Agnieszka Lipińska*

The Digital Future of Information. Determinants of the Use of Open Source Intelligence[1]

Abstract

Cyberspace as a place of information acquisition is in constant flux. Recognizing the threats and challenges associated with it is one of the key elements influencing national security. Knowledge of the current conditions affecting information security and the possibility of obtaining information is an essential element of the work of the institutions forming the state security system. This article will outline the factors affecting the future of information operation and distribution in the digital world[2] confirming the increased need for OSINT in state institutions, especially in the face of new challenges. These include: hacktivism, the dissemination of specialized tools and technologies for data acquisition and analysis among the network user community, hybrid and diplomatic-propaganda activities carried out in the info-sphere by nation states. The article will also provide a forecast of the development of cyberspace in the context of future OSINT activities.

Key words: OSINT, hacktivism, hybrid warfare, disinformation, cyber security, data analytics, internet blocking

* PhD Agnieszka Lipińska, War Studies University in Warsaw, e-mail: lipinskaagnieszka065@gmail.com, ORCID: 0000-0003-3108-8095.

1 This article is based on an updated excerpt from a PhD thesis entitled OSINT in a time of disinformation and post-truth. Opportunities and threats to national security and the use of Open Source Intelligence, defended at the War Studie University, Warsaw, on 14.04.2023.

2 The ongoing war in Ukraine, dubbed the first digital war by R. Clarke, National Security Council advisor to the US President, has accelerated and highlighted some of the threats mentioned. More extensively on this in R. Clarke, *First Major Cyber War Between Two Powers*, https://www.pbs.org/video/richard-clarke-first-major-cyber-war-between-two-powers-veby/ [access: 3.09.2023].

The future of the functioning of information in cyberspace depends largely on factors related to the nature of the actions taken by democratic countries and the way in which they exercise their oversight of networks and instant messaging. The uneven course of technological development in different regions of the world highlights the widening digital inequalities and differences in users' access to information across countries and regions. These factors affect how and how much data is acquired, the nature of intelligence work, diplomacy and policy-making, and cooperation between countries. They also pose a challenge to Open Source Intelligence analysts, challenging them to understand the processes and conditions that govern information on the web. This is because, in recent years, tendencies to emulate the Chinese and Russian models of data management and information surveillance have emerged in some countries and regions, especially in Africa and Asia, which have affected in societal formation. This manifests itself in the following activities, among others:

1. Internet blocking: Ad hoc disabling and blocking of internet and mobile access is increasingly reported. Such operations took place in 2019 in. Bangladesh, the Democratic Republic of Congo, Sudan, Gabon[3], or Myanmar[4] and in Belarus[5] in 2020. They were intended to restrict citizens' access to information, prevent them from organizing protests and hide news of often violent actions taken by the authorities against citizens from the international community. Such blockades can not only result in an information embargo (disinformation, lack of access to information). Widespread use of them may result in such actions being widely regarded in the future as a justified element of ongoing preventive operations rather than a restriction of civil liberties.

2. Control and censorship of the internet and instant messaging to fight political opponents and manage society. Such measures have been carried out for years by the Chinese and Iranian authorities against web users in their country. In 2020, control was also tightened by Belarus and Vietnam, which enforced Facebook to remove posts presenting opinions unfavorable

3 https://www.accessnow.org/sudan-bangladesh-drc-gabon-start-2019-with-major-digital-rightsviolations/ [access: 8.09.2023].

4 A. Januta, M. Funakoshi M., *Myanmar's internet suppression*, https://www.reuters.com/graphics/MYANMAR-POLITICS/INTERNETRESTRICTION/rlgpdbreepo/ [access: 20.09.2023].

5 https://belarusinfocus.pro/we-found-out-how-internet-was-blocked-belarus-august-2020-why-it-didnot-and/ [access: 6.2023].

to the authorities[6]. Restrictions were stepped up by the Russian Federation in 2022. Also noteworthy is the example of censorship to secure military data introduced by the Ukrainian authorities during the 2022 war.

3. Influence operations – actions carried out by hostile states by exploiting the segmentation of the Internet and the low digital competence of users from South American, Middle Eastern and African countries to steer public opinion or introduce disinformation narratives into cyberspace directed de facto against Western countries. Operations of this type are already being carried out on a large scale, such as the ongoing Pan-African action against colonialism promoted mainly on Twitter under the slogan #NoMoreColonialism since 2021. Emotional pan-African tweets aim not only to inspire pride of origin, but above all to remind people of colonial wrongs and to provoke anti-French and anti-American sentiment[7]. This disinformation, probably controlled by the Russian Federation (the PRC is also economically and politically involved in Africa), is accompanied by real ventures to strengthen the Russian political and military presence in some African countries. The ongoing information war between Ukraine and the Russian Federation since early 2022 is the latest example of large-scale influence operations.

The above-mentioned developments clearly affect the reliability and accessibility of information on the web. The issue of access to data has been a subject of discussion in democratic states for years, and is now not only about the extent of freedom and privacy in the state-citizen or concern-citizen relationship. In the near future, data protection in its broadest sense will become an important issue facing the state. In this context, for example, the widespread exposure of sensitive databases belonging to the Russian Federation, including the publication of numerous materials of a classified nature, is noteworthy. As part of the hacking activities carried out against the Russian Federation by the Anonymous group during the Russian-Ukrainian war of 2022, a amount of data of crucial importance to Russia's security was exposed. Among other things, the hackers published online the IT resources of the Russian Central Bank[8], the results of research by the Russian Nuclear

6 *Vietnam: Facebook, Pressured, Censors Dissent: Company Caves to Government After Local Servers Disrupted*, https://www.hrw.org/news/2020/04/23/vietnam-facebook-pressured-censors-dissent [access: 5.10.2023].

7 Examples of posts tagged with the hashtag #NoMore: https://twitter.com/search?q=%23Nomore [access: 10.09.2023].

8 P. Paganini, *Anonymous leaked 28GB of data stolen from the Central Bank of Russia*, https://securityaffairs.co/wordpress/129490/hacking/central-bank-of-russia-data-leak-anonymous.html [access: 27.09.2023].

Institute[9] and the arms industry[10] and many others. Such actions also braze the opportunities currently offered by the use of the internet as a source of information.

In the face of these changing cyberspace conditions and the need for multifaceted analysis of online material, the importance of cooperative and interdisciplinary OSINT groups operating within and outside state institutions will increase. The most recent example of the effectiveness of such groups, including those created on an ad hoc basis, are the events of early 2022 related to the concentration of Russian troops near the border with Ukraine and the subsequent attack on that country. These resulted in the formation of groups of people verifying and analyzing data in the info-sphere. There was an ongoing assessment of the relevance of information and a discussion debunking fake news. Commentaries on material from videos recorded in the Russian Federation and Belarus on Tik Tok[11], posts and satellite imagery were also carried out. In the most popular group, the core consisted of Rob Lee, a military analyst and PhD student at King's College London, Benjamin Stark, an OSINT analyst, and Polish military analyst Konrad Muzyka. Together with other users, they formed one of the more important informal centers for analyzing the current situation. They agreed on the standardization of nomenclature or how to aggregate and assess the reliability of data. Similar activities were also carried out by others, such as the British NGO The Centre for Information Resilience. As part of its statutory activity, i.e., verifying disinformation online in cooperation with the OSINT community, this group was also involved in documenting, verifying and mapping Russian was also involved in documenting, verifying and mapping Russian troop movements along the border with Ukraine[12].

The war in Ukraine also brought about new ways of managing large-scale information on the Internet. Information were presented directly to the

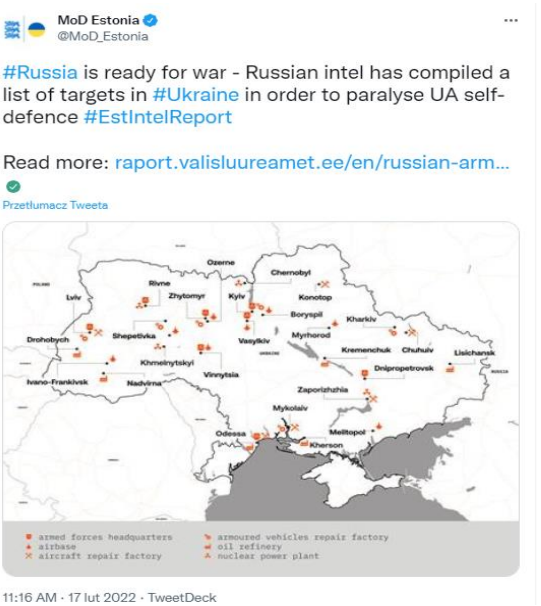
9 P. Paganini, *Anonymous hit Russian Nuclear Institute and leak stolen data*, https://securityaffairs.co/wordpress/128527/hacktivism/anonymous-hit-russian-nuclear-institute.html [access: 25.10.2023].

10 J. Lee, *Russian Defense Export Hacked, 500+MB Data Leaked By @Rucyborg (UPDATED)*, https://www.databreaches.net/russian-defence-export-hacked-500mb-data-leaked-by-rucyborg/ [access: 24.09.2023].

11 The Russian Federation and Belarus prohibit the publication and distribution of material on military issues.

12 Updated warfare map with links to videos and photos http://maphub.net/Cen4infoRes/russian-ukrainemonitor [access: 13.09.2023].

international community. For the first time, web users witnessed increased diplomatic activity conducted using social and electronic media. Statements, Russian proposals to change the architecture of European security and tweets from leading European politicians were published online. Unprecedented outreach activities also took place on the part of NATO. Shortly before the outbreak of war, the US officially publicized on social media information obtained by classified means about the planned date of the Russian attack on Ukraine. A particular form of dissemination of sensitive data was used, for example, by the intelligence services of the UK and Estonia in 2022, before the start of the war in Ukraine. In turn, in mid-February 2022, the Estonian and British Ministries of Defense published plans for a Russian attack on Ukraine's critical infrastructure (Estonia) and plans to strike the country (the UK) on their websites and tweet accounts.



Source: MoD Estonia, tweet of 17 February 2022, https://twitter.com/mod_estonia/status/1494254467595878403 [access: 9.09.2023].

Source: MoD UK tweet of 17 February 2022, https://twitter.com/DefenceHQ/status/1494315294382297091 [access: 20.09.2023].

The war in Ukraine has also been used by non-democratic states for unprecedented operations on large social groups. Such operations have been carried out via the popular Chinese app Tik Tok, whose algorithms enable audience profiling and control of public sentiment on a massive scale. This is demonstrated by the example of a Russian disinformation operation carried out in early 2022 among Swedish children and teenagers. Videos predicting an imminent Swedish Russian war presented on the app[13] caused panic and fear among the youngest. This resulted in the reinstatement of the psychological warfare agency, which was closed in Sweden in 2008[14]. Given the mass nature and low cost of such operations, a similar type of social engineering is bound

13 The app's algorithms profiled and suggested films without user input. Available: E. Braw, *'War Is Coming': Mysterious TikTok Videos Are Scaring Sweden's Children*, https://www.defenseone.com/ideas/2022/01/war-coming-mysterious-tiktok-videos-are-scaring-swedens-children/360808/ [access: 22.09.2023].

14 M. Bryant, *Sweden returns to cold war tactics to battle fake news*, https://www.theguardian.com/world/2022/feb/06/sweden-returns-to-cold-war-tactics-to-battle-fake-news, [access: 27.09.2023].

to be used more and more, and the number of similar applications collecting detailed data about users will increase in the future. This trend in the use of information in cyber-espionage must also be investigated by OSINT experts.

With the spread of technologies that until recently were only available to commercial entities or state players, the boundary between intelligence (economic, political) in its classic form and civil intelligence, which makes the information it acquires public, is also blurring. This is evidenced by the following examples:

1. Swiss journalists F. Pilet and E. Free initiated a citizens' project in 2019 called dictatoralert.org. Its premise is to reveal the overflights of aircraft belonging to non-democratic states that are kept secret by commercial air operations surveillance portals. As of February 2022, the project's website recorded 16,870 flights, covering the UAE, Saudi Arabia and the Russian Federation, among others[15];

2. The Bellingcat group, in view of the concentration of Russian troops on the border with Ukraine in 2022, has posted a tool on its website to measure Russian military radar activity[16];

3. In 2021, the Bellingcat group hired the Planet Labs commercial satellite for a month and conducted a ranking among the international OSINT community of topics that needed to be further explored using satellite imagery. From a number of suggestions, the following were chosen: the Jiangnan shipyard in China (Chinese aircraft carriers that could threaten Taiwan were being built there), the Al Wariyah airbase in Libya (an operations center for paramilitary groups supported by Turkey, Russia and the UAE), the US military base on Diego Garcia (a strategic US base) and the La Palma volcano in the Canary Islands (there was a volcanic eruption at the time)[17]. A similar action was carried out in September 2023[18];

4. Politically motivated hacktivism is becoming more widespread, the most recent example being an interactive map drawn up in late 2021 by Belarusian cyber-partisans on the basis of databases stolen from the Belarusian authorities. The database contains names, addresses, photographs

15 *Dictator Alert*, https://dictatoralert.org/ [access: 11.09.2023].

16 *Radar Interference Tracker: A New Open Source Tool to Locate Active Military Radar Systems*, https://www.bellingcat.com/resources/2022/02/11/radar-interference-tracker-a-new-open-source-toolto-locate-active-military-radar-systems/ [access: 20.09.2023].

17 https://twitter.com/bellingcat/status/1440319337072447502 [access: 10.09.2023].

18 https://www.bellingcat.com/resources/2023/09/25/we-tasked-a-satellite-based-on-your-suggestionshere-are-the-results/ [access: 8.10.2023].

of state functionaries and officials involved in the suppression of protests in Belarus, identifies whistleblowers or reveals some of A. Lukashenko[19].

The proliferation of mobile phones provides the opportunity to document events, and the ability to purchase good quality satellite imagery cheaply enables extensive analysis of sensitive data. The growing number of whistleblowers and activists is feeding the info-sphere community with new information that was until recently strictly regulated secrets. The analysis of data from the Internet of Things and CCTV cameras is significantly expanding the possibilities of obtaining information about selected objects. This makes publicly available data increasingly valuable. Easy access to information is both a benefit and a threat in this case. The above examples – in addition to the obvious need for data acquisition by OSINT analysts working in state institutions – therefore point to the need to reformulate the working models of nation-state intelligence and counterintelligence. An unambiguous definition of the future functioning and role of OSINT in the area of information security of the state and citizens is doomed to fail in a dynamically changing reality. However, it seems that an in-depth, responsible analysis of open ource materials that constitute a valuable source of knowledge for the institutions that make up the state security system is already possible, as well as necessary. It must take place under certain conditions (background knowledge, understanding of contexts, fine-grained assessment of the reliability of the material, knowledge of disinformation techniques, etc.) and using modern methods and technologies for aggregating and analyzing data, such as artificial intelligence. The responsibilities for data acquisition, aggregation and analysis are already defined by the so-called Berkeley Protocol[20], the principles for conducting analysis and verification are identical to those for intelligence analysis[21], and their rules are defined by NATO handbooks[22]

19 https://blackmap.org/ [access: 5.10.2023].

20 *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source and Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*, https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source [access: 29.09.2023].

21 S. Stenslie, L. Haugom, B. Haar Vaage, *Intelligence Analysis in The Digital Age*, London 2023.

22 *NATO OSINT Handbook V 1.2*, https://archive.org/details/NATOOSINTHandbookV1.2/page/n3/mode/2up?q=osint+sources [access: 20.09.2023]; *NATO Open Source Intelligence Reader*, https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf [access: 29.09.2023]; http://www.informationretrieval.info/privacy/NATO-OSINT-internet-exploit.pdf [access: 13.09.2023].

or scientific publications. The benefits of OSINT for institutions and society are significant, as it allows a large amount of data to be obtained with relatively little effort.

Bibliography

Braw E., *'War Is Coming': Mysterious TikTok Videos Are Scaring Sweden's Children*, https://www.defenseone.com/ideas/2022/01/war-coming-mysterious-tiktok-videosare-scaring-swedens-children/360808/ [access: 22.09.2023].

Bryant M., *Sweden returns to cold war tactics to battle fake news*, https://www.theguardian.com/world/2022/feb/06/sweden-returns-to-cold-war-tactics-tobattle-fake-news [access: 27.09.2023].

Clarke R., *First Major Cyber War Between Two Powers*, https://www.pbs.org/video/richard-clarke-first-major-cyber-war-between-two-powers-veby/ [access: 3.09.2023].

Dictator Alert, https://dictatoralert.org/ [access: 11.09. 2023].

https://www.belarusinfocus.pro/we-found-out-how-internet-was-blocked-belarusaugust-2020-why-it-did-not-and/ [access: 22.09.2023].

https://www.bellingcat.com/resources/2022/02/11/radar-interference-tracker-a-newopen-source-tool-to-locate-active-military-radar-systems/ [access: 22.09.2023].

https://www.bellingcat.com/resources/2023/09/25/we-tasked-a-satellite-based-onyour-suggestions-here-are-the-results/ [access: 22.09.2023].

https://www.blackmap.org/ [access: 22.09.2023].

http://www.information-retrieval.info/privacy/NATO-OSINT-internet-exploit.pdf [access: 20.09.2023].

https://www.twitter.com/bellingcat/status/1440319337072447502 [access: 20.09.2023].

https://www.twitter.com/DefenceHQ/status/149431529438229709 [access: 20.09.2023].

https://www.twitter.com/mod_estonia/status/1494254467595878403 [access: 20.09.2023].

Januta A., Funakoshi M., *Myanmar's internet suppression. Reuters* https://www.reuters.com/graphics/MYANMAR-POLITICS/INTERNET-RESTRICTION/rlgpdbreepo/ [access: 20.09.2023].

Lee J., *Russian Defence Export Hacked, 500+MB Data Leaked By @Rucyborg (UPDATED)*, https://www.databreaches.net/russian-defence-export-hacked-500mbdata-leaked-by-rucyborg/ [access: 24.09.2023].

NATO Open Source Intelligence Reader, https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf [access: 29.09.2023].

NATO OSINT Handbook V 1.2, https://archive.org/details/NATOOSINTHandbookV1.2/page/n3/mode/2up?q=osint+sources [access: 20.09.2023].

Paganini P., *Anonymous hit Russian Nuclear Institute and leak stolen data*, https://securityaffairs.co/wordpress/128527/hacktivism/anonymous-hit-russian-nuclearinstitute.html [access: 25.08.2023].

Paganini P., *Anonymous leaked 28GB of data stolen from the Central Bank of Russia*, https://securityaffairs.co/wordpress/129490/hacking/central-bank-of-russiadata-leak-anonymous.html [access: 27.09.2023].

Radar Interference Tracker: A New Open Source Tool to Locate Active Military Radar Systems, https://www.bellingcat.com/resources/2022/02/11/radar-interference-tracker-a-new-open-source-toolto-locate-active-military-radar-systems/ [access: 20.09.2023].

Stenslie S., Haugom L., Haar Vaage B., *Intelligence Analysis in the Digital Age*, London 2023.

Sudan, Bangladesh, DRC, Gabon start 2019 with major digital rights violations, https://www.accessnow.org/sudan-bangladesh-drc-gabon-start-2019-with-majordigital-rights-violations/ [access: 22.09.2023].

Vietnam: Facebook, Pressured, Censors Dissent: Company Caves to Government After Local Servers Disrupted, https://www.hrw.org/news/2020/04/23/vietnam-facebook-pressured-censors-dissent [access: 5.10.2023].

Cyfrowa przyszłość informacji. Uwarunkowania stosowania open source intelligence

Streszczenie

Cyberprzestrzeń jako miejsce pozyskiwania informacji podlega ciągłym przemianom. Rozpoznawanie związanych z nią zagrożeń i wyzwań stanowi jeden z elementów wpływających na bezpieczeństwo narodowe. Znajomość aktualnych uwarunkowań wpływających na bezpieczeństwa informacji i możliwości ich uzyskania stanowi niezbędny element pracy instytucji tworzących system bezpieczeństwa państwa. W niniejszym artykule przedstawiono czynniki wpływające na przyszłość funkcjonowania i dystrybucji informacji w świecie cyfrowym potwierdzające wzrost konieczności stosowania OSINT w instytucjach państwowych, szczególnie w obliczu nowych wyzwań. Należą do nich: haktywizm, upowszechnienie wśród użytkowników sieci specjalistycznych narzędzi i technologii do pozyskiwania i analizy danych, działania hybrydowe i dyplomatyczno-propagandowe prowadzone w infosferze przez państwa narodowe. Ponadto przedstawiono prognozę rozwoju cyberprzestrzeni w kontekście przyszłych działań OSINT.

Słowa kluczowe: OSINT, haktywizm, działania hybrydowe, dezinformacja, cyberbezpieczeństwo, analiza danych, blokada internetu