CHAPTER «SOCIAL COMMUNICATIONS»

EXPLORING OSINT: A KEY TOOL IN INVESTIGATIVE JOURNALISM, SECURITY, AND EDUCATION

Mariana Kitsa[1]

DOI: https://doi.org/10.30525/978-9934-26-562-4-18

Abstract. This paper focuses on the importance of the use of OSINT technology by journalists on the example of Ukraine. In particular, this tool proved its convenience during the Russian-Ukrainian war. *The purpose* of the paper is to find out if OSINT technologies are useful and should be taught by journalists. To determine whether journalists are taught OSINT intelligence technologies, it was conducted an analysis of the educational programs of Ukrainian higher education institution. It is outlined that OSINT- techniques were mostly used in Ukraine for fighting against corruption. However, at the beginning of Russian-Ukrainian war it can be an effective tool for Ukrainian journalists to refute fakes and disinformation. *The methodology* included analyzing 36 of educational programs in the universities where the journalists are taught. During the writing of the work, the following research methods were used: general scientific – for description, and the analysis of theoretical aspects of the research; dialectical and historical methods helped to consider and analyze the history of CPC development, as well as the evolution of the use of OSINT techniques in the public and private sectors; the structural and functional approach made it possible to take into account all components of the process of conducting intelligence on the basis of open sources. *Results.* It was discovered that the journalists in Ukraine doesn`t use OSINT-technology in their proficient activity. One of the reasons of this phenomenon may be the lack of knowledge. It is found out that there are some disciplines that can get acquainted

[1] PhD, Associate Professor,
Department of Journalism and Mass Communication,
Lviv Polytechnic National University, Ukraine

with future journalists with OSINT-techniques. *Practical implications.* The content analyses of the work program of such subjects showed that there are no themes which include open source intelligence, or OSINT as a subject of study. To improve public control, it is necessary to implement a study of the discipline of OSINT -intelligence for future journalists. *Value/originality.* During the Russian-Ukrainian war, to acquire skills of intelligence using open sources in the shortest possible time, it is necessary to organize master classes and trainings of leading foreign experts for Ukrainian journalists and representatives of state and public organizations.

Introduction

In the era of digital transformation, open data has become an essential resource for journalists, researchers, and media professionals. Open-source intelligence (OSINT) offers powerful tools for verifying information, uncovering hidden connections, and enhancing investigative journalism. As misinformation spreads rapidly, the ability to analyze and interpret publicly available data is more critical than ever. The development of information technology has made open source intelligence an integral part of many professions. Whereas OSINT used to be the prerogative of intelligence services alone, these techniques are now used in many areas, including journalism and anti-corruption.

OSINT – techniques for detecting abuse of power – is a relatively new phenomenon in Ukraine and is just gaining momentum. Simultaneously with the beginning of Russia's war in Ukraine, this technology gained new significance. The use of OSINT technology can help to detect Russian crimes against Ukrainian civilians and the military, confirm or refute information, document events, and so on. Until recently, OSINT – technique was associated in Ukraine only with detection and overcoming corruption in Ukraine as one of the biggest problems that hinders its internal development and creates a negative image in the international arena. However, during the war, this problem receded into the background. At the same time, OSINT - technology as an analysis of open data can and should be a tool for investigative journalism, as well as for the activities of both government and non-governmental organizations operating in Ukraine. At present, there is no comprehensive study that would reveal the practical aspects of the fight in Ukraine using intelligence based on open sources.

Instead, this topic is especially relevant now, during the Russian-Ukrainian war, because OSINT technology can help to detect fakes, assets of pro-Russian politicians and figures, and so on.

Reviewing the source base, the foundation of our study consists of the works of Ukrainian and foreign authors. Among them are Kozhushko [14], Vasiliev [29], and Zharkov [30]. We also considered the Law of Ukraine "On Information", the Law of Ukraine "On Prevention of Corruption" [20], the US Intelligence Community Directive №301 [20], the Law on the US State Defense Permit for Fiscal Year 2006 [17], and the US Military Doctrine Manual Interim № 2-22.9.

Kozhushko [14] examines the definition of Open Source Intelligence (OSINT) through the perspective of intelligence services. His work explores the main characteristics and sources of intelligence derived from open sources. Pastor-Galindo et.al [21] analyze the role of information and analytical activities in public administration, focusing on analytical work and monitoring.

The problem of combating corruption is discussed by Butkevych [4, p. 90], who argues that OSINT can be a key tool for detecting and preventing corruption in official institutions. The study by Arslan, C. & Yanık, M. [1, p.69] provides insights into OSINT within private organizations, detailing its methods and principles, thus offering a broader perspective on OSINT applications.

Among the foreign works, it was considered the research material edited by H. Minas "Can intelligence based on open sources appear as an independent discipline for the US Intelligence Community in the XXI century?" [5]. This paper systematically presents information on the definition and sources of OSINT. Of particular interest is the disclosure of such categories as "OSINT Manufacturers" and " OSINT Consumers".

O. Minko also dealt with OSINT issues. The article "Using OSINT technologies to obtain intelligence information" [16] highlights the prospects for the use of OSINT technology as one of the ways to obtain intelligence information in the context of the Russian-Ukrainian war.

A fundamental source is the publication of the NATO Open Source Intelligence Handbook. It highlights the main aspects of OSINT, as well as a list of open source and publicly available information. It should be noted that this work can serve as a textbook for students, journalists, analysts,

and other professionals. Moreover, we can't mention Guides to open source intelligence [18, p. 2] where there are detailed instructions how to use open source.

However, we were interested in the importance and relevance of the application of OSINT in journalism. Therefore, in the more recent source Guide to Open Source Intelligence (OSINT), OSINT is considered as «one of the most valuable tools to a contemporary reporter, because of the vast amount of publicly available online information». About the line between journalism, OSINT, and civil war, it is written in the article «Yankee Reporters and Southern Secrets: Journalism, Open Source Intelligence, and the Coming of the Civil War: by Michael Fuhlhage» [13, p. 243].

Olaru and Stefan declare that for intelligence analysts who count on open sources (OSINT), this level of mistrust in massmedia has significant and permanent implications on the way they do their job [23].

OSINT can be a tool for refuting fakes. This thesis is also approved in the article «Fake news – a challenge for OSINT» [19, p. 391]. The authors declare that «the increasingly use of fake content or alternative facts, coupled with the dynamics of social networks, has generated a special concern to understand and counteract this phenomenon. In the intelligence activity, the extent of the phenomenon and the magnitude of its consequences, amplified by the facilities provided by the social platforms, create significant difficulties in collecting and analyzing information from open sources (OSINT)» [19, p. 391].

Nevertheless, Potz declares that OSINT can give good indications of possible threats, but one problem remains: there will always be hidden actors that OSINT cannot help with. For making forecasts, more information certainly helps, while important anti-state actors tend to conceal their existence and intentions. That, combined with disinformation, makes a significant disadvantage for OSINT [23].

Web resources served as important empirical materials of our research. Among them are the website of the Center for Combating Corruption and its official Facebook page. With the help of these sources, it was possible to obtain data on the history of the CPC, its structure, goals, and methods of activity, as well as individual projects.

For a better study of the practical use of OSINT techniques in Ukraine, there were considered the websites of organizations that oppose Russian

propaganda. In particular, these are Proof (Dokaz), Bellingcat Ukraine, Conflict Vehicle Tracking Project, Stopterror. Anti -corruption resources, including «Our Money» (Nash groshi), Bihus Info, Anti-Corruption, were also useful for examining how OSINT technologies can be used for creating journalistic materials, in particular, journalistic investigations.

During the writing of this work, the following research methods were used: general scientific methods for the description and analysis of theoretical aspects of the research; dialectical and historical methods, which helped examine the history of CPC development as well as the evolution of OSINT techniques in the public and private sectors; and the structural-functional approach, which allowed for the consideration of all components involved in conducting intelligence based on open sources. The empirical method was used for document analysis, helping to establish a source base, particularly by examining journalism education programs for the inclusion of disciplines related to OSINT studies.

One of the main methods used in this study was document analysis. To determine whether Ukrainian journalists are taught OSINT intelligence technologies, it was conducted an analysis of the educational programs of Ukrainian higher education institutions. According to the United State Electronic Database on Education (EDEBO), as of 2022, journalists are being trained in 48 higher education institutions in Ukraine, but only 36 higher education institutions provide free access to educational programs on their websites. There were considered educational programs of both bachelor's and master's levels of higher education, which prepare students for the specialty "Journalism". Were taken into account the latest educational programs, which are presented on the official websites of higher education institutions for 2021-2022. Curricula were reviewed in the educational program. The subject of research was a discipline that would include the concept of OSINT, open data analysis, or competitive intelligence. The next stage of the analysis was to eradicate those disciplines, the name of which included investigation, analysis of exposed data, applied communication, and information technologies. We also took into account which cycle of educational components the discipline belongs to – compulsory or elective discipline. This was followed by a search for work programs of the eradicated disciplines and an analysis of the topics to be studied. The main focus of the search was the concept of OSINT, open data analysis,

or competitive intelligence. As a result of the preanalysis of materials and documents, the following research questions were identified:

RQ 1 What is OSINT and how can it be used in Ukraine?

RQ 2 How can OSINT be used by Ukrainian journalists?

RQ 3 Does Ukrainian universities provide knowledge of OSINT for future journalists?

Results

What is OSINT and when did it occur?

The history of OSINT dates to 1941, when the Foreign Broadcasting Monitoring Service was established in the United States (Broadcast Monitoring Service). The purpose of this organization was to collect information broadcasted from abroad, its translation and sending to military departments. The information was provided in the format of weekly reports. A classic example of this is obtaining data on the success of information of the bombing of enemy bridges by obtaining and analyzing changes in orange prices in Paris [2].

There is currently no single definition of OSINT. However, it is believed that the basic concept of the term "open source intelligence" was introduced in the US intelligence community after the creation of the FBIS. In the official documents of this organization, OSINT is defined as one of the types of military intelligence, which is designed to search, collect, and analyze information from publicly available sources. It should be added that the term "open source intelligence" is still identified with the accepted in the foreign literature term "competitive intelligence" and its equivalent term "business intelligence" [3, p. 30].

It should be added that competitive intelligence became widespread in the 1960s. The reason for this was the massive concern of American and European entrepreneurs about the penetration of Japanese companies in their markets. According to A. Vasiliev [29, p. 34], competitive intelligence is a system of measures for constant search, detection, collection from various sources (open, corporate, or restricted), accumulation of information on changes in the conditions of commercial activity, and its analysis to timely prepare reports on its real state of affairs and identify trends in the situation.

Over the time and the development of information technology, the concept of OSINT has evolved and began to cover increasingly issues.

If you are looking at this term from the point of view of intelligence activities, you should refer to the "US Intelligence Community Directive № 301". In this document, the information obtained in the OSINT process is defined as “publicly available material that anyone can legally obtain through a request, purchase or observation. The collection of such information must comply with applicable copyright requirements. In fact, this information, which is in the public domain, is not a state secret and is not classified as "secret".

During World War II, intelligence services began to actively use various OSINT methods, including collecting newspaper clippings, listening to radio broadcasts, and so on. B. Hamilton identifies the following terms to describe the information:

– non-secret / unclassified information;
– open / overt information;
– overt intelligence;
– public information – publicly available information;
– white intelligence (Hamilton 2007).

Speaking about OSINT legislation, a fundamental source legal framework has US. The Military Doctrine contains a section "Field Manual Interim № 2-22.9" which is presented in the format of a manual (instructions) for the military, which contains a detailed description of intelligence from open sources. The Doctrine states that the main difference between OSINT and other types of intelligence is that it is based on the source information and methods of their collection, and not a certain category of technical or human resources. It should be noted that this document is highly specialized, but according to O. Kozhushko [14, p. 73], it can be considered as a guide to the theory and practice of OSINT for common citizens.

Another definition is contained in the U.S. Fiscal Permit Act for the 2006 fiscal year, which states that open source intelligence is an intelligence that is conducted by collecting, processing, and transmitting information to the target recipient from publicly available open sources for solving specific intelligence tasks. The document also notes the importance and significance of this type of information. Among the advantages of OSINT is the ability to exchange in intelligence activities without the use of covert methods and secret sources.

Media companies, colleges, journalists, and scholars have been analyzing OSINT data in the private sector, hundreds of years ago before the advent of the internet. In 2001, Wikipedia was established in the U.S., a nonprofit organization and website that collects, analyzes, and discloses OSINT. It is the world's largest private nonprofit OSINT collection, analysis, and open site on the internet. Currently, the importance of OSINT has rapidly emerged as much information overflows because of the development of computers and the internet in the twenty-first century [11] Hwang.

Having analyzed the works of Ukrainian and foreign scientists, it is worth adding that the term "Intelligence from open sources" is not used in direct interpretation. The glossary of Ukrainian terms provides the following definition of the term "information from open sources" – this is information that is intended for the public; information from external sources, such as scientific literature; official information; information published by public organizations, commercial companies and media [8].

If we consider open sources in the context of international information, it is necessary to distinguish the term "source of information" and its variety "open sources of information". Thus, the term source of information means "statutory databases and data banks with a wide range of representations, which are used in diplomatic practice, the activities of international organizations, in the settlement of international conflicts, in the transfer of personal information." The sources of information are divided into open and closed [25].

Open sources of information include: interpersonal sources and indirect sources. Interpersonal sources are sources of information, which include interpersonal contacts at various levels of representation, for example, interpersonal contacts of foreign policy representatives, agencies, and heads of relevant agencies in all areas of cooperation, as well as diplomatic contacts and contacts presented in the country in international forums (organizations). Special structures are used to obtain confidential information. Indirect sources are sources of information that act as a mediator between a particular source of information and the subject of international relations. These include: mass media, electronic means of communication, information centers, archives, libraries, and other sources of information storage. Indirect sources, in turn, are divided into official and unofficial [22].

The NATO Open Source Intelligence Handbook provides a list of open source and publicly available information. They include:

– diplomatic missions;
– Chambers of Commerce and Industry;
– Non-Governmental Organizations;
– Religious Organizations;
– National-Level Intelligence Organizations;
– academic sphere – software, dissertations, lectures, presentations, research, knowledge in print and electronic form in economics, geography (physical, cultural, military-political), international relations, regional security, science and technology;
– governmental, intergovernmental, and non-governmental organizations – databases, published information and printed reports, reviews of a wide range in economics, environment, geography, humanities, security, science, and technology;
– commercial and public information services – disseminated, published, printed news of current international, regional, and local events;
– archives (libraries) and research centers – printed documents and digital databases on a number of issues such as knowledge and skills of information retrieval;
– individual and group information – handwritten, drawn, published, printed, or disseminated information (eg, art, graffiti, postcards, posters, or websites);
– "gray literature" – scientific reports, technical instructions, economic reports, working papers;
– unofficial government documents, dissertations, marketing research, newsletters [24].

Using OSINT in various fields in Ukraine and abroad

For better understanding the concept of OSINT, it is also worth considering such categories as "OSINT Manufacturers" and "OSINT Consumers", which are found in American sources. "OSINT manufacturers" are engaged in open source intelligence, using various methods and tools, which is carried out in the interests of the government or the client. OSINT consumers are governments, international organizations, corporations, and other nongovernmental actors. Those are bodies or individuals who are responsible for making important decisions [10].

"Manufacturers" can be divided into two groups – government agencies and private organizations. Among the government agencies are the Open Source Center (USA) and the BBC Monitoring Division (UK). Among the private organizations – Jane Information Group, the Economist Intelligence Unit and Oxford Analytics. State institutions act in the interests of the government and are financed from the state budget. For example, the Open Source Center is a network of more than 180 analysts who speak more than 80 languages. This network gathers information about everything that may be of interest to the US government. In the case of private organizations, they may be partly funded by governments, but act in their own interests or in the interests of the client. It should be added that quite often the clients are government agencies themselves. As an example, the Jane Information Group specializes in military issues and has a wide network of clients from more than 180 countries. Among them are the governments and military departments of individual countries.

Since we have considered the category "OSINT Consumer", it is also worth considering the derived concept – "OSINT Product". By "product" is meant the end result of open source exploration. In fact, these are services that can be provided by an organization that uses OSINT methods. Among the most common services are analysis, consulting, and forecasting (short or long term). It can also be a collection of information about important people who are involved in the media space and whose opinions influence government, businesses, and public interests. Widely spreading are publications in the form of reports, which comprehensively contain translations, expert assessments and forecasts on political, economic, or military issues.

For a broader understanding of the concept of OSINT, it should be noted that this activity has its advantages and disadvantages, as well as a number of properties. The advantages of open source intelligence include the availability of information sources, the volume of information sources, versatility, efficiency of receipt, ease of further use, and cost of obtaining.

Accessibility means that you do not need to take special measures or create complex technical intelligence systems to use OSINT information sources, you just need to know where and what to look for. The advantage is also that OSINT allows you to process a large amount of information resources, which continues to grow rapidly.

Moreover, given the constant increase in available information resources in the world, with the help of OSINT, journalists can meet most of the information needs of consumers of intelligence information, which indicates its diversity. However, the biggest advantages, in our opinion, are efficiency, ease of use, and low cost. The data obtained with the help of OSINT make it possible to track changes in the situation intelligence objects in real time. This information can be easily passed on to all interested institutions, in contrast to that which is classified as "secret". The cost of such exploration does not impose great difficulties on the budget. For example, the share of open source intelligence spending in the US intelligence budget is only about 1%.

The widespread use of the term OSINT in the post-Soviet space began with information on the widespread use and effectiveness of OSINT in the United States during and after World War II in research by the non-governmental Center for Strategic Research RAND Corporation and a division of the US CIA 's OSINT Foreign Broadcast Monitoring Service, FBMS (Foreign Broadcasting Information Service) [12].

The particular elements of the phenomenon today are related to the increasing trend of fake news, most of them produced and posted on the obscure sites. Their spreading is facilitated by the social platforms, that extended the possibilities of generating content directly by the user and global coverage of publishing [19, p. 395].

In Ukraine, OSINT began to be actively used after the beginning of the Russian aggression in eastern Ukraine in 2014. In the conditions of the information war with the Russian Federation, false information about Ukraine began to spread actively. This prompted NGOs and government agencies to actively refute Russian myths and misinformation by gathering information from open sources. This became a direct evidence of Russia's war crimes in Ukraine. At present, there are three organizations and resources which have been formed in Ukraine to search for information or counteract hostile propaganda. Among them are:

– *Dokaz* is a resource that publishes evidence of the presence of the Russian military in eastern Ukraine, materials on the crimes of terrorists and occupiers in the Ukrainian Donbass [9].

– *Bellingcat* Ukraine Conflict Vehicle Tracking Project – this site collects and publishes data on the movement of Russian military equipment in the Donbass [29, p. 37].

– *Stopterror* – the project visualizes on an interactive map, the fighting in Ukraine, publishes information about illegal armed groups and the presence of Russian military personnel. You can also report any other events on these topics through the site [26].

OSINT is also actively used by the Security Service of Ukraine, the Central Intelligence Agency, and the Ministry of Internal Affairs. Moreover, quite often the information received by means of OSINT is used during the information war against the enemy.

OSINT methods based on semantic technologies support analysts by obtaining and monitoring thousands of pieces of data contained in open source, social networks and within specific information flows – Facebook, Instagram, Twitter. Once the risks have been identified, a system such as the Anti-Corruption Center can select and highlight critical information that analysts should review.

Multinational corporations need to step up their corporate security activities to identify dangerous phenomena that may require real-time tactical action and to identify potentially negative trends and phenomena that may require strategic action to protect the company. OSINT methods based on semantic technology process a large amount of data generated from different sources (internal, external, and specialized providers) and different types (news reports, notifications, tweets, etc.). Each piece of data is selected and qualified so that, if necessary, a tactical action can be taken (for example, @Anonymous has announced its intention to carry out a series of attacks against companies in the industry). Other data are considered from a strategic point of view to avoid future threats (for example, to identify the evolution of opinions and/or related influences).

Through semantic analysis, OSINT processes millions of pieces of open source content daily (including social media and targets such as people, places, organizations, topics, etc.), selects and directs information of interest. The indexing process extracts the "atoms of knowledge"; thus, the client does not receive the whole document as an output, but only a part of the text, where the goal of interest is contextualized in relation to its semantic environment, providing an optimized overview of the information which is available at the moment.

The best example of the use of OSINT technology is in the Center for Combating Corruption – the Rotterdam + case. At the beginning of

2016, the NCRECP introduced the so-called "Rotterdam +" formula for calculating the electricity tariff. According to the investigation, this formula provides conditions for an artificial increase in the price of electricity sales and caused 18.9 billion hr. in losses to electricity users. The case is currently under active investigation [27].

The case of possible corruption in the formation of the price of coal "Rotterdam +" is one of the most relevant for detectives of the National Anti-Corruption Bureau and the Center for Combating Corruption. The case was started with the use of open sources – the Rotterdam + contract and calculations performed according to a special formula. According to the new methodology, the cost of coal in the production of coal-fired heat generation is calculated by the formula "the cost of coal in the port of Rotterdam plus the cost of its delivery to Ukraine" [7].

Due to the application of the new formula, heat generation, including the generation of DTEK, Rinat, Akhmetov, and the state-owned Centerenergo, began to sell more expensive electricity. The high-profile topic has been circulating in the information space in recent years and has almost completely disappeared today. At least we do not hear critical thoughts about Rotterdam + anymore. However, we hear that the price of Rotterdam + is the lowest, and Rotterdam has been replaced by imports of electricity from Russia [6]. Therefore, although the Rotterdam + case was extremely high-profile, it did not correspond to the reality of the anti-corruption investigation. In contrast to the expensive payment according to the Rotterdam + formula, there was an even more expensive scheme of buying electricity from Russia and Belarus. Therefore, this case was the first investigation provided by Ukrainian journalists on the use of OSINT-technology [28]. Nowadays, during the Russian war in Ukraine, OSINT technologies can be used widely for journalistic investigations, but in fact, they are provided only by 3 organizations, which we have mentioned above. Therefore, to determine was is the reason of such situation, we analyzed of the educational programs for journalists in Ukrainian institutions of higher education.

One more complex of methods of OSINT technology is financial. Financial monitoring is an integral part of the Ukrainian anti-corruption center. This activity is carried out in order to prevent the legalization of proceeds from crime. In conducting financial monitoring, the organization

analyzes the financial transactions of persons suspected of corruption. One of the most effective control tools is the verification of electronic declarations of high-ranking officials.

V. Shabunin and the Center for Combating Corruption were among the first to support the idea of creating a system of electronic declarations of civil servants, which was to be a prerequisite for combating corruption, as well as the creation of a semi-public and semi-public anti-corruption control body NABU [27].

The implementation of basic anti-corruption laws, which establish stricter administrative and criminal liability for violating property requirements and income tax returns, has taken the prevention and fight against corruption to a new level. The system of electronic declarations of Ukraine has gained both national and international recognition as an innovative phenomenon both in technology and scale. This is confirmed by the fact that EU anti-corruption bodies (such as the Central Anti-Corruption Bureau of the Republic of Poland, the National Integrity Agency of Romania and the Anti-Corruption Agency of the Republic of Serbia) are increasingly interested in using Ukrainian experience in administration and electronic declaration systems.

The electronic declaration system is one of the key mechanisms for preventing and an effective tool for detecting corruption. First of all, it allows the public to check the assets of government officials and civil servants who receive their payment from the State budget, and promotes zero tolerance and negative public attitudes towards corruption.

Therefore, it is indisputable that the electronic declarations contained in the Unified State Register of Declarations of Persons Authorized to Perform the Functions of the State or Local Authorities ("Register of e-declarations") are a source of information for both competent anti-corruption bodies. and civil society activists to detect corruption. This justifies the EU's requirements for the proper functioning of the electronic declaration and verification system.

Further technical improvement of the register of electronic declarations will reduce the time required to verify declarations and reduce the hassle in the verification process, which together will significantly increase the efficiency and effectiveness of monitoring the financial condition of a person in public service.

In total, at the end of 2022, more than 2 million users were registered and more than 2,885 million submitted electronic documents, including more than 2,457 million electronic declarations, about 313,000 modified electronic declarations and almost 115,000 notifications of significant changes in declarants' assets.

Declarants demonstrate a more responsible approach to filing declarations and submitting them on time, and make fewer common mistakes at each stage of the declaration. Free access to the declarations is an effective tool for journalists to control the earnings of politicians and high-ranking officials.

The effectiveness of the National Agency for the Prevention of Corruption (NAPC) in verifying declarations of civil servants and verifying the timely submission of declarations and reports on significant changes in declarant assets has increased along with the disciplined approach of declarants. Last year's results show that compared to 2017, the number of decisions after full verification of declarations tripled to 472, the number of reports on administrative offenses prepared after financial supervision and submitted to the court increased almost sevenfold to 310, while the number of reasoned opinions, sent for pre-trial investigation by law enforcement agencies, increased twelve times to 243.

To increase the effectiveness of full declaration verifications, the NAPC has introduced an electronic declaration verification system. In addition, a system for managing the arithmetic and logic of declarations has been put in place, the rules governing such controls have been revised and approved, and a full declaration verification procedure has been introduced as necessary.

It is expected that the automation of the collection of information for full inspections will help to increase the number of automated control of electronic declaration and data exchange with state registers. The functioning of the electronic declaration control system provides for the automated exchange of information with 16 registers and databases of public authorities of Ukraine. NABU has already approved rules and procedures for automated information exchange for access to 13 state registers. The enactment of Bill № 7276, which was introduced in parliament in November 2017 but is unfortunately not yet ongoing, will launch an automated information exchange with three key registries of the Ministry of Justice (State Register

of Civil Status Records, Unified Register of Powers of Attorney and Register of deceased estates). The results of the activity of NABU, NAPC and other anticorruption institutions are sources of journalistic materials and own investigations. In general, checking the declarations, reports of the new founded anticorruption institutions and individual social activists, NGOs and other associations, cooperation between them and journalists, using OSINT – tools and free access data is a key for forming an information society in the democratic state.

OSINT training for Ukrainian journalists

To determine whether Ukrainian journalists are taught OSINT intelligence technology, it was analyzed of the educational programs of Ukrainian higher education institutions where journalists are trained (Figure 1).

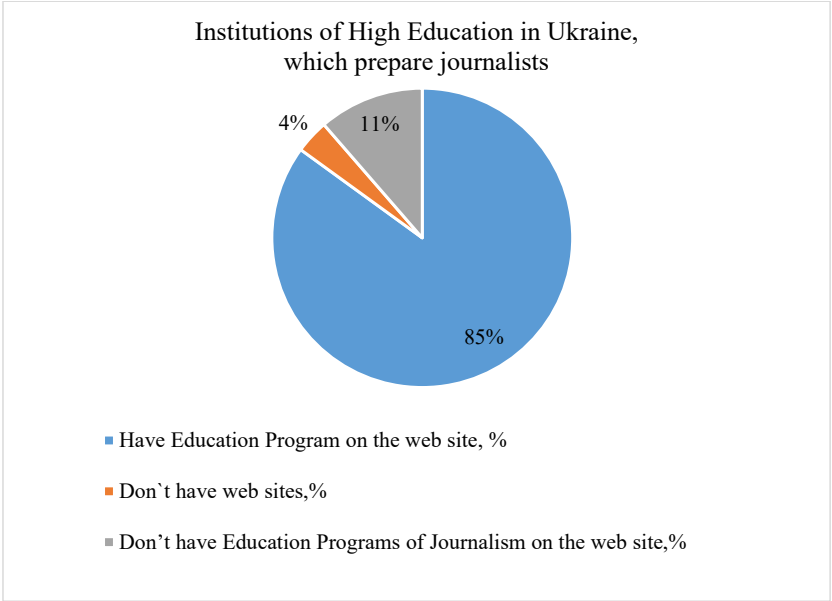

Figure 1. Higher education institutions in Ukraine, which have education program "Journalism"

In Ukraine, journalists are trained in 48 educational institutions, but only 36 higher education institutions have free access to educational programs. The educational programs of both bachelor's and master's levels of higher education, which prepare students for the specialty "Journalism" were considered.

The subject of our study was a discipline that would include the concept of OSINT, open data analysis, or competitive intelligence. As a result of the study of documents, namely, 36 educational programs (bachelor's and master's), no discipline was identified that included the word OSINT, open data analysis, or competitive intelligence. However, there have been found disciplines that could involve the study of OSINT. These are: "Journalistic Investigation", "Media Technologies and Media Techniques" (Sumy State University), "Applied Social and Communication Technologies" (Zaporizhzhya National University, Kyiv International University), "New Information Technologies" (National University "Odesa Polytechnic"). Of the above subjects, the most common discipline was "Journalistic Investigation". It is taught as a subject of the obligatory cycle of training (Odesa Law Academy, S. Demyanchuk International University of Economics and Humanities, V. Stus Donetsk National University) or as an elective course (Lviv Polytechnic National University, Lviv National I. Franko University, J. Fedkovych Chernivtsi National University). The working programs of the obligatory disciplines were posted on the website of the university. The analysis of the programs confirmed our hypothesis that OSINT technologies are not the subject of discipline for journalists. None of the topics in the disciplines defined above contained the concepts of OSINT, open data analysis, or competitive intelligence. In particular, no specific or even related topic for the use of OSINT techniques in the work programs of the above disciplines is provided.

According to the Standard for Higher Education in Journalism, approved in 2019 [15], educational programs that train journalists should include the acquisition of, among other things, general competencies: the ability to search, process and analyze information from various sources and skills, and use of information and communication technologies. Therefore, a discipline that would involve the study of OSINT techniques could ensure the acquisition of these competencies.

Conclusions

We found out that there is no single definition of OSINT technology. Moreover, there are no concrete recommendations how OSINT can be used by journalists. We can outline that OSINT is the use of free access data in official sources, bases, media, and social networks to provide investigations on the basis of competitive intelligence for a noble public aim.

Unfortunately, Ukrainian journalists do not often use OSINT technology, although it would be very appropriate during the war. For example, the British online publication Bellingcat is a leader in the use of OSINT-intelligence technology in Ukraine. One of it`s investigations revealed the use of cluster munitions, weapons designed to destroy unprotected civilians at nonmilitary facilities. Thanks to the use of this technology, the facts that confirm war crimes in Russia are analyzed, recorded, and stored. An analysis of 36 educational programs on journalism in Ukraine confirmed that future Ukrainian journalists are not taught disciplines that would include studying OSINT tools. Therefore, to improve public control over the activities of both Russian troops in Ukraine and Ukrainian officials, it is necessary to introduce a study of the discipline of OSINT -intelligence for Ukrainian journalists. Such a discipline would be of practical value and would comply with the Standard of Higher Education in Journalism, which was approved in Ukraine in 2019 and is in force.

During the Russian-Ukrainian war, to acquire skills of intelligence using open sources in the shortest possible time, it is necessary to organize master classes and trainings of leading foreign experts for Ukrainian journalists and representatives of state and public organizations.

Notes on contributors

Disclosure statement

The author(s) declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article. The author report there are no competing interests to declare.

This research wasn’t funded or sponsored by any organization, third person, etc.

References:

1. Arslan, C., & Yanık, M. (2015). A new discipline of intelligence: Social media. *Military and Security Studies, 2015*(69).

2. Barnouw, E. (1968). *A history of broadcasting in the United States*. New York: Oxford University Press.

3. Bochert, F. (2022). Open source intelligence: The untapped intelligence treasure for United Nations organizations. *Harvard International Review, 42*(4), 28-33.

4. Butkevych, A. (2012). Money laundering and corruption: Current problems of counteraction and ways to solve them. *Fight Against Organized Crime (Theory and Practice), 2*, 88-97.

5. Can the open source intelligence emerge as an independent discipline for the intelligence community in the 21st century? (2010). *Research Institute for European and American Studies.* Retrieved from https://www.files.ethz.ch/isn/111330/rieas139.pdf

6. Dilo. (2022). *Online media.* Retrieved from https://dilo.net.ua/

7. Economic Truth (Ekonomichna Pravda). (2022). *Online media.* Retrieved from https://www.epravda.com.ua/

8. Explanatory dictionary of Ukrainian terms. (2005). *Dictionaries of terms: Ukrainian-English-Russian, Russian-Ukrainian-English, English-Russian-Ukrainian.* NP 306.7.086-2004.

9. Facts about the Russian Federation's involvement in supporting terrorists in eastern Ukraine. (2020). *Proof.* Retrieved from http://www.dokaz.org.ua/

10. Hamilton, B. (2007). The DNI's Open Source Center: An organizational communication perspective. *International Journal of Intelligence and Counterintelligence, 20*(2), 240-257.

11. Hwang, Y.-W., et al. (2022). Current status and security trend of OSINT. *Wireless Communications and Mobile Computing.*

12. Intelligence Community Directive Number 301. (2006). Retrieved from https://fas.org/irp/dni/icd/icd-301.pdf

13. Jackson, C. (2021). *Yankee reporters and Southern secrets: Journalism, open source intelligence, and the coming of the Civil War.* New York: Peter Lang.

14. Kozhushko, O. (2011). Open source intelligence (OSINT) in US intelligence practice. *Scientific Bulletin of the Institute of International Relations of NAU, 2*, 68-74. Retrieved from http://jrnl.nau.edu.ua/index.php/IMV/article/view/3264

15. Ministry of Science and Education of Ukraine (MOES). (2019). *Standard of high education: Journalism.* Retrieved from https://mon.gov.ua/storage/app/media/vishchaosvita/zatverdzeni%20standarty/2021/07/28/061-Zhurnalistyka-bakalavr.28.07-1.pdf

16. Minko, O. (2016). Use of OSINT technologies to obtain intelligence. *Control, Navigation and Communication Systems, 4*, 81-84. Retrieved from http://www.irbisnbuv.gov.ua

17. National Defense Authorization Act for Fiscal Year 2006. (2006). Retrieved from https://www.congress.gov/109/plaws/publ163/PLAW-109publ163.pdf

18. Norton, R. (2011). *Guide to open source intelligence: A growing window into the world. The Intelligencer: Journal of US Intelligence Studies, 2*.

19. Olaru, G., & Ștefan, T. (2018). Fake news – a challenge for OSINT. *International Conference RCIC.*

20. On the prevention of corruption: Law of Ukraine. (2014). № 1700-VII. Updated 19.04.2020. Retrieved from https://law.work.gov.ua/laws/show/1700-18

21. Pastor-Galindo, J., Nespoli, P., Mármol, F. G., & Pérez, G. M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges, and future trends. *IEEE Access, 8*, 10282-10304.

22. Political analytics in public administration: A textbook. (2012). Kyiv: National Academy of Public Administration under the President of Ukraine. Retrieved from http://academy.gov.ua

23. Potz, T. (2021). *The increasing importance of OSINT as a source of intelligence.* (Doctoral dissertation, University of Zagreb). Retrieved from https://repozitorij.unizg.hr/islandora/object/fpzg:1381/datastream/PDF/download

24. Open Source Intelligence: FMI 2-22.9. (2006). *Federation of American Scientists.* Retrieved from http://www.fas.org/irp/doddir/army/fmi2-22-9.pdf

25. Scott, B. (2024). "Everyone freaks out when the leaks are made": data leaks, investigative journalism and intelligence practice. *Journal of Financial Crime*, *31*(3), 545-557.

26. Stop Terror: Public organization, security and cooperation in Ukraine. (2022). Retrieved from https://stopterror.in.ua

27. The Rotterdam + case is a priority for us – NABU. (2018). *Economic Truth.* Retrieved from https://www.epravda.com.ua/rus/news/2018/06/11/637668/

28. The Rotterdam case is falling apart. This is already a fact – lawyer Natalia Drygval. (2020). *Delo.* Retrieved from https://delo.ua

29. Vasiliev, A. (2013). Scientific approaches to determining the essence of intelligence from open sources. *Bulletin of the Taras Shevchenko National University of Kyiv, 30*, 33-37.

30. Zharkov, Y. (2006). *NATO handbook.* Brussels. Retrieved from https://www.nato.int/docu/other/ukr/handbook/2001/pdf/handbook.pdf