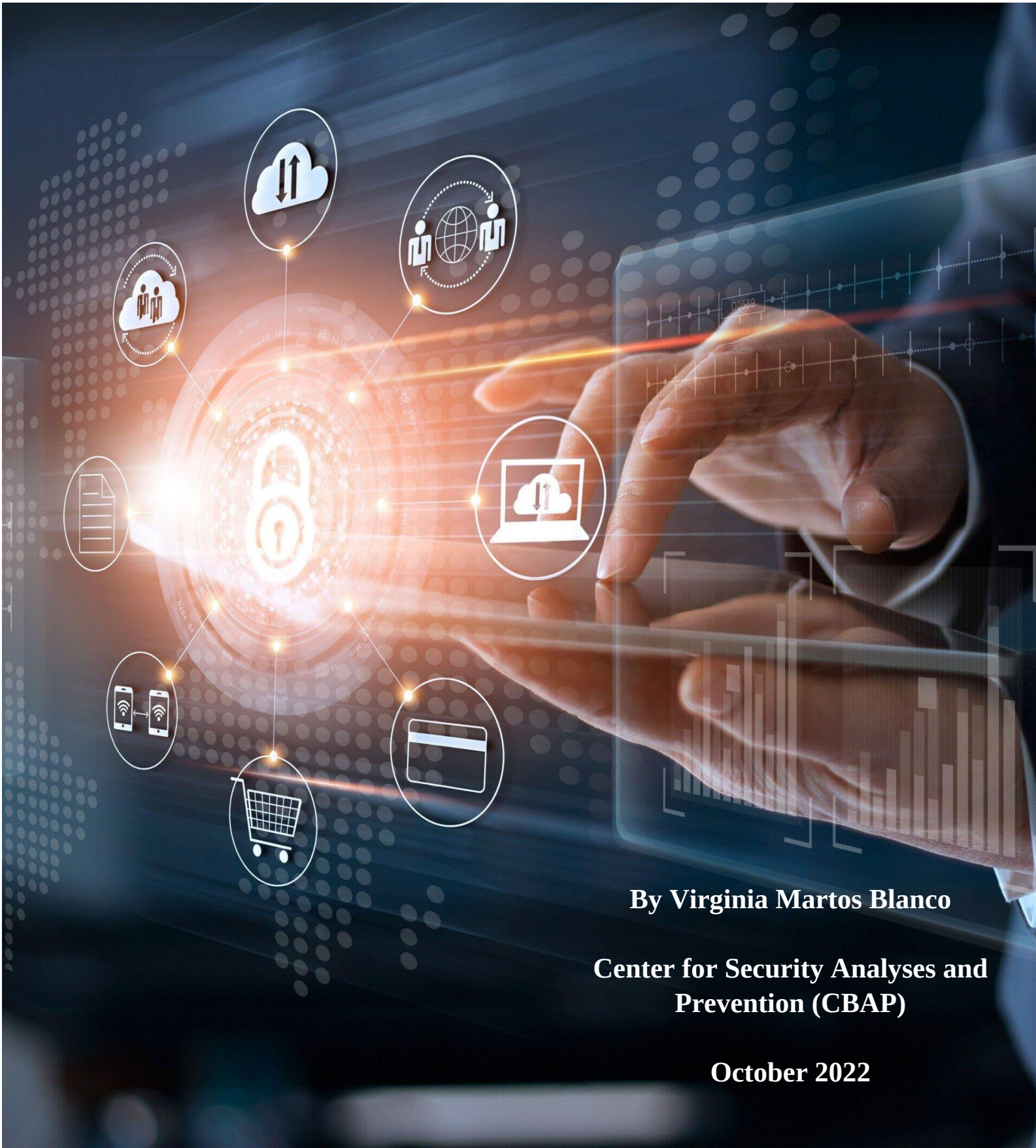
AN INTRODUCTION TO OPEN SOURCE INTELLIGENCE (OSINT)



By Virginia Martos Blanco

Center for Security Analyses and Prevention (CBAP)

October 2022

1. INTRODUCTION: DEFINITION AND HISTORICAL ORIGINS OF OSINT

Open Source Intelligence (OSINT) is the creation of intelligence through the collection and dissemination of information that is available to the public in general. According to the NATO Open Source Intelligence Handbook (2001: 2-3) "OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience, generally the commander and their immediate staff, in order to address a specific question."

OSINT became crucial for intelligence gathering in general with the "information revolution" at the end of the twentieth century, since a vast quantity of information could be found online thanks to the sharp increase of internet users. After the Cold War, Western states moved from an era based in secret intelligence in which the Soviet Union was the major threat, to another one in which threats diversified and intelligence analysts gave preference to open sources (Schaurer and Störger 2013: 54). In the years after the 9/11 terrorist attacks and the 2003 Iraq War, policy-makers' and intelligence analysts' awareness increased regarding OSINT's value in the fight against terrorism (A. Best and Cumming 2008). The 9/11 Commission in 2004 as well as the Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction in 2005 finally created an organ focused on OSINT research to reinforce national security in the US, as findings showed that some of Osama bin Ladin's public statements to carry an attack in the US had been unnoticed by intelligence analysts (Smith 2022: 9). These facts are of great importance because, as it will be discussed later, public statements constitute one of the OSINT's sources indeed.

9/11 Commission Review Panel (2004)

Source: National Commission on Terrorist Attacks Upon the United States. 16.06.2004. https://govinfo.library.unt.edu/911/press/photos/index.htm

President George W. Bush meeting with members of his national security team to discuss findings of the Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction (2005)

Source: News and Policies. March 2005. The White House. https://georgewbush-whitehouse.archives.gov/news/releases/2005/03/images/20050331_p44650-107-515h.html

However, OSINT's use goes back to approximately a century ago, pioneered by the United States, as governments started realizing the importance of intelligence for making decisions in the national and international arena, although priority was then given to classified sources of information (A. Best and Cumming 2008). Similarly, in the European Union, OSINT's importance rose after the 2004 Madrid attacks and the 2005 London attacks, although its institutionalization came a few years later with the Lisbon Treaty in 2009 (Cross 2019).

Therefore, states are no longer the sole producers of intelligence as it used to be years ago. With the increase of the generalised use of the internet especially and globalisation, intelligence is no longer based on classified information, and almost everyone can collect it. The following sections will elaborate on the reasons why OSINT is used today and by which actors, the sources and tools to do it and the opportunities and challenges that OSINT has, followed by a brief conclusion.

2. WHO USES OSINT AND ITS PURPOSE

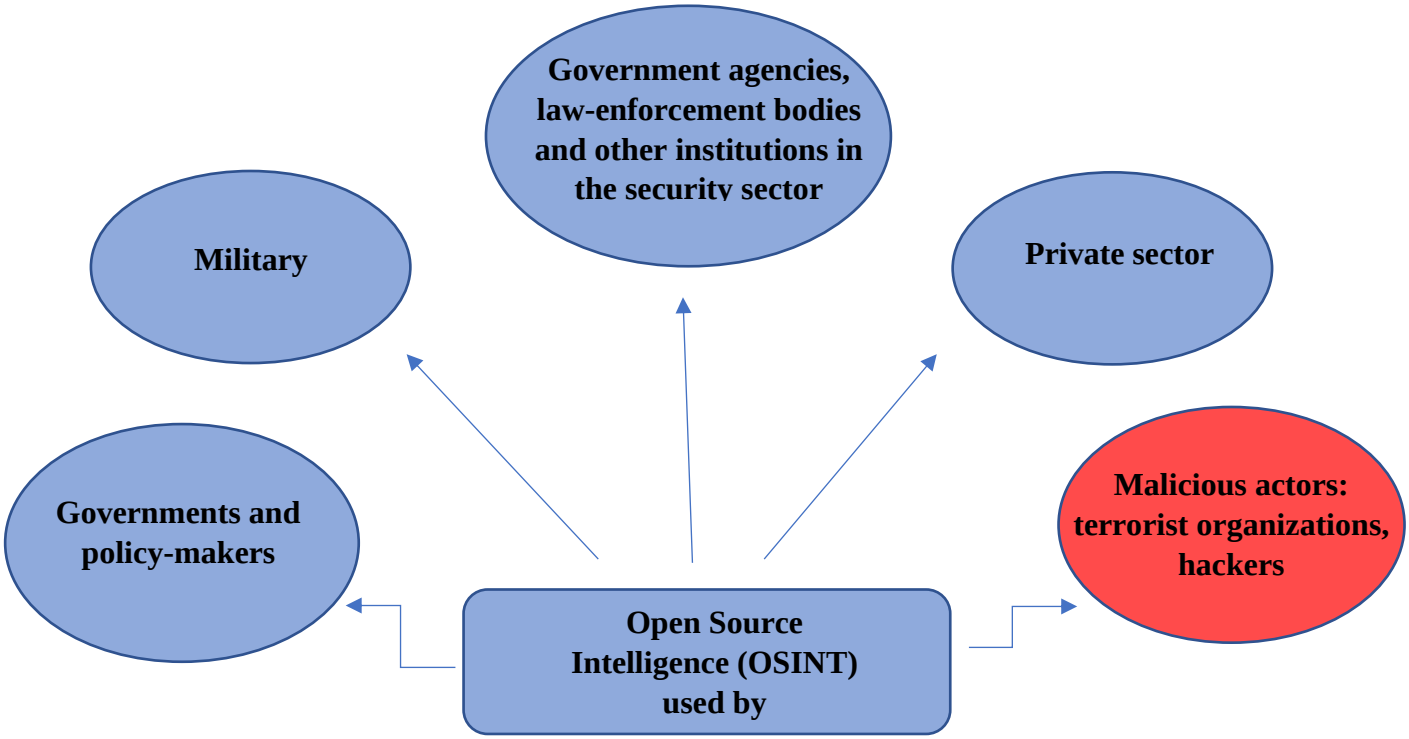
Governments, the military and policy-makers around the globe have a long history of relying on open source intelligence for decision-making on national security and defence matters. Hence, OSINT was mostly used to gather information on their enemies' strategies during wars (Elguindy 2021). Today, it is still crucial for government agencies, law enforcement bodies and institutions working in the security field, but also by other private-sector actors in different areas, such as the economic, and actors include even terrorist organisations, who are known to use open sources to recruit or train members, among other purposes (Tylutki 2018: 400; Ziółkowska 2018: 68). In the field of counterterrorism, for instance, open source intelligence has proven to be essential to combat Daesh, as information is extracted from foreign fighters' social media, including their location or details about certain activities related to the group (Klečková 2021). During the Covid 19 pandemic, OSINT was also of immense value to combat misinformation about it, and it gave governments the chance to address it.

Moreover, taking into account the quantity of information available online today, OSINT becomes extremely important for intelligence analysts to enhance their perception of the real world as well as to provide early warnings and support evidence in judicial trials (Elguindy 2021:37). To have a clearer picture of its role in today's intelligence services, it is calculated that around 80 to 90 percent of the intelligence derives from open sources (Hribar, Podbregar and Ivanuša 2014:532; Cross 2019:5). Hence, open source information contributes today in a large scale to the total data gathered by intelligence services.

There is a wide range of information that can be obtained using open sources, such as "on internal, economic, social, scientific and technical policies as well as demographic issues" (Ziółkowska 2018: 68). This is especially valuable during crisis, as open sources provide real-time information that everyone can access for little or no cost, so intelligence analysts and policy-makers can act faster against threats. These are some of OSINT's advantages that will be discussed in the last section of the paper. Open source can also be used by

governments to secure transportation facilities by learning in advance about vulnerable information that compromises its safety (Tilston 2021).

OSINT, however, is also used by other actors with malicious intentions, such as hackers and terrorists. The publicly available information about a company or its employees, on the one hand, can be potentially exploited by hackers (Sharma, Breeden and Fruhlinger 2021). On the other hand, terrorists use in the same way OSINT to learn about their enemies' weaknesses and plot a future attack (Khera 2020).



3. WHAT ARE THE SOURCES AND TOOLS FOR CONDUCTING OSINT?

The sources from which information is gathered include several types, from physical sources to online ones. The sources include newspapers, public speeches, conferences, academic publications, the radio, the television, databases, geospatial information and the Internet, being this last source the most significant for intelligence gathering today (Elguindy 2021).

Social media, such as Facebook, Twitter, YouTube, Instagram and LinkedIn, is without any doubt a great source on individuals' personal information and opinions. Terrorist organisations, in fact, manage to spread through these online platforms their ideologies, details about their organisation or future strategies, and share inappropriate content. This leads to the radicalisation of other users, but it also serves to gather valuable information about them (Chadhary and Bansal 2021:10). Databases are very useful as well for counterterrorism purposes. There are a vast number of them available online that record terrorist attacks, terrorist organisations, such as the GTD (Global Terrorism Database), ITERATE (International Terrorism: Attributes of Terroristic Events) or SATP (South Asian Terrorism Portal), to mention a few (Chaudhary and Bansal 2022). The Global

Terrorism Database is especially used by governments and international companies for policy and research-related purposes (Lafree 2022). In fact, I consulted some of these databases myself as a student to draft academic papers.

Therefore, search engines provide a very efficient tool to conduct OSINT research. Given the extent of the amount of information that is available today, intelligence analysts use methods of data mining, crawling techniques and data extraction to make this process as less time-consuming as possible (Tilston 2021). As previously mentioned, open source can also be used by hackers and other individuals with malicious intents. To avoid cybersecurity attacks, there are today several OSINT tools in use, such as Maltego, Mitaka, SPiderFoot or Intelligence X, among others. These programs help companies discover what type of information is there available, assess whether it is sensitive or not, and then remove it in order to reduce cyberattacks (Sharma, Breeden and Fruhlinger 2021).

4. OPPORTUNITIES AND CHALLENGES

Open source intelligence has an unbeatable advantage, as it can be collected at almost no cost and in a legal way considering that information is freely available online for everyone. Thus, almost anyone can conduct OSINT research, which also lowers the cost of training very reduced personnel (Klečková 2021). Taking everything into account, governments and other public and private bodies have very rational reasons to resort to this type of intelligence gathering. Moreover, "it can reduce the burden placed on classified intelligence" and allow this sector to focus on gathering information of a classified nature (Elguindy 2021). Another advantage that comes with its free availability is that information can be shared, as opposite to classified intelligence. This allows many governments, organizations, NGOs and other actors to cooperate and share intelligence among each other, that might be valuable to prevent possible threats in the highly globalized world we live in today. This also entails that no security clearance is necessary for conducting OSINT research, and therefore the process for intelligence analysts is faster and that allows them to also warn about risks in a quicker way.

Nevertheless, open source is time consuming, which is its biggest challenge combined with the requirement to check the information for its reliability. First of all, analysts have to assess which information is valuable or needed. Then, they need to be efficient and trained in order to find the right information through large amounts of data (Hribar, Podbregar and Ivanuša 2014). And even when this information is efficiently collected, it still needs to be correctly interpreted so that intelligence is produced; in this sense, personal biases come into play and there are risks for fogging the results. Hence, trained and capable personnel is also needed for open source intelligence research for these reasons.

Another disadvantage is related to the fact that terrorists and hackers also use OSINT for their purposes. Google Maps, for instance, is a very common tool among terrorists for plotting terrorist attacks ((Klečková 2021). Social media especially can also be useful to spread fake news or hoaxes by terrorist groups, so the collection of valuable and real intelligence becomes difficult for analysts. Regarding terrorism databases, they also have

important shortcomings to keep in mind. The information that was collected for the database can be biased or fake, thus altering results. Multiple terrorist groups sometimes claim responsibility for an attack, while other times there is not a clear responsible group. Countries under a dictatorial regime or with high governmental control might share inaccurate data (Lafree 2022). Moreover, the definition of terrorism differs between countries, which also causes variations in datasets depending on which country or organisation creates them. These drawbacks are also applicable in every other field that is important to consider when conducting OSINT research.

Finally, there are legal challenges to consider. The information might be available online and open for everyone, but there are still Data Protection Rules that researchers and investigators must be aware of. The collection of personal data, thus, should have a legal purpose for them to be able to act within the boundaries of the law and human rights. However, it has been questionable the extent to which conducting OSINT is in line with human rights and privacy (Hribar, Podbregar and Ivanuša 2014). In some instances, the legality of the data used might even vary between countries, or it has copyright issues. In addition, combatting cybercrime has increased the controversies over this debate, since researchers are allowed to go beyond data privacy policy in order to prevent cyberattacks (Elguindy 2021). This issue is a whole bigger problem that democratic governments always face when choosing whether it is more important to safeguard national security at the expense of the people's privacy, or the other way around.

5. CONCLUSION

Open source research is crucial for the creation of intelligence today. In a globalised world, in which threats might have direct or indirect consequences for several actors at the same time, OSINT is an affordable intelligence-gathering process that opens the door for international cooperation and contributes to reduce future risks.

Even though OSINT is quite cheaper than classified intelligence, it still comes at a cost since it has undeniable shortcomings. Used by the wrong people, open source intelligence can be very dangerous and can threaten national and international security in many levels. Hence, it is important that these challenges are acknowledged and the competent authorities are aware of them to lower the chances that OSINT is used against international security. Neglecting OSINT's utility today would be naïve, as it would be impossible to act efficiently and promptly towards new threats by just relying on classified intelligence. However, more resources might be needed in order to train professionals and this way overcome the overflow of information as well as the other disadvantages that open source intelligence entails.

6. REFERENCES

Photo: European Commission (2019). Deconstructing the terrorism discourse on social media. 17.04.2019. (https://ec.europa.eu/research-and-innovation/en/projects/success-stories/all/deconstructing-terrorism-discourse-social-media/, 26.10.2022).

Best, Richard, A. – Cumming, Alfred (2008). Open Source Intelligence (OSINT): Issues For Congress. In. Paulson, Terrance M. (eds.), *Intelligence Issues and Developments* (New York: Nova Science Publishers), pp. 75-97.

Cross, M.K.D. (2019). Counter-terrorism and the intelligence network in Europe. *International Journal of Law, Crime and Justice*. 16.12.2019 (https://doi.org/10.1016/j.ijlcj.2019.100368/, 13.10.2022).

Elguindy, Mohamed (2021). Applying Digital Forensics Methodology to Open Source Investigations in Counterterrorism. *Journal of law and Emerging Technologies*, 1(1):11-64. 20.10.2021 (https://jolets.org/ojs/index.php/jolets/article/view/32/, 13.10.2022).

Hribar, Gašper – Podbregar, Iztok – Ivanuša, Teodora (2014). OSINT: A "Grey Zone"? *International Journal of Intelligence and CounterIntelligence*, 27(3):529-549. 12.05.2014 (https://infosec-journal.com/article/osint-grey-zone/, 13.10.2022).

Khera, Varin (2020). An Introduction to Open Source Intelligence (OSINT). *Cyber Protection Magazine*. 02.11.2022. (https://cyberprotection-magazine.com/an-introduction-to-open-source-intelligence-osint/, 16.10.2022).

Klečková, Adéla (2021). Open Source Intelligence and Terrorism. *Prague Security Studies Institute*. 19.03.2021(https://www.pssi.cz/publications/48-open-source-intelligence-and-terrorism/, 14.10.2022).

Lafree, Gary (2022). Terrorism Open Source Databases. In. Muro, Diego – Wilson, Tim (eds.), *Contemporary Terrorism Studies* (Oxford, UK: Oxford University Press), pp. 113-134.

National Commission on Terrorist Attacks Upon the United States. 16.06.2004. (https://govinfo.library.unt.edu/911/press/photos/index.htm/, 26.10.2022).

NATO Open Source Intelligence Handbook. *NATO*. 01.11.2001. (https://www.academia.edu/4037348/NATO_Open_Source_Intelligence_Handbook/, 12/10/2022).

News and Policies. March 2005. *The White House*. 01.03.2005. (https://georgewbush-whitehouse.archives.gov/news/releases/2005/03/images/20050331_p44650-107-515h.html/, 26.10.2022).

Schaurer, Florian – Störger, Jan (2013). The Evolution of Open Source Intelligence (OSINT). *Intelligencer: Journal of U.S. Intelligence Studies*. (https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf/, 13.10.2022).

Sharma, Ax – Breeden, John – Fruhlinger, Josh (2021). 15 top open-source intelligence tools. *CSO*. 28.06.2021. (https://www.csoonline.com/article/3445357/what-is-osint-top-open-source-intelligence-tools.html/, 17.10.2022).

Smith, Michael S. (2022). Perils in Plain Sight. *Strife Policy Papers*. 01.06.2022 (https://www.strifeblog.org/wp-content/uploads/2022/06/Perils_In_Plain_Sight_Smith_June2022.pdf/, 13.10.2022).

Tylutki, Krzysztof (2018). The information of a mass destruction range – OSINT in intelligence activities. *The Central European Journal of Social Sciences and Humanities*, 10(19): 384-404. 19.10.2018 (http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-aed6f6f9-eee6-4bc8-8457-6425cc6fb58d/, 12.10.2022).

Ziółkowska, Agata (2018). Open source intelligence (OSINT) as an element of military recon. *Security and Defence Quarterly*, 19(2):65-77. 30.06.2018 (https://securityanddefence.pl/OPEN-SOURCE-INTELLIGENCE-OSINT-nAS-AN-ELEMENT-OF-MILITARY-RECON,103337,0,2.html#S2/, 10.10.2022)