# The Increasing Importance of OSINT as a Source of Intelligence

**Potz, Tin**

**Master's thesis / Diplomski rad**

**2021**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **University of Zagreb, The Faculty of Political Science / Sveučilište u Zagrebu, Fakultet političkih znanosti**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:114:806851

Sveučilište u Zagrebu

Fakultet političkih znanosti

Diplomski studij politologije

Tin Potz

# THE INCREASING IMPORTANCE OF OSINT AS A SOURCE OF INTELLIGENCE

DIPLOMSKI RAD

Zagreb, 2021.

Sveučilište u Zagrebu

Fakultet političkih znanosti

Diplomski studij politologije

# THE INCREASING IMPORTANCE OF OSINT AS A SOURCE OF INTELLIGENCE

DIPLOMSKI RAD

Mentor: doc. dr. sc. Robert Barić

Student: Tin Potz

Zagreb

srpanj, 2021.

**IZJAVA O AUTORSTVU RADA I POŠTIVANJU ETIČKIH PRAVILA**

Izjavljujem da sam diplomski rad The Increasing Importance of OSINT as a Source of Intelligence, koji sam predao na ocjenu mentoru doc. dr. sc. Robertu Bariću, napisao samostalno i da je u potpunosti riječ o mojem autorskom radu. Također, izjavljujem da dotični rad nije objavljen ni korišten u svrhe ispunjenja nastavnih obaveza na ovom ili nekom drugom učilištu, te da na temelju njega nisam stekao ECTS bodove.

Nadalje, izjavljujem da sam u radu poštivao etička pravila znanstvenog i akademskog rada, a posebno članke 16-19. Etičkoga kodeksa Sveučilišta u Zagrebu.

Tin Potz

**CONTENTS**

CONTENTS ..... 2

1. INTRODUCTION ..... 4

1.1. Methodology ..... 6

1.2. The structure of the paper ..... 6

2. DEFINING AND UNDERSTANDING INTELLIGENCE AND OSINT ..... 8

2.1. Definition of intelligence ..... 9

2.2. Meaning of the term „OSINT” ..... 12

3. HISTORY AND DEVELOPMENT OF OSINT ..... 15

3.1. OSINT before WWII ..... 15

3.2. OSINT in the Cold War ..... 16

3.3. The shift in requirements and intelligence culture ..... 19

4. Utility of Web intelligence (WEBINT) ..... 25

4.1. Social networks ..... 26

4.2. The utility of WEBINT in cases of terrorism and organized crime ..... 27

4.3. Other WEBINT usage ..... 31

5. ANALYSIS OF FIVE MODERN DIMENSIONS OF OSINT ..... 34

5.1. The Internet as a source ..... 35

5.2. Privatization of intelligence ..... 37

5.3. Forecasting ..... 39

5.4. High-tech solutions ..... 40

5.5. Responsibility ..... 41

6. POSITIVE AND NEGATIVE ASPECTS OF OSINT ..... 43

6.1. Positive aspects of OSINT ..... 43

6.2 Negative aspects of OSINT ..... 45

7. FINAL INTERPRETATION OF THE RESULTS OF ANALYISIS ..... 49

8. CONCLUSION ..... 52

REFERENCES ..... 54

SUMMARY ..... 66

SAŽETAK ..... 67

**TABLES**

Table 1: Five dimensions of OSINT……34

## 1. INTRODUCTION

Intelligence agencies have come a long way from initially being considered ungentlemanly institutions. Because of their utility in World War II, they have been continuously used throughout the Cold War, developing their influence in international relations. After the Cold War, they were being questioned on their goals and techniques, only to become more important after 9/11. Their post-Cold War challenge is to follow changes of the interests of their states. While in the Cold War expensive spy satellites were essential to find out the number of enemy's intercontinental ballistic missiles, today's enemies, and the character of warfare has changed significantly. In light of the changed concept of security, the depiction of the Cold War intelligence methods does not fit in. By 2000, most democratic countries have some kind of mechanism for overseeing their intelligence organizations. Furthermore, covert actions and general espionage have come under increased public scrutiny, nationally and internationally. Thus, one part of the warfare has transferred into the less apparent cyber domain. In that regard, World Wide Web became an important source of information. Aside from cyberattacks, other activities such as propaganda, disinformation campaigns, or terrorist recruitment are severe in their consequences. As of 9/11, intelligence needs were dramatically enlarged. The answer to those needs laid in the analysis of all available sources, containing open ones, as well.

In such context, the technique and a product called OSINT (Open-source intelligence) is an important method of intelligence gathering that significantly adds to the answer of most intelligence needs. Open-source intelligence is a product of analyzing open information sources, making it possible for intelligence to be more transparent, less costly, and faster. When combined with high technology, OSINT is capable of bringing more insights. OSINT is not a new form of intelligence, as it was present from WWII. However, it became a second-class form of intelligence in the Cold War because of closed societies like the SSSR, whose open publications were tailored and filled with disinformation. A new incentive for capitalizing the value of OSINT came with the open-source movement in the 90s, whose initial idea was to create free software available to everyone. Connected to that, an idea emerged that knowledge should also be widely available, so programmers started sharing code with each other. By leaving the code of the software open, it was made possible to upgrade software by other user's knowledge. That can be connected to the idea of fluid information that takes shape over time, while no one has exclusive privilege over it. OSINT is a part of that since its sources and intelligence can be easily shared with others because of

lack of classification. It, however, does not come without dilemmas on privacy issues connected to leaked or sensitive information that is made public. Nonetheless, it is still considered the least intrusive intelligence-gathering technique.

Our new digital and public way of life brought greater possibilities for conducting OSINT. Because of the Internet, a large pool of primary information was created that can be processed by a computer and analyzed by human analysts for insights. It becomes even more important as the concept of security has changed to encompass more non-classical and somewhat invisible threats. In such conditions, secrets can be of less value as there are none regarding ecological or societal risks. The only way to understand the new threats and new forms of old threats is to understand the whole picture, making all-source analysis a base for that task. OSINT is often needed because of the large volume of information on the Internet, containing books, articles, blogs, comments, metadata, and other. Technology is especially important for its attainment and processing while including foreign languages adds to that necessity. Though OSINT can be made out of "offline" sources, such as academic publications, magazines, or radio, the Internet has become the most significant part of OSINT's sources. That kind of intelligence, called Web intelligence (WEBINT), is also used by the private sector and threats to national security. This makes it more critical for OSINT to follow up on technological advancements since national intelligence is starting to compete with other actors that could possibly exploit open sources even better.

The past research on OSINT has mainly focused on the positive aspects and its possibilities for the future. However, this paper's focus is placed on both positive and negative aspects, comparing them to show the relative value of OSINT in the all-source analysis. The question behind this research is: Has the importance of OSINT increased in the 21st century? Judging by the new configurations of intelligence requirements, the modern way of living and the expected responsibilities behind intelligence work, the hypothesis that will be accepted or rejected is: The value of OSINT has increased, thus increasing its importance in the 21st century.

This research and the answer to its question carries importance because of the formerly neglected value of OSINT. If it is true that OSINT can bring insights unachievable by other techniques, then its value in the analysis is at least equal to the other techniques. Additionally, by putting more focus on OSINT, certain cultural barriers of intelligence

communities need to be overcome, making the real intelligence hero "Sherlock Holmes, not James Bond "(Best and Cumming, 2008: 78).

### 1.1. Methodology

To answer the research question, an analysis will be made on five modern dimensions of OSINT. Those dimensions were abstracted out of literature on OSINT containing research articles, monographs, expert recommendations, and others. The five dimensions were taken according to their nature. They were not chosen because of their exclusivity to OSINT techniques since they can be found in other techniques, as well. Instead, they are chosen because of their crucial role in today's OSINT and because they pose essential questions with or without using OSINT. The five dimensions of analysis are the Internet as an information source, privatization of intelligence, forecasting, high-tech solutions, and responsibility. There may be other dimensions worth analyzing, as the hierarchy behind certain intelligence or biases that occur with specific techniques. However, they can mostly be placed under one of the chosen dimensions or are not crucial for proving the increased importance of OSINT. All of the five dimensions are then assigned their positive and negative aspects, with the goal of comparing their relative added value. Doing so makes it possible to analyze the real impact of open sources while also finding the slight differences in the value of OSINT. It is worth noting that these dimensions of problems are not problematic per se rather they are frameworks through which it is possible to overview the technique. Afterward, a comparison between dimensions is made to show where specifically OSINT brings added value. Thus, a greater value of OSINT in a dimension would justify using its techniques.

### 1.2. The structure of the paper

After the introduction, the paper starts by defining intelligence, OSINT, and the difference between raw open-source information and the final product. Then, a historical role of OSINT is shown, mainly focusing on the 20th century when OSINT became institutionalized. Afterward, the modern usage of OSINT is examined through technological advancements, new security requirements, and the problem of the cultural shift in intelligence agencies according to those requirements. The fourth chapter contains actual uses of OSINT made of sources on the Internet (Web intelligence), on examples of terrorism, organized crime, and a few other uses. The fifth chapter contains the analysis of the five modern dimensions of OSINT through their specific positive and negative aspects. The sixth chapter is the general overview of the positive and negative aspects of OSINT, while the seventh chapter contains

the interpretation of results of the complete analysis. Finally, the last chapter is left for the conclusion.

## 2. DEFINING AND UNDERSTANDING INTELLIGENCE AND OSINT

OSINT is a technique of gathering information that belongs to the five main types of intelligence[1] (Hensley, 2016: 12). Apart from being a technique, the term is also being used for an intelligence product made of publicly available information. To be a product, information needs to be processed, analyzed, timely distributed to the end-users, and must meet given intelligence requirements (Recordedfuture.com, 2019). Publicly available information means that „anyone can lawfully obtain it by a request, purchase or observation" (DNI, 2006: 8). That also implicates the lack of necessity of having special skills or education for its attainment. Thus, such public information can be found in books, news, public events, or anything that can be heard in public space. More recently, geospatial images became widely accessible, while subscription-based magazines and databases should also be noted. Today most of this information can be found on the Internet that combines them all on one platform (Pritchard, 2020). From an intelligence point of view, open-source gathering means overt in contrast to the covert gathering. This fact is important since using OSINT brings a difference in real operations and the perception of intelligence work popularly represented through secret operations or secret information gathering. However, this covert domain of intelligence work is still the core of intelligence, while such agencies are given rights for using those tools.

When it comes to the difference between overt and covert, gathering information from someone's social media account is considered OSINT, while an entry into that same account through a stolen or found password is not considered OSINT. How does OSINT, then, fit into intelligence work? From a dictionary of military terms of the Department of Defence, OSINT is a product of systematically gathered, processed, and analyzed information on known or expected requirements of the client (DOD, 2021: 159). As such, the OSINT technique belongs to the intelligence cycle (process) and its rules[2]. OSINT is yet another intelligence technique, but it still has some problems connected to its acceptance. One of the main reasons for the

1 Five main types of intelligence are Human intelligence (HUMINT), Signals intelligence (SIGINT), Imagery Intelligence (IMINT), Open-source intelligence (OSINT), and Measurement and signatures intelligence (MASINT).

2 Intelligence cycle is a simplification of the intelligence-making process, usually divided into five or six steps. It contains planning and direction, collection, analysis and production, dissemination, and sometimes feedback or requirements that start the process all over again (McGlynn and Garner, 2019: 13).

lack of broader acceptance of OSINT is the divergence of opinions over the primary purpose of intelligence agencies. Such opinions often stem from a culture of intelligence agencies but also from their perceived goals. To clarify the paper, it is important to note that OSINT has been much privatized, but that the focus will be placed on state intelligence agencies. However, privatization of intelligence will be briefly addressed later on in the paper.

### 2.1. Definition of intelligence

Why do intelligence agencies exist? Lowenthal (2009: 20) writes that there are at least four main purposes: „to avoid strategic surprise; to provide long-term expertise; to support the policy process; and to maintain the secrecy of information, needs, and methods.“. From many definitions that came out of security studies, all of them share a similar stance on the importance of the national security apparatus existence. They all state that there is an objective need for its existence. Objective indicators of threats show why states should maintain their militaries and require further intelligence. After the Cold War, security studies have shifted their focus, from states as former primary threats to the new non-state actors. Boundaries between partners and enemies became unclear, while occurrences on the other side of the planet became even more important. In such conditions, information also became more important. It is especially so since national governments are expected to make decisions based on rational choices or limited rationality with the available resources (Prunckun, 2010: 2). For rational choices regarding national security, they have to be aware of their surroundings while also seeking to be warned of possible threats. Besides that, they want to know alternative outcomes caused by their actions, while all of that is on intelligence services to provide (Lowenthal, 2009: 21).

In the last thirty years, there has been a reduction of most European state's militaries due to their professionalization and restructuring towards tasks connected to the expeditionary warfare. This was followed by the privatization of security while the number of private military and intelligence companies arose. Despite those changes, militaries are still key organizations tasked with national defense. The same is true for intelligence, as state intelligence agencies are still the key players. National security is still, in essence, the protection of the key values (interests) of the particular state. Those values are often described in strategic documents that are made public. On a strategic level, an important part of intelligence work is analyses made by crossing the impact and likelihood of possible incoming events (Lowenthal, 2009: 77). In the outcomes of such analyses, there will always be events that are low on probability but have an enormous impact, such as terrorist acts,

international conflicts, or disasters. All of such instances are under the special focus of the intelligence systems. Those intelligence products also need to be timely, relevant, and actionable to be useful (Andregg, 2007: 52). Though today's intelligence is under more public scrutiny than before, the intelligence profession of the 21st century still does not differ much from the Cold War concept of espionage. This may not be evident from legal norms, but it is from the reality of their actions. Popular examples are assassinations in Europe conducted by Russian foreign intelligence, U.S. National Security Agency illegally collecting information out of Europe's citizens, or Israel's foreign intelligence stealing Iran's secret documents in 2018. Though it is so, the public and non-governmental sector have been pointing out the need to regulate intelligence. One of the first such activities being under increased public scrutiny were covert operations, then came the question of whistleblowers, the politicization of intelligence, and such. The problem of intelligence oversight is especially evident from the fact that an average person walking around London is recorded up to 50 times a day (Andregg, 2007: 59). Handling such information certainly requires some oversight. The politicization of intelligence is also a big problem, in which intelligence is manipulated for the benefit of the policymakers (Denécé, 2014: 37). Some of this public appeal has turned out to be transforming for the system, especially regarding states that went through democratization and are still in the process of consolidating their political systems. However, from Snowden's case can be seen that even consolidated democracies have huge intelligence impairments with establishing responsibility (Campbell, 2015).

The usual saying that information is power greatly coincides with the general definition of intelligence (not limited only to the work of intelligence agencies), which says that intelligence is the ability to use knowledge to manipulate one's surrounding (Merriam-Webster.com, 2021). From the same dictionary, a definition can be found of intelligence in its secret service meaning. It is defined as information on the enemy or a potential enemy and the same organization that collects or uses that information. Macmillan dictionary also quotes that intelligence is secretly gathered information about an enemy and the organizations that gather them (Macmillandictionary.com, 2021). Those definitions somewhat coincide with the official intelligence definitions coming from intelligence authorities. Maybe the most famous one comes from Sherman Kent, who said that intelligence embodies at least three things: a product that contains useful processed information, a technique of gathering information, and the organization that conducts those techniques (Kent, 1949: xxi-xxii). There is an almost identical definition in the military dictionary that considers the whole three elements of

intelligence (DOD, 2021: 107). Britannica states (2021) that intelligence is information about the enemy or a probability of a future event that may affect national security. Except for those definitions, intelligence is used to represent the whole intelligence cycle and covert operations.

In the broadest sense, intelligence is an ability to think and understand then gather and use knowledge (Macmillandictionary.com, 2021). What can be noticed from these broad term definitions is that they always have an element of action. That is why sheer information is not good enough: there is a tremendous amount of information that is not useful by itself but becomes so when we know how to use it and then do so. Intelligence is intended to give leverage by assessment of the situation, insights into important phenomena, knowledge on the adversaries on high-level political meetings, and such. Although capable of doing all of that, intelligence cannot predict the future, only forecast likely alternatives (IC, 2009: 11). Even though it may seem straightforward, there are still many different confronting definitions of intelligence. McGlynn and Garner wrote that intelligence is, in essence, gathering and using knowledge and skills. However, the problem with such a simple definition is that everyone understands the word gather and the word use differently, so the simple definitions are often not good enough either (McGlynn and Garner, 2019: 2), but will suffice for this work.

There is a difference between classical intelligence and modern one. OSINT has been in use for some time (see chapter on the history of OSINT) but has rapidly evolved in the past twenty years. A great deal of modern OSINT is comprised of open sources on the Internet. Such information is usually intended to be seen by many people, but some of that information is not intended for wider use. World Wide Web (WWW) is a platform that can never guarantee complete privacy of information, not just of what is shared on the Internet, but also what is on other devices connected to it (Recordedfuture.com, 2019). Books, magazines, and public events are made public to be seen by those interested or who should know about them. That may also be the significant difference between old and modern public sources: the Internet brings everything to the public, often unwillingly. There are hidden pieces of information on the Internet that can be collected, but its obtainment requires special skills. It usually is not enough to visit somebody's web page or a profile on social media for that information to be gathered. However, with knowledge in accessing meta-data and an ability to analyze „big data”, intelligence can be produced that has more value in its content than sheer information. That points to the possibility of enriching information by the intelligence analysis, in a part of the intelligence-making process where insights are derived from

processed data. There is almost a common understanding that intelligence agencies should not deal with public information that is easily attainable since it is considered a waste of resources. The only time that it is considered justified for those agencies to analyze public information is when the expertise of the analysts and their skills make a difference, possibly enabling new insights (DCAF, 2003: 17).

### 2.2. Meaning of the term „OSINT"

Since OSINT is intelligence, it also needs to be of a greater level of insight than data or information. In an intelligence-making process, that is usually done by processing and analyzing. There are many definitions of OSINT bearing subtle differences. NATO defines OSINT as „unclassified information that has been deliberately discovered, discriminated, distilled and disseminated to a select audience in order to address a specific question" (NATO, 2001: V). This definition shows how OSINT is always a part of a planned action with its explicit goals. U.S. Department of Defense similarly defines OSINT, stating that it is a result of systematically collected, processed, and analyzed open information as a response to a given intelligence requirement (DOD, 2021: 159). This definition also clearly places OSINT into the intelligence cycle. In addition, RAND corporation defines OSINT with one added element. They have added that OSINT must be disseminated by a member of the intelligence community (Williams and Blum, 2018: 8). From these definitions, it is evident that OSINT results from an intelligence-making process that addresses a particular requirement. Most importantly, OSINT is different from public information.

The NATO's OSINT Handbook (NATO, 2001: 2-3) states four types of open information.

- Open Source Data (OSD): They are raw data and are considered primary sources. It includes photographs, recordings, notes, etc.

- Open Source Information (OSINF): This kind of information is filtered and edited for a purpose. These are considered to be secondary sources, like books, articles, and broadcasts.

- Open Source Intelligence (OSINT): This kind of information is intelligence already processed and disseminated to selected end-users. It also has the purpose of addressing a specific question.

- Validated OSINT (OSINT-V): This is OSINT of the highest level of validity, coming from a reliable source. In intelligence terms, it is often a product of all-source analysis, where open sources are tested by comparison with classified sources.

From the above, we can notice two types of sources used for OSINT, while there is one type of intelligence that is greater than OSINT. Depending on their nature, OSINT sources can also be divided into four types.

- Academic sources: Books, articles, scientific journals, etc.
- Internet sources: Social media, blogs, personal websites, etc.
- Non-internet media: Radio, TV, magazines, etc.
- Other sources: Official documents, leaflets, publications, grey information (non-official documents, notes, rumors), etc.

While many of these sources are usually used for creating OSINT, only a small amount of them will ever end up in the final product. There is even a dilemma on exploiting some of those sources, as they can contain sensitive information that can be harmful to individuals. Other public sources, like those gathered from blogs or comments, may be private and public at the same time. Leaked or unintentionally shared private information is a serious issue for OSINT, and it will be addressed in the sixth chapter.

The new informational technology has not changed anything about the goals of OSINT, which still need to be as other intelligence products: timely, accurate, precise, and bringing competitive advantage (Benes, 2013: 25). It needs to be clarified that OSINT should not be competing with other intelligence but instead used in an all-source combination for its maximum effect. This can be found in the concept of validated OSINT, where the value of OSINT is risen by its mixed usage with classified sources. However, that process is not one way since OSINT is often used to validate secrets (Marzell, 2017: 44). All-source intelligence is a product of analyzing different single-source information, often containing secrets and OSINF. That can be done to detect the level of reliability of open sources (Bernard et al, 2018: 510). Single-source intelligence usually comes from departments or agencies that specialize in one type of gathering. Thus, they produce only SIGINT, IMINT, OSINT, etc. Because of its reliability, all-source analysis is especially encouraged (Herman, 1996: 43). The intelligence cycle then seems to look a bit different. After the first step of planning, the

steps of collecting and processing can be considered single-source activity (Herman, 1996: 39). From then on, the process can take three different forms. Firstly, this processed information can be analyzed as single sources for single-source intelligence. Secondly, they can be mixed with other types of intelligence to form all-source intelligence. This can also be evident from the concept of OSINT making process[3], where the third step consists of verifying the data, often by other forms of sources (Hassan and Hijazi, 2018: 343). Thirdly, the step of processing and analysis can be omitted, thus disseminated directly to the end-users. The third possibility is the most problematic one, especially since it is single-source based. It is generally accepted that all-source intelligence is of a greater value than single-source intelligence (Omand et al, 2014: 35; Mercado, 2004: 45; Herman, 1996: 39). History, as well, has shown evident problems connected to the usage of single-source intelligence. Winston Churchill, thus, used Rommel's enigma-encrypted messages to the Reich as facts, while the British navy in WWI experienced intelligence failures because of focusing only on signal intelligence (Herman, 1996: 96). Regarding that, OSINT should be used in an all-source analysis and not as the only intelligence source.

The information revolution led to significant changes regarding requirements and capabilities of the gathering of information. In such conditions, OSINT came to have a more significant role in the intelligence-making process. Although, not everyone is certain of its actual utility. There are generally three main views on OSINT's value:

1. Secrets are of more importance to the end-users. It is so because the end-users are most interested in knowing the enemy's intentions.

2. OSINT is not just a small addition to the intelligence product but rather a good source on its own.

3. View which can be put somewhere in the middle of those opinions. By it, OSINT's only value is in mapping out the unknowns that are then to be approached by covert means of gathering (Best and Cumming, 2008: 77).

In the next chapter, the focus will be put on the historical role of OSINT and changes in perception of it.

---

3 The OSINT process or cycle is consisted of identifying the needed sources, harvesting the data, processing and verifying, analyzing, and delivering the results.

## 3. HISTORY AND DEVELOPMENT OF OSINT

### 3.1. OSINT before WWII

Espionage is considered to be the second oldest profession (the first one being prostitution), but it should be understood that secrets were not the only focus of intelligence in history (Bean, 2011: 23). The most famous spies from history could be considered the men that Moses sent to scout the land of Kanaan. However, the fact is that his men were not actually gathering secrets. They were sent to count the number of soldiers, state of the city's fortifications, fertility of the land, and other information that are indeed open. Another usage of OSINT in history can be vividly seen from Napoleon's quote, in which he said that hostile newspapers are more dangerous than thousand bayonets (Lathrop, 2004: 275). Regarding modernity, one of the important moments that showed the value of OSINT was the novel „The Riddle of the Sands“ written by Erskine Childers (published in 1903). He made somewhat of a prophecy, written to propagate the possibility of a German attack on Britain from the Frisian coast, where Netherlands and Germany are connected to the North Sea. Because of his travels as a British imperialist, he traveled through the described region and made detailed coast maps. He also described the sailing conditions and the rivers that are available for sailing. Ultimately he showed the reality of the British sea border, which is very porous. His novel is, however, fictitious, but fiction with many facts in it. As proof of its OSINT value, the author received a dinner invitation by the Naval Intelligence Department since their eyes were stuck on his four maps of the North Sea and the Frisian coast. Later on, War Office Staff College made a classified book „The Special Military Resources of the German empire“ in which Childer's book was praised and recommended for further reading for other agents (Caponi, 2014: 39-41). Before satellite photography and electronic reconnaissance, an essential source of intelligence was a military attache. However, in the early 20th century, attaches were given many tasks and not enough instructions on how to gather information. In such conditions, some half-fictitious novels proved to be quite helpful to the new agents, as they contained operational knowledge placed in a fictional context. One such novel was „Ashenden: Or The British Agent“ from 1928, written by the British ex-secret service agent Somerset Maugham that was employed in World War I. Maugham was later persuaded by Winson Churchill not to publish the last 14 stories he intended to, on the fact that they would violate the Official Secrets Act (Caponi, 2014: 42).

World War II was, in reality, a catalyst for the development of OSINT as it has created the first open-source analyses and institutions for gathering open-source information. One

such institution was Foreign Broadcast Monitoring Service, which collected, transcribed, translated, and processed radio signals. Most of its information was coming from Axis power's propaganda (Bean, 2011: 24). FBMS was one of the seldom intelligence initiatives and institutions made public, while its goals were kept transparent to American citizens. In the 60s, its activity has expanded to monitor all foreign media (Bean, 2011: 24). Office of Strategic Services, the US wartime intelligence agency in WWII, despite its reputation of secrecy, made most of its analyses on open sources. Such open sources were gathered with the intent to combine them into a mosaic. OSS had a department for open sources, research and analysis that collected newspapers, articles in foreign languages, and photographs; all brought together to make useful intelligence (Colquhoun, 2016). By so, it has collected information on imperial Japan through encyclopedias, short-wave radio signals, and guide books for tourists (Bloomsbury.com, 2012). The creator of OSS believed in the importance of using open sources on fact that they show many elements of foreign states. Mainly, they show how foreign industries function, their railway connectivity, and their economy, but most importantly, OSINT brings contextual information and knowledge on the enemy's psyche (Bean, 2011: 26). From the examples of the OSINT usage in WWII, there is a recurring motive that information is not as important as connecting it in a specific way to make a broader picture of the phenomenon. Even before WWII, in 1895, a British colonel wrote that seemingly unimportant information from newspapers could reveal important matters when combined and analyzed (Lathrop, 2004: 286). In such a way, conclusions were made about the connectivity between the prices of oranges and efficient railways, finding out the amount of damage it would do if those railways were bombarded at night. OSINT in WWII also introduced transparency of sources to intelligence with its practice of writing a list of used sources. Those lists of sources made it possible for the end-users to examine that same information further and possibly make their own judgments (Glassman and Kang, 2012: 675).

### 3.2. OSINT in the Cold War

In the Cold War, the CIA has bought, on average, one thousand books annually and translated them from foreign languages, thus enabling the creation of knowledge about the Soviet Union (Croom, 1969). The CIA has, in its beginnings (1948), made a library filled with all sources. The library contained classified documents and other secrets but was mostly made of books and publicly available articles. Most books were on political systems, economy, science, and technology, or other general academic work (CIA, 2015). The usage of publicly available information was just at its rise after the war, while at the end of the Cold War, it became the

main source of information about the Soviets. There are estimates that OSINT contained 20% of intelligence after the war, the rest going on satellite imagery and electronic reconnaissance. Those numbers have by the years completely turned around to make 80% of intelligence on Soviets (Best and Cumming, 2008: 78; Lowenthal, 2009: 121). Information on the Soviet entry into Budapest in 1957 was mainly gathered by listening to the radio, as it would seem that: there always comes a time when bits of public information destroy everything built by hardly obtained secret information (Mercado, 2004: 47). The value of OSINT could most clearly be shown in the fact that at the end of the Cold War, western intelligence officers watched the unpredicted fall of the Berlin wall on their tv screens (Mercado, 2004: 3). Similar methods were used in proxy wars, like in Vietnam, where it was essential to listen to their news broadcasts and radio, even just for obtaining the opposition's propaganda (Mercado, 2004: 2). The USA also gathered much information about the intentions of Cuba through public channels, mostly over television. Other information was collected over Cuban diplomats, officials, and diplomatic forums while analyzing Cuba's interference with the USA's radio broadcasts showed Cuban technological capabilities (Beebe and Pherson, 2011: 43). On the other hand, that same public information gathering through radio and television always brought danger regarding its reliability. Regardless, OSINT has proven its relative worth even when it comes to gathering information on closed societies.

In a now declassified CIA document, Herman Croom in 1969 wrote a paper on open-source information in which he demonstrated its importance. He takes an example of nuclear programs, which can by no means stay internationally invisible. Preparations for such a program take at least five years and 100 million dollars. That information can be gathered by monitoring economic data, proving OSINTs value. Apart from that, Croom wrote that even when being flooded by fake stories from official foreign media, the opposing side's real technological advance can be seen from scientific academic papers (Croom, 1969). Many CIA officers were embarrassed to present to Congress that they mostly deal with public information. They assumed that the legislator might oppose the idea of intelligence officers reading newspapers, while in reality, OSINT often bears solutions to many different questions (Lathrop, 2004: 288). Accordingly, the existence of a possible foreign secret research facility can be brought to light by noticing the sudden disappearance of published works of particular foreign scientists. The non-existence of their new research in scientific journals may point precisely to that (Lathrop, 2004: 289). There is also an open-source HUMINT method. An informational talk can be conducted with a specific researcher to find out details about the

development of science in the field of his work. In the talk, the researcher must not know the real purpose of the conversation, while similar information can be gathered by reading the researcher's works (Lowenthal, 2009: 121). Some consider such methods more open-sourced than they are classical espionage.

By keeping the sources of the intelligence product transparent, the knowledge stays dynamic and open for further examination. Such openness enables the easier building of concurrent conclusions. The knowledge stays horizontally available, as well, compared to the state where knowledge is reserved for the chosen few. The Open-source movement has introduced such a perception of the value of open sources. The movement arose from a loose organization of internet hackers that believed in the value of leaving their written codes open, accessible to other users. Such open codes made it easier for technical knowledge to transfer to others, making problem-solving more efficient (Glassman and Kang, 2012). Their idea coincides with the fact that the World Wide Web was initially created to connect scientists and academics, while open sources can be seen as an extension of that will to share knowledge. From the movement's perspective, OSINT is used to encourage and enable innovations that are not determined by preceding inventions. It is an idea of altering old inventions to create something entirely new (Stalder and Hirsh, 2002). That movement substantially influenced modern OSINT and found its hidden usage for many problems. One such problem is the aforementioned reliability of the information, and the possible solution is leaving the sources open for further examination. By doing so, it also becomes easy to upgrade knowledge, create new solutions, or view the problem from another angle. That is not possible with the knowledge that is restricted and of limited accessibility. With it, an idea has evolved that rejects the premise of having a status of an expert only by being a part of a certain organization. It was depicted by qualifications that would presumably come with the lab coat itself and not the reality. Such openness enables the cooperation of everyone on all levels, bringing richer insights. The same idea can be translated into good governance that is expected from the modern democratic authorities.

To some, Open-source intelligence may still seem contradictory since intelligence is widely perceived as an opposition to anything open. That is, of course, a problem of the historical role of intelligence agencies and considerable use of covert operations by both sides in the Cold War. This perception can be clearly portrayed by a quote of the CIA's director of public affairs in which he said that the role he bears is „The world's ultimate oxymoron" (Lathrop, 2004: 281). By saying so, he shows his belief that intelligence services should not

be exposed to the public. Thus, the dilemma of value between OSINT and other covertly obtained intelligence stems from secret services' clandestine and covert history.

### 3.3. The shift in requirements and intelligence culture

The Internet has transformed many things, along with intelligence that had to follow up these changes. In the past few decades in the USA, there has been a reevaluation of the value of OSINT as it was formerly regarded as second-class information (Best and Cumming, 2008: 76). The change in attitude and the sudden need for innovation could be connected to their will to understand jihadists. The usage of OSINT increased as jihadists were using the Internet as a platform for recruiting and creating their own OSINT from the Internet. One senior intelligence officer said that the Internet is becoming a new America's battlefield (Best and Cumming, 2008: 76), and intelligence had to adapt. Mostly all intelligence officers could agree that there is value to Open-source intelligence; therefore, OSINT was never disregarded as a whole. Famous intelligence figure Sherman Kent said that 80% of all intelligence in peacetime could be gathered by open sources (Best and Cumming, 2008: 78). Allen Dulles used the same numbers in 1947 in a speech to the Senate Committee on Armed Services (Gibson, 2014: 9). So the main debate is not about the value of Open-source intelligence, but rather about its value compared to classical covert means of gathering information. At the end of the day, covert means of gathering are considered the core of intelligence work, by which the intelligence is mostly known for. Former Defense Intelligence Agency director said that 90% of information is gathered from open sources, so the „real hero is Sherlock Holmes, not James Bond“ (Best and Cumming, 2008: 78). The changes that have taken place after the Cold war certainly attributed to OSINT usage. In the Cold war, open sources were sometimes as hard to get as secrets, while one intelligence officer even said that it took 14 days to get the newspapers from the Caribbean and Latin America (Bean, 2011: 25). Since then, much has changed, along with the understanding that many of the new intelligence workforces will come outside the intelligence community. That new workforce will be more connected to the new technological advances, especially with techniques of exploiting the Internet (Bean, 2011: 6). Still, most of the disputes over the value of OSINT come from cultural barriers. It is often portrayed that OSINT and covert intelligence are competing rather than being complementary. Also, there is a considerable faulty belief that OSINT is always internet-based, while in fact, OSINT is also based on photographs, books, public speeches, and other (Gibson, 2014: 11).

Through the Cold War, intelligence services were characterized by gathering expensive information through satellites, covert operations, and infiltrated agents. When the change took place, in the form of openness of information, intelligence services weren't really reconsidering their established means of gathering. Certainly, the closed culture of intelligence services also added to secrecy and the will to focus only on secrets. It can also be seen from their relentlessness to share information on their budget, operations, effectiveness, and so on. They are still the only ones that have exclusive rights to covertly obtain information for the sake of the state's well-being. However, when it comes to open sources, they might be losing their primacy. The increasing number of private organizations used for outsourcing OSINT may be the proof of the reluctance to adapt. Privatization of intelligence led to state agencies having competition for the first time (Denécé, 2014: 36). However, they are not only competing, as they cooperate extensively, as well. Numbers show that vividly, as 70% of the U.S. intelligence budget in 2010 was allocated to private contractors (Denécé, 2014: 36). Nevertheless, it is generally expected for intelligence agencies to follow up with the technology.

In an open-source world, it is hard to neglect the importance of easily available useful information instead of searching only for secrets. Nevertheless, a belief can still be felt that the more classified information is, the more value it bears to intelligence (Burke, 2007: 2). With the classification of information comes the personal power over knowledge, while a former director of the NSA labeled it as „stovepipe mentality“ (Burke, 2007: 2). That kind of mentality retains knowledge from moving horizontally, while the direction of its sharing is always from the top on a vertical axis. The open-source movement believed in the necessity of exactly the opposite mentality, trying to interconnect people and information on a horizontal line. This kind of approach proved to have a better effect than holding a stance of informational superiority, which focuses on stopping the flow of information (Burke, 2007).

If we were to examine the reevaluation of the concept of security in the last thirty years, postmodernism would easily come to mind. Postmodernism is a broad social process that is mostly known by its relativity. In postmodernism, the one and only truth is no longer sought, while any established boundaries become fluid. Regarding methodology, all of the conventions are being questioned, as well (Barić, 2014: 1365). When it comes to intelligence, this could lead to reexamining of using open sources since focusing on secrets is an established convention of intelligence. Though that may be possible, facts show differently, especially when in 2005 a Director of Central Intelligence said „I only have money to pay for

secrets!“ (Best and Cumming, 2008: 77). The information revolution and the end of the Cold War changed the reality of security. The change has manifested in shifting focus to the new threats that are often less visible and less clear. With it also came new objects of reference that need to be secured. When it comes to intelligence objectives, it can be considered that intelligence is no longer needed to solve puzzles; rather, it is needed to solve mysteries (Nye according to Barić, 2014: 1365). The real problem ceases to be finding the missing piece and figuring out where to put it since mysteries are often unsolvable even by using scientific methods. Thus, the intelligence community can no longer stick to the same methods if the objectives have changed. Solving mysteries is much different from finding secrets because a mystery's solution isn't hidden somewhere to be found. Not all security problems can be posed as mysteries, but for those that can, classical espionage is not enough (Russell, 2007: 8). Mysteries are often formed as questions on possible outcomes or „what if“ situations that need to be addressed more creatively. The human factor brings this creativity in the analysis, so the role of analysts becomes more important in the intelligence-making process. There are three main intelligence analysis requirements are: descriptive, explanatory, and anticipatory (McGlynn and Garner, 2019: 4). Only the first requirement is to be done with facts that can be gathered. For the other two, especially anticipation, pure facts are not enough. It is so because a higher level of cognitive involvement is needed for understanding or speculating future trends (McGlynn and Garner, 2019: 6).

After the fall of the Soviet Union, the number of open societies and unrestricted areas grew. Most of the former Warsaw Pact countries entered NATO (Lowenthal, 2009: 123), which meant that much information on their political systems, defense, and intelligence had to be „screened“ for their integration. Regarding political elites, they also expressed serious will to cooperate on many different levels. That, for example, takes away some level of the necessity of gathering secret information. In addition, Today's most prominent threats to global security seem to correlate with OSINT as the means of gathering information on them. Intelligence on economic and social threats (95%), inner state conflict (75%), nuclear weapons (75%), and terrorism (80%) can mostly be acquired by OSINT (Steele, 2007: 134). OSINT can, therefore, be connected to the democratization of the world after the 90s. As Steele has poetically written: „OSINT is democracy. OSINT is moral capitalism. OSINT will make our lives better and offer hope for future generations.“ (Steele, 2007: 144). It is a rather romantic view of OSINT, but it does bring an interesting idea of the role of OSINT in

intelligence responsibility. Every so often, that topic becomes popular to the news agencies, especially combined with the problem of politicization of intelligence.

Connected to these changes, OSINT brings citizens closer to national security as they become rather important figures of its realization. Academics, actors from non-profit organizations, or laymen, become viable sources of intelligence. In an ever-so-open world, many organizations share their insights and analyses openly. For example, World Economic Forum creates Global Risks Reports containing analyses on future trends and possible new paradigms (WEF, 2021). Those yearly reports also contain expert's perceptions of long-term and short-term global risks, which can be seen as ranked global security issues. For an illustration, some of the top-ranked risks are informational technology infrastructure breakdown, natural resources crisis, and weapons of mass destruction. From the list of risks ranked by impact, it can be seen that only one risk is geopolitical (the aforementioned weapons of mass destruction), while most of the others are of environmental nature. From that, it could be assumed that classical threats are replaced by the modern way of living itself. In addition, from the top ten risks by likelihood, only two are actively dealt with by intelligence agencies: interstate relations fracture and Cybersecurity failure (WEF, 2021: 12).

Aside from the new security threats, OSINT can still be used for the classical threats. In an article on military usage of OSINT, Steele wrote how OSINT is usually utilized on every level of action. On a strategic level, OSINT is mostly used for warnings of hostile intents, cultural, and geographic intelligence. On an operational level, OSINT provides generalized information on air, ground, and sea for force employment. Finally, on a tactical level, it provides detailed maps (Steele, 1995: 460). OSINT can thus contribute to Strategic intelligence (STRATINT)[4]. It has been shown that the end of the Cold War did not end the need for STRATING. In 2013 White House advisors warned Obama that the U.S. intelligence community is paying too little attention to China and the Middle East because of its immense focus on Al-Qaeda (Denécé, 2014: 38). One part of STRATINT requirements is also foresight, as an ability to spot trends (Ardelean, 2015: 231). In one example of foresight, a Romanian researcher analyzed Russia's aggressive military operations in Ukraine. He pointed out Russia's possible interest regarding Romanian territory, which is the mouth of the Danube

4 STRATINT is intelligence necessary for creating national and international policies and military plans (DOD, 2021: 203)

river. Since the Black Sea became Russia's "lake", controlling the Danube river would imply diversifying its commerce towards Europe. OSINT is also useful for monitoring foreign crises' outbursts while providing commanders and policymakers a good start for making further plans. It is done by examining foreign media, experts, satellite imagery, etc. (Minas, 2010: 25). This kind of information also proves valuable in ongoing operations, as they often give real-time broadcasts of what is happening on the opposition side. This real-time element is especially important for military intelligence to be successful, thus being a great opportunity for OSINT usage (Thespectrum.tech, 2021). Social media can also be monitored to analyze the sentiment or intents of the local people (more on social media intelligence in chapter four). Open-source tools can bring the time of the post, location, tone of the post, topic, and else (Penninger, 2019). The proof of its utility may explain why the Russian Federation's armed forces prohibited its personnel from using social media (Kasapoglu, 2021). One more good example would be OSINT analysis of Balakot airstrikes. In it, in 2019 a commercial software "flightradar24" was used to prove that Indian Air Forces conducted bombings on Balakot city in Pakistan (Panag, 2018). UN and NATO also extensively use OSINT for peacekeeping missions to bypass information from members of the conflict, which are often conflicting (Hassan and Hijazi, 2018: 11). All of which proves its relative utility as a part of military intelligence.

To completely utilize these open-sources, the research needs to be done in many languages. When it comes to English, at least 16.5% of the world's population do use it as their first or second language. However, the most spoken first language is Mandarin Chinese (12.3%). Then comes Spanish (6%), English (5.1%), Arabic (5.1%), and Hindu (3.5%) (CIA, 2020). If French and Russian were to be added, then still 55% of the world's population would not understand any of them (CIA, 2020). Having that in mind, the scope of the available information becomes far wider when foreign-language information is included. Furthermore, when it comes to STRATINT, foreign languages are a must. On the Internet, it would mean using software that can translate searched terms. One such software is Searchbox, which was overviewed by a military institute in Italy (Baldini et al, 2007). Searchbox has a clever way of classifying information on the Internet by the given keywords. It also creates transcripts of videos so that they can be searched as well. It then performs an analysis on morphological, syntactic, functional, and statistical criteria. In such a way, the program analyses the meaning of searched words according to their context, giving more quality results. Chinese is said to soon surpass English as the most popular language on the Internet. Also, more and more

internet domains are written in Arabic, Chinese, or Korean (Mercado, 2004: 7). Some state that there is still some negligence towards using foreign languages for intelligence. Mercado stated an example of a book made by a filmmaker that worked for Kim Jong-Il for years. The filmmaker documented the life of the North Korean Supreme Leader, including pictures and other details. The book was published in Seoul and Tokyo in 1988 when he escaped North Korea but was never translated to English (Mercado, 2004: 7).

## 4. Utility of Web intelligence (WEBINT)

While OSINT is not only internet-based, internet sources do make the largest portion of today's OSINT. It is so because more and more of the offline sources, like books, articles, or documents, are uploaded on the Internet (Chauhan and Panda, 2015: 16). WEBINT or Web intelligence is the name for such OSINT that is comprised only of internet sources. There is, however, another more narrow definition of WEBINT. In it, WEBINT is different from OSINT because it uses only internet data (OSD) and not information on the Internet (OSINF) (Recordedfuture.com, 2014). In this paper, WEBINT will be used as a broader definition including all internet sources.

In a paper published by RAND corporation (Williams and Blum, 2018: 2), a distinction of OSINT was made between the first and the second generation of OSINT. In it, the first-generation OSINT was the physical one, while the second generation is, in fact, WEBINT. This new generation started somewhere at the end of the 90s, but RAND purposely points at the year 2005 as the real turning point for OSINT. That was the year when most Internet social networks appeared (Facebook, Youtube, and Twitter in 2006). This process aligns with the development of the Internet into version 2.0. That new Internet has brought interaction onto web pages which were all previously static regarding their content. From then on, it became possible for users to generate their own content in the form of writing comments or sharing thoughts and videos. In that way, individuals could easily express themselves, while groups of similar-minded people could be brought together (Chauhan and Panda, 2015: 19-20). At that point, SOCMINT or Social media intelligence emerged as a subcategory of WEBINT. SOCMINT, consequently, focuses on internet social networks for extracting data and information about a wide range of phenomena. This intelligence is still evolving, but it is slowly becoming a more important part of the overall concept of OSINT.

The modern way of living brought most of its elements into the digital realm. WEBINT, thus, tries to exploit these ever-expanding pools of resources. One of the main tools of WEBINT are internet search engines (Norton, 2011: 66), the most popular being Google and Yahoo. Though they are popular and easy to use, special skills are needed for a thorough web search. In addition, they are not enough for searching the Deep Web since they do not show (index) web pages from that part of the Internet. For either purpose, the lack of information on the Internet is not a problem; the problem is rather the opposite of it. Thus, filtering the content may be the biggest task of an OSINT researcher (Chauhan and Panda, 2015: 16).

Judging by the growing presence of internet sources in OSINT, this chapter is focused solely on WEBINT. The first subchapter will show the general role of social networks in WEBINT. The second subchapter will demonstrate how analysis of web sources can be used against terrorist and criminal organizations, while the third subchapter will cover some other uses for WEBINT.

### 4.1. Social networks

The great value of social media intelligence comes from the fact that its information is mostly original and is, in essence, a primary source of information (Williams and Blum, 2018: 18). However, it is to be noted that information put on social media does not always have to be truthful. Many people are prone to tweaking information they share to fit their created picture of themselves (Lapid, 2016: 39). However, these internet social networks have created an interconnected world in which the economy and social capital can grow. More importantly, for intelligence, they have created the afore-mentioned pools of sources that can shed light on threats to society (Omand et al, 2012: 9). A big part of conducting SOCMINT means dealing with big data amounts. Such data are characterized by large quantities of different varieties of sources. For example, tweets on Twitter are those kinds of data if we consider that there are 200 million new ones every day. The value of big data can be seen from the fact that some even consider it to be an economic asset, like a currency (Omand et al, 2012: 15). SOCMINT has turned out to be very useful at identifying certain criminal activity, forecasting violent riots, sexual abuse, and other public security problems. This virtual reality has created information closest to the source, but it also means that sensitivity is even more present. The problem of privacy will be addressed later in the chapter on the negative aspects of OSINT. For now, it is important to note that not all information on the Internet is intentionally shared information. Some of it can be chunks of unintentional data, like the clues that users leave behind after their participation on the Internet.

Much research on the topic of social media points out the new way of communicating that has developed on them. It was shown that anonymity might be the biggest cause for it, making users more direct, honest, and often more aggressive (Omand et al, 2012: 56). If such information were to be analyzed without contextual knowledge, the intelligence would probably be invalid. Another similar problem comes with the fact that radical thoughts do not always have to be connected to radical acts. So, the specific culture and norms of a certain network have to be considered for information to have validity (Omand et al, 2012: 10).

To solve these contextual and cultural problems, intelligence studies tend to be interdisciplinary. It reflects in the fact that its methodological perspectives come from history, political science, psychology, sociology, etc. When it comes to sociology, Social Network Analysis (SNA) may be the most well-known analysis from that field of study. SNA has emerged in the 90s[5] (Walsh, 2011: 243), but its utility has become more apparent as social media usage began to grow. SNA as a method can vary to have a more descriptive or more predictive value. The main idea of SNA is to map out existing individuals in a network, their relations, and the strength of those relations. That is done by drawing connections between individuals and assigning values to those relations. For example, their relations can be interpreted as the number of times two individuals spoke in a certain range of time or the matter they spoke of (Burcher, 2020: 13). By using computers and mathematical concepts, such analysis can shed light on the most important or weakest links in a network. It is done by calculating the degree of centrality (indicating essential individuals) or betweenness centrality (indicating important information brokers) (Burcher, 2020: 36-37). Furthermore, SNA can detect all sorts of other roles in a network. One important role is an equivalent role, which can point to the leader's possible successor (Burcher, 2020: 14). Thus, using mathematics and statistics makes it possible to predict the future dynamic of networks (Walsh, 2011: 244). For that reason, SNA is frequently used for analyzing criminal and terrorist networks.

### 4.2. The utility of WEBINT in cases of terrorism and organized crime

Penetrating terrorist organizations has been proven immensely difficult since they are mostly closed societies, often people that have known each other for a long time (Denécé, 2014: 31). Thus, performing only HUMINT can be challenging and unsuccessful too. Terrorism can be generally considered a wicked problem, like other problems that seem unsolvable. For those problems to be solved, effective leadership is needed, along with a multidisciplinary approach with multiple types of sources (Ashwell, 2017: 22). In this need of an all-source solution, Social network analysis has especially shown its utility. SNA is often created out of all

5 Network analysis dates back to the 1930s with the idea that the world is „shrinking" due to globalism. The analysis was popularized with research like the one on six degrees of separation. The research claimed that it is possible to get in touch with anyone on the planet by only having five people as brokers of information (Burcher, 2020: 31). Network analysis can be simple with descriptive purpose, which was characteristic for the first generation, while the second generation tried to automate the process by using computers. The third generation, called Social network analysis, is different by having mathematical outputs and the possibility of statistical analysis (Burcher, 2020: 13).

sources, but even only open sources have shown useful insights on terrorist organizations. It is so because terrorists are more and more using the Internet for recruitment, political messages, and other sharing of information (Akhgar, 2017: 4). The Internet has become the main source of radicalization because it provides anonymity with a wide range of possibilities (Staniforth, 2017: 14). Counterterrorism strategy is usually divided into four parts: prevention, pursuing, protection, and preparation. WEBINT can have its role in all of the steps. In prevention, WEBINT provides valuable information on terrorist narratives that can then be counteracted by creating counter-extremist narratives (Akhgar, 2017: 6). Pursuing can be done by tracking terrorist activity on the Deep Web (see below). Protection can be done by assessing one's own vulnerabilities. Finally, preparation is done by early warnings based on WEBINT (also below). SNA of 9/11 and the Bali and Madrid bombings (2002 and 2004) clarified the structure of modern terrorist networks, which has changed our perception of them. Those analyses showed that modern terrorist organizations are not based on rigid hierarchical structures but rather on weak connections (Burcher, 2020: 39). Having such a structure makes them harder to detect while making the mode of decapitation (removing the leader) futile. Thus, the already mentioned centrality measures made it possible to figure out the network's hierarchy (Berzinji, 2011: 5). In SNA, central actors of a network are called hubs because of their connectivity with most other actors. Elimination of hubs often causes a network to separate into many small groups that cease to be functional (Berzinji, 2011: 15). However, today terrorist organizations are mostly decentralized, making them more sustainable if an attack on the network occurs. In addition, SNA has also shed light on the role of financial managers in terrorist organizations. Such managers are becoming the most important actors in their network since they can distribute resources. Except for that, analyses showed that they are connected to most of the other actors. Also, it was shown that the financial manager is the only person directly connected to the organization's leader (Berzinji, 2011: 21). All of those insights bring actionable knowledge of terrorist organizations.

Furthermore, SNA can be enriched by making a simulation of a specific network. It is a method that takes a lot of data, but in return, gives a possibility to simulate an experiment. Simulations with different parameters and assumptions can be run, leading to insights on possible future actions. By simulated micro-level agent interactions, the macro-level picture is created (Knoke, 2015: 6). Thus, a researcher could experiment by removing certain actors to observe how the network would react. In one such example, a simulation of Al-Qaeda's network was created based on its activities in Iraq. The simulation, supported by big data,

showed that Al-Qaeda had a cellular structure (Knoke, 2015: 7). Another similar analysis was done on Jemaah Islamiyah, which conducted series of bombings in Bali in 2002. The analysis showed its high-density network, meaning that law enforcers could easily penetrate it if one of the members was caught and interrogated. Further analysis also located the leader without whom the operation could not have carried out (Koschade, 2006: 571). SNA, as well, proved useful when analyzing lone-wolf terrorists. One such WEBINT based analysis brought insights into the socialization of lone wolves. The analysis showed that they do, in fact, have a network but a loose one. Inside that network, they communicate with similar-minded people or get information from them. All of that points to the fact that their radicalization does not take place in an impenetrable bubble (Hofmann, 2018). At least a third of the lone wolf's network that carried out the Oklahoma bombing in 1995 had some knowledge of what was going to happen (Hofmann, 2018). Such SNA can, thus, improve counterterrorism activity.

WEBINT that is done on criminal or terrorist organizations often contains sources from the so-called Deep Web. Common internet search engines show only about three to five percent of all information on the Internet, while the rest is on Deep Web (Lowenthal, 2009: 122). The main technical difference is that common browsers show hyperlinks, which are structured, while the unstructured links need to be specifically inserted (Hassan and Hijazi, 2018: 97). Thus, Deep Web is still reachable by standard search engines, but only with specific knowledge of its internet address. On the other hand, Darknet (Dark web), as the dark part of Deep Web, is not reachable by the common search engines. It is so because it is purposely made to be secret and anonymous (Hassan and Hijazi, 2018: 101). As might be expected, Darknet is most often used for illicit purposes. Thus, the surface web is used for psychological and emotional tactics, while the other is more operational, like explosive making (Akhgar, 2017: 5). On Darknet, there are approximately 100 thousand web pages with extremist or terrorist content (Chen, 2011: 327). Apart from SNA, other analyses can be very useful on such web pages. Some of them are content analysis (detects important phrases), web metric analysis (tests the authors' web capabilities), or sentiment analysis (measures radicalization) (Chen, 2011: 330). One researcher combined all of those analyses in a program that creates extensive intelligence visualizations. The program can search a term on Darknet forums and create a network of people who used that term in their comments (Chen, 2011: 340). It is very specific by its nature while also updated with just one click. There are also other good examples of using WEBINT on common social media. One such analysis has dealt with Al-Shabaab's internet involvement. Al-Shabaab is an Islamic terrorist organization

operating in East Africa, but it is mainly known for using Twitter, Youtube, and other social media to contact the public. An analysis of their content made clear that they are trying to recruit Somali diaspora while at the same time trying to secure funds (Menkhaus, 2013: 313). These kinds of instances also made clear that terrorist organizations are more and more focused on the power of their narrative, not just the plain hard power (Menkhaus, 2013: 309-310). It is clear how WEBINT plays a big part in analyzing terrorist narratives that are ever more often shared on the most common internet media.

When it comes to criminal networks, charting out inner connections is almost as old as crime analysis itself. Today, many analysts still do it manually for the sake of their own thought processes (Burcher, 2020: 66). Like with terrorist organizations, SNA makes it possible to understand influences inside a group and pinpoint where law enforcers could get further information. Such SNA is often done on all sources, while WEBINT is used for the broader picture of the analyzed network. In such a way, the network is analyzed both from the inside and outside, making it more probable for an unexpected link to come up (Burcher, 2020: 76). Rhodes, in his article, showed how an SNA can be made on criminal organizations, only using public information, like testimonies and news articles (Rhodes, 2011). For example, he analyzed Revolutionary Organization November 17, a Greek terrorist organization, but one with at least 11 conducted bank robberies. The public information identified perpetrators, their crimes, their connection to the others, while the author assigned them a role from this information. Alongside SNA, the author performed his own method of detecting actors that aren't shown in the network because of a lack of information. Its analysis showed which actors are probably in the network but invisible to the data. Such an analysis is complex, timely, and can only be done on a smaller amount of nodes, but it shows promising results of WEBINT's utility.

When analyzing terrorist or criminal networks, there is always a certain level of uncertainty. That uncertainty is a constant variable when dealing with dark networks. Actors of such networks always try to mask their affairs, which on the Internet is often done by different aliases and encryptions. Other problems, such as the dynamics of all real networks that are always fluid, can make the analysis quickly outdated. The boundaries of a network are also always unclear, with the question of who is and who is not to be included in the analysis. SNA, as well, has a problem of the need for skilled analysts. Such analyses tend to be counterintuitive, while their data entry is rather time-consuming (Kriegler, 2014: 3). Aside from the time, a lot of data is needed to make any useful results.

There are many software that monitor social media, while content analysis ones are the most popular for intelligence and law enforcement agencies. One such program is OsintLab that can globally search social media by given textual inputs (Delavallade et al, 2017: 174). Its main characteristic is its possibility to visualize the analyzed data so that clear clusters of information form. The program does all of the collecting, processing, and analyzing as well. Its results bring deep situational awareness of the researched term, which can also mean uncovering unknown threats (Delavallade et al, 2017: 184). As with terrorism, Darknet is also a rich source of information on criminal organizations. It is so because it is essentially a platform of illegal services and products where stolen credit cards, crowdsourced assassins, drugs, and many more can be bought and served. That layer of the Internet is also famous for services that cannot be found anywhere else, like custom-made malware that can exploit mostly anyone's information. For intelligence agencies, arms dealers, terrorists, and cybercriminals are of most interest. For three years until 2017, a platform called Alphabay existed on Darknet. It was a market platform for illegal services and goods but also a forum for criminals. A network of 190 thousand people used Alphabay, while it was perfect for finding out information about criminal interests, thoughts, intentions, and the overall functioning of criminal organizations (Quinn, 2018). Of course, that information was not always specific about what organization, when, and towards whom they will act. However, the other contextual information that was gathered could have earlier only been available by physical infiltration. Thus, WEBINT can enrich underground intelligence as a technique of gathering information about criminal organizations from directly connected sources.

### 4.3. Other WEBINT usage

The Internet has become one of many battlefields of political warfare where each opposing side tries to realize their interests. The Internet has thus, become a tool of Information warfare. By definition, Information warfare is the employment of information to influence, disrupt, corrupt, or usurp adversaries (Brunetti-Lihach, 2018). It used to be that informational operations were a part of armed conflicts, but today it has transferred onto any kind of conflict or actors, including private actors (Tekir, 2012: 4). A win in such an informational battle would mean the realization of the famous Sun Tzu's argument that the real victory is won without fighting (Tekir, 2012: 6). Disinformation, as a phenomenon, is not new, but the Internet brings a new dimension to it. It is often that disinformation, hidden in the form of news, is shared across many news agencies, therefore seeming reliable. It is done by automated bots that extensively comment on specific news articles, making them seem more

authentic. Another version of it uses „trolls", which are people that are paid to do the same, only manually (Walker, 2015). These sorts of „fake news" are hard to detect, but hints point to WEBINT for a solution. Bellingcat, a private company of OSINT activists, often solves global disinformation attempts. In one such example, they investigated the crash of the MH-17 commercial flight that was shot down over Ukraine. The disinformation campaign was done by the Russian side, as the Russian Ministry of Defence publicly shared fabricated satellite imagery that pointed towards the Ukrainian military. Bellingcat analyzed information gathered by social media, geolocation software, and the local people. As a result, they have proved the falsehood of the image while also discovering the real perpetrators, the Russian military (Higgins, 2016). It is important to note that such a result came out of the all-source analysis. Bellingcat constantly compares its open-source finding with covertly gathered information from their partners (probably state agencies).

However, fake news are often very successful. It is because they contain so-called white lies. Those are information of which one part of them is true, while the other is false. This mixing makes people more susceptible to accept disinformation. To solve this problem of reliability, some researchers are trying to find conflicts of information in the news by mapping out used phrase words and calculating their difference (Levchuk and Shabarekh, 2017: 2). Another similar solution is to go back to the basics of critical thinking, but this is impossible when dealing with huge amounts of data. Artificial intelligence seems to be the solution to that. Spam filters can be made that categorize information according to what has been given before. By „feeding" the program with many instances of fake news, the spam filter can easily categorize anything that is being tested. All that brings us to the point that OSINT should be combined with advanced technological solutions, as it could bring added value and reliability.

WEBINT has also proven its worth as threat intelligence. This sort of intelligence is knowledge that helps prevent or mitigate cyberattacks (Recordedfuture.com, 2021). This term is familiar to larger private companies, as they try to incorporate it in their Business intelligence. However, it is often costly and complex, even for state intelligence agencies. Luckily, a few studies have shown how WEBINT could be used as threat intelligence (Nair and Puri, 2015). Two researchers have managed to make an easy and inexpensive solution to threat intelligence in the form of open-source software. The program they've made used internal data of the company and free databases on the Internet that contain lists of already observed cyber threats. This system was tested by monitoring the company's computer

activity during weekends when the company is closed. They eventually found out that two software were constantly running and transferring some data over the Internet. Though they might not be malware, if they were, they could be easily dealt with (Nair and Puri, 2015: 362). This type of system is called an Intrusion Detection System (IDS). Such systems are behavior-based, meaning that they alarm the system when something out of the ordinary is happening inside the network. There is also another system that is signature-based. That type of system detects malware by the pattern of the attack, which is formerly given to the program as a sample. In that way, WEBINT can be made out of databases that contain phishing links (frauds in which sensitive data is being stolen), malware domains, and such. That kind of WEBINT, as an aggregation of all of those data, would then be placed as a base for IDS software to make its analysis (Vacas et al, 2018: 130). All of this can be used to secure critical infrastructure and other systems that the state is responsible for securing, while it does not require any extra expenses.

Technological advances always seem to add potential value to OSINT. Another example of using AI for national security is WEBINT based program for early warnings. Such warnings are one of the main objectives of intelligence agencies. They are usually made by gathering a lot of information, categorizing it, and finding patterns that would indicate certain actions in the future. Indicators are made of many variables that need to have certain values for an indicator to be positive. One researcher (Best, 2011) showed how the methodology African Union (AU) uses for early warnings of conflicts coincides with information that WEBINT can gather. Their indicators contain information about a foreign country's profile, structural indicators, information about terrorist groups, a list of leaders, and other important personas. Alongside those, dynamic indicators are also created which monitor news articles and categorize their content. All of those values are publicly available. Most of them are found inside databases and indexes made by NGO's or other information from governmental agencies, like the CIA's world data. A similar approach is done by another researcher (Carroll, 2005) using an algorithm for clustering objects that would indicate their magnitude. Thus, AI can be seen as a solution to a big part of internet analyses, but its full potential is still to be capitalized on.

## 5. ANALYSIS OF FIVE MODERN DIMENSIONS OF OSINT

**Table 1: Five modern dimensions of OSINT**

| | Positive | Negative |
|---|---|---|
| Internet as a source | - Low cost (money, time, productivity)<br>- Brings closer far-away problems<br>- Exploratory value<br>- Combined with foreign languages brings to lesser-known information | - Dis/misinformation<br>- Dark, smart, and powerful actors are off the grid<br>- Large amount of information (often creating noise) |
| Privatization of intelligence | - Expertise without investment<br>- Insights from OSINT activists | - Not classifying sensitive information found overtly<br>- Availability of OSINT techniques to the enemy |
| Forecasting | - Encourages creativity<br>- Provides context | - Problem with reliability<br>- Dark side often hidden |
| High-tech solutions | - Low cost (money, time, productivity)<br>- Handles big volumes<br>- Insights that are hardly possible by humans<br>- Possibility of forecasting | - Special education<br>- Human factor always necessary |

| | | |
|---|---|---|
| Responsibility | - Less intrusive than other techniques<br>- Less of a risk for gatherers<br>- Classification not necessary (ability to share with others) | - Reliability of the sources |

*Source: author*

### 5.1. The Internet as a source

By using the sources on the Internet for creating intelligence, there are many logical advantages over other sources. The first one would be the cost over the benefits of such information. One of the highly considered positive aspects of OSINT is its ability to produce many insights in a fast manner and on a lower budget. Apart from the cost and efficiency, the explorative value of OSINT is significantly present in the use of the Internet. The starting point of intelligence gathering is usually the Internet, may that be for researching ordinary or extraordinary phenomena. However, for OSINT to have a higher value, it has to be gathered using many foreign languages. With the lack of usage of other languages, a language bubble creates which consequently causes biased information. Not considering everything can be seriously deadly, especially when operating in a foreign country. Foreign languages also help find lesser-known information on the Internet, so the horizons of knowledge become wider. Thus, it brings foreign information closer while making it possible to analyze far away states where HUMINT would be somewhat unfavorable. It is important to note that the modern way of living is more online than offline, while trends show that it will be more true in the future. The COVID-19 pandemic also indicates the necessity for citizens to adapt to the online future. Whether such a life will have a good impact on humans or not, OSINT will certainly have its utility in such conditions.

A good example of utilizing internet sources for investigations is the afore-mentioned Bellingcat's investigation on the shot-down civilian airplane over Ukraine (see the end of the chapter „The shift in requirements and intelligence culture"). For intelligence, Bellingcat has used the local people, news articles, metadata from photographs, information from Facebook accounts, etc. By so, they have managed to identify Russian military personnel that shot the plane down. Similar has happened with Bellingcat's investigation of propaganda coming from the Russian Ministry of Defence. The mentioned ministry shared a video on Twitter in which

a USA's military drone is allegedly helping ISIS from the air. An investigation based on open sources showed that the video is fake, being recognized by Internet members as an excerpt from a video game (Higgins, 2017). By doing so, they have shown a good example of how disinformation campaigns can be counteracted, and the truth demystified from the noise.

Another important moment for internet investigation can be found in 2009 during the Green Revolution in Iran. In the revolution, the Iranian public started sharing videos and messages from the protest to encourage others to join them. This advertisement was essential since most of the world's media did not follow up on those events in Iran. Internet activism was primarily present on Twitter, which encouraged other Iranians also to use Twitter to share their own videos, thoughts, and pictures. Eventually, it brought to a rich pool of open-source information that came from primary sources, ready to be processed and analyzed. That crowdsourced information was quicker than news, while its reliability could be seen from the fact that the news agencies published the same information later on (Colquhoun, 2016). Such cases point to OSINT being able to fast-track political and other processes from the ground. Nevertheless, it all came to an end when the Iranian government took control over the Internet and disabled further coordination of the loose movement. Such censorship clearly shows that OSINT made from internet sources can be very productive, but only where there is freedom of speech.

On the other side, the number of information on the Internet has already proven to be a major challenge for OSINT. The sheer volume of data and information makes filtering more important than finding more of it. Also, when the research is done in many different languages, that problem becomes even more significant. Intelligence agencies that have enough servers, physical space, electrical power, cybersecurity measures, and other, are dealing with petabytes[6] of data. In 2013 NSA claimed that the agency covers only 1.6% of the Internet, which would translate into 29 petabytes a day (Jarvis, 2013). Also, NSA's Utah Data Center supposedly has an annual power bill of 40 million dollars (Miller, 2013), which seems to be the price for handling so much data. Facebook, as well, is building a data center with a surface of 274 square kilometers (Miller, 2021), while it will all become a more serious question in the future when the 5G network comes into place.

6 One petabyte is a million gigabytes

Along with that, there are many information hubs with the purpose of overloading the information channels with false information. It takes more and more effort to validate sources and to find out which hubs are reliable. That could be examined in the light of the new battleground called cyberspace, in which the control over information gives more relative power. It can be clearly seen from a concept and the method called reflexive control. The method was used by the Soviets, in which the attacking side conveys tailored information that will make the opponent act in a suboptimal manner (Kowalewski, 2017). Such methods are conducted a lot easier over the Internet, bringing intelligence officers to the need of always staying skeptical. Apart from the large amount of information and disinformation, a lack of information is another possible problem. Major underground actors are always somewhat cautious, while the Internet can only bring informational crumbs on them. For example, OSINT did help with tactical intelligence when catching Bin Laden in Operation Neptune Spear (Cozine, 2013: 86), but it did not help find Osama bin Laden's location. That information was obtained by intercepting calls of his courier. So, OSINT can bring a lot to the all-source intelligence, but it stops giving when actors are cautious and stay off the grid. The dark web may be some kind of a window of opportunity for OSINT to get closer to those actors. On the other hand, that layer of the Internet is certainly filled with awareness of its dangers, making OSINT useful only on more negligent actors.

### 5.2. Privatization of intelligence

Privatization of OSINT and cooperation of its elements with government intelligence can lead to skillful analysts without the general cost of their education (viewed from the government's perspective). The private sector also seems to hold more qualified people as businesses need to operate on principles like effectiveness (producing something, having a real impact) and efficiency (doing more for less). On the other hand, the government's bureaucracy is prone to the employment of those more politically suitable. That not only makes the system more corrupted but also more incompetent. Government agencies are also more inflexible and prone to the status quo rather than changes. Private agencies, though, have to adapt; otherwise, they will cease to exist. There is also an added value to privatization when government intelligence gets help from activists that share the same interest.

A positive aspect of OSINT activism can be seen from the aforementioned Bellingcat and their analyses. From their beginnings in 2014, they have become pioneers of a new form of citizen open-source investigations on major global events (Evans, 2018). Bellingcat's website holds many solved cases containing used methodology that anyone can learn from. One

puzzle that they have solved brought insights on who killed Skripal, the Russian double agent. Firstly, they were able to verify the popular hypothesis that GRU agents killed Skripal. It was done by analyzing the passports of the suspects, finding out their peculiarity. There was an uncommon stamp on Russian on their passports that reads: Do not provide any information. Next to the stamp was a number, whose combination turned out to be one of the telephone numbers of the military headquarters where GRU is allegedly located (Bellingcat.com, 2018a). Afterward, they have found a link between suspects and an expelled Russian military attache in Poland that was accused of espionage. All of them had a similar number pattern in their passports (Bellingcat.com, 2018b). Then, they have clarified the suspect's real identities. It was done by supposing where the suspects could have studied or worked. Eventually, through photos from military schools' websites, they have found the actual name of the first suspect (Bellingcat.com, 2018c). Similar methods were used to identify the second agent. It was also discovered that he is a trained military doctor, which implies that the team's mission was not intelligence gathering. The inclusion of such a person would indicate a different purpose of the mission (assassination by poison) (Bellingcat.com, 2018d). The Russian government denied the suspects' former accusations, while Putin publicly vowed that both of the suspects were uninvolved civilians. Bellingcats research, however, revealed that the first suspect has formerly received the highest state award for his service (Bellingcat.com, 2018c). It is worth noting that Bellingcat also uses insiders to get some information, but it is often used only for verifying the findings. All of this points out the value of cooperation between OSINT activists and intelligence agencies.

On the other hand, sharing OSINT findings with the public has shown to be dangerous in some instances. Private OSINT can assist government agencies, but it needs to be supervised by the state. For example, after the storming of the U.S. Capitol in Washington D.C. in 2021, the city's police department encouraged the public to help with identifying the insurgents. As a part of it, a few private OSINT findings were shared that later turned out to be false. It became a problem when the alleged rioter, falsely identified by the analysis, received death threats and needed police protection of his home (Sherman, 2021). It all happened because of the direct communication with the public, without checking the sources with intelligence agencies. An official investigation showed that the accused individual was actually celebrating his wife's birthday at the time of the storming. Similar OSINT failure can be found in an OSINT investigation of the 2013 Boston Marathon Bombing. The investigation assisted by three thousand people falsely identified the perpetrator, who, in reality, committed a suicide

month before the bombing (Sherman, 2021). This problem goes hand to hand with the problem of leaked sensitive information that is falsely considered public. As seen from the examples, this problem is amplified when false information becomes the new public truth. Private OSINT investigation, thus, becomes a problem when in collision with official intelligence work. By competing and not cooperating, it can make more mess out of an already sensitive situation.

Another critical problem of OSINT in the domain of privatization is the accessibility of open sources to threats of national security. All actors that want to destabilize society, cheat the system, steal or make a profit can use the same techniques to create their own OSINT. All serious terrorist organizations have intelligence staff, technical equipment, and others that can take advantage of open sources just as well as government agencies. The trend of mirroring government agencies ' capabilities will only become more existing. It is so because technologies that were previously exclusive to government intelligence now become widespread and free. Google Earth is one such example, as it gives everyone a free possibility to analyze satellite photos. In contrast, a single satellite image cost 14 thousand dollars in the year 2000 (Doorey, 2007: 5). Therefore, it seems certain that counterintelligence will have to be seriously reassessed in the future, taking OSINT into account.

### 5.3. Forecasting

As the world becomes filled with easily accessible information, creativity becomes somewhat more appreciated than knowledge. Creativity brings the possibility of imagining the unimaginable, which is especially important for national security. It has been shown that expert knowledge does not always give an advantage over future events. It is so because that type of knowledge is often descriptive and founded on history. One of the findings from Philip Tetlock's book on „Expert Political Judgement" shows that experts are not significantly more effective at predicting than non-experts (Tetlock according to Kopal, 2018: 11). That, however, is changed when adding creativity to the process. Analyzing a wide range of different sources may probably be good at awakening creativity. The ability to solve a problem can even be enhanced by using information that isn't connected to the problem. That can be done by analogies or by forcing a connection between the problem and a random idea. By doing so, the brain is forced to think differently. Therefore, it is likely that OSINT to lead to insights by connecting dots that seem counterintuitive (Glassman and Kang, 2012: 676). Asides from creativity, OSINT can be great at forecasts based on data. One such example is forecasting infectious disease spreading. Some private OSINT companies have made software

that monitor keywords on local news sites all over the world. Google is also using OSINT for such forecasts, only doing it by terms that people have searched on Google. That is possible because people with illnesses search words related to the illness (Bernard et al, 2018: 2). Furthermore, OSINT is constantly being valued by its context-giving ability. Individuals, academic researchers, and intelligence officers all look for context in the same way, using open sources. Context is especially important for forecasting, as it deepens the overall understanding of the subject.

Exactly the context was needed to prevent the attack on the U.S. diplomatic compound in Libya in 2012. It is, unfortunately, a good example of not considering the context as the CIA was focused on Al-Qaeda while the attack was done by the local Ansar Al-Sharia (see chapter six). The results were the death of two people, including the U.S. Ambassador. After that event, Senate Committee on Homeland Security and Governmental Affairs made a report stating that there were a lot of open sources that could have been used to prevent that. For example, from OSINF could have been seen that the Al-Sharia was capable of endangering U.S. facilities in Lybia, but there was a serious lack of focus on them (Hensley, 2016: 49).

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. Western intelligence efforts from the Cold war vividly show problems that arise when analyzing closed societies. U.S. had to build expensive spy planes (U2, SR-71) to create military intelligence, while the Soviets could watch tv channels from the West and read science magazines. Soviet agents also had the possibility to attend "open house" military equipment displays (Hulnick, 2002: 10). Except for the mentioned problems, there is a need for reliable sources; otherwise, the forecasts become unreliable. That again points to all-source analysis since OSINT is most valuable when mixed with other sources.

### 5.4. High-tech solutions

Using OSINT in combination with high-tech solutions brings intelligence to a new level of insight. The new solutions that will come with the evolution of AI and quantum computers (soon commercially available) will bring added value to OSINT. For now, simple AI solutions are the ones that are mostly used. In them, the afore-mentioned "spam" method is very usual for filtering data, or somewhat more advanced methods of face recognition that are often used

for reverse image searches. The added value of OSINT is present even by using only computational and statistical software. Furthermore, when combined with technological solutions, OSINT becomes the least costly and most productive intelligence. It is most productive by the number of insights from its quantitative analysis, which can not be gathered else how. However, there is a permanent problem of depth of understanding when it comes to that level of analysis since only human cognition can delve deeper into any matter.

Gathering big data is possible only by technology, but that process is not always optimal. None of the high-tech solutions are automated, while further education is necessary for its utility (Sparks, 2014: 38-39). It takes special skills to interpret and use the results of modern OSINT methods, which differentiates it from the OSINT in the Cold war. Because of those necessary skills, there is a serious question of whether it will ever become possible to substitute humans with computers in intelligence analyses. In a report made by ISN (International Relations and Security Network, Zürich ), OSINT is portrayed as just another domain of intelligence in which human expertise is the one that makes all the difference (ISN, 2010: 7). Additionally, political decisions, like those on national security matters, should not be left to automation. It can be justified with the fact that computers still do not have „understanding" as their ability (Schaurer and Störger, 2010: 7). While the automation of decision-making may come in the future, for now, the human factor is inevitable in the usage of OSINT.

### 5.5. Responsibility

When it comes to responsibility, OSINT may be the most responsible intelligence technique. By so, it may be more suitable for democracies. Autocratic regimes have much fewer constraints when providing national security to their citizens. Democracies, on the other hand, have responsibility as their core principle, which also transfers to intelligence agencies. Regarding OSINT, oversight is not generally necessary. In the next chapter, there will be more on the unsettled privacy problems, but conducting OSINT is surely different from covert means of gathering. Considering that OSINT deals with open sources, the intelligence product can be shared with non-intelligence actors, while higher clearance for its attainment is often unnecessary. If compared with HUMINT or SIGINT, OSINT is much safer and less intrusive. Also, the gathering of information can be done almost anywhere, without leaving a trail behind its operations.

Though OSINT can be made out of primary sources (OSD), secondary sources are the ones that are mostly used. They include research papers, news articles, or interviews, which all bear the problem of reliability. Dealing with such sources requires significant efforts directed towards verifying their truthfulness. While this issue is not exclusive to OSINT, it is important to note it because the human factor has a significant role in OSINT. In reality, the responsibility lies on the interpreter of the data, not the source itself.

## 6. POSITIVE AND NEGATIVE ASPECTS OF OSINT

### 6.1. Positive aspects of OSINT

When looking at the positive aspects of using OSINT, there are at least four major advantages over other techniques: it is context giving, less intrusive, explorative, and of lower cost. OSINT is the leading source for mapping out the context of the situation. It is also a very versatile solution, as it can be used for many matters, such as economics, crime, environment, psychology, national security, etc. (Pastor-Galindo et al, 2020: 10285). Secrets and other covertly gathered information tend to be very specific in their nature. However, OSINT provides a broader picture, which can help with the understanding of the matter in question. Such contextual knowledge often comes from academics that have been devoted to the subject for many years (Steele, 2001: 48). Also, the context is crucial when an intelligence agency or military operates outside their country. Open sources, thus, give necessary cultural information, socio-economic conditions, geospatial data, and other information for strategic needs (Olaru, 2015). One such fail to consider the context could be seen in the 2012 attack on the American diplomatic compound in Benghazi - Lybia. The reason for the failure to secure the compound can be found in the fact that the CIA had its focus only on Al-Qaeda, ignoring other terrorist organizations that eventually committed the attack (Hensley, 2016: 48-49). This points to the fact that early warnings, which are important goals of intelligence agencies, can often be successfully created by OSINT (Steele, 2001: 240). OSINT can also detect early signs of radicalization in online communities, making it another tool for preventing terrorism and extremism (Staniforth, 2017: 17).

Aside from that, the second major advantage of OSINT is its lack of intrusiveness. When citizens seek more responsibility from intelligence services, OSINT can be a technique that is closest to that state. Though this is not without dilemmas (see negative aspects), it is by far the most legal and ethical technique (Steele, 2001: 242), thus more appealing to the wider public. Thirdly, OSINT is a good starting point for covert means of gathering. It is usually used to direct the focus of covert means of gathering by mapping out the known and the unknown. Thus, it has a great explorative value since it is generally considered uneconomical to spend resources on covert gathering if open sources can suffice (Gibson, 2014: 16; DCAF, 2003: 16). The last of the frequently noted advantages is its cost. OSINT is very efficient in terms of how much is invested and how much is gotten as a result (Bule, 2020). Resources can be money, as OSINT is the cheapest technique (not free), but most often, it is time. Speed can be vital for intelligence operations, and by using OSINT, intelligence officers do not need a

higher clearance. Another speed advantage is present by using digital technologies, eventually speeding up the decision-making process. This is rather important for military action, as it shortens the time necessary for observation and orientation in the command giving process (Ashwell, 2017: 20). The analysis of open sources can also be very fast, but the structuring of gathered data is still mostly done manually, slowing down the process dramatically. However, the results of such automated analysis can bear results that are not possible by humans, such as correlations and forecasts based on big data (Pastor-Galindo et al, 2020: 10285). Software can, thus, easily spot subtle differences that humans can not, like spotting bots on Twitch or any other internet social media (Sferrella and Conger, 2020: 43). OSINT software can detect anything out of the ordinary, which can help with early warnings. When creating OSINT from free secondary sources, the cost of intelligence is also lowered. It is so because the expertise behind the sources is maintained by someone else (Steele, 1995: 466). So the ratio of input and output results makes OSINT the most productive intelligence technique (Gibson, 2014: 16).

Aside from those constant four advantages, other advantages can sometimes be leveraged. For example, when conducting OSINT on the Internet, an ever-increasing amount of data is waiting to be collected and analyzed. Such sources are data from social media, reports, documents, multimedia, Deep web, etc. Any other technique cannot achieve this quantity of information. OSINT can also do the opposite of finding context. It can lead to particular lesser-known information that may prove insightful. One Australian researcher interested in counterinsurgency found out about a successful case performed by the Indonesian government on Darum Islam insurgents. The information was found in an Indonesian museum, while that case was never mentioned elsewhere in the West (Packer, 2006). Another advantage is that OSINT shortens the distance between geographically far countries, making it possible to analyze events in countries where agents would not probably be sent to perform HUMINT (Steele, 2001: 240). OSINT, thus, has a low level of risk, making it more responsible. One big advantage of OSINT is the possibility of sharing data between intelligence agencies and private companies easily. Though this is somewhat questionable, OSINT is still considered unclassified information by many (Holland, 2012: 2). Last but not least, OSINT can be used as an ignition for imagination. When confronted with new problems or old transformed ones, many of the answers can not be found in history. Imagination can, however, encourage innovative thinking. Innovation is, by definition, the usage of creative ideas that come from imagination (Korkut and Kopal, 2018: 6-8). That is why OSINT is often used for viewing the

same situation from another angle, which can fill in the blanks, find the enemy's weaknesses, and ultimately find opportunities that can bring to an advantage (Benes, 2013: 25). For certain forecasts, analysts have to think of the issues that are still not real or may never be. Being able to imagine and recognize new forms of threats can be an invaluable skill for risk assessment. However strangely, even reading fiction can help an analyst to get to that state of all possibilities.

### 6.2 Negative aspects of OSINT

Though there are fewer negative aspects of OSINT in their quantity, they can significantly impact its utility. The first and the most eminent problem of OSINT are its legal and ethical implications. Though OSINT is created from open sources, it does not mean that it is only made of public information. There are shades of privacy regarding all open sources since information can be unclassified but sensitive at the same time (Hu, 2016). Thus, there are serious considerations on whether OSINT should exploit private information that can be found in the public sphere. It is up to OSINT investigators to take privacy into account, acting coherently with private data regulations, like GDPR[7] in European Union (Ten, 2020: 14). There are at least three ethical issues regarding open sources (Hu, 2016). The first one would be the sensitivity of the source. OSINF often contains sensitive personal information (SPI), like sexual orientation, political inclination, or other information that may be compromising (Eijkman and Weggemans, 2012: 10286). That SPI can also be considered date and place of birth, parent's names, or any kind of identification number (Hassan and Hijazi, 2018: 18). The second problem would be the origin of the source. This issue regards the problem of treating leaked classified information as if they were public information. Some even call that kind of information NOSINT (N standing for NOT) since it is actually based on classified information (Hassan and Hijazi, 2018: 3). This problem is directly connected to whistleblowing[8]. Whistleblowing has, in many cases, led to revealing insights on illegal government activities (Dunn, 2016), but it does not come without repercussions. Though leaks may come from ethical intentions, the real intent behind them is never clear. Also, the leakage may contain more information than is necessary, making it even more of an issue for

7 The most important data protection regulation in the EU; The General Data Protection Regulation.

8 Whistleblowing is an act of publicly exposing information on illicit or other wrong actions of an organization.

counterintelligence. The third issue is the problem of reliability. Much public information is not reviewed, which can lead to false information ending up in the final intelligence. This can lead to harming of individuals or groups.

Furthermore, OSINT conducted on social media is done without the subject's consent. That kind of secrecy is standard for intelligence work, but the lack of consent would also imply the need for higher clearance for conducting OSINT. There is also a problem with downloading content from social media, as it makes it impossible for anyone to revert their information to be private (Ten Hulsen, 2020). However, most people on social media are not afraid of their data being used, insomuch being used out of context (Eijkman and Weggemans, 2012: 292). An opinion posted in comments on social media is information shared with a specific purpose. That comment is also intended to be viewed by a specific audience, while its abstraction from the context can lead to misrepresented information (Eijkman and Weggemans, 2012: 292). Courts are often guided by the idea of "reasonable expectation of privacy", which is lost when someone shares their information online (Ssclegacy.com, 2021). This brings responsibility to the individuals for sharing their information (Ten, 2020: 36). Though this may seem logical, it neglects that not everyone is familiar with the possibility of their data being exploited. In fact, someone else may also share others' private information, like the option to "tag" someone in a photograph on social media (Edwards and Urquhart, 2016: 294). One small study on 63 students showed that every student had some private information disclosed on Facebook, often unknowingly (Edwards and Urquhart, 2016: 295). In the UK, authorization by a senior police officer is sometimes needed for conducting SOCMINT. It is so because of the UK's Regulation of Investigatory Powers Act (RIPA). By interpretation of that act, it can be seen that SOCMINT sometimes falls into the category of "directed covert surveillance". By definition, such surveillance is covert research through which private information is obtained (Edwards and Urquhart, 2016: 296). Private OSINT investigators especially have to care for privacy laws, as their OSINT is not useful if it cannot be admissible at court (Ssclegacy.com, 2021)

Another problem may be the usage of high-tech solutions for OSINT. Despite the human brain's weaknesses, technology is still unable to match its abilities. Human analysts are irreplaceable in their ability to compare evidence, develop alternative hypotheses, create judgments, etc. (Benes, 2013: 29). Though human brains are not unaffected by biases, the expertise of an analyst is still the core of intelligence (see subchapter on high-tech solutions) (Schaurer and Störger, 2010: 7). That can be seen from the fact that analysts are still the ones

who assess analytical and statistical software (Bernard et al, 2018: 2). Aside from affecting many aspects of human lives, using technology grows dependencies on it (Benes, 2013: 31). There is a recurring problem of being dependent on technology, like in an example of critical infrastructures that cannot function without it. The same problem can be evident with modern OSINT. Today's OSINT mainly relies on analytical software and "big data" gathered on the Internet, while the more traditional sources are being somewhat neglected.

Another apparent problem that is connected to technological advances is the sheer amount of available information. Paradoxically, that is also the exact reason why OSINT is such a versatile solution. That information overload is evident from the amount of noise in the communication channel that can be overwhelming. The noise can sometimes disregard most OSINT's advantages, such as speed and low cost (Expert.ai, 2017). With the new generation of Internet (5G) coming to place, many Internet users will be encouraged to share more data, making this even a bigger issue (Hassan and Hijazi, 2018: 342). It is one of the biggest obstacles, while currently, the only way for gapping it is expertise in particular fields of research and mastering certain analytical skills (Best and Cumming, 2008: 81). One observed phenomenon that can cause a disturbance regarding OSINT is the news „echo", which is done by many news portals publishing the same story. Such an echo makes it hard to detect where the information originated and is it true (Best and Cumming, 2008: 81). Connected to that, another essential negative aspect of OSINT is possible misinformation. OSINT made of books and journal articles may not have this problem, but it is hard to discern what may or may not be true on the Internet. This leads to the question of the validity of content as it equates OSINT with HUMINT in their need to validate sources (Expert.ai, 2017). As stated before, people often joke on social networks or say whatever is on their minds without intending to act upon those thoughts (Edwards and Urquhart, 2016: 290). That can lead to a problem in the phase of data mining since most of the OSINT software still does not detect these subtle differences. That can easily lead to bad data (Edwards and Urquhart, 2016: 291). Generally, it is very challenging to conclude which information is valid, which false, and which is meant to deceive (Apteditor, 2020). When venturing into internet social networks, the reliability of content becomes especially questionable. Also, the usual advice to stick to authoritative lines of information is not of much use. It is so because these are the places with almost no such information. Though information on the Internet is content-rich, much of it is unstructured and unreliable compared to books or magazines (Pastor-Galindo et al, 2020: 10285). The last evident problem would be the fact that OSINT cannot be used when exactly secrets are

needed. OSINT is by no means a full intelligence solution, and it does not prove to be an alternative to covert gathering as it only scrapes the surface of hidden problems in some cases. It is so especially when subjects of matter are cautious and aware, as underground actors usually are (Pallaris, 2008: 2). So, it is generally accepted that OSINT can not substitute all source analysis (Holland, 2012: 1).

## 7. FINAL INTERPRETATION OF THE RESULTS OF ANALYISIS

It is clear that there are positive and negative aspects of every dimension of OSINT, so the possible advantage is dependent on the specific situation with its specific needs. Regarding modern dimensions, there is a great difference between individual positive and negative aspects, so it would be hard to compare their value only by the number of items in the list. However, that number does provide a general picture of which dimensions have an ambivalent value and which dimensions do not. When examining the table of five modern dimensions, a clear positive advantage can be seen in responsibility. Some positive advantages, but smaller, can be seen in forecasting (those advantages being even smaller when combined with high-technology). Logically, responsibility has such a high positive value since there is hardly anything safer or more transparent than using open sources for creating intelligence. Nonetheless, there are many dilemmas regarding ethical and privacy issues when conducting OSINT, but much of it concerns only private OSINT investigations. It may be less of a problem for state's intelligence agencies since OSINT is conducted alongside other forms of gathering on the same rules and principles of covert gathering. That means dealing with ethical considerations, along with legal authorizations (Wells, 2017: 63). Forecasting has more positive aspects because of a wide variety of open sources that can lead to an understanding of the broader picture. Besides that, OSINT tends to leave its sources more transparent, making it possible for others in the intelligence process to further interpret, add, criticize, create, and else that can lead to a better product. This tends to have a big impact when dealing with a lack of information or unreliable one, which is common for intelligence work.

Using the Internet as a source is the main characteristic of today's OSINT, but it is certainly hard to discern does it bring more value to OSINT. The amount and value of positive and negative aspects of the Internet are about equal. WEBINT does produce more for less, can explore any subject and bring new insights, but the high volume of information (often unreliable) brings new problems that need to be addressed. In addition, the logical critique still stands that the powerful actors are not negligent of their internet presence as they bring it to a non-existing level. The second listed dimension, privatization of intelligence, is yet to be capitalized on and, until then, stands as more of a problem. OSINT is a good example of a double-edged sword technique, not because of the need to compete with private OSINT companies, but rather because OSINT is a tool available to individuals and organizations with dangerous intents. Finally, high-tech solutions that OSINT is filled with have many positive

advantages, but for now, lack the number of skilled people to bring its added value. Besides, the human factor in the automated analysis is still crucial and the core of the intelligence process. However, most of the negative aspects of high-tech solutions will probably be solved in the future, regarding using neural networks and other machine learning that can mimic the human brain and its decisions making process.

The importance of OSINT in today's intelligence has increased since the way of living has modernized and in part transferred into the virtual realm, thus accepting the starting hypothesis of the paper. Web intelligence has become more useful since users of the Internet became creators, sharers, interpreters, and validators of the shared content. This created a pool of primary and secondary sources that are closest to the source or are the source itself. OSINT is part of the core techniques of intelligence gathering but was always considered of a lesser value, a byproduct, or a starting point of the „real" intelligence gathering. Regarding the changes of the concept of security, OSINT can, because of its wide utility, actually have primacy and bring leading insights. The solution to modern security problems, such as ecological disasters, migration, infectious diseases, or plain old terrorism, seems to lay in all-source analysis, also containing OSINT (Ashwell, 2017: 25). Classical security threats should also be mentioned since OSINT has been proven useful from strategic to tactical levels of action. Unreliable open sources can be tackled by using different types of sources, validating OSINT (OSINT-V). By doing so, OSINT can create insights that can not be found anywhere else. All of the dimensions analyzed (Internet, privatization, forecasting, high-tech solutions, and responsibility) will stay important for intelligence, as they are all still unsettled and changing. Intelligence communities still have to react to most of them, making it an interesting topic to follow in the future. Negative aspects of OSINT will surely be diminished through technical advancement, but nothing guarantees that positive aspects will not diminish as well. That can be done in many ways. Democratic societies could go off the democratic course and become more closed. People could generally develop a culture of privacy instead of publicity, or some different cultural tide could emerge that would counter the technological aspects of modern societies and nurture the offline realm of our ancestors. In such conditions, OSINT would certainly lose its added value. The idea of this paper was to prove the increasing importance of OSINT and why it is so, but this may still change. For now, the world is becoming more interconnected and more public, while a variety of open-source tools are becoming widely available (face recognition, speech to text, free access to books and

articles, image analysis, etc.). All of that points towards OSINT having an important role in intelligence gathering of the future, as well of today.

## 8. CONCLUSION

This paper has shown the evolution of OSINT from the founders of its institutionalization (Office of Strategic Services and Foreign Broadcast Monitoring Service in the U.S.) to the new private actors (private intelligence companies or threats to national security). The early OSINT manifested in listening to foreign radio broadcasts, reading economy magazines to monitor nuclear developments, and even reading spy novels that transferred certain skills. That conversion from Open-source information (OSINF) to Open-source intelligence (OSINT) has been modernized since. That is especially so after 2005 when the World Wide Web experienced a revolution to 2.0. The new WWW made it possible to make personalized content on the Internet (Facebook, Youtube, and Twitter). Consequently, our modern and digital way of life made a pool of primary and secondary sources publicly available for gathering. That helped OSINT to leave the category of second-class intelligence, even though many still remark that it isn't used as much as it should be. Intelligence analysis tends to cope with modernity by having an interdisciplinary approach to solving problems. Connected to that, analyses made of all sources are being encouraged, as they lift reliability and insight to a higher level. One popular example of it is the methodology taken from sociology, called Social Network Analysis (SNA). Today, SNA can be made that figures out the important actors in a network and the power of their relation. All of that information can be gathered from Facebook or similar social media on the Internet. Aside from that, underground intelligence can also be created out of information from Dark Net markets. Another usage are early warning systems that based on tweets on Twitter, etc. These possibilities nudge intelligence work into a safer, cheaper, faster, and less intrusive zone. However, only open sources are not always enough. The best intelligence is considered to be all-source intelligence, meaning that OSINT should be used in combination with other sources. That way, the reliability of intelligence is much higher while also diminishing some of the biases. That is especially important when dealing with sources on the Internet. Doing so makes it possible to discern what is real, what is radical in thoughts (but not in acts), and what is a construct of reality that is tweaked to match one's own perception.

The increasing importance of OSINT was proved by analyzing its positive and negative aspects across five dimensions: Internet as a source, privatization of intelligence, forecasting, high-tech solutions, and responsibility. The truth about the value of OSINT is nuanced, just as other truths are in life, so OSINT often has positive and negative repercussions on intelligence. All of the chosen dimensions will be important in the future as

some of them haven't been dealt with effectively. That is making the topic of OSINT and dilemma on its real value relevant after this paper.

The fact about the importance of OSINT and its value greatly affects intelligence work. It is so because secrecy is embedded into the culture of intelligence communities, while danger and exclusiveness over information have always been the main associations with intelligence. If OSINT can bear insights that can not be claimed else how, it should be considered equal to other techniques. Thus, its second-class position can be disregarded. The specialty of OSINT could be considered creativity. This is especially important when dealing with modern security threats, as creativity is the only solution for thinking of the unthinkable but dangerously probable. Regarding classical threats, OSINT has also proven its value. It can be used for contextual knowledge in expeditionary warfare, strategic intelligence, or tactical intelligence in the form of detailed open-source maps. More importantly, OSINT can be used for early warnings of possible regional conflicts. It is important to note that ordinary citizens are given a more important role as they often create the sources that are later to be used in intelligence analysis. For a while now, a window of opportunity has been opened for intelligence agencies to use the new tools to their advantage. Intelligence agencies must follow technological advances, including OSINT advances. That is immensely important because if they do not, someone else certainly will.

All of this points to all-source analysis for a solution to the shifted global paradigm. Global risks are becoming less classical, probably increasing the role of OSINT in intelligence. It is so because there is not a secret that can prevent an ecological disaster, on which research wasn't already published in a scientific journal. There is not an expensive satellite photo that can not, to some extent, compare to free satellite photographs. Finally, there is no progress in intelligence without the cooperation between the public and the private sector. All of that is greatly embodied in OSINT. Open sources, in combination with covertly gathered ones, can increase the value of final intelligence. Such all-source intelligence may be the only way to resolve some of the wicked problems of national security.

**REFERENCES**


Andregg, Michael (2007) Intelligence ethics - Laying a foundation for the second oldest profession. In: Johnson, Loch K. (ed.) *Handbook of Intelligence Studies* (str. 52-63). New York: Routledge.

Akhgar, Babak (2017) Osint as an integral part of the national security apparatus. In: Akhgar, Babak, Bayerl, Saskia and Sampson, Fraser (eds.) *Open Source Intelligence Investigation* (pp. 3-9). Cham: Springer.

Apteditor.com (2020) Open-Source Intelligence. http://apteditor.com/2019/11/open-source-intelligence-osint/ Accessed on March 22, 2021

Ardelean, Mihai (2015) The Importance Of Strategic Intelligence In Relation To Romania's Geopolitical Imperative Of Securing The Mouth Of The Danube Following The Events In Eastern Ukraine. *International Scientific Conference - Strategies XXI*. Bucharest: National Defence University

Ashwell, Mark Lawrence (2017) The digital transformation of intelligence analysis. *Journal of Financial Crime* 24(3): 1-32.

Baldini, N. et al. (2007) A Multilanguage Platform For Open Source Intelligence. In: Zanasi, Alessandro (ed.) *Data Mining VIII - Data, Text and Web Mining and their Business Applications* (str. 325-334). UK: Wessex Institute of Technology.

Barić, Marijan (2014) Strateška-obavještajna djelatnost u doba obavještajne postmoderne. *Zbornik radova: Dani Kriznog Upravljanja, 2014.*: 1361-1381.

Bean, Hamilton (2011) *No More Secrets. Open Source Information and the Reshaping of U.S. Intelligence*. Santa Barbara: Praeger.

Beebe, Sarah and Pherson, Randolph (2015) *Cases in Intelligence analysis – Structured Analytic techniques in Action*. London: SAGE Publications.

Bellingcat.com (2018a) Skripal Poisoning Suspect's Passport Data Shows Link to Security Services. https://www.bellingcat.com/news/uk-and-europe/2018/09/14/skripal-poisoning-suspects-passport-data-shows-link-security-services/ Accessed on April 23, 2021

Bellingcat.com (2018b) Skripal Suspects Confirmed as GRU Operatives: Prior European Operations Disclosed. https://www.bellingcat.com/news/uk-and-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-european-operations-disclosed/ Accessed on April 23, 2021

Bellingcat.com (2018c) Skripal Suspect Boshirov Identified as GRU Colonel Anatoliy Chepiga. https://www.bellingcat.com/news/uk-and-europe/2018/09/26/skripal-suspect-boshirov-identified-gru-colonel-anatoliy-chepiga/ Accessed on April 23, 2021

Bellingcat.com (2018d) Full report: Skripal Poisoning Suspect Dr. Alexander Mishkin, Hero of Russia. https://www.bellingcat.com/news/uk-and-europe/2018/10/09/full-report-skripal-poisoning-suspect-dr-alexander-mishkin-hero-russia/ Accessed on April 23, 2021

Benes, Libor (2013) OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm. *Journal of Strategic Security* 6(3): 22-37.

Bernard, Rose et al. (2018) Intelligence and global health: assessing the role of open source and social media intelligence analysis in infectious disease outbreaks. *Journal of Public Health* 26(5): 509-514.

Berzinji, Ala (2011) Detecting key players in terrorist networks. http://uu.diva-portal.org/smash/get/diva2:442516/FULLTEXT01.pdf Accessed on March 22, 2021

Best, Clive (2011) Challenges in open source intelligence. *2011 European Intelligence and Security Informatics Conference*: 58-62.

Best, Richard and Cumming, Alfred (2008) Open Source Intelligence: Issues for Congress. In: Paulson, Terrance M. (ed.) *Intelligence Issues and Developments* (str. 75-97). New York: Nova Science Publishers.

Bloomsbury.com (2012) About Anthony Olcott's book: Open Source Intelligence in a Networked World. https://www.bloomsbury.com/us/open-source-intelligence-in-a-networked-world-9781441140715/ Accessed on February 27, 2021

Britannica.com (2021) Intelligence – international relations. https://www.britannica.com/topic/intelligence-international-relations Accessed on February 27, 2021

Brunetti-Lihach, Nick (2018) Information Warfare Past, Present, and Future. https://www.realcleardefense.com/articles/2018/11/14/information_warfare_past_present_and_future_113955.html Accessed on June 4, 2021

Bule, Guise (2020) A Guide To Open Source Intelligence (OSINT). https://itsec.group/blog-post-osint-guide-part-1.html Accessed on March 22, 2021

Burcher, Morgan (2020) *Social Network Analysis and Law Enforcement: Applications for Intelligence Analysis.* Cham: Springer Nature.

Burke, Cody (2007) Freeing knowledge, telling secrets: Open source intelligence and development. *CEWCES Research Papers - Bond University* (13): 1-22.

Campbell, Duncan (2015) Global spy system ECHELON confirmed at last – by leaked Snowden files. *Theregister.com* 3. kolovoza. https://www.theregister.com/2015/08/03/gchq_duncan_campbell/ Accessed on February 18, 2021

Caponi, Paolo (2014) "ALHS! ALHS! Why Are You So OSINT?" Reading Books During Office Hours. *Altre Modernità* (7): 37-53.

Carroll, Jami. M. (2005) OSINT Analysis using Adaptive Resonance Theory for Counterterrorism Warnings. *Artificial Intelligence and Applications*: 756-760.

Chauhan, Sudhanshu and Panda, Nutan K. (2015) *Hacking Web Intelligence - Open Source Intelligence and Web Reconnaissance Concepts and Techniques*. Waltham: Elsevier Inc.

Chen, Hsinchun (2011) From terrorism informatics to dark web research. In: Wiil, Uffe K (ed.) *Counterterrorism and Open Source Intelligence* (pp. 317-341). Vienna: Springer.

CIA (2015) Where Spies Go When They Don't Know. https://www.cia.gov/stories/story/where-spies-go-when-they-dont-know/ Accessed on April 25, 2021

CIA (2020) The World Factbook. https://www.cia.gov/the-world-factbook/countries/world/#people-and-society Accessed on February 27, 2021

Colquhoun, Cameron (2016) A Brief History of Open Source Intelligence. *bellingcat.com* 14. srpnja. https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/ Accessed on February 26, 2021

Cozine, Keith (2013) Teaching the intelligence process: The killing of Bin Laden as a case study. *Journal of Strategic Security* 6(3): 80-87.

Croom, Herman (1969) The Exploitation of Foreign Open Sources. *Studies in Intelligence* 13(): 129-134.

DCAF (Ženevski centar za demokratsku kontrolu oružanih snaga) (2003) *Obavještajna praksa i demokratski nadzor*. Ženeva: DCAF.

Delavallade, Thomas et al. (2017) Extracting future crime indicators from social media. In: Larsen, Henrik Legind et al. (eds.) *Using open data to detect organized crime threats* (pp. 167-198). Cham: Springer.

Denécé, Eric (2014) The revolution in intelligence affairs: 1989–2003. *International Journal of Intelligence and CounterIntelligence* 27(1): 27-41.

DNI (U.S. Director of National Intelligence) (2006) Intelligence Community Directive 301 - National Open Source Enterprise. https://fas.org/irp/dni/icd/icd-301.pdf Accessed on February 26, 2021

DOD (U.S. Department of Defence) (2021) DOD dictionary of military and associated terms. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf Accessed on February 26, 2021

Doorey, Timothy J. (2007) Intelligence Secrecy and Transparency: Finding the Proper Balance from the War of Independence to the War on Terror. *Strategic Insights* 6(3): 1-13.

Dunn, Alix (2016) Responsible data leaks and whistleblowing. https://www.theengineroom.org/responsible-data-leaks-and-whistleblowing/ Accessed on June 4, 2021

Edwards, Lilian and Urquhart, Lachlan (2016) Privacy in public spaces: what expectations of privacy do we have in social media intelligence? *International Journal of Law and Information Technology* 24(3): 279-310.

Eijkman, Quirine and Weggemans, Daan (2012) Open source intelligence and privacy dilemmas: Is it time to reassess state accountability. *Sec. & Hum. Rts.* 23(1): 285-296.

Evans, Gareth (2018) Bellingcat: The website behind the Skripal revelation. *bbc.com* 27. rujna. https://www.bbc.com/news/uk-45665380 Accessed on April 22, 2021

Expert.ai (2017) Advantages and disadvantages of open source intelligence. https://www.expert.ai/blog/advantages-disadvantages-open-source-intelligence/ Accessed on March 22, 2021

Gibson, Stevyn D. (2014) Exploring the Role and Value of Open Source Intelligence. In: Hobbs, Christopher et al. (eds.) *Open Source Intelligence in the Twenty-First Century. New Approaches and Opportunities* (str. 9-23). Hampshire: Palgrave Macmillan.

Glassman, Michael and Kang, Min (2012) Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior* 28(2): 673–682.

Hassan, Nihad A. and Hijazi, Rami (2018) *Open Source Intelligence Methods and Tools - A Practical Guide to Online Intelligence.* New York: Apress.

Hensley, Patrick D. (2016) *Shades Of Gray: Releasing The Cognitive Binds That Blind Us* (MA Dissertation). Monterey: Naval postgraduate School.

Herman, Michael (1996) *Intelligence power in peace and war*. Cambridge: Cambridge University Press.

Higgins, Eliot (2016) Finding truth in a post-truth world | Elliot Higgins | TEDxAmsterdam (video). https://www.youtube.com/watch?v=mozxTk3Brqw&ab_channel=TEDxTalks Accessed on February 18, 2021

Higgins, Eliot (2017) The Russian Ministry of Defence Publishes Screenshots of Computer Games as Evidence of US Collusion with ISIS. *Bellingcat.com* 14. studenoga. https://www.bellingcat.com/news/mena/2017/11/14/russian-ministry-defence-publishes-screenshots-computer-games-evidence-us-collusion-isis/ Accessed on February 18, 2021

Higgins, Eliot (2019) How to expose the Russian government's lies | Bellingcat founder Eliot Higgins on MH-17 (video).

https://www.youtube.com/watch?v=6muSJCSXgjY&t=1089s&ab_channel=JOE Accessed on February 27, 2021

Hofmann, David (2018) Questioning the "Loneliness" of Lone-Wolves: A Social Network Analysis of Lone-Wolf Terrorists (video). https://www.youtube.com/watch?v=7EQjS7Lz3V4&ab_channel=SmartCybersecurity Network%28SERENE-RISC%29 Accessed on March 22, 2021

Holland, Benjamin (2012) *Enabling Open Source Intelligence (OSINT) in private social networks* (MA Dissertation). Ames: Iowa State University.

Hu, Evanna (2016) Responsible Data Concerns with Open Source Intelligence. https://responsibledata.io/2016/11/14/responsible-data-open-source-intelligence/ Accessed on March 22, 2021

Hulnick, Arthur S. (2002) The downside of open source intelligence. *International Journal of Intelligence and CounterIntelligence* 15(4): 565-579.

IC (U.S. Intelligence Community) (2009) National Intelligence – a consumer's guide. https://www.dni.gov/files/documents/IC_Consumers_Guide_2009.pdf Accessed on February 27, 2021

ISN (International Relations and Security Network) (2010) OSINT Report 3/2010. The Evolution of Open Source Intelligence. https://www.files.ethz.ch/isn/122008/osint_final_Q3-2010.pdf Acessed on June 4, 2021

Jarvis, Jeff (2013) How much data the NSA really gets. *theguardian.com* 13. kolovoza. https://www.theguardian.com/commentisfree/2013/aug/13/nsa-internet-traffic-surveillance Accessed on April 22, 2021

Kasapoglu, Can (2021) ANALYSIS - Re-thinking open-source intelligence in the information age and digital change. https://www.aa.com.tr/en/analysis/analysis-re-thinking-open-source-intelligence-in-the-information-age-and-digital-change/2125883 Accessed on June 4, 2021

Kent, Sherman (1949) *Strategic Intelligence for American World Policy.* New Jersey: Princeton University Press.

Knoke, David (2015) Emerging trends in social network analysis of terrorism and counterterrorism. *Emerging Trends in the Social and Behavioral Sciences*: 1-15.

Kopal, Robert (2018) Međunarodna sigurnost: primjena strukturiranih analitičkih tehnika u predviđanjima. *Zbornik sveučilišta Libertas* 3(3): 9-22.

Korkut, Darija and Kopal, Robert (2018) *Kreativnost 4.0. Evolucija i revolucija*. Zagreb: Visoko učilište Effectus.

Koschade, Stuart (2006) A Social Network Analysis of Jemaah Islamiyah: The Applications to Counterterrorism and Intelligence. S*tudies in Conflict & Terrorism* 29(6): 559–575.

Kowalewski, Annie (2017) Disinformation and Reflexive Control: The New Cold War. *georgetownsecuritystudiesreview.org* February 1. https://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/ Accessed on April 22, 2021

Kriegler, Ana (2014) Using social network analysis to profile organised crime. https://www.files.ethz.ch/isn/183611/PolBrief57.pdf Accessed on March 22, 2021

Lapid, Ephraim (2016) OSINT: A Major Source of Up-to-Date Information. *National security and the future 17*(1-2): 37-42.

Lathrop, Charles E. (2004) *Literary Spy – The Ultimate Source of Quotations on Espionage & Intelligence*. New Haven: Yale University Press.

Levchuk, Georgiy and Shabarekh, Charlotte (2017) Using soft-hard fusion for misinformation detection and pattern of life analysis in OSINT. *Next-Generation Analyst V* 10207(4): 1-9.

Lowenthal, Mark M. (2009) *Intelligence - From Secrets to Policy*. Washington DC: CQ Press.

Macmillandictionary.com (2021) Intelligence – definitions and synonyms. https://www.macmillandictionary.com/dictionary/british/intelligence Accessed on February 18, 2021

Marzell, Laurence (2017) OSINT as Part of the Strategic National Security Landscape. In: Akhgar, Babak, Bayerl, Saskia and Sampson, Fraser (eds.) *Open Source Intelligence Investigation* (pp. 33-56). Cham: Springer.

McGlynn, Patrick and Garner, Godfrey (2019) *Intelligence Analysis Fundamentals*. Boca Raton: CRC Press.

Menkhaus, Ken (2013) Al-Shabaab and Social Media: A Double-Edged Sword. *Brown J. World Aff.* 20(2): 309-327.

Mercado, Stephen (2004) Sailing the Sea of OSINT in the Information Age. *Center for Study of Intelligence* 48(3): 45-55.

Merriam-Webster.com (2021) Definition of intelligence. https://www.merriam-webster.com/dictionary/intelligence Accessed on February 26, 2021

Miller, Rich (2013) NSA Utah Data Center Facing Unexpected Energy Taxes. *datacenterknowledge.com* 20. svibnja. https://www.datacenterknowledge.com/archives/2013/05/20/utah-legislators-hit-nsa-data-center-with-energy-tax#menu Accessed on April 23, 2021

Miller, Rich (2021) Facebook to Expand Utah Data Center Campus by 900,000 SF. *datacenterfrontier.com* Febraury 12. https://datacenterfrontier.com/facebook-to-expand-utah-data-center-campus-by-900000-sf/ Accessed on April 23, 2021

Minas, Harris (2010) *Can The Open Source Intelligence Emerge As An Indispensable Discipline For The Intelligence Community In The 21 St Century?* (MA Dissertation). Athens: RIEAS.

Nair, Sabari G. and Puri, Priti. (2015). Open Source Threat Intelligence System. *International Journal of Research* 2(4): 360-364.

NATO (North Atlantic Treaty Organisation) (2001) NATO Open Source Intelligence Handbook. http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf Acessed on June 4, 2021

Norton, R. A. (2011) Guide to Open Source Intelligence. A Growing Window into the World. *The Intelligencer: Journal of US Intelligence Studies* 18(2): 65-67.

Olaru, Gherghina (2015) Historical Reference Points Of Open Source Utility In Intelligence. *Redefining Community in Intercultural Context* 4(1): 234-238.

Omand, David Sir et al. (2012) A balance between security and privacy online must be struck - Intelligence Report. https://demosuk.wpengine.com/wp-content/uploads/2017/03/intelligence-Report.pdf Accessed on March 22, 2021

Omand, David et al. (2014) Towards the discipline of social media intelligence. In: Hobbs, Christopher et al. (eds.) Open Source Intelligence in the Twenty-First Century. New Approaches and Opportunities (str. 24-43). Hampshire: Palgrave Macmillan.

Packer, George (2006) Knowing the Enemy - Can social scientists redefine the "war on terror"? *newyorker.com* 10. prosinca. https://www.newyorker.com/magazine/2006/12/18/knowing-the-enemy Accessed on March 22, 2021

Pallaris, Chris (2008) Open source intelligence: A strategic enabler of national security. *CSS Analyses in Security Policy* 3(32): 1-3.

Panag, H. (2019) Balakot, China 'incursions' prove OSINT images are new threat for democracies and military. https://theprint.in/opinion/balakot-china-incursions-osint-images-new-threat-democracies-military/303565/ Accessed on June 4, 2021

Pastor-Galindo, Javier et al. (2020) The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Access 8()*: 10282-10304.

Penninger, Ron (2019) Operationalizing OSINT Full-Spectrum Military Operations. https://smallwarsjournal.com/jrnl/art/operationalizing-osint-full-spectrum-military-operations Accessed on June 4, 2021

Pritchard, Stephen (2020) OSINT: What is open source intelligence and how is it used? *The Daily Swig* 19. studenoga. https://portswigger.net/daily-swig/osint-what-is-open-source-intelligence-and-how-is-it-used Accessed on February 18, 2021

Prunckun, Hank (2010) *Handbook of scientific methods of inquiry for intelligence analysis*. Lanham: Scarecrow Press.

Rhodes, Christopher J. (2011) The use of open source intelligence in the construction of covert social networks. In: Wiil, Uffe K. (ed.) *Counterterrorism and Open Source Intelligence* (pp. 159-170). Vienna: Springer.

Quinn, Christy (2018) AlphaBay Market: Lessons From Underground Intelligence Analysis - SANS CTI Summit 2018 (video). https://www.youtube.com/watch?v=XwBwuUg3fQc&ab_channel=SANSDigitalForensicsandIncidentResponse Accessed on February 18, 2021

Recordedfuture.com (2014) Putting Data in Perspective With Web Intelligence. https://www.recordedfuture.com/web-intelligence-perspective/ Accessed on June 4,2021

Recordedfuture.com (2019) What Is Open Source Intelligence and How Is it Used? https://www.recordedfuture.com/open-source-intelligence-definition/ Accessed on February 18, 2021

Recordedfuture.com (2021) What Is Threat Intelligence? https://www.recordedfuture.com/threat-intelligence/ Acessed on June 4, 2021

Russell, Richard L. (2007) *Sharpening Strategic Intelligence - Why the CIA Gets It Wrong and What Needs to Be Done to Get It Right*. Cambridge: Cambridge University Press.

Schaurer, Florian and Störger, Jan (2010) The Evolution of Open Source Intelligence. *OSINT report* 2010(3). https://www.files.ethz.ch/isn/122008/osint_final_Q3-2010.pdf Accessed on March 22, 2021

Sferrella, Alexander and Conger, Joseph Z. (2020) Discovering Influence Operations on Twitch.tv: A Preliminary Coding Framework. *Global Security and Intelligence Studies* 5(1): 43-53.

Sherman, Rachel (2021) The dark side of open source intelligence. *codastory.com* 15. siječnja. https://www.codastory.com/authoritarian-tech/negatives-open-source-intelligence/ Accessed on April 23, 2021

Sparks, Timothy (2014) *Why haven't technologies fixed open source intelligence?* (MA Dissertation). Harrisonburg: James Madison University.

Ssclegacy.com (2021) OSINT and the law. https://ssclegacy.com/open-source-intelligence-osint-and-the-law/ Accessed on June 4, 2021

Stalder, Felix and Hirsh, Jesse (2002) Open Source Intelligence. *First Monday* 7(6).

Staniforth, Andrew (2017) Open source Intelligence and the protection of national security. In: Akhgar, Babak, Bayerl, Saskia and Sampson, Fraser (eds.) *Open Source Intelligence Investigation* (pp. 11-19). Cham: Springer.

Steele, Robert D. (1995) The Importance Of Open Source Intelligence To The Military. https://arnoreuser.com/wp-content/papercite-data/pdf/steele1995.pdf Acessed June 4, 2021

Steele, Robert D. (2001) *On Intelligence - Spies and Secrecy in an Open World*. Oakton: OSS International Press.

Steele, Robert D. (2007) Open source intelligence. In: Johnson, Loch K. (ed.) *Handbook of Intelligence Studies* (str. 129-147). New York: Routledge.

Steele, Robert D. (2016) Presentation on Open Source Intelligence (video). https://www.youtube.com/watch?v=p9qLlSSHo7I&ab_channel=Forsvarsakademiet Accessed on February 18, 2021

Thespectrum.tech (2021) Open source intelligence platforms for the military. https://thespectrum.tech/solutions/%D0%BEpen-source-intelligence-military/ Accessed on June 4, 2021

Tekir, Selma (2012) Overt information operations during peacetime. https://openaccess.iyte.edu.tr/xmlui/handle/11147/5140 Acessed on June 4, 2021

Ten Hulsen, Leonore (2020) Open sourcing Evidence From The Internet – The Protection Of Privacy In Civilian Criminal Investigations Using Osint (Open-Source Intelligence). *Amsterdam Law Forum* 12(2): 3–48.

Vacas, Ivo et al. (2018) Detecting network threats using OSINT knowledge-based IDS. *14th European Dependable Computing Conference (EDCC):* 128-135.

Walker, Shaun (2015) The Russian troll factory at the heart of the meddling allegations. *Theguardian.com* April 2. https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house Accessed on February 18, 2021

Walsh, Patrick F. (2011) Intelligence and Intelligence Analysis. New York: Routledge.

WEF (World Economic Forum) (2021) The Global Risks Report 2021. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf Accessed on February 18, 2021

Wells, Douglas (2017) Taking stock of subjective narratives surrounding modern OSINT. In: Akhgar, Babak, Bayerl, Saskia and Sampson, Fraser (eds.) *Open Source Intelligence Investigation* (pp. 57-65). Cham: Springer.

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

**SUMMARY**

Intelligence agencies have been using open sources since WWII, but the intelligence made of such sources (OSINT) was always considered second-class. It was mostly so because secrets were always regarded as more valuable. Today, due to the new digital and more public way of life, the value of OSINT has been reassessed. Another reason for the change of view comes with the modern concept of security which encompasses threats that can only be addressed by a fusion of all sources. Therefore, all-source analysis with a multidisciplinary approach may be the only way to resolve wicked national security problems. OSINT, thus, in combination with technology (computers), becomes a useful tool that enriches the intelligence analysis. The paper focuses on determining whether the importance of OSINT is increasing by analyzing OSINT through its five modern dimensions. In every dimension, the positive and the negative aspects are compared, creating a picture of the relative value of today's OSINT. Those five dimensions are the Internet as a source, privatization of intelligence, forecasting, high-tech solutions, and responsibility. The research confirms the increasing importance of OSINT. Since OSINT is not given enough attention in intelligence communities, this topic will stay important in the foreseeable future.

**Keywords**: open sources, OSINT, intelligence agencies, social network analysis, Internet

## SAŽETAK

Obavještajne službe koriste otvorene izvore još od Drugog svjetskog rata, ali obavještajni proizvodi takvih izvora (OSINT) su uvijek bili smatrani drugorazrednima. To je uglavnom tako jer su se tajne uvijek smatrale vrjednijima. Danas, uslijed novog digitalnog i sve više javnijeg načina života, vrijednost OSINT-a se ponovno razmatra. Takva promjena u pogledu dolazi i zbog moderne koncepcije sigurnosti koja uključuje prijetnje na koje se može odgovoriti samo fuzijom svih mogućih izvora. Stoga, analiza svih izvora, kao i multidisciplinarni pristup, možda je jedini način za rješavanje naizgled nerješivih (wicked) problema nacionalne sigurnosti. OSINT tako, u kombinaciji s tehnologijom (kompjuterima), postaje sredstvo obogaćivanja obavještajne analize. U radu se pokušava utvrditi postoji li rastući značaj obavještajne informacije temeljene na javnim izvorima, tako što se OSINT analizira kroz njegovih pet dimenzija. U svakoj dimenziji uspoređuju se pozitivni i negativni aspekti, stvarajući sliku relativne dodane vrijednosti suvremenog OSINT-a. Tih pet dimenzija su: internet kao izvor, privatizacija obavještajne djelatnosti, predviđanje, visoko-tehnološka rješenja i odgovornost. Istraživanje potvrđuje rast značaja OSINT-a. Pošto se OSINT-u još uvijek ne pridaje dovoljno pozornosti u obavještajnim zajednicama, ova tema ostat će važna u doglednoj budućnosti.

**Ključne riječi**: otvoreni izvori, OSINT, obavještajne službe, analiza društvenih mreža, internet