BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 3 (XLVIII)
DOI: 10.48269/2451-0718-btip-2022-3-022
Received: 19.01.2022
Accepted: 6.05.2022

Miron Lakomy
PhD, Associate Professor, University of Silesia, Katowice, Poland
https://orcid.org/0000-0002-7591-1402

Assessing the potential of OSINT on the Internet in supporting military operations

Introduction

Open-source intelligence (OSINT) has usually been defined as "intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."[1] While open-source information is as old as humanity itself, its collection and analysis in a deliberate manner to meet the needs of the intelligence community has emerged relatively recently. The first dedicated OSINT cells were developed in the United States and the United Kingdom during World War II. In the United States, the University of Princeton established a Foreign Broadcast Monitoring Service (FBMS), which was tasked with monitoring radio propaganda of the Axis powers. After the war, the Central Intelligence Agency took over the cell. In Great Britain, BBC Monitoring was created. It recorded and translated broadcasts from Nazi Germany and other Axis states.[2] During the Cold War, the significance of OSINT increased. Both sides of the international rivalry collected

[1] H.J. Williams, I. Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, Santa Monica: RAND Corporation, 2018, p. 1.

[2] A.A. Imholtz Jr., "The American (FBIS) Side of the Story", https://www.iwm.org.uk/sites/default/files/files/2018-11/The%20American%20%28FBIS%29%20Side%20of%20the%20Story%20-%20August%20Imholtz%20.pdf [accessed: 5 January 2022].

and analysed open-source information in a deliberate and massive manner. For instance, the East German Stasi was capable of analysing approximately as many as 1000 Western magazines and 100 books per month.[3]

However, the real breakthrough in OSINT activities took place in the post-Cold War era. Three processes contributed to this shift. To begin with, we could witness the process of broadening the concept of security.[4] In effect, while collecting open-source information related to military affairs was somewhat difficult at the time, OSINT offered tremendous opportunities in understanding economic and social processes. Secondly, the 9/11 terrorist attacks took place. They proved that traditional forms of intelligence, such as Human Intelligence (HUMINT) and Signals Intelligence (SIGINT), were insufficient. State authorities reacted to these events by placing greater emphasis on collecting and analysing open-source data. This trend was manifested in creating the Open Source Center under the U.S. Director of the National Intelligence in 2005.[5] Last but not least, we witnessed the advent of the Internet becoming the medium consisting of an unprecedented – and constantly growing – amount of open-source data that can be manually, semi-automatically and automatically detected, extracted, processed, and analysed.[6]

In this context, the Internet has become an environment offering enormous opportunities to military intelligence. It consists of a variety of communication layers that can be utilised to benefit the armed forces. Aside from Web 1.0, composed of ordinary standalone websites or message boards, there is also Web 2.0, which is abundant in open-source data.[7] It comprises social networks, gathering billions of Internet users, blogs, file-sharing and file-stream services, and a broad spectrum of more specialised services, including web mapping platforms. Finally, in the 21st century, the so-called "dark web" emerged. This anonymity-oriented environment has become

---

3 K. Tylutki, "Informacja masowego rażenia – OSINT w działalności wywiadowczej", *Przegląd Bezpieczeństwa Wewnętrznego*, no. 19, 2018, p. 178.

4 See: R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego*, Warszawa: Wydawnictwo Scholar, 1999.

5 H. Bean, "The DNI's Open Source Center: An Organizational Communication Perspective", *International Journal of Intelligence and CounterIntelligence*, vol. 20, issue 2, 2007, pp. 240–257, https://doi.org/10.1080/08850600600889100; *Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Riskd Assessment of the Committee on Homeland Security House of Representatives, One Hundred Ninth Congress, First Session, June 21, 2005, Serial No. 109-22*, Washington: U.S. Government Printing Office, 2007, https://www.govinfo.gov/content/pkg/CHRG-109hhrg24962/html/CHRG-109hhrg24962.htm [accessed: 5 January 2022].

6 I. Böhm, S. Lolagar, "Open source intelligence. Introduction, legal, and ethical considerations", *International Cybersecurity Law Review*, no. 2, 2021, pp. 318–319, https://doi.org/10.1365/s43439-021-00042-7.

7 Ł. Sarowski, "Od Internetu Web 1.0 do Internetu Web 4.0 – ewolucja form przestrzeni komunikacyjnych w globalnej sieci", *Rozprawy Społeczne*, vol. 11, no. 1, 2017, pp. 32–39, https://doi.org/10.29316/rs.2017.4.

a significant point of contact for the cybercriminal underground.[8] This means that it holds tremendous importance for the law enforcement and intelligence communities.

This paper aims to briefly discuss how the immense potential of the Internet can be utilised to support activities of the armed forces. It explores this topic in two particular dimensions. On the one hand, it examines how OSINT on the Internet can support conventional military operations. On the other, it also overviews the basic techniques that allow supporting cyber warfare. However, it should be emphasised that this paper has a significant limitation. Primarily due to the length limit, it mentions only a fraction of the existing and dominating approaches to military OSINT investigations subject to continuous and dynamic changes related to the development of new technologies, services, and software. Thus, this article should be treated as a mere introduction to this subject. This paper is based on the content and critical analysis of literature on OSINT and its potential for supporting military operations.

The advent and evolution of military-related open-source intelligence on the Internet

The military application of open-source intelligence on the Internet can be traced back to the beginning of the 21st century. Its significance and potential grew in time due to several processes. The first is related to the fact that in the last two decades, the number of Internet users has dynamically increased from approximately 400 million in 2000 to 4.6 billion in 2022.[9] Most of these users leave their posts, comments, pictures, and videos online, contributing to the constantly increasing amount of publicly available open-source data. This process has become especially evident since the advent of Web 2.0. When social media emerged, the Internet users became more engaged in creating online content. This process was combined with the emergence of a variety of new technologies. For instance, the introduction of smartphones with cameras enabled ordinary users to quickly and cheaply take pictures and record videos, which could be instantly posted online.[10] This was combined with the popularisation of broadband Internet access, which facilitated prompt uploading of these materials. This also corresponded with the emergence of the satellite imagery services.

Overall, the emergence of Web 2.0 marked a significant breakthrough in military intelligence, as a variety of new open sources of data emerged. This became evident

---

8 D. Mider, "Czarny i czerwony rynek w sieci The Onion Router – analiza funkcjonowania darkmarketów", *Przegląd Bezpieczeństwa Wewnętrznego*, no. 21, 2019, pp. 154–190.

9 See: M. Roser, H. Ritchie, E. Ortiz-Ospina, "Internet", *Our World in Data*, https://ourworldindata.org/internet [accessed: 17 January 2022].

10 See, for instance: D.R. Brake, "Are We All Online Content Creators Now? Web 2.0 and Digital Divides", *Journal of Computer-Mediated Communication*, vol. 19, issue 3, 2014, pp. 591–609, https://doi.org/10.1111/jcc4.12042.

in 2011, during the Arab Spring revolutions. On the one hand, some of them proved to rely heavily on online communication.[11] Thus, social media chatter analysis enabled important political events to be closely followed. On the other hand, the military conflicts originating from the Arab Spring were subject to interesting technological developments. Belligerents of Libya and Syria, including especially non-state actors, have recognised the immense potential offered by the Internet to distribute war propaganda directly to the online audience. It was manifested by the popularisation of audio-visual and visual content documenting combat and its aftermath. Belligerents were also increasingly keen to use social media and new technologies to boost their image, for instance, by publishing their pictures in daily life situations. Overall, since at least 2011, the Internet has become abundant in war-related footage.

This constituted a significant opportunity for military-related OSINT. Raw data related to the activities of state and non-state actors during ongoing military conflicts could be analysed by armed forces. Effectively, since 2011 we have been able to witness a considerable increase in publicly available military-related OSINT investigations. Some of the most eye-catching were carried out by the Bellingcat Investigation Team. It showed that skilful exploitation of geospatial intelligence (GEOINT), combined with imagery intelligence (IMINT) and a variety of other Internet sources, may provide valuable insights into the activities of violent extremist organisations. For instance, in 2014, the team managed to geolocate the Islamic State's training camp in Mosul by analysing propaganda images released by this terrorist organisation.[12] More recently, it also uncovered a pro-Chinese government information operation on Twitter and Facebook. Bellingcat's findings were mostly founded on analysing the social media chatter.[13] Other state and non-state actors have followed in the same footsteps. For at least a decade, we have been able to observe many interesting OSINT investigations that allowed, for instance, to geolocate military infrastructures or troops on the battlefield, measure casualties of belligerents, and determine their capabilities. Overall, there has been plenty of evidence indicating that the usability of OSINT in gathering military-related intelligence has steadily increased.

---

[11] G. Wolfsfeld, E. Segev, T. Sheafer, "Social Media and the Arab Spring: Politics Comes First", *The International Journal of Press/Politics*, vol. 18, no. 2, 2013, pp. 115–137, https://doi.org/10.1177/1940161212471716.

[12] Bellingcat Investigation Team, "Gun Safety, Self Defense, and Road Marches – Finding an ISIS Training Camp", Bellingcat, 22 August 2014, https://www.bellingcat.com/resources/case-studies/2014/08/22/gun-safety-self-defense-and-road-marches-finding-an-isis-training-camp [accessed: 5 January 2022].

[13] B. Strick, "Uncovering A Pro-Chinese Government Information Operation on Twitter and Facebook: Analysis of the #MilesGuo Bot Network", Bellingcat, 5 May 2020, https://www.bellingcat.com/news/2020/05/05/uncovering-a-pro-chinese-government-information-operation-on-twitter-and-facebook-analysis-of-the-milesguo-bot-network [accessed: 5 January 2022].

Open-source intelligence on the Internet as a means of improving armed forces' situation awareness in conventional warfare

The available examples of the aforementioned open-source intelligence investigations that have been publicly debated in recent years enable several interesting methods of gathering military-related open-source data to be identified. They include mainly:

- detection and analysis of military infrastructure;
- detection and analysis of military build-ups, including the assessment of the adversary's potential;
- monitoring the ongoing military operations, including war casualties' assessment;
- geolocating troops on the battlefield.

Most of these applications are primarily based on the combination of GEOINT and IMINT.[14] One of the most valuable services of this type is Google Maps. It offers detailed and usually up-to-date satellite imagery, aerial photos, and street views. On top of that, layouts of transport routes and traffic are available. The combination of these options opens up immense possibilities for gathering military intelligence. Careful analysis of available satellite pictures, combined with open-source information related to the general whereabouts of military bases, allows their geolocation and analysis of their features. In certain cases, even more sensitive information may be determined this way, including the specificity of air defence systems or surveillance installations. In order to do so, Google Maps usually needs to be combined with imagery or recordings available through other services, such as, Bing Maps (in the Aerial View mode) or Zoom Earth. Moreover, while based on a similar set of satellite pictures, the Google Earth Pro application offers interesting options. For instance, it is possible to compare up-to-date pictures with older images taken from the Google database. Effectively, it is possible to determine the evolution of the military infrastructure over time or to carry out GEOINT related to past events. Overall, GEOINT/IMINT usually focuse on specific traits visible in analysed pictures, such as buildings, the layout of roads, rivers, mountains, military equipment or vegetation. Their specificity, shapes, and perspective are considered.

Aside from the mainstream apps, more specialised national-level services may be exploited. This was proven by the investigation of the Polish cyber security firm Niebezpiecznik.pl. In 2018, their experts combined data available in Poland's Ministry of National Defence's public information bulletin with spatial data shared at geoportal.gov.pl. Effectively, they managed, for instance, to determine the location of the U.S. National Security Agency's eavesdropping station in Poland.[15]

---

[14] See: J.L. Ware, "Geospatial Intelligence and Engineers", *Military Engineer*, vol. 98, no. 640, 2006, pp. 57–58.

[15] M. Maj, "Jak namierzyć lokalizację (tajnych) polskich baz wojskowych?", Niebezpiecznik.pl, 23 August 2018, https://niebezpiecznik.pl/post/polskie-bazy-wojskowe-lokalizacja [accessed: 14 January 2022].

The detection and analysis of military installations can and should be combined with other, less evident open sources. There is a variety of ways to collect data from the areas under consideration, including primarily social media. For instance, Twitter allows monitoring tweets posted in certain areas either through geotags or a "geocode:" command.[16] Dashcam recordings are also an obvious and promising choice. Even data originating from fitness applications can help determine or verify the locations of military bases. Similarly, they may allow the profiling of armed forces or the intelligence community members. This was demonstrated in 2018 by the case of the Strava fitness app that shared data allowing to pinpoint locations of secret military installations or reveal information about their layout in great detail.[17] Excellent opportunities in this regard are also provided by the Radar Interference Tracker, which is based on data provided by the SENTINEL-1 satellite system. This tool allows geolocating air defence elements (radars) both on land and sea.[18]

There are also various tools enabling military deployments to be detected and assessed. Aside from the up-to-date – and mostly subscription-based – geospatial intelligence on the Internet, the monitoring of social media chatter provides interesting results. This is mostly due to the fact that civilians using social networks tend to take pictures or record videos of the encountered military convoys. They are subsequently posted online and can be analysed with various techniques. For instance, the combination of GEOINT and IMINT allows learning the scale of military movements, their whereabouts, and the types of equipment deployed. This has been recently confirmed by the events taking place at the Russian-Ukrainian border. The accumulation of the Russian troops near Ukraine since the end of 2021 did not go unnoticed by the OSINT community. Aside from satellite imagery, the monitoring of the social media posts by experts provided definite evidence indicating that Moscow moved a large number of its troops to the vicinity of Donbas and the Crimea.[19]

The movement of troops, in certain circumstances, can be monitored with flight and maritime communication trackers, such as Flightradar24 or MarineTraffic. However, these services have certain limitations, as they do not track planes and ships carrying out military operations. Effectively, their movements can be monitored only in "ordinary" situations. Moreover, there were known cases of spoofing Automatic

[16] "How to use the Twitter geocode to search tweets by location", TweetBinder, https://www.tweetbinder.com/blog/twitter-geocode [accessed: 14 January 2022].

[17] "Tajne obiekty wojskowe z całego świata zaświeciły się na żółto na tej mapie. Sprawdź, czy twój dom także", Niebezpiecznik.pl, 29 January 2018, https://niebezpiecznik.pl/post/tajne-obiekty-wojskowe-z-calego-swiata-zaswiecily-sie-na-zolto-na-tej-mapie [accessed: 14 January 2022].

[18] brO, 5Ghz Interference Tracker, OSINT Editor, 14 February 2020, https://www.osinteditor.com/resources/guides/5ghz-interference-tracker [accessed: 14 January 2022].

[19] W.P. Strobel, M.R. Gordon, "Russia's Military Buildup Near Ukraine Is an Open Secret", *The Wall Street Journal*, 4 January 2022, https://www.wsj.com/articles/russias-military-buildup-near-ukraine-is-an-open-secret-11641292202 [accessed: 14 January 2022].

Identification System (AIS) data that feeds MarineTraffic. This means that this type of information is not always reliable.[20] Still, Flightradar24 and similar services have proven to be a valuable source of information related to the Russian military deployment in Kazakhstan in January 2022.[21]

Finally, there is a variety of other less evident tools and applications allowing military build-ups to be detected. For instance, the analysis of live streaming webcams showing transport routes can be utilised. Even dating apps may be helpful in certain circumstances. This was proven in 2021, when the military build-up at the Polish-Belarussian border could be spotted on Tinder.[22]

On top of that, quite a similar set of OSINT methods may be used to geolocate troops on the battlefield and monitor ongoing military conflicts. As mentioned above, Internet propaganda or amateur content documenting events on the battlefields have become an integral part of most wars nowadays. Subsequently, these materials posted on, e.g., YouTube or social media can be extracted and analysed. In this context, social media chatter analysis may reveal interesting information related to ongoing events, aside from purely visual and audio-visual content. For instance, the combination of IMINT, GEOINT, and analysis of posts on Twitter was utilised by the OSINT community to learn how the situation on the frontlines of Syria, Nagorno-Karabakh, and Libya evolved. Among others, war propaganda released by both sides of the conflict served to measure casualties suffered by Armenians and Azeris during their conflict in 2020.[23]

Potential of OSINT to support cyber warfare operations

Publicly known cases of state-sponsored cyber operations show that open-source intelligence techniques can be used as a means allowing designating targets of computer attacks. This was proven, among others, by the "Glowing Symphony" operation carried out in 2016 against the Islamic State's digital assets. The operation was preceded

[20] T. Bateman, "HMS Defender: AIS Spoofing is opening up a new front in the war on reality", Euronews, uptaded 28 June 2021, https://www.euronews.com/next/2021/06/28/hms-defender-ais-spoofing-is-opening-up-a-new-front-in-the-war-on-reality [accessed: 14 January 2022].

[21] A. Aidarbekova, A. Kaparov, "Launching an Open Source Flight Database for Kazakhstan in Wake of Protests", Bellingcat, 8 January 2022, https://www.bellingcat.com/resources/2022/01/08/launching-an-open-source-flight-database-for-kazakhstan-in-wake-of-protests [accessed: 14 January 2022].

[22] A. Coakley, "Borderline: Tinder profiles of Polish troops appear in Belarus", *The Independent*, 15 November 2021, https://www.independent.co.uk/news/world/europe/belarus-poland-border-tinder-troops-b1957953.html [accessed: 14 January 2022].

[23] Oryx, "The fight for Nagorno-Karabakh: Documenting Losses on The Sides of Armenia and Azerbaijan", Oryx blog, 27 September 2020, https://www.oryxspioenkop.com/2020/09/the-fight-for-nagorno-karabakh.html [accessed: 14 January 2022].

by an intelligence-gathering phase that also employed OSINT techniques.[24] In similar fashion, state-sponsored Distributed Denial of Service (DDoS) attacks, such as those against Estonia in 2007, were also frequently supported by OSINT determining suitable targets.[25] Thus, OSINT offers a variety of opportunities related to detecting and examining digital infrastructure and communication channels exploited by the adversary. Moreover, it can also be used to identify and profile members of the adversary's armed forces or employees of its institutions. It should be emphasised that the same set of techniques applies to both state- and non-state actors.

There are plenty of OSINT methods allowing the digital infrastructure of the enemy to be detected, scanned, and mapped. To begin with, each investigation aiming to gather intelligence related to hostile Internet communication channels initially relies on the so-called "Google hacking," which uses the advanced operators and options of the Google search engine. The skilful combination of available operators, such as "site:", "OR," "AND," "-", "cache:" or "filetype:,"[26] with properly selected keywords and advanced search options usually allow identifying valuable surface web locations associated with the adversary. Depending on the specificity of the potential targets of cyber operations, other search engines may also be utilised (Yandex, Baidu, Bing). Alternatively, this first step of all investigations can be automated with the use of web crawlers, such as Scrapy. Moreover, a similar set of techniques can be applied to the deep and dark web, but they depend on the specificity of the scanned environment. For instance, some social networks, such as Twitter, allow valuable search tools based on API to be created.[27] In contrast, the anonymity-oriented TOR (The Onion Router) makes browsing its content much more difficult. Still, there is a number of available search engines (Torch, Recon, Ahmia.fi), link directories (Hidden Wiki), and dedicated crawlers, such as ACHE or Scrapy. All of them facilitate gathering intelligence.

Another step of OSINT investigations allowing the digital infrastructure of the potential adversary to be mapped is mainly based on web scanning and scraping software. Tools and services allowing the interconnectedness of the communication channels to be measured can also be used. Each initially detected Internet address may be subject to more thorough analysis using the potential of web scanners, such as Shodan

---

[24] D. Temple-Raston, "How the U.S. Hacked ISIS", NPR, 26 September 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis [accessed: 14 January 2022].

[25] See: M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice: Wydawnictwo Uniwersytetu Śląskiego, 2015, pp. 184–201.

[26] See: *Google Search Appliance. Search Protocol Reference*, Mountain View, CA: Google, 2015, https://static.googleusercontent.com/media/www.google.com/pl//support/enterprise/static/gsa/docs/admin/current/gsa_doc_set/xml_reference/xml_reference.pdf [accessed: 25 May 2022].

[27] OSINT Essentials, Twitter, https://www.osintessentials.com/twitter [accessed: 17 January 2022].

or SpiderFoot. For instance, Shodan's ability to scan ports provides interesting opportunities to plan and carry out cyber-attacks. SpiderFoot, on the other hand, enables external links leading to other interconnected domains to be extracted. These tools may be combined with other publicly available services, such as ViewDNS.info. Its Reverse IP Lookup option allows determining other domains co-hosted at the same server. Effectively, these and many other methods enable the digital infrastructure of the adversary to be mapped in detail.[28]

Each discovered Internet address may be subject to more careful analysis focused on extracting and analysing metadata. There is a variety of ways to do this. Among others, Recon-ng or Metagoofil scripts allow detecting files of certain types at a given domain, downloading them, and extracting available metadata automatically. This leads to discovering, for instance, the identity of an individual who created these files or software used by the adversary. Alternatively, when it comes to published pictures, it is possible to extract EXIF metadata, which enables the place where it was taken to be geolocated.

It should be stressed that this approach is especially efficient in collecting intelligence related to non-state actors, such as terrorist organisations or rebel groups. Due to the shortage of skilled IT staff, their digital infrastructure is usually much less developed and secure when compared to state actors. This, in turn, means that it is usually more susceptible to OSINT methods, which has been demonstrated by numerous studies focused on online terrorism and political violence.[29] Still, similar methods are also applicable to state actors or enterprises. However, their cyber-security solutions frequently force the attacking side to use much more advanced scanning techniques that fall outside the remit of OSINT.[30]

In this context, the OSINT analysis may also help identify employees of the adversary's institutions. For instance, due to frequent operational security (OPSEC) mistakes, this may be done by analysing files published on official websites, e.g., of ministries. Extraction of their metadata may lead to identifying officials responsible for creating them. This process can be automatised, for instance, with the aforementioned Metagoofil script. Subsequently, each discovered individual may be profiled based on analysis of their social media activity or public databases. Alternatively, the activity of their family members may also be investigated, which sometimes provides

---

[28] See: M. Lakomy, "Listening to the 'Voice of Islam': The Turkestan Islamic Party's Online Propaganda Strategy", *Studies in Conflict & Terrorism*, https://doi.org/10.1080/1057610X.2021.1914361.

[29] See: *idem*, "Mapping the online presence and activities of the Islamic State's unofficial propaganda cell: Ahlut-Tawhid Publications", *Security Journal*, vol. 34, 2021, pp. 358–384, https://doi.org/10.1057/s41284-020-00229-3.

[30] See: E. Bou-Harb, M. Debbabi, C. Assi, "Cyber Scanning. A Comprehensive Survey", *IEEE Communications Survey & Tutorials*, vol. 16, no. 3, 2014, pp. 1496–1519, https://doi.org/10.1109/SURV.2013.102913.00020.

valuable results. It was proven by the famous case of the MI6 chief's wife, who shared information related to their family life and activities on Facebook.[31] Such a somewhat simplistic OSINT approach may facilitate planning and executing high-profile spear-phishing cyber-attacks aimed at infecting adversary networks with malware.[32]

Conclusions

This article should be considered as a brief introduction to how the constantly changing techniques of open-source intelligence may support conventional and cyber operations. There is no doubt that the opportunities in this area have become unprecedented, mostly due to the continously growing amount of open-source data in all layers of Internet communication. In the future, even the Extended Reality applications or apps for teenagers may be used for this purpose. Their skilful detection, extraction, and analysis by military intelligence enable the situation awareness of the armed forces to be significantly increased. These opportunities are especially evident when it comes to events and processes which fall outside the scope of the traditional intelligence-gathering capabilities.

Aside from those general uses mentioned above, OSINT may fulfil various other organisational unit-level functions. It might reinforce high-ranking officers' operational security, especially when dealing with non-state institutions and individuals. Moreover, OSINT may be applied for accumulating knowledge on military-related events, which can be subsequently used in briefings with cadres or even practically employed during military exercises. These opportunities mean that creating dedicated OSINT cells at a brigade level should be considered. Obviously, much more developed and specialised structures need to be developed by military intelligence units and the broadly understood cyber troops.

Nevertheless, this does not mean that OSINT should be treated as a panacea for all military intelligence problems. All OSINT-based investigations face serious challenges that need to be tackled thoughtfully. Firstly, OSINT may respond to a wide range of operational needs of the armed forces. However, it has by no means the potential of answering all questions that might emerge. Results of OSINT need to be combined with other types of intelligence, including HUMINT, SIGINT and GEOINT. Secondly, using OSINT faces significant problems related to the widespread online disinformation. It takes time and effort to verify extracted open-source

[31] "MI6 chief's cover blown by wife's holiday snaps on Facebook", *The Indian Express*, 6 July 2009, https://indianexpress.com/article/news-archive/web/mi6-chiefs-cover-blown-by-wifes-holiday-snaps-on-facebook [accessed: 17 January 2022].

[32] See: J.W. Bullee, L. Montoya, M. Junger, P. Hartel, "Spear phishing in organisations explained", *Information and Computer Security*, vol. 25, no. 5, 2017, pp. 593–613, https://doi.org/10.1108/ICS-03-2017-0009.

data and information.[33] Thus, the risk of being misled needs to be considered. Last but not least, OSINT may be susceptible to information overload. Dealing with these – and many other – challenges should be considered a *sine qua non* requirement enabling the maximum usability of OSINT for the armed forces to be ensured.

References

Aidarbekova A., Kaparov A., "Launching an Open Source Flight Database for Kazakhstan in Wake of Protests", Bellingcat, 8 January 2022, https://www.bellingcat.com/resources/2022/01/08/launching-an-open-source-flight-database-for-kazakhstan-in-wake-of-protests/ [accessed: 14 January 2022].

Bateman T., "HMS Defender: AIS Spoofing is opening up a new front in the war on reality", euronews, uptaded 28 June 2021, https://www.euronews.com/next/2021/06/28/hms-defender-ais-spoofing-is-opening-up-a-new-front-in-the-war-on-reality [accessed: 14 January 2022].

Bean H., "The DNI's Open Source Center: An Organizational Communication Perspective", *International Journal of Intelligence and Counter Intelligence*, vol. 20, issue 2, 2007, pp. 240–257, https://doi.org/10.1080/08850600600889100.

Bellingcat Investigation Team, "Gun Safety, Self Defense, and Road Marches – Finding an ISIS Training Camp", Bellingcat, 22 August 2014, https://www.bellingcat.com/resources/case-studies/2014/08/22/gun-safety-self-defense-and-road-marches-finding-an-isis-training-camp [accessed: 5 January 2022].

Böhm I., Lolagar S. "Open source intelligence. Introduction, legal, and ethical considerations", *International Cybersecurity Law Review*, no. 2, 2021, pp. 317–337, https://doi.org/10.1365/s43439-021-00042-7.

Bou-Harb E., Debbabi M., Assi C., "Cyber Scanning. A Comprehensive Survey", *IEEE Communications Survey & Tutorials*, vol. 16, no. 3, 2014, pp. 1496–1519, https://doi.org/10.1109/SURV.2013.102913.00020.

Brake D.R., "Are We All Online Content Creators Now? Web 2.0 and Digital Divides", *Journal of Computer-Mediated Communication*, vol. 19, issue 3, 2014, pp. 591–609, https://doi.org/10.1111/jcc4.12042.

brO, 5Ghz Interference Tracker, OSINT Editor, 14 February 2020, https://www.osinteditor.com/resources/guides/5ghz-interference-tracker [accessed: 14 January 2022].

Bullee J.W., Montoya L., Junger M., Hartel P., "Spear phishing in organisations explained", *Information and Computer Security*, vol. 25, no. 5, 2017, pp. 593–613, https://doi.org/10.1108/ICS-03-2017-0009.

Coakley A., "Borderline: Tinder profiles of Polish troops appear in Belarus", *The Independent*, 15 November 2021, https://www.independent.co.uk/news/world/europe/belarus-poland-border-tinder-troops-b1957953.html [accessed: 14 January 2022].

Google Search Appliance. Search Protocol Reference, Mountain View, CA: Google, 2015, https://static.googleusercontent.com/media/www.google.com/pl//support/enterprise/static/gsa/docs/admin/current/gsa_doc_set/xml_reference/xml_reference.pdf [accessed: 25 May 2022].

[33] See: A. Školkay, J. Filin, "A Comparison of Fake News Detecting and Fact-Checking AI Based Solutions", *Studia Medioznawcze*, vol. 20, no. 4, 2019, pp. 365–383, https://doi.org/10.33077/uw.24511617.ms.2019.4.187.

Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security House of Representatives, One Hundred Ninth Congress, First Session, June 21, 2005, Serial No. 109-22, Washington: U.S. Government Printing Office, 2007, https://www.govinfo.gov/content/pkg/CHRG-109hhrg24962/html/CHRG-109hhrg24962.htm [accessed: 5 January 2022].

"How to use the Twitter geocode to search tweets by location", TweetBinder, https://www.tweetbinder.com/blog/twitter-geocode [accessed: 14 January 2022].

Imholtz A.A. Jr., "The American (FBIS) Side of the Story", https://www.iwm.org.uk/sites/default/files/files/2018-11/The%20American%20%28FBIS%29%20Side%20of%20the%20Story%20-%20August%20Imholtz%20.pdf [accessed: 5 January 2022].

Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice: Wydawnictwo Uniwersytetu Śląskiego, 2015.

Lakomy M., "Listening to the 'Voice of Islam': The Turkestan Islamic Party's Online Propaganda Strategy", *Studies in Conflict & Terrorism*, https://doi.org/10.1080/1057610X.2021.1914361.

Lakomy M., "Mapping the online presence and activities of the Islamic State's unofficial propaganda cell: Ahlut-Tawhid Publications", *Security Journal*, vol. 34, 2021, pp. 358–384, https://doi.org/10.1057/s41284-020-00229-3.

Maj M., "Jak namierzyć lokalizację (tajnych) polskich baz wojskowych?", Niebezpiecznik.pl, 23 August 2018, https://niebezpiecznik.pl/post/polskie-bazy-wojskowe-lokalizacja [accessed: 14 January 2022].

"MI6 chief's cover blown by wife's holiday snaps on Facebook", *The Indian Express*, 6 July 2009, https://indianexpress.com/article/news-archive/web/mi6-chiefs-cover-blown-by-wifes-holiday-snaps-on-facebook [accessed: 17 January 2022].

Mider D., "Czarny i czerwony rynek w sieci The Onion Router – analiza funkcjonowania darkmarketów", *Przegląd Bezpieczeństwa Wewnętrznego*, no. 21, 2019, pp. 154–190.

Oryx, "The fight for Nagorno-Karabakh: Documenting Losses On The Sides of Armenia and Azerbaijan", Oryx blog, 27 September 2020, https://www.oryxspioenkop.com/2020/09/the-fight-for-nagorno-karabakh.html [accessed: 14 January 2022].

OSINT Essentials, Twitter, https://www.osintessentials.com/twitter [accessed: 17 January 2022].

Roser M., Ritchie H., Ortiz-Ospina E., "Internet", *Our World in Data*, 2015, https://ourworldindata.org/internet [accessed: 17 January 2022].

Sarowski Ł., "Od Internetu Web 1.0 do Internetu Web 4.0 – ewolucja form przestrzeni komunikacyjnych w globalnej sieci", *Rozprawy Społeczne*, vol. 11, no. 1, 2017, pp. 32–39, https://doi.org/10.29316/rs.2017.4.

Školkay A., Filin J., "A Comparison of Fake News Detecting and Fact-Checking AI Based Solutions", *Studia Medioznawcze*, vol. 20, no. 4, 2019, pp. 365–383, https://doi.org/10.33077/uw.24511617.ms.2019.4.187.

Strick B., "Uncovering A Pro-Chinese Government Information Operation on Twitter and Facebook: Analysis of the #MilesGuo Bot Network", Bellingcat, 5 May 2020, https://www.bellingcat.com/news/2020/05/05/uncovering-a-pro-chinese-government-information-operation-on-twitter-and-facebook-analysis-of-the-milesguo-bot-network [accessed: 5 January 2022].

Strobel W.P., Gordon M.R., "Russia's Military Buildup Near Ukraine Is an Open Secret", *The Wall Street Journal*, 4 January 2022, https://www.wsj.com/articles/russias-military-buildup-near-ukraine-is-an-open-secret-11641292202 [accessed: 14 January 2022].

"Tajne obiekty wojskowe z całego świata zaświeciły się na żółto na tej mapie. Sprawdź, czy twój dom także", Niebezpiecznik.pl, 29 January 2018, https://niebezpiecznik.pl/post/tajne-obiekty-wojskowe-z-calego-swiata-zaswiecily-sie-na-zolto-na-tej-mapie [accessed: 14 January 2022].

Temple-Raston D., "How the U.S. Hacked ISIS", NPR, 26 September 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis [accessed: 14 January 2022].

Tylutki K., "Informacja masowego rażenia – OSINT w działalności wywiadowczej", *Przegląd Bezpieczeństwa Wewnętrznego*, no. 19, 2018, pp. 166–192.

Ware J.L., "Geospatial Intelligence and Engineers", *Military Engineer*, vol. 98, no. 640, 2006, pp. 57–58.

Williams H.J., Blum I., *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, Santa Monica: RAND Corporation, 2018.

Wolfsfeld G., Segev E., Sheafer T., "Social Media and the Arab Spring: Politics Comes First", *The International Journal of Press/Politics*, vol. 18, no. 2, 2013, pp. 115–137, https://doi.org/10.1177/1940161212471716.

Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego*, Warszawa: Wydawnictwo Scholar, 1999.

Assessing the potential of OSINT on the Internet in supporting military operations

Abstract

This article briefly discusses some of the selected open-source intelligence methods on the Internet, which may be utilised to support activities of the armed forces. The paper examines this issue in two particular dimensions. On the one hand, it overviews some of the most popular means allowing supporting conventional operations, for instance, by geolocating hostile military infrastructure or troops. On the other hand, it explores some of the selected methods allowing to support cyber warfare. It concludes that open-source intelligence offers increasing capabilities, for instance, in detecting targets for offensive cyber operations or geolocating hostile troops. Nevertheless, it also has considerable limitations, particularly in terms of susceptibility to disinformation.

Key words: open-source intelligence (OSINT), armed forces, military, the Internet