Open Source Intelligence for War Crime Documentation

Vladyslav Bilous[1], Dmytro Bodnenko[1], Oleksii Khokhlov[1], Oleksandra Lokaziuk[1], and Iryna Stadnik[1]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2, Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

The use of Open Source Intelligence (OSINT) tools for military intelligence in wartime is a hot topic with a wide range of controversial issues. The results of this study confirm that OSINT can provide valuable information about potential adversaries, maintain situational awareness, and assist in the planning and execution of military operations. This type of intelligence can come from a variety of sources, including social media, news articles, and scientific research. However, it is important to recognize that OSINT is susceptible to disinformation, which can limit its accuracy and reliability. Therefore, it is crucial to use OSINT in conjunction with other intelligence-gathering methods to ensure that the information obtained is accurate and reliable. The study highlights the importance of resource management, as OSINT provides a significant advantage in this regard. The tools and methods used for OSINT analysis, in particular in social media, are based on social media analysis and geospatial analysis. The article proposes the author's software "Cyber Eye" for tracking war crimes and documenting them based on the use of OSINT, and analyses the functionality, advantages, and disadvantages of the developed software. The results of the study show that OSINT can serve as a valuable tool for military intelligence.

Keywords

Open Source Intelligence, OSINT, Cyber Eye, social media analysis, geospatial analysis, military intelligence.

1. Introduction

Open Source Intelligence (OSINT) refers to the collection, analysis, and dissemination of information obtained from publicly available sources, including social media, news articles, and other online platforms [1]. In conflict zones, OSINT plays a crucial role in documenting human rights violations and war crimes. By providing valuable information and evidence, OSINT can help to establish the identity of a person (location at a certain point in time) and bring perpetrators to justice. It is an important tool for investigators, prosecutors, lawyers, and judges who may lack experience in dealing with specific categories of serious violations, such as war crimes [2–3].

In Ukraine, OSINT plays a crucial role in documenting war crimes committed during the war. Europol has set up a special team to support investigations of major international crimes committed in Ukraine, which will assist with open-source intelligence [4–5]. The General Prosecutor's Office of Ukraine also supports the decision of Europol to create a working group on open-source intelligence [6]. The situation in Ukraine is complex, with several parties involved in the conflict, making it difficult to obtain accurate information. OSINT is a valuable source of information for documenting war crimes and bringing perpetrators to justice [1, 7–9].

The importance of OSINT goes beyond the direct documentation of war crimes in Ukraine. It is also needed by organizations seeking to facilitate the investigation of war crimes committed on the territory of Ukraine in foreign jurisdictions, by the principle of

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine

EMAIL: v.bilous@kubg.edu.ua (V. Bilous); d.bodnenko@kubg.edu.ua (D. Bodnenko); okkhokhlov.fitu20@kubg.edu.ua (O. Khokhlov); o.lokaziuk@kubg.edu.ua (O. Lokaziuk); ipstadnik.fitm22@kubg.edu.ua (I. Stadnik)
ORCID: 0000-0001-6915-433X (V. Bilous); 0000-0001-9303-6587 (D. Bodnenko); 0009-0001-6560-1398 (O. Khokhlov); 0000-0001-9663-251X (O. Lokaziuk); 0009-0009-8568-3843 (I. Stadnik)

universal jurisdiction [10]. In addition, OSINT can help prevent future war crimes by providing early warning of potential violations and identifying patterns of behavior that could lead to further abuses [1]. The obligation of parties to a conflict to distinguish between civilians and combatants at all times is a fundamental norm of international humanitarian law [11]. OSINT can help ensure that this obligation is upheld and that perpetrators of war crimes are held accountable for their actions.

The purpose of the article is to reveal the possibilities of using OSINT as a tool for documenting war crimes.

The purpose of the study is specified in the following tasks: to reveal the capabilities, tools, and functionality of OSINT for tracking useful information; to develop software and reveal examples of the use of OSINT to document war crimes, and to analyze the shortcomings and limitations of its use.

The research resulted in the development of tracking software to document war crimes.

2. Research Methodology

The following methods were used during the research: analysis of scientific literature on clarifying Open Source Intelligence; analysis of programming environments and online services for creating software; modeling the life cycle of software development product; testing of the developed author's software to form the stability of the software code; visualization (presentations, drawings, conversion of the obtained data into appropriate formats) to present the research results.

The research was carried out within the framework of the complex scientific theme of the Department of Mathematics and Physics "Mathematical methods and digital technologies in education, science, technology," DR No. 0121U111924, and the scientific theme of the Department of Information and Cyber Security named after Professor Volodymyr Buryachok of Borys Grinchenko Kyiv Metropolitan University "Methods and models of ensuring cyber security of information processing systems and functional security of software and technical complexes of critical infrastructure management," DR No. 0122U200483.

3. Results and Discussion

A structured OSINT investigation is important for several reasons.

It helps to increase efficiency by allowing you to find the information you need faster and minimize distractions.

Ensures completeness by covering all important aspects.

Provides repeatability for reviewing or sharing results.

Facilitates documentation, making the process and results transparent and traceable.

Encourages creativity by providing a solid foundation for innovative approaches.

Improves organization by allowing better structuring and analysis of information.

Provides control to better manage the process and track progress.

Minimises errors by promoting systematic and methodical approaches.

Ideally, you should start the investigation process with the option that requires the least amount of effort and at the same time offers the highest probability of a productive outcome. OSINT functionality allows you to search the following sources:

- Internet—search engines, forums, blogs, websites, etc.
- Databases—government, medical, educational databases, etc.
- Social media—Facebook, Twitter, LinkedIn, Instagram, Reddit, etc.
- Technical analysis—metadata, IP addresses, domain registrations, WHOIS information, network data, etc.
- Images and video—identify people, objects, places, or events.
- Geosocial intelligence—geotagging, logging, and location information to identify the location, activities, and connections of people/organizations.

This structure may vary depending on the purpose of the investigation and is not exhaustive.

OSINT tools essentially perform three functions:

Identify public assets: The most common function of OSINT tools is to help IT teams identify public assets and the information they contain. This includes data that could potentially contribute to the development of attack vectors. However, this does not mean identifying security vulnerabilities or penetration testing—it is only about information that can be accessed without using hacking methods [12].

Finding relevant information outside the organization: Another function of open source intelligence tools is to track information that resides outside your organization—for example, on social media platforms or in domains. This feature should be of particular interest to large companies integrating new IT assets as part of an acquisition. Given the rapid growth of social media, it makes sense for every organization to check for sensitive information outside the company.

Some OSINT tools can summarise the information and data collected in a usable form. In the case of a large organization, an OSINT scan can produce hundreds of thousands of results—especially if it covers both internal and external sources. Structuring the data and addressing the most pressing issues first is not only useful in such cases.

3.1. Publicly Available Tools

Recon-ng is a multi-level OSINT tool for software developers working with Python. The interface is similar to Metasploit, which significantly reduces the learning curve for experienced users of the popular framework. Thanks to the interactive help function (which is missing from many Python modules), developers can get started right away. In the case of Recon-ng, this includes automated processing of time-consuming and repetitive OSINT tasks (e.g. copy and paste marathons). This creates more time for things that need to be done manually. The OSINT tool has a modular structure with numerous integrated functions, so even Python beginners can master Recon-ng. These include common tasks such as standardizing output, interacting with databases, running web queries, and managing API keys. Instead of programming Recon-ng at great expense, developers simply select the functions they need and create an automated module in just a few minutes.

Recon-ng is free and open-source software.

Shodan is a specialized search engine that provides information about devices—for example, the millions of IoT devices already in use. The OSINT tool can also be used to find open ports or vulnerabilities in specific systems. Some other open-source intelligence tools use Shodan as a data source but a paid account is required for in-depth interaction.

The potential applications of Shodan are impressive: it is one of the few tools that also includes Operational Technology (OT) in its analysis, such as those used in industrial control systems in power plants or factories. Therefore, any OSINT initiative in an industry where IT and OT go hand in hand would have significant gaps if it were not based on Shodan. The OSINT tool can also be used to analyze databases: Under certain circumstances, information can be accessed publicly through workarounds.

A freelancer license ($59 per month) for Shodan allows you to scan up to 1,520 IP addresses per month, with up to a million results. The enterprise license promises unlimited results and allows you to scan 300,000 IP addresses per month for $899 per month but with a vulnerability filter and premium support.

The DarkSearch.io platform is a good starting point for those new to the dark web. You don’t even need a Tor browser to use DarkSearch.io—the search engine works with all common browsers. However, interested companies or individuals should contact the operators by email to gain access.

3.2. Examples of the Use of OSINT to Document War Crimes in Ukraine

One of the most effective ways to document war crimes in Ukraine is through the use of OSINT [1]. OSINT involves collecting and analyzing publicly available information such as social media, news, and satellite images [8].

To collect personal data, geodata, and metadata in social networks, and filter people by parameters (fields: gender, age, date of birth, place of birth, etc.), we have created the Cyber Eye software with the following functionality:

Tab “REST API”

Receiving information from various API services has been implemented:

- About the operator/region by IMSI identifier.
- About the Russian/international subscriber number.
- About the IP address.
- About the location by coordinates, getting the coordinates of the object.
- Information about nearby GSM, UMTS, and LTE base stations around the specified point (saves a report with a list of stations to display on a map).
- The engine makes it possible to view a user’s nickname in the database of 1027 sites.
- Search by IMEI.
- Geocoding to get the coordinates of places by name, latitude, and longitude.
- Search for base stations by specified coordinates and export to HTML from Google Maps.
- Scan images for viruses.

VK

- It is possible to create infographics.
- Lists.
- Search for people.
- Search for communities.
- Keeping statistics.

Instagram

- Identifier definition.
- User data by nickname.
- Number of likes, comments, views.
- Addresses on photos (GeoSint).

TikTok

- Get basic information about the user.

Telegram

- Allows you to receive user data, as well as find the administrator of a group or channel, bot.

Search engines

- Allows you to get results from a global search on the Internet using deep dark search.

Databases

- Allows you to get results by criteria in the specified databases The search is performed by the following parameters:
  - by surname
  - outside the city/village
  - by phone number
  - by region.

Bombing (currently SMS)

- Used for mass mailing of messages The mailing is carried out according to the parameters:
  - single number
  - room group.

The program, at the moment, is available in Ukrainian, in the future it is planned to localize at the first stage in the languages English, Polish, German, and French, by the formation of a multi-language file and dependency system Localization.xml.

There are situations when the results have links to graphic objects or the user found is of interest and you need to find more information manually—there are modules for viewing pictures on the right side of the application. There is also a field for notes—“Draft”. The ability to change the color scheme and enable sound notifications has been implemented.

Python programming language was used to write the software, based on open databases and common APIs.

It is possible to use copyrighted software:

Search for a person on various social networks and informers, including OSINT VK, TikTok, Telegram, GetContact, and Instagram.

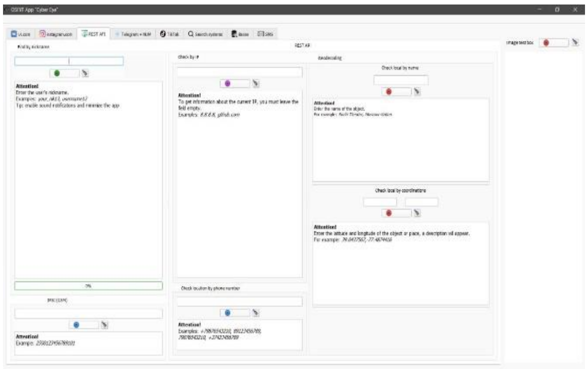
In addition to people, you can search for various geo data, base stations, and geo decoding.

Region identification by operator and domain and IP information.

Search by username is possible (returns a matching recursion).

Also check the image (if everything is fine, it will show the photo, if not, the file is suspicious).

The interface of the b-version of the software contains 7 tabs for searching for information and 1 for SMS in Fig. 1:



Attention!
Enter the user's nickname.
Examples: your_nik13, username12
Tip: enable sound notifications and minimize the app

Attention!
To get information about the current IP, you must leave the field empty.
Examples: 8.8.8.8, github.com

Attention!
Enter the name of the object.
For example: Bolshoi Theatre, Moscow station

Attention!
Enter the latitude and longitude of the object or place, a description will appear.
For example: 70.0437567, 77.4874416

Attention!
Example: 250012345678910

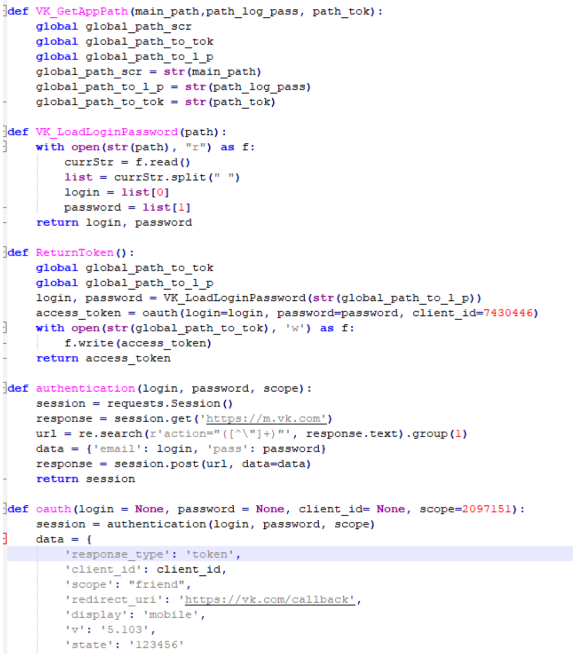
Attention!
Examples: +79876543210, 89123456789,
79876543210, +37423456789

Figure 1: Home screen interface of the application

Based on the analysis of open data, the author's software "Cyber Eye" can perform several tasks related to the selection, accumulation, and systematization of data to form a documentary evidence base for further judicial proceedings, and search for both war crimes and criminals.

For example, here is a screenshot of the code that allows you to search for a person through the VK platform to identify general information and family ties, general information for collecting a person's data in Fig. 2.

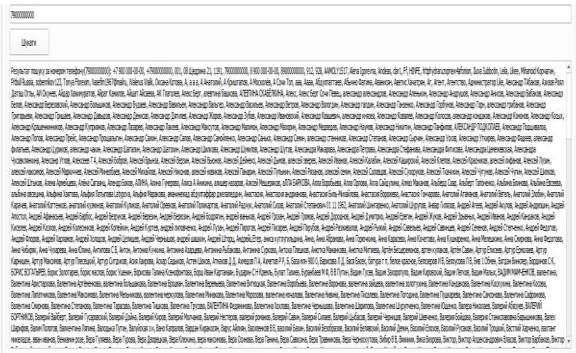
Social media platforms have become a valuable source of evidence for documenting war crimes, as they allow for the collection of real-time information and eyewitness accounts [13]. By analyzing social media posts, investigators can identify potential perpetrators and gather evidence to support court cases against them.



```
def VK_GetAppPath(main_path,path_log_pass, path_tok):
    global global_path_scr
    global global_path_to_tok
    global global_path_to_l_p
    global_path_scr = str(main_path)
    global_path_to_l_p = str(path_log_pass)
    global_path_to_tok = str(path_tok)

def VK_LoadLoginPassword(path):
    with open(str(path), "r") as f:
        currStr = f.read()
        list = currStr.split(" ")
        login = list[0]
        password = list[1]
    return login, password

def ReturnToken():
    global global_path_to_tok
    global global_path_to_l_p
    login, password = VK_LoadLoginPassword(str(global_path_to_l_p))
    access_token = oauth(login=login, password=password, client_id=7430446)
    with open(str(global_path_to_tok), 'w') as f:
        f.write(access_token)
    return access_token

def authentication(login, password, scope):
    session = requests.Session()
    response = session.get('https://m.vk.com')
    url = re.search(r'action="([^\"]+)"', response.text).group(1)
    data = {'email': login, 'pass': password}
    response = session.post(url, data=data)
    return session

def oauth(login = None, password = None, client_id= None, scope=2097151):
    session = authentication(login, password, scope)
    data = {
        'response_type': 'token',
        'client_id': client_id,
        'scope': "friend",
        'redirect_uri': 'https://vk.com/callback',
        'display': 'mobile',
        'v': '5.103',
        'state': '123456'
```

Figure 2: A snippet of code for searching through the VK platform

In addition, social media can be used to track the movement of troops and military equipment, providing valuable information about the development of a conflict. For example, identifying the identity of a person by recording the phone number of other people in Fig. 3.



Результат пошуку за номером телефону(79000000000): +7 900 000-00-00, +79000000000, [illegible]

Figure 3: The result of detecting the identity of a phone number recorded by other people

Although OSINT has certain limitations, it also has undeniable advantages that make it an important tool in modern warfare. One of the most important advantages is that OSINT provides more reliable and verifiable information than covert intelligence. This is because OSINT relies on publicly available information that can be verified and corroborated from multiple sources [1]. In addition, OSINT provides decision-makers with a wider range of information, which helps them make more informed decisions. This is especially important in modern warfare, where information overload can be a serious problem and quick decisions must be made based on incomplete data. Besides, OSINT can provide decision-makers with a more complete and detailed understanding of the battlefield and the enemy. This is because OSINT can provide insight into the social, cultural, and economic factors that shape enemy behavior [4]. Another advantage of OSINT is its cost-effectiveness. Compared to other intelligence-gathering methods, OSINT is relatively inexpensive and requires minimal resources. This makes it an attractive option for military organizations with limited resources [5]. Finally, OSINT provides a significant advantage in terms of resource management [14, 15]. By assuming responsibility for collecting and analyzing information from open sources, OSINT frees up resources that can be used for other intelligence-gathering activities [5]. In general, the use of OSINT in wartime provides military intelligence with several advantages over other intelligence-gathering methods that can help achieve decision-making superiority and gain an advantage over the enemy [6].

Another valuable application of OSINT for documenting war crimes in Ukraine is the analysis of satellite imagery [1].

Satellite imagery can provide important evidence of the destruction and damage caused by military operations, as well as the location of military objectives and troop movements. By analyzing satellite imagery, researchers can identify patterns of destruction and track changes in conflict over time. This information can be used to support prosecutions against those responsible for war crimes and to provide a more complete understanding of the conflict.

Cooperation with local civil society organizations and journalists is also an important aspect of documenting war crimes in Ukraine [16]. These groups can provide valuable field reports and first-hand accounts of the conflict, as well as access to local communities and sources of information [14, 17]. By working together, OSINT investigators and local organizations can collect and analyze evidence more effectively, increasing the likelihood of successful prosecutions of war crimes [18]. In addition, countering disinformation is an important area of OSINT, as propaganda can be used to legitimize violence and war crimes [13]. By detecting and countering disinformation, investigators can ensure that accurate information is used to bring perpetrators to justice and bring justice to victims [8].

Moreover, one of the necessary elements is the geodetic decoding of the mobile network area, including the detection of base station points and repeaters in Fig. 4.

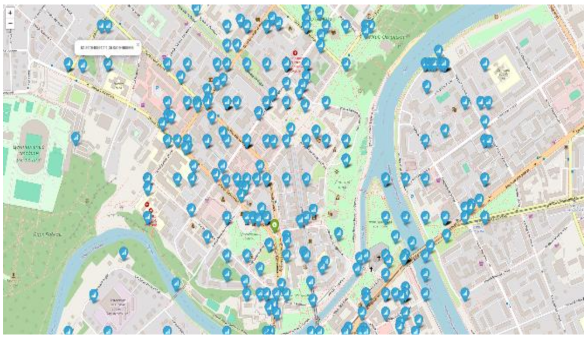


Figure 4: The result of detecting base station points and repeaters

Having identified the coverage area, you can track the location of a particular person through the network channels.

3.3. Problems and Limitations of Using OSINT in Documenting War Crimes

While OSINT can be a valuable tool for documenting war crimes in Ukraine, there are several challenges and limitations to consider. One of the main challenges is the need to verify information obtained through OSINT [19]. As with any source of information, there is a risk of false or misleading data, so it is important to confirm the accuracy and reliability of any data before using it as evidence. This process can be time-consuming and resource-intensive, requiring significant effort to cross-check information from multiple sources and ensure its reliability.

Another limitation of using OSINT to document war crimes is the need for access to reliable sources [11–21]. In many cases, this may require cooperation with ministries of defense or relevant UN bodies, which can be difficult to obtain. In addition, even if reliable sources are available, there may be restrictions on the amount and type of information that can be shared, especially when it comes to confidential or sensitive data. This can make it difficult to obtain a complete picture of the events in question, limiting the ability to fully document war crimes.

Thus, there are legal and ethical considerations that need to be taken into account when using OSINT to document war crimes [2]. For example, there may be concerns about privacy and data protection, especially when collecting information from social media or other publicly available sources. In addition, there may be questions about the admissibility of OSINT data as evidence in court proceedings, especially if it has not been independently verified or subjected to appropriate retention procedures. Thus, it is important to ensure that OSINT is used to document war crimes in a manner that is consistent with legal and ethical principles to avoid any potential challenges to its credibility and reliability.

In summary, OSINT plays a crucial role in documenting war crimes in conflict zones, including Ukraine. The use of social media, satellite imagery, and cooperation with local organizations and journalists have proven to be effective in gathering evidence. However, there are limitations to the use of OSINT, including the need to verify information, access to reliable sources, and legal and ethical considerations. Despite these challenges, the importance of OSINT in documenting war crimes cannot be overstated, as it provides valuable evidence to bring perpetrators to justice and seek justice for victims. As technology continues to evolve, OSINT will undoubtedly play an increasingly important role in documenting war crimes and human rights violations.

Potential limitations of using OSINT tools in wartime for military intelligence:

Although OSINT has become increasingly popular in recent years due to its ability to provide valuable information about potential adversaries, it is not without its limitations. First, like any intelligence-gathering tool, OSINT has limitations in terms of its ability to support conventional warfare and cyber operations. While OSINT can provide useful information, it is not always reliable or accurate, which can be a significant drawback in a wartime environment. In addition, OSINT can be vulnerable to disinformation and propaganda, making it difficult to distinguish legitimate sources from those that are intentionally misleading [7]. One of the most significant limitations of OSINT is its susceptibility to disinformation. This is because much of the information obtained through OSINT channels is publicly available, which means that it is more likely to be manipulated or distorted by disinformation campaigns [7]. Therefore, when using OSINT tools for military intelligence, it is important to be aware of these limitations and use them in conjunction with other intelligence-gathering methods to ensure that the information obtained is accurate and reliable.

4. Conclusions

The article theoretically reveals the methods of using Open Source Intelligence to track personal activities and presents the author’s software “Cyber Eye” for documenting war crimes through the analysis of social networks, cooperation with local organizations, and the use of satellite images. The functionality, advantages, and disadvantages of the developed software are analyzed.

In the process of modeling the application, three main OSINT functions were defined: identifying publicly available assets to find useful information, searching for relevant information outside the organization, and collecting and structuring the information received. In particular, OSINT: Recon-ng and Shodan simplify asset discovery and provide information on IoT devices and system vulnerabilities; DarkSearch.io helps to search for information on dark networks without the Tor browser.

The use of OSINT in Ukraine is appropriate for intelligence purposes and for documenting war crimes through social media analysis, cooperation with local organizations, and the use of satellite imagery. Prospects for using this type of tracking/intelligence can be useful for providing documentary support for court proceedings, identifying criminals, and tracking troop movements.

At the same time, despite the possibility of obtaining valuable data for military intelligence during conflicts, OSINT is vulnerable to disinformation, which can complicate the accuracy and reliability of information.

Prospects for further research are the implementation of best practices for integrating OSINT with traditional intelligence-gathering methods.

References

[1] H. Williams, I. Blum, Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise, RAND, National Defense Research Institute. (2018). doi: 10.7249/rr1964.

[2] M. Glassman, M. Kang, Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT), Computers in Human Behavior, 28 (2012) 673–682. doi: 10.1016/j.chb.2011.11.014.

[3] S. Minner, M. Va, Overcoming Information Overload: Open Source Intelligence in a Modern Threat Environment, DTIC (2018). URL: https://apps.dtic.mil/sti/citations/AD1177126

[4] A. Dupont, Intelligence for the Twenty-First Century, Routledge (2013). doi: 10.4324/9780203695685.

[5] I. Sutea, Tracking the Flow of Military Assets and Logistics for OSINT: The Case of the Syrian Civil War, Univerzita Karlova, Fakulta sociálních věd (2019). URL: https://dspace.cuni.cz/handle/20.500.11956/178282

[6] T. Potz, The Increasing Importance of OSINT as a Source of Intelligence, University of Zagreb. The Faculty of Political Science (2021). URL: https://repozitorij.unizg.hr/islandora/object/fpzg:1381

[7] M. Lakomy, Assessing the Potential of OSINT on the Internet in Supporting Military Operations, Bezpieczeństwo. Teoria i Praktyka 13 (2022) 297–309.

[8] V. Butuzov, D. Kovtonyuk, I. Luhovskyi, Peculiarities of the Organization and Conduct of Personal Intelligence by the Intelligence Bodies of the Formations of the National Guard of Ukraine During Participation in Repelling Armed Aggression, State Secur. 1 (2023) 13–20.

[9] Truth-Hounds.org, Documentation, Monitoring, Investigation (2023). URL: https://truth-hounds.org/

[10] J. Evangelista, et al., Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence, J. Appl. Secur. Res. 16 (2020) 345–369. doi: 10.1080/19361610.2020.1761737.

[11] Yahoo!, Europol Creates OSINT Group to Investigate Russian War Crimes, Yahoo! News (2023). URL: https://news.yahoo.com/europol-creates-osint-group-investigate-182812762.html

[12] P. Skladannyi, et al., Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 97–106.

[13] M. Astafieva, et al., Formation of High School Students' Resistance to Destructive Information Influences, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 87–96.

[14] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, no. 2 (2022) 197–206.

[15] H. Hulak, et al., Dynamic Model of Guarantee Capacity and Cyber Security Management in the Critical Automated System, in: 2nd International Conference on Conflict Management in Global Information Networks, vol. 3530 (2023) 102–111.

[16] D. Smiljanic, Development of the Croatian National Security Strategy in the Hybrid Threats Context, Croatian International Relations Review 80 (2017) 97–129. doi:10.1515/cirr-2017-0022.

[17] V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.

[18] V. Rodríguez, A. Moreno, Osint y Análisis Forense Para Combatir Bulos, Vulnerabilidad Digital, Desafíos y Amenazas de La Sociedad Hiperconectada 18 (2023) 45–60. doi: 10.2307/jj.1866697.7.

[19] D. Fernández-Rojo, Bilateral and Multilateral Operational Cooperation Among Frontex, EASO and Europol, EU Migration Agencies (2021) 114–157. doi: 10.4337/9781839109348.00012.

[20] Open-Source Intelligence, J. Japan Soc. Fuzzy Theory Intell. Inform. 34(4) (2022) 123–123. doi: 10.3156/jsoft.34.4_123_2.

[21] I. Kalpouzos, War Crimes, Int. Law. (2020). doi: 10.1093/obo/9780199796953-0199.