships but also refers to wrangling over advantage on a grand, global scale (Gaens and Sinkkonen 2020, 16). Since 2017, the Trump administration has reshaped American strategic guidelines to confront the rise of China and Russia, and the focus of U.S. foreign policy has shifted from unipolar hegemony to great-power competition (Colby and Mitchell 2020, 118–19). Great-power competition can be understood as power competition and geopolitical rivalry between the US, China, and Russia (Porter 2019, 7–9). The strategic planning and thinking of the US and China have shifted into competition modes in the trade, geopolitical, institutional, or pandemic realms (Goh 2022, 33). Hence, the contemporary great-power competition usually refers to competition among major countries such as the US, China, and Russia on a global scale to enhance their influence and geopolitical position. This competition involves multiple fields, including military, economy, diplomacy, and information.

The evolution of technology has made the media an extension of human beings, and the media has shifted from its original immateriality to materiality. As general social practices become entangled with the media, the line between communicative and physical action becomes blurred (Hepp 2020, 11). In the last decade, the internet has become the media of media, with the internet and social media redefining the concept of media and having a profound impact on how information is produced, disseminated, and consumed. The internet, especially social media, has become the primary source of data for OSINT (Omand et al. 2014, 24–25; Weissmann et al. 2021, 40; Henschke et al. 2024, 16–17), and its dependence on the internet continues to grow as a result of the increasing availability of online content and the emergence of artificial intelligence-driven data-processing tools. Therefore, OSINT is both a subject and an object, and its essence is a medium for dissemination.

In sum, incorporating OSINT into the perspective of mediatization and great-power competition can improve the understanding of information warfare,

psychological warfare in great-power competition, and the impact of mediatization on international politics. In particular, the 2022 Russo-Ukrainian War and the 2023 Israel-Hamas War highlighted the competition among great powers in the field of OSINT.

Methodology

Intelligence communication is a multifaceted process involving various actors, and the actions on OSINT from various actors form a complex network. Among the great powers, intelligence agencies and diplomatic missions aim to control the OSINT gathering from other entities. States utilize media as a crucial avenue for OSINT gathering. Simultaneously, states regulate media through various legislation to manage the information that circulates publicly. Non-state actors likewise engage with media for intelligence purposes while navigating state-imposed controls to ensure that their activities align with governing laws and regulations.

Waltz (2001, 16, 80, 159) designed three images in his work, *Man, the State, and War,* to explain the causes of war, which represented the individual, the state, and the state system. Recognizing the significance of individual decision-makers and the potential contributions of behavioral sciences, Singer (1960, 454–59) advocated for a more integrated and interdisciplinary method that carefully considers the interplay between the individual, the state, and the state system. Based on the level of analysis, this article places the concept of OSINT in the context of mediatization and great-power competition and explores how these two factors influence the concrete international practices of OSINT with qualitative cases.

At the first level, non-state actors utilize OSINT to alter their political influence on other entities. Non-state actors attempt to shift power paradigms, advocate for specific interests, or influence the actions of the state and other non-state actors. At the second level, state actors such as the US and China use national power to enhance their intelligence capability and compete with each other. The purpose of state actors is to change political influence and implement threats to other states. This is where the application of both hard and soft power comes into play. At the third level, the Russo-Ukrainian War and Israel-Hamas War demonstrate how major powers and non-state actors can influence the practical application of OSINT at the state system level.

The characteristics of OSINT under mediatization

With the evolution of media and changes in the forms of warfare, the sources of OSINT have become increasingly rich. At the same time, the main actors utilizing OSINT have evolved from state actors to a balance of state and non-state actors. OSINT, which was initially used in hot wars, gradually transitioned to the US-Soviet Cold War, after which it became part of hybrid warfare (Table 1). Although OSINT can provide critical intelligence support to states launching hybrid warfare, the process of mediatization (especially social media) is the main battleground for information warfare in hybrid warfare. By spreading fake news and disinformation on social

Table 1 Impact of Mediatization on Intelligence *Source: By author*

Actors	Form of Media	Media Process	Evolution of Intelligence Sources	Form of Warfare
State actors	Print media	Mass media becomes the main source of information	Letters, documents, newspapers, telegraphs	Hot war
Primarily state actors	Print media, electronic media	Mass media is independent of political forces	Television, radio	Cold War
State and non-state actors	Print media, electronic media, digital media	Political and social actors accept the internalization of mass media and media logic	Social media, blogs, online news, satellite images, Geographic Information Systems (GIS), public databases	Hybrid warfare

media, it is possible to influence the public opinion of hostile countries for the strategic purpose of hybrid warfare.

Hybrid warfare, a military strategy that encompasses conventional and irregular warfare, as well as cyber and information warfare, has significantly blurred the distinctions among terrorism, cyber terrorism, activism, and full-scale conflict, especially in the context of evolving social network media technologies (Nissen 2015, 10, 89). The concept of hybrid warfare has diffused across issues ranging from intelligence and propaganda to cyber war (Rauta 2020, 15).

In modern intelligence practice, OSINT plays an important role in helping actors obtain all types of information from open channels, which in turn provides valuable contributions to national security, business analysis, and many other areas, and its value is not limited to the individual value of its components but is also reflected in its role in the collection, synthesis, and presentation of information, which results in a unified and coherent media system. The main process of obtaining OSINT includes information gathering, collating, and analyzing, integrating its inherent value into different disciplines, and then transforming the raw information into actionable intelligence, which is ultimately disseminated through various forms of media. Based on the new media environment, OSINT retains its original characteristics while integrating new characteristics of the internet and intelligence.

OSINT, while remaining open, has become more timely with the growth of social media. New technologies are transferring previously nonpublic information from political and commercial elites to the global public, and ordinary citizens can relatively easily obtain information from various channels. Social media has become the mainstream mode of interaction in the "global village," and through the media of text, sound, image, and video, social media has built a complete virtual world. Thus, social media platforms are a major venue for the exchange of OSINT.

Given that people are reluctant to interact with their political opponents daily and that many build impressions of their opponents through the media, social media has increasingly become a means of influencing individuals' perceptions of the political environment (Kubin and von Sikorski 2021, 188). Platforms such as X/Twitter, Telegram, 4Chan, Discord, and SideChat diversify the obtainable intelligence. The political inclinations of different individuals and collectives will also be reflected in the process of OSINT communication.

Second, OSINT is a form of decentralized intelligence. OSINT may be subcontracted to other entities, and the more developed the intelligence gathering system or country is, the greater the need to subcontract intelligence. Especially in the era of mediatization, the ease of intelligence gathering is unparalleled. The *Wall Street Journal* has noted that OSINT poses a revolutionary challenge to the Central Intelligence Agency (CIA) and its sister spy agencies (Strobel 2022).

As network devices make it easier to access most information, texts, and images from anywhere in the world, intelligence faces new challenges. Its functioning is affected by conditions and phenomena created during civilization, namely, the development of information technology, the transparency of the modern world, and non-state actors (Ziółkowska 2018, 73). OSINT has become a form of media in its own right, and its impact on international political events of all kinds has become an inescapable issue for states.

Third, OSINT encompasses information from three areas: white, gray, and black. The use of special techniques in OSINT may hover at the edge of legality and illegality (Hribar et al. 2014, 530). With the rapid growth of open-source materials, OSINT managers face the challenge of effectively managing and utilizing massive amounts of information. To solve this issue, OSINT managers have no choice but to rely on various forms of data mining, utilizing computer-driven algorithms to classify sources as vast as the sea, creating useful and viable databases (Hulnick 2010, 234). In a rapidly evolving digital world, adhering to legal and ethical norms in OSINT operations is not just the right thing to do—it is crucial for maintaining professional credibility, avoiding litigation, and ultimately harnessing the full power of open-source materials responsibly.

Fourth, because OSINT is extracted from publicly available information, it is legally obtained and has a dual political and commercial logic. Political logic refers to the use of OSINT by government agencies to obtain intelligence information about potential opponents or enemies, especially military intelligence. Currently, OSINT is gradually moving from commercialization to security and militarization. Commercial logic refers to the fact that companies or organizations can use OSINT to obtain key information about their competitors' strategic intentions, product innovations, market trends, etc. The data provided by GM Insights show that the global OSINT market size will exceed $5 billion in 2022, and it is expected to grow at a compound annual growth rate of nearly 25% from 2023 to 2032.[1]

OSINT changes the asymmetrical standing of individuals and collectives

The information age has broadened access to offensive and investigative capacities for an array of non-state actors, thereby eroding the dominance of state intelligence services in producing and collecting information on security issues (van Puyvelde 2023, 19–37). From the perspective of Fidler (2008, 259), the anarchy of the international system is undergoing a transformation from the monopoly of state actors to the inclusion of non-state actors in the so-called "open source" international system. Therefore, unofficially supported non-state actors play the role of "players" and "spoilers" in great-power competition through a multiplicity of OSINT tools.

Bellingcat has emerged as a notable entity within the realm of the intelligence community. It conforms to the characteristics of open source, decentralization, and mediatization and has been featured in a series of international political events. Bellingcat has become the definitive judge in the information warfare, setting the standard for disinformation investigation techniques across journalism, academia, and cyber-intelligence. It has positioned itself as a "white-hat" hacking group and a public intelligence agency by leveraging its expertise in big data and open-source intelligence derived from sources like social media, satellites, and aviation trackers (Jutel 2023, 282).

[1] Data source: https://www.custommarketinsights.com/report/open-source-intelligence-osint-market/.

Members of Bellingcat are dispersed around the globe and form an "online collective" whose main findings are based on social media posts, leaked databases, and free satellite maps (Higgins 2022, 3). Bellingcat provides a general guide for beginners, resource materials for experienced investigators on specific techniques (e.g., geolocation, reverse image search, flight tracking), and an active, ongoing schedule of introductory and intensive seminars offered online according to time zones around the world, which specializes in the cumulative accumulation of small bits of evidence into a holistic, unified narrative in which every aspect and detail fits together coherently, reliably, and persuasively as evidence (Lievrouw 2011, 1941). In July 2017, Bellingcat published a summary of all OSINT data on the downing of Malaysia Airlines flight MH17, proving once again that the culprit in the incident was the Russian BUK-1 missile system, which was shipped from Russian territory and returned to Russia after the incident (McNair 2018, 32).

Apart from OSINT organizations such as Bellingcat, individuals are surrounded by numerous mediums, especially the increasing use of social media, which enables intelligence to spread rapidly through this carrier. The collection and dissemination of information by individuals may lead to black swan events. In light of the Snowden incident, black swan events related to OSINT, such as the Pentagon intelligence leak in early 2023, have often upended the traditional international political landscape in unexpected ways. On the other hand, national authorities can also identify and analyze potential black swan events through OSINT. In particular, the introduction of artificial intelligence technology may improve the prediction of black swan events (Wright 2020).

The 2023 Pentagon intelligence leak revealed the wide-ranging effects of the dissemination of OSINT through social media. The secretive global surveillance conducted by U.S. intelligence agencies on both allies and enemies has garnered widespread international attention and criticism. According to Bellingcat, the leaked documents were posted on the online chat platform Discord around the beginning of March 2023 and then spread to YouTube, 4chan, Telegram, Twitter, and other platforms. The leaker, United States National Guard Airman, Jack Teixeira, advocated a Discord chat group, bragging about the classified information he had received to a group of mainly teenagers.

Although the leaked document held South Korea-related information, South Korean media downplayed the Pentagon intelligence leak-related reports, while the government stated that the information contained in the leaked documents was inconsistent with the facts. At the same time, they indicated that the leaked documents might be evidence of American espionage and will ask the United States to take appropriate measures. The Pentagon announced that they would cooperate with South Korea. The main opposition party's whip, Park Hong-geun, stated that the U.S. government should thoroughly explain this case to the Korean people and protest strongly against allies. Israel denied the content in the Pentagon intelligence leaked documents related to Mossad. The Biden administration assured Israeli officials that Washington would uphold the security relations between the US and Israel.

Moreover, members of the Islamic State have previously camouflaged themselves as avid gamers, utilizing popular first-person shooter games such as the *Call of Duty*, among other social media platforms, in their attempts to appeal to

younger demographics for recruitment. The Black Lives Matter movement ignited in 2020 was a response to a series of incidents involving police brutality. This led to an alignment of U.S. government leaders with public sentiment, culminating in the apprehension of law enforcement officials implicated in these transgressions against black lives. Deploying OSINT, the public swiftly identified the associated police officer and subsequently uncovered details of his activities on Facebook. In the following developments, a photograph allegedly featuring the involved officer, Derek Chauvin, emerged.

OSINT from individuals can also provide exact information reference for certain government authorities. For instance, the X/Twitter user "Joseph-Wen___" maintains detailed deployment information of the People's Liberation Army (PLA) units through public data, using Google Maps' open platform for upload and update. The primary source of this user's information comes from military news reported on the China Central Television's *Xinwen Lianbo* (News Broadcast). By recording details such as types and numbers of military equipment, troop numbers, or honorific titles, as well as general geographic locations, the user progressively refines the data through public information sources and updates it daily.

As both the traditional media and the government succumb to the Tacitus Trap, public confidence in them progressively waned, with OSINT emerging as a perceived dependable and impartial information resource. Information overload has ushered in multitudinous avenues and a broader spectrum of content for individuals and collectives to access information. The advent of new media has exerted a significant influence on the traditional media industry, and the surge of social media platforms has amplified the velocity and expansion of information dissemination. Often, governments employ public relations strategies in the wake of unpredicted events aiming to curtail the proliferation of information that could tarnish their image. With enhancements in OSINT, the fidelity and trustworthiness of information sources have substantially increased, swaying public preference toward unofficial information over official information.

The proliferation of public spheres has enhanced the inclusivity and democracy of the intellectual milieu. This advancement has lessened the significance of traditional media, paving the way for novel means of journalist–audience interaction and encouraging dialogic and polyphonic discourse. New media channels act not only as outlets for unprocessed news but also as venues where analysis, interpretation, and the pursuit of truth transpire, permitting them to shape narratives and viewpoints on a range of issues. Interactions between OSINT subjects have become more frequent, with a convergence of OSINT gathering capabilities between state and non-state actors. Governments, journalists, and nongovernmental organizations now have access to a wealth of publicly available information from commercial surveillance satellites, drones, smartphones, and computers. Rapid advances in information technology have fueled an explosion in commercial surveillance capabilities, making it increasingly difficult for state actors to conceal their operations (Larkin 2016, 136).

Therefore, the process of mediatization leads both governments and individuals or collectives to conform to the logic of media, with an increase in information causing asymmetry for individuals and collectives when facing the government. The

political objectives behind individuals and collectives collecting and sharing OSINT are increasingly influential in international politics.

Chess in the China-US strategic competition

From the perspective of state actors, OSINT has become a key field for great-power competition, serving as an important tool for understanding opponents' capabilities and intentions, influencing policy decisions, and gaining an advantage in economy, military, and diplomacy, especially in the fields of artificial intelligence development, information warfare, and public opinion warfare. The main actors in the great-power competition in the OSINT field have transitioned from the US and Soviet Union to the US, Russia, and, notably, China. Its rapid rise in economic, technological, and military fields in recent years has made it a strategic competitor to the US.

In the field of OSINT, both countries have implemented several measures. One intelligence veteran observed that during the Cold War, 80 percent of the information about the Soviet Union was secret, and 20 percent was open (Lowenthal 2012, 84). After the Cold War, OSINT built a more sophisticated intelligence system for state actors, and government intelligence services have long used OSINT as a primary source of intelligence. Statistically, most of the 18 U.S. spy agencies have open-source programs, from the CIA's Open Source Enterprise (OSE) to the 10-person program of the Department of Homeland Security's intelligence division (Merchant 2023). Since China-US relations entered a period of strategic competition, the information war and the war of public opinion have become areas of competition among major powers in the new era.

The US has already begun to exaggerate the argument that China's OSINT gathering capabilities are stronger than those of the US. Based on findings from the Recorded Future, the PLA almost certainly views OSINT as an increasingly valuable source of military intelligence that can support decision-making, and state-owned companies, private companies, and think tanks also serve the PLA (Insikt Group 2023).

The U.S. intelligence community has revealed its *OSINT Strategy for 2024–2026*, highlighting OSINT's vital role in supporting national security policymakers comprehensively. The strategy is divided into four strategic focus areas: coordinating open-source data acquisition and expanding data sharing, establishing integrated open-source collection management, promoting OSINT innovation to provide new capabilities, and cultivating the next-generation OSINT workforce and skills. Furthermore, the strategy also recognized the need for effective governance and cooperation with industry, academia, and foreign peers (ODNI 2024a).

In the *2024 Annual Threat Assessment* released by the Office of the Director of National Intelligence (ODNI), the U.S. intelligence community identified China as the most active and persistent cyber threat, with the Chinese government's cyber espionage and promotion of surveillance technologies increasing the risk of cyber-attacks against the U.S., while also aiming to bolster its domestic tech sectors, challenge U.S. national security, and enhance its global influence (ODNI 2024b, 11–12). China is employing data exploitation and technology as a weapon to achieve

strategic goals and undermine its opponents' will and capacity to resist (McNeil 2023).

The Federal Bureau of Investigation (FBI) spent $27 million on social media search software to collect information on platforms such as Twitter, even involving Chinese microblogs, and the demand includes services such as region-specific social media searches, foreign-language translations, and user sentiment analysis. The CIA established two new mission centers in 2021, one of which is aimed at China.

The U.S. intelligence community has also adopted a "whole-government, whole-society" approach to counter China's intelligence threats. For instance, intelligence tasks can be subdivided among technology companies. The technology firm Leidos secured a $143 million contract with the Defense Intelligence Agency (DIA) for the creation and execution of a Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED) system, catering to DIA's Open Source Intelligence Integration Centre (OSIC). This initiative is a part of the wider-ranging DOMEX Technology Platform (DTP), with the objective of optimizing the processing and enrichment process of significant volumes of unstructured, varied multimodal data throughout the Department of Defense and the intelligence community.

From the side of Congress, actions on China's threat have been taken. The U.S. House Select Committee on Strategic Competition between the United States and the Chinese Communist Party (CCP) has actively addressed a range of intelligence issues related to China since its formation. The committee held hearings on "The CCP Cyber Threat to the American Homeland and National Security" and "The CCP's Strategy to Shape the Global Information Space," emphasizing America's ongoing concerns about China's cyber espionage capabilities and their impact on American national security. In the *Intelligence Authorization Act for Fiscal Year 2023*, the House Intelligence Committee illustrated that the Fiscal Year 2023 budget request for the CIA's OSE did not include new investments in OSINT capabilities, and the Committee has authorized additional funding.

The U.S. intelligence community has also been issuing guidelines and ethical codes for the use of OSINT, and congressional bills targeting the so-called Chinese OSINT gathering have been gradually introduced. The U.S. *Global Technology Leadership Act* established an "Office of Global Competitive Analysis," composed of experts from the intelligence community, the Pentagon, and other relevant agencies, to conduct assessments using intelligence and private sector commercial data. In the future, the US will take more measures to improve OSINT gatherings, especially for OSINT gatherings from China.

In response to U.S. accusations, China faces increased cyberattacks and intelligence threats. China's National Virus Emergency Response Center (NVERT) published an analysis named "'Empire of Hacking': The U.S. Central Intelligence Agency," in which various cyber weapons, hacking tools, and methods utilized by the CIA for their cyber espionage operations, including Fluxwire, Athena, Grasshopper, Hive, and ChimayRed, were identified.[2] Additionally, reports from NVERT

[2] See the report: http://ge.china-embassy.gov.cn/eng/xwdt/202305/P020230504759606506706.pdf.

and tech-company 360 have noted that the CIA often uses off-the-shelf open-source hacking tools to carry out attacks and plan "color revolutions."

To address the increasing severity of external intelligence gathering, China has taken corresponding measures to strengthen domestic security control. Balding (2020, 2–4) found that leaked data from a particular company in Shenzhen, the China Revival, disclosed a database named the Overseas Key Information Database (OKIDB) containing vast information about approximately 2.4 million people worldwide through open-source channels. This approach has led to accusations against China of using data to enhance its intelligence and security measures and influence its operations. Since 2015, China has successively passed the *National Security Law*, *National Intelligence Law*, *Cyber Security Law*, and *Anti-Espionage Law*. The expansion of the *Anti-Espionage Law* has made it difficult for foreign firms to access key business data, such as financial information, patents, and yearbooks, which negatively affects foreign investment in China (Palmer 2024).

From a broader perspective, the competition between the US and China, pertaining to OSINT, has intensively flourished to the point of incorporating a "whole-government, whole-society" approach. This intense competition is projected to maintain its presence in the dynamics of the future. The tireless efforts poured into intelligence aggregation and scrutiny by both of these countries indicate a nascent and accelerating pattern in strategic competition. This escalating trend has been accompanied by an upsurge in claims relating to the exploitation of intelligence made by each country, signifying an increasingly complex narrative of mutual mistrust and apprehension.

Simultaneously, both countries have robustly scaled up their governmental intelligence machinery to respond effectively in this playing field. Intelligence agencies have maximized the use of open-source tools to improve their ability to gather, analyze, and translate raw data into actionable insights. Moreover, both China and the US have delegated intelligence gathering tasks to technology companies.

Shine brilliantly through contemporary war

The evolution and expansion of OSINT, facilitated by new information and communication technologies, have enabled civilians to play a larger role in providing information for intelligence gathering (Henschke et al. 2024, 196–97). The information age and subsequent data revolution have led to a persistent call for increased OSINT capability following the outbreak of the 2022 Russo-Ukrainian War (Farhadi et al. 2023, 231). It has been a typical form of hybrid warfare under mediatization, in which OSINT played a crucial role in debunking disinformation and providing evidence of the truth (Varzhanskyi 2024, 427–28; Karalis 2024, 515–17).

Prior to the war, journalists and researchers from Western countries confirmed the claims about Russia preparing a special military operation through commercial satellite images and video footage of Russian convoys on TikTok and traffic jam information displayed on Google Maps. During the war, analysts were able to judge battlefield situations through key information. For example, an amateur analyst on Twitter tracked the progress of the Ukrainian military in the battle of Kherson by

geographically locating images and comparing trees, buildings, and other features with satellite images on Google Maps and similar services. Furthermore, analysts such as Rob Lee have already posted nearly four thousand tweets, including battle damage assessments, weapon videos, and ongoing records of aerial losses. Christov Grozev, a Bulgarian investigative journalist, has also conducted an in-depth analysis of disinformation (Kemp 2022). UAWarData has created a moving map of the Russian military on the front lines, updated approximately every three days, while a user of MapHub has created an "Eye on Russia" project, setting up a database of images organized by content.

In the Russo-Ukrainian War, weaponized disclosure has been employed by various actors, including intelligence agencies and governments, to disseminate information that supports their respective positions. For instance, the Open Source Center (OSC) at the University of California, Berkeley, has been actively involved in collecting and analyzing publicly available information related to the war, including social media posts, news articles, and other online content. This information is then used to inform policy decisions and shape public opinion. In addition, by risking the exposure of sensitive intelligence, the US effectively communicated its advanced awareness of Russia's plans and intentions, possibly achieving deterrence. In this crisis, the open-source community has demonstrated its value, but particularly for the Western body politic (Huminski 2023, 10–15).

The impact of the weaponization of social media on contemporary international politics includes the redistribution of international power relations, changes in contemporary conflicts, and changes in the objectives and modalities of warfare. The weaponization of social media has also altered traditional conceptions of war and the environment in which war is fought, creating new asymmetries and virtual battlefields. Zegart (2023, 54–55) calls the Russo-Ukrainian War a watershed moment for the intelligence community, with technological advances at the center of this evolution and individual citizens and groups becoming contributors to OSINT. Meanwhile, OSINT turned the Russo-Ukrainian War into a live war, which refers to real time. Asmolov (2021, 2) has even proposed the concepts of couch warfare and couch forces, which refer to remote participation in war.

Despite being absorbed by Western war narratives, OSINT has assisted entities such as the US and NATO in exposing Russia's war crimes and human rights violations in Ukraine. As such, OSINT has also been declared a legitimate tool for international criminal justice investigations (Hogue 2023, 108).

In addition to being a unique occurrence, the 2023 Israel-Hamas War has also become a typical case of OSINT application in contemporary war. OSINT offers insights into military operations, human rights violations, and the verification of contested events. The origins of the Israel-Hamas War can be traced back to the blockade of Gaza, which incited a humanitarian crisis in the region. Hamas, the de facto governing authority of Gaza, has long been an adversary of Israel. In retaliation against Israel or in an effort to dismantle the blockade, Hamas utilized OSINT to identify vulnerabilities within Israel's defense system along the Gaza-Israel border area.

This war involves not only Hamas and Israel but also the competition between pro-Israel Western countries, represented by the US, and those supporting Hamas.

Once again, digital media and social networks have become the major sources of intelligence gathering and dissemination; meanwhile, they are filled with propaganda, analysis, disinformation, etc., related to both sides of the war. One of the notable examples of OSINT in this war was the investigation of the deadly blast at the al-Ahli Arab Hospital in Gaza City. Initial reports suggested that the bombing from the Israeli Defence Forces resulted in casualties, but OSINT analysis from various institutions in Western countries indicated that the explosion was due to a failed rocket launch from Gaza.

The intelligence from the US has to some extent helped Israel gain a voice. The White House National Security Council spokesperson Adrianna Watson refuted allegations that Israel had bombed a hospital in Gaza City shortly after the war broke out. She announced that aerial imagery, intercepted information, and open-source information were the real culprits of misfired rockets launched by a terrorist organization in Gaza. By November, the White House spokesman John Kirby shared a declassified intelligence assessment indicating that Hamas had been using the hospital as a command and control node, a weapon depot, and a hiding place for Israeli hostages (Gioe and Morell 2024, 146).

Non-state actors notably emerged and demonstrated their influence in the Israel-Hamas War. OSINT analysts and journalists controlled Israel's information environment during the war and became pro-Israel and anti-Hamas channels, such as the X account "OSINT Defender," which mistook civilians for Hamas terrorists (Kenney-Shawa 2024). On the other hand, Bellingcat has developed a process intended to use OSINT in legal processes for the Russo-Ukrainian War and hopes to apply this process in the Israel-Hamas War (IWPR 2023). Bellingcat analyzed footage from the sites of two attacks at Kibbutzim in Israel using geolocation to learn what happened, and the *Washington Post* used videos, photos, and satellite images to map some of the places where the Israeli Defence Forces have advanced inside Gaza (Kahn 2023).

In the two wars, the presence of OSINT was clearly discernible. It has embroidered a fresh media logic within the interaction between non-state actors and state actors. This kind of logic fundamentally restructures how these entities communicate and negotiate, intensifying the complexities of their interactions. At the same time, when observed from the perspective of the international system, the open-source international system accentuates the struggle surrounding various interests. The entities engaged in the system, whether state or non-state, are vying for benefits in this new landscape of open-source networks and systems. Social media will never be seen as just another platform for dialog but rather as the "go-to" platform for shaping narratives within each sphere of national power to secure national interests (Putter and Henrico 2022, 21).

Conclusions

The first impact of OSINT is that individuals and collectives can access intelligence more easily, narrowing the information gap between government agencies and political elites. Second, OSINT has itself become an integral part of great-power

competition, involving information warfare, psychological warfare, public opinion warfare, and technological competition. In the future, OSINT gathering and analysis driven by artificial intelligence technology will be more precise and convenient, further enhancing the intelligence acquisition and analysis capabilities of states, individuals, and collectives. This poses certain challenges to national security for various countries and necessitates greater requirements for the reform of international cyberspace security mechanisms.

However, with the advancement of artificial intelligence, the interweaving of truth and disinformation has placed greater demands on the capabilities of intelligence analysts in various countries. The evolution of digital media has expanded both the subjects and scope of dissemination, increasing the speed and reach of disinformation. Disinformation will lead to miscalculation by the government and the public and disturb the normal information dissemination environment, which will affect social stability and interstate relations. The ability to collect OSINT under mediatization requires not only individuals with rich professional knowledge, open internet media tools, networked OSINT collectors, and professional intelligence agencies for further analysis and research but also for verifying the authenticity of the information.

Declarations

Conflict of interest No potential conflicts of interest were reported by the author.

References

Akhgar, Babak, P. Saskia Bayerl, and Fraser Sampson, eds. 2016. *Open source intelligence investigation: From strategy to implementation*. 1st ed. Cham: Springer

Asmolov, Gregory. 2021. From sofa to frontline: The digital mediation and domestication of warfare. *Media, War & Conflict* 14 (3): 342–365. https://doi.org/10.1177/1750635221989568.

Baker, Rae L. 2023. *Deep dive: Exploring the real-world value of opensource intelligence*. Indianapolis: John Wiley and Sons.

Balding, Christopher. 2020. *Chinese open source data collection, big data, and private enterprise work for state intelligence and security: The case of Shenzhen Zhenhua*. Rochester: SSRN Scholarly Paper.

Block, Ludo. 2023. The long history of OSINT. *Journal of Intelligence History*, 1–15. https://doi.org/10.1080/16161262.2023.2224091.

Chauhan, Sudhanshu. 2015. *Hacking web intelligence: Open source intelligence and web reconnaissance concepts and techniques*, 1st ed. Amsterdam: Elsevier.

Colby, Elbridge A., and A. Wess Mitchell. 2020. The age of great-power competition: How the Trump administration refashioned American strategy. *Foreign Affairs* 99 (1): 118–130.

Gaens, B., and V. Sinkkonen, eds. 2020. *Great-power competition and the rising US-China Rivalry: Towards a new normal?* Helsinki: Finnish Institute of International Affairs.

U.S. Congress. 2006. *National defense authorization act for fiscal year 2006*. Washington, DC: U.S. Government Printing Office. https://www.govinfo.gov/app/details/PLAW-109publ163. Accessed 22 Jul 2023.

Couldry, Nick, and Andreas Hepp. 2013. Conceptualizing mediatization: Contexts, traditions, arguments. *Communication Theory* 23 (3): 191–202. https://doi.org/10.1111/comt.12019.

Evangelista, João Rafael Gonçalves, Renato José Sassi, Márcio Romero, and Domingos Napolitano. 2021. Systematic literature review to investigate the application of open source intelligence (OSINT)

with artificial intelligence. *Journal of Applied Security Research* 16 (3): 345–369. https://doi.org/10.1080/19361610.2020.1761737.

Farhadi, Adib, Mark Grzegorzewski, and Anthony J. Masys, eds. 2023. *The great power competition volume 5: The Russian invasion of Ukraine and implications for the central region*. Cham: Springer Nature Switzerland.

Fidler, David P., 2008. A theory of open-source anarchy. *Indiana Journal of Global Legal Studies* 15 (1): 259–284. https://doi.org/10.2979/gls.2008.15.1.259.

Gioe, David V., and Michael J. Morell. 2024. Spy and tell: The promise and peril of disclosing intelligence for strategic advantage. *Foreign Affairs* 103 (3): 138–152.

Glassman, Michael, and Min Ju Kang. 2012. Intelligence in the internet age: The emergence and evolution of open source intelligence (OSINT). *Computers in Human Behavior* 28 (2): 673–682. https://doi.org/10.1016/j.chb.2011.11.014.

Goh, Evelyn. 2022. The Asia–Pacific's "age of uncertainty": Great power competition, globalisation and the economic-security nexus. In *From Asia-Pacific to Indo-Pacific: Diplomacy in a contested region*, ed. Robert G. Patman, Patrick Köllner, and Balazs Kiglics, 29–52. Singapore: Springer. https://doi.org/10.1007/978-981-16-7007-7_2.

Hatfield, Joseph M. 2024. There is no such thing as open source intelligence. *International Journal of Intelligence and Counterintelligence* 37 (2): 397–418. https://doi.org/10.1080/08850607.2023.2172367.

Henschke, Adam, Seumas Miller, Andrew Alexandra, Patrick F. Walsh, and Roger Bradbury. 2024. *The ethics of national security intelligence institutions: Theory and applications*. London: Routledge. https://doi.org/10.4324/9781003106449.

Hepp, Andreas. 2020. *Deep Mediatization: Key ideas in media and cultural studies*. London: Routledge

Higgins, Eliot. 2022. *We are bellingcat: An intelligence agency for the people*. London: Bloomsbury Publishing.

Hjarvard, Stig. 2008. The mediatization of society. *Nordicom Review* 29 (2): 102–131. https://doi.org/10.1515/nor-2017-0181.

Hogue, Simon. 2023. Civilian surveillance in the war in Ukraine: Mobilizing the agency of the observers of war. *Surveillance & Society* 21 (1): 108–112. https://doi.org/10.24908/ss.v21i1.16255.

Hribar, Gašper, Iztok Podbregar, and Teodora Ivanuša. 2014. OSINT: A 'grey zone'? *International Journal of Intelligence and CounterIntelligence* 27 (3): 529–549. https://doi.org/10.1080/08850607.2014.900295.

Hulnick, Arthur S. 2010. The dilemma of open sources intelligence: Is OSINT really intelligence? In *The oxford handbook of national security intelligence*, ed. Loch K. Johnson, 229–241. New York: Oxford University Press.

Huminski, Joshua C. 2023. Russia, Ukraine, and the future use of strategic intelligence. *Prism* 10 (3): 8–25.

Hwang, Yong-Woon., Im-Yeong. Lee, Hwankuk Kim, Hyejung Lee, and Kim Donghyun. 2022. Current status and security trend of OSINT. *Wireless Communications and Mobile Computing* 2022: 1–14. https://doi.org/10.1155/2022/1290129.

Insikt Group. 2023. "Private Eyes: China's Embrace of Open-Source Military Intelligence." Recorded Future. June 1, 2023. https://go.recordedfuture.com/hubfs/reports/ta-2023-0601.pdf. Accessed 13 May 2024.

IWPR. 2023. "Interview: The War on Disinformation." Institute for War & Peace Reporting. November 1, 2023. https://iwpr.net/global-voices/spotlight/israel-hamas-conflict. Accessed 10 May 2024.

Jarmon, Jack A. 2019. *The new era in U.S. national security: Challenges of the information age*. Lanham: Rowman & Littlefield.

Jutel, Olivier. 2023. Platform governance and the hybrid war industrial complex. In *Russiagate revisited: The aftermath of a hoax*, ed. Oliver Boyd-Barrett and Stephen Marmura, 271–93. Cham: Springer. https://doi.org/10.1007/978-3-031-30940-3_13.

Kahn, Gretel. 2023. "The Israel-Hamas War Highlights the Power (and the Limits) of Open-Source Reporting." Reuters Institute for the Study of Journalism. December 8, 2023. https://reutersinstitute.politics.ox.ac.uk/news/israel-gaza-war-highlights-power-and-limits-open-source-reporting. Accessed 10 May 2024.

Karalis, Magdalene. 2024. Fake leads, defamation and destabilization: How online disinformation continues to impact Russia's invasion of Ukraine. *Intelligence and National Security* 39 (3): 515–524. https://doi.org/10.1080/02684527.2024.2329418.

Kemp, Robin. 2022. "OSINT's Influence on the Russian Air Campaign in Ukraine and the Implications for Future Western Deployments." Atlantic Council. August 30, 2022. https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/osints-influence-on-the-russian-air-campaign-in-ukraine-and-the-implications-for-future-western-deployments/. Accessed 1 Aug 2023.

Kenney-Shawa, Tariq. 2024. "Israel's Disinformation Apparatus: A Key Weapon in Its Arsenal." Al-Shabaka. March 12, 2024. https://al-shabaka.org/briefs/israels-disinformation-apparatus-a-key-weapon-in-its-arsenal/. Accessed 10 May 2024.

Kortti, Jukka. 2017. Media history and the mediatization of everyday life. *Media History* 23 (1): 115–129. https://doi.org/10.1080/13688804.2016.1207509.

Kubin, Emily, and Christian von Sikorski. 2021. The role of (social) media in political polarization: A systematic review. *Annals of the International Communication Association* 45 (3): 188–206. https://doi.org/10.1080/23808985.2021.1976070.

Larkin, Sean P. 2016. The age of transparency: international relations without secrets. *Foreign Affairs* 95 (3): 136–146.

Lievrouw, Leah A. 2011. *Alternative and activist new media*. 1st ed. Malden: Polity.

Lowenthal, Mark M. 2012. *Intelligence: From secrets to policy*. Washington, DC: CQ Press.

McNair, Brian. 2018. *Fake news: Falsehood, fabrication and fantasy in journalism*. London: Routledge

McNeil, Shane. 2023. "China's Data War Against the U.S." American Purpose. November 30, 2023. https://www.americanpurpose.com/articles/chinas-data-war/. Accessed 13 May 2024.

Merchant, Nomman. 2023. "US Spies Lag Rivals in Seizing on Data Hiding in Plain Sight." AP News. January 12, 2023. https://apnews.com/article/politics-russia-government-ukraine-china-us-central-intelligence-agency-6ed827c92bfbdca0c033483b5cc28d9d. Accessed 23 Jun 2023.

Nissen, Thomas Elkjer. 2015. *#TheWeaponizationOfSocialMedia-@Characteristics_of_Contemporary_Conflicts*. Copenhagen: Royal Danish Defence College.

ODNI. 2024b. *Annual Threat Assessment of the U.S. Intelligence Community*. Washington, DC: Office of the Director of National Intelligence.

Omand, David, Carl Miller, and Jamie Bartlett. 2014. Towards the discipline of social media intelligence. In *Open source intelligence in the twenty-first century: New approaches and opportunities*, ed. Christopher Hobbs, Matthew Moran, and Daniel Salisbury. London: Palgrave Macmillan UK.

Palmer, James. 2024. "China's latest data restrictions could scare off investors." Foreign Policy. May 2, 2023. https://foreignpolicy.com/2023/05/02/china-anti-espionage-law-foreign-investment-business-data/. Accessed 13 May 2024.

Porter, Patrick. 2019. Advice for a dark age: Managing great power competition. *The Washington Quarterly* 42 (1): 7–25. https://doi.org/10.1080/0163660X.2019.1590079.

Putter, Dries, and Susan Henrico. 2022. Social media intelligence: The national security-privacy nexus. *Scientia Militaria, South African Journal of Military Studies* 50 (1): 19–44. https://doi.org/10.5787/50-1-1345.

Rauta, Vladimir. 2020. Towards a typology of non-state actors in 'hybrid warfare': Proxy, auxiliary, surrogate and affiliated forces. *Cambridge Review of International Affairs* 33 (6): 868–887. https://doi.org/10.1080/09557571.2019.1656600.

ODNI. 2024a. "The IC OSINT Strategy 2024–2026." Office of the Director of National Intelligence. March 8, 2024. https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf. Accessed 6 May 2024.

Singer, J. David. 1960. International conflict three levels of analysis. *World Politics* 12 (3): 453–461. https://doi.org/10.2307/2009401.

Stoddart, Kristan. 2022. Non and sub-state actors: cybercrime, terrorism, and hackers. In *Cyberwarfare: threats to critical infrastructure*, ed. Kristan Stoddart, 351–399. Cham: Springer.

Strobel, Warren P. 2022. "Rise of Open-source Intelligence Tests U.S. Spies." Wall Street Journal. December 11, 2022. https://www.wsj.com/articles/rise-of-open-source-intelligence-tests-u-s-spies-11670710806. Accessed 23 Aug 2023.

van Puyvelde, Damien. 2023. Intelligence adaption from the cold war to the resurgence of great power politics. In *Intelligence cooperation under multipolarity: non-american perspectives*, ed. Thomas Juneau, Justin Massie, and Marco Munier, 19–37. Toronto: University of Toronto Press.

Varzhanskyi, Illia. 2024. Reflexive control as a risk factor for using OSINT: Insights from the Russia-Ukraine conflict. *International Journal of Intelligence and CounterIntelligence* 37 (2): 419–449. https://doi.org/10.1080/08850607.2023.2228489.

Waltz, Kenneth N. 2001. *Man, the state and war: A rheoretical analysis*. New York: Columbia University Press.

Weissmann, Mikael, Niklas Nilsson, Per Thunholm, and Björn Palmertz, eds. 2021. *Hybrid warfare: Security and asymmetric conflict in international relations*. Bloomsbury Academic, 2021, New York: I.B. Tauris.

Williams, Heather J., and Ilana Blum. 2018. *Defining second generation Open source intelligence (OSINT) for the defense enterprise*. Santa Monica: RAND | National Defense Research Institute.

Wright, Alex. 2020. "Using AI to Predict Black Swan Events in Insurance." Raconteur. November 19, 2020. https://www.raconteur.net/finance/ai-black-swan. Accessed 10 Aug 2023.

Zegart, Amy. 2023. Open secrets: Ukraine and the next intelligence revolution. *Foreign Affairs* 102 (1): 54–70.

Ziółkowska, Agata. 2018. Open source intelligence (OSINT) as an element of military recon. *Security and Defence Quarterly* 19 (2): 65–77.