Advances in Science and Technology Research Journal

Advances in Science and Technology Research Journal 2024, 18(3), 123–139
https://doi.org/10.12913/22998624/186036
ISSN 2299-8624, License CC-BY 4.0

Received: 2024.02.10
Accepted: 2024.03.13
Published: 2024.04.20

Open Source Intelligence Opportunities and Challenges – A Review

Sabina Szymoniak[1*], Kacper Foks[1]

[1] Department of Computer Science, Częstochowa University of Technology, ul. Dąbrowskiego 69, Częstochowa, Poland

* Corresponding author's e-mail: sabina.szymoniak@icis.pcz.pl

ABSTRACT

Data files, photos, and videos on the internet are vast sources of information about the person who posted them. These files contain content about appearance, behaviour, views, and material status. Analyzing these files helps verify the accuracy of the content and helps verify the creation method. Social media platforms like Facebook, Twitter, and Instagram often post this information. Public databases provide information about enterprises, corporations, and public figures, enabling access to government trips, scientific articles, and company reputations. These resources help in understanding potential collaborations and identifying potential partners. Open-source intelligence (OSINT) is a collection of tools and methods for extracting information from publicly available sources. It helps verify the accuracy and authenticity of information, as seen in the FBI's 2020 investigation of a Philadelphia woman involved in protests and preparing precise attacks like spear phishing. In this manuscript, we present an up-to-date overview of research that uses open-source methods and techniques. We will concentrate on the tools and methods advancing the cybersecurity industry. Studying the manuscript of OSINT opportunities and challenges can help readers understand the state of the art in theory and practice. We will also highlight the future directions and requirements for OSINT methods and the newly designed tools using these methods.

Keywords: open-source intelligence, OSINT tools, OSINT techniques, social media.

INTRODUCTION

Every data file, photo, video or note posted on the Internet is a vast source of information about the person who posted it. Files (text, graphics, audiovisual) primarily contain content that may provide information about someone's appearance, behaviour, views or material status. In turn, a thorough analysis of the content of the information posted in this way may also help verify the accuracy of the content posted. For example, confirm that our friend went on an exotic vacation and did not post a doctored photo on one of the social networking sites. In addition, the files contain metadata, which, among other things, enable verification of the manner and time of their creation. We post much of this information on social networks like Facebook, Twitter or Instagram [1, 2]. On the other hand, publicly available databases contain information about enterprises, corporations or public figures. From the Internet, we can find out what trips the head of our state is preparing for. Scientists publish a list of their scientific articles and interests so we know with whom and on what topic we can discuss. We can also find the reputation of a particular company we want to cooperate with.

It is worth noting that posting various information on the Internet has good and bad sides. The advantages and disadvantages of sharing information online can be considered on many levels. The mere possession and transfer of information are beneficial because, thanks to the information, we can learn something, help someone, get help, show off, express our opinion, and make new friends and relationships [3, 4]. Nevertheless, on the other hand, publicly posting information that we are on holiday abroad may allow thieves to rob our place of residence. By informing about the purchase of a new car, we

can provoke its theft, but by posting information about the theft, we can contribute to finding the perpetrator. If someone goes missing, information posted on social networking sites can also contribute to finding that person. The same information can hurt our lives because the information provided is not true. Similarly, opinions posted on the Internet can be harmful due to the desire for revenge and thus spoil someone's reputation. Publicly available information is also used as part of an intelligence operation, such as the search for evidence of a crime [5].

Obtaining information from publicly available sources is called Open-Source Intelligence (OSINT) [6, 7]. It is a collection of tools and methods that allow us to download and process data to extract even more information. These methods will also allow us to verify the accuracy of the information posted and the authenticity of photos or videos on the web [8, 9, 10]. Similarly, as in the case of posting various information on the Internet, OSINT techniques are not always malicious. They are used for secure purposes, such as threat analysis and cybersecurity. However, in the hands of dishonest individuals, information collected using OSINT techniques can be used to harm others. Therefore, individuals and organizations must be aware of the potential risks associated with excessive disclosure of information online. It was with the help of OSINT methods that in 2020, the FBI found a woman from Philadelphia who participated in the protests after George Floyd's death and set fire to two police cars [11].

On the other hand, computer hackers use OSINT methods to carry out various attacks, especially in the information-gathering phase of the reconnaissance stage. For example, hackers can use information collected using OSINT to personalize phishing attacks. A phishing attack can be more credible and effective by collecting data about the victim, such as name, surname, position or interests. Also, hackers may carry out spear phishing, an advanced form of phishing in which hackers target a specific person or organization. Information gathered through OSINT can help personalize an attack, increasing the chances of success. OSINT techniques can gather information about a target, which is then used to manipulate the victim. For example, hackers can use information about professional or personal relationships to gain the victim's trust. Before launching attacks on IT infrastructure, hackers often conduct a reconnaissance phase using publicly available information such as WHOIS data, DNS records, and information about organizational systems. Hackers can use OSINT to gather information about the physical location where they want to launch an attack. This may include building plans, security system diagrams, or employee data [12, 13].

It is worth mentioning that the evolution of OSINT in the context of cybersecurity highlights its key role in identifying, analyzing and countering threats in a dynamic cyber environment. Constant adaptation to changing challenges and innovation in this field is essential for adequate protection against cyber threats. With the development of the Internet and globalization, the amount of information available to the public has increased significantly. OSINT began to be used to monitor threats and track activities in cyberspace. As technology advances, the nature of cyber threats has changed. More advanced attacks emerged, and hackers began to use publicly available information to personalize and target attacks. OSINT has become a key tool in the reconnaissance phase of cyberattacks. Before an attack, hackers collect information about targets, their infrastructure, employees and technologies that may be used in the attack. Security agencies and cybersecurity companies use OSINT for threat analysis. By monitoring activities in cyberspace, you can identify potential attacks, analyze hacking techniques and develop defence strategies. The complexity of cyber-attacks continues to increase, and hackers are using increasingly advanced techniques. OSINT provides the tools to understand and predict such attacks, which is crucial for effective defence. OSINT has contributed to the growth of a knowledge-sharing culture and cooperation in cybersecurity. Security teams share information about new threats to protect against attacks effectively. With the increase in the use of OSINT, privacy challenges have also arisen. Public awareness of the need to share information responsibly online has increased, impacting how individuals and organizations use social media and other public sources. Law enforcement agencies and regulators use OSINT to identify and prosecute cybercriminals. Analyzing public information can help track down perpetrators and understand the motivations of attackers [13, 14].

Motivations and contributions

Access to the Internet gives us a vast data space that we can use. All data provided, including by us, can be used for various ethical and

unethical purposes. When collecting data, OSINT methods and tools allow for in-depth analysis. These methods and tools provide ethical investigators many opportunities to help others and enable attackers to obtain confidential information and further nefarious activities.

In this manuscript, we present an up-to-date overview of research that uses open-source methods and techniques. We believe that studying the manuscript of OSINT opportunities and challenges can help readers understand the state of the art in theory and practice. We will also highlight the future directions and requirements for OSINT methods and the newly designed tools using these methods.

Methodology

During our research, we collected articles using various search engines (such as Google Scholar, Web of Science, Scopus, IEEE Xplore, and DBLP). We analyzed references from found articles and citations to these papers from 2020–2023. We aimed to compose the most complete and up-to-date review of open-source intelligence opportunities and challenges. We mainly used the keywords OSINT and Open Source Intelligence and their combinations with expressions: tools, opportunities, and solutions.

Organisation

The rest of this paper is organized as follows. Section 2 describes the Open-Source Intelligence purposes and tasks. Also, it describes spear phishing attacks, in which the attackers use the OSINT method to possess information about the target. Section 3 describes tools used during OSINT investigations. Section 4 describes and discusses the current OSINT opportunities, solutions and challenges. The last Section summarizes the whole manuscript and discusses open-source intelligence opportunities, challenges and future directions.

OPEN-SOURCE INTELLIGENCE

Open-source intelligence relies on legally and ethically gathering, processing and correlating information from publicly available data sources. The goal of OSINT is to obtain data and information legally and ethically, using open sources such as websites, social media, public documents, press articles and other publicly available resources. However, OSINT practice should always respect privacy rights and principles and follow applicable regulations.

Data sources may be from social networking sites, media, online scanners, and other publicly available databases, such as public administration or commercial data [15]. OSINT techniques can be used to obtain information about individuals and entire corporations or countries. When obtaining data within OSINT, illegal activities such as password cracking, impersonation or manipulation are not used [16, 17]. Using OSINT techniques enables the gathering and processing of information about the chosen target [18].

OSINT is used in many situations, such as national security, law enforcement, or business intelligence. It is most often used in business activities when enterprises seek information about another enterprise's legal, financial, commercial and economic situation to assess the risk of cooperation with it. There are also situations in which government bodies use OSINT techniques to study the current political situation and create a strategy for governing the state. In this way, crime-fighting authorities learn about the functioning of criminal groups, terrorist organizations [19], and specific people [20, 21, 10]. Figure 1 summarizes prominent Open-Source Intelligence use cases.

Open-source intelligence methods are used in cybersecurity as well as by computer hackers. Reconnaissance performed using OSINT methods is usually the first step in penetration testing. The test result makes it possible to build a clear picture of the tested object and partially detect significant irregularities [22].

Computer hackers' use of OSINT methods makes it possible to extract much information about their victims from publicly available sources. Here, the most significant mine of knowledge is social networking sites, where users share vast amounts of private information. The information provided in this way can make it easier to guess the password, which was created based on the date of birth or children's names. Meticulously collected information can allow attackers to conduct precise attacks such as spear phishing [23].

OSINT methods meet with verifying the information to detect and avoid replicating fake news and conveying false information. OSINT employs critical thinking, searching and verification techniques to assess the credibility and reliability of information gathered from publicly available sources. Firstly, OSINT analyst

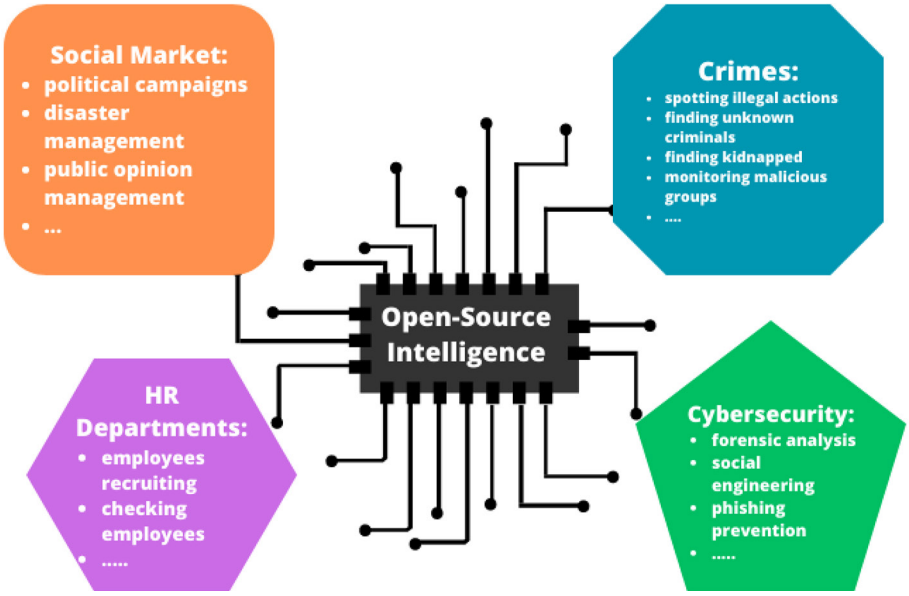

Figure 1. Main open-source intelligence use cases

thoroughly examine the source of the information (investigating the website, author, or organization behind the information to assess their credibility and potential biases). So, if various reliable outlets report a piece of information, it is more likely to be accurate. However, if conflicting information exists, further investigation is needed to determine the most likely explanation. The critical analysis of the information content is also an effective OSINT method. Logical inconsistencies, factual errors, or emotional manipulation tactics are often employed in misinformation.

Ethical and legal aspects

Open-source intelligence uses publicly available data, so it is entirely legal. However, it can also be used in an unethical way. The first example may be the use of data that has been made publicly illegally. An example of such data may be data from leaks. Be ethical when investigating, and do not overstep other people's boundaries. This type of activity is called stalking and is punishable in many countries.

Spear phishing

Spear phishing is a type of phishing that targets specific people or groups. Unlike traditional phishing, which involves sending mass emails to random recipients, spear phishing is more personalized. The attacker collects information about their targets, such as their names, job titles, companies, or interests. It then uses this information to create an email that appears to come from a trusted source, such as a colleague, customer, or government agency.

In 2021, 51% of social engineering attacks were spear phishing, and the most popular attacked company was Microsoft [24]. This is a particular type of phishing attack. The main difference between phishing and spear phishing is the specially selected target group of the attacker. The attackers want confidential information such as passwords, user data or company secrets. The high efficiency of the attacks performed features it. Spear techniques are used in 91% of attacks [25]. The spear phishing attacks use open-source intelligence to gather information about individuals and organizations [26, 27, 28, 29].

OSINT techniques are being used to gather more information about victims of spear phishing attacks. This action is intended to personalize the attack better and increase the chances of a successful attack. OSINT techniques are being used to gather more information about victims of spear phishing attacks. This action is intended to better personalize the attack and increase the chances of a successful attack.

Example of spear phishing

Figure 2 shows the typical anatomy of spear phishing attacks. This type of phishing attack is heavily correlated with SocMINT because they are full of information about people, and the

Figure 2. Typical anatomy of a spear phishing attack

victim's profile can be created. Figure 3 shows a real example of spear phishing with a political thread. Hackers are expanding their attacks on Tibetan activists and employing increasingly sophisticated virus delivery mechanisms. Following these spam efforts, Fire Eye analyst Alex Lanstein has discovered an unusual example of such a malicious email. The attacker gathers much information from the victim's social media. The attachment of an email message had a suspicious file with backdoor malware. The attacker encouraged the victim to open the infected attachment [30, 31, 32].

OSINT in capture the flag competitions

Capture the flag (CTF) in cybersecurity is a special competition designed to test competence and knowledge about cybersecurity. Competitors can try themselves in various challenges of different difficulty levels in different categories, such as web, cryptography, and forensics, but increasingly in the OSINT category. The competition is to find and enter the right flag, which we need to get differently depending on the category of the challenge. The confessions themselves in the OSINT category can take different forms. They often require knowledge of the field and familiarity with special tools, which will be discussed later in this article. Tasks in the OSINT category can vary, depending on the creator's creativity and the difficulty level. We often need to find where the photo was taken or information regarding the people in question.

Operational security

Operational Security is also known as the shorter version of OPSEC. The US Army pioneered this concept. This term refers to practices and activities that protect information privacy, confidentiality, and Security. The main goal of OPSEC is to minimize the risk of revealing key information that potential adversaries could use to harm a given enterprise, organization or institution. OPSEC practice analyzes potential threats, identifies key information to be protected, and introduces measures to minimize risk. OPSEC elements include information access control, confidentiality rules, information manipulation, masking activities and disinformation. In the digital realm, OPSEC can also address computer security and cybersecurity. In short, OPSEC is an approach to maintain secrecy and security during operations, considering various threats and potential attack points [33].

TOOLS AND FRAMEWORKS

For every new OSINT investigation, the best practice is to use a fresh virtual machine with


From: [redacted]
Hide
Subject: Spearphishing with malicious attachments
Date: April 6, 2012 12:19:36 AM PDT
To: victoria.2006@yahoo.com

2 Attachments, 716 KB Save Quick Look

Hello,

My name is [redacted] with a security company called FireEye. We deal with targeted attacks against large organizations that come in via email attachment or email links. Essentially, I do malware analysis for a living.

If I have you on the BCC list, you have submitted more than one targeted malicious attachment to virustotal over the past few months. Please understand that when you send a file to VT, many researchers like myself get a copy of the email in order to test our products.

I would love to write a blog entry at my corporate site about a few of these attacks and mention you by name. Keep in mind I already have this information, but I would like your permission in addition, as it might not have been an IT person who uploaded the file, not you specifically.

Thanks in advance,

[redacted]

Direct: +1 (860) 625-4277

Email: [redacted]

FireEye

Malware Protection System

http://www.FireEye.com

Figure 3. Typical anatomy of a spear phishing attack

special built-in tools. The most popular operating system for OSINT investigations is Kali Linux, which is also very popular for penetration testing purposes. Some alternatives for Kali Linux exist, e.g., Buscador, Parrot OS, or Trace Labs OSINT VM. The virtual machine without any previous signs of use is the best practice because of the more universal results of every new investigation. Virtual machines are easy to use and more flexible than standard machines. Many preinstalled and ready-to-use tools can speed up the investigation process. Virtual machine snapshots are very helpful, allowing us to perform new investigations without reinstalling, as we can restore the machine to a fresh state. In addition, investigators can edit or install more tools on snapshots and create their workspace for investigations [34].

These are certainly only some of the available categories of tools for OSINT. Some of these tools may no longer be available after some time, or new and better replacements are developed in their place. There are many websites with collections of tools for OSINT. Examples of such sites are OSINT Framework [35] or Awesome OSINT on GitHub [36]. It is worth noting that many tools or data sets may only be available in certain countries or regions:

- search engines – are the fundamental tools used in OSINT investigation. They are often the first tool used for each investigation before using more complex and advanced tools. The result may be different depending on the language and location of the search. Some search engines have a built-in language or country search filter. The most powerful thing in search engines is operators. They are symbols and keywords that can narrow the investigation but may differ in each search engine. The list of the operators is very long. It is worth remembering that search engines produce the most universal results when they do not have the user's previous activity;
- image search engines are similar to search engines, only that of images. Modern search engines allow not only whole images but also their elements dynamically, allowing for even

better search results. Many search engines have built-in image search engines, but also they are standalone tools. With these tools, it is possible to search for exactly where a particular photo was taken, or it is possible to find out where that photo can be found on the Internet.

- maps – these tools are used for geographical and graphical searches of places. In some tools, we can also find reviews of specific places, which can be used to see if certain people have been to a particular place. In the case of web mapping, it is worth to mention about the weather services. This application shows much information about the weather worldwide. It can be helpful, for example, in analyzing a web camera view. They may differ in accuracy or timeliness. Some maps may have hidden objects, such as military bases or other strategic points for a country. That is why it is good to use multiple tools during each OSINT investigation and compare the results with each other;
- metadata – metadata is additional information on the file. They can include much information like date and time, creator information, device information, GPS coordinates, resolution, frame rate, codec and others. It depends on the file type and with which the software and hardware were made. This tool can also remove or edit the metadata information;
- network – Web resources have much information. Using tools from this category, we can collect much information about the network infrastructure, such as IP address, DNS servers, SSL/TLS, IP localization ISP, and Whois data. Tools in this category are used not only to conduct OSINT investigations but also by cybercrime investigators or web security researchers;
- SocMINT (Social Media Intelligence) – this category is specifically for searching for information about people on social media. The society leaves much information in those services, which can be collected and further searched. Such data include personal data, images, locations, education, friendships, interests, and other activities. Some tools allow detecting and searching for photos of faces and searching for similar ones on other social media. Company recruiters also use tools in this category to get to know job candidates better;
- OSINT Automation – to automate OSINT investigation, special tools aggregate results from many different sources and tools. Often, these tools combine listed tools into one unit and much more. Using automation during an investigation can save much time and increase the scope of the investigation. Some of them require paid licenses or paid APIs. OSINT operating systems have preinstalled many tools (summarised in Table 1).

Table 1. Example OSINT tools

Category	Tool name	Description	Effectiveness	Limitations
Search engine	Yandex	Russian search engine, with which it is possible to obtain very interesting search results. It will be very good not only for conducting investigations in Russia but also because the operators of this browser may work differently from other devices of this type.	Returns very relevant search results.	Some results it can only return in Cyrillic
Search engine	Baidu	This search engine is equivalent to Google but for China. It will be a great tool to start an investigation within China.	The most popular browser in the Chinese market, making it give the best investigation results for that language.	Works only for Chinese language.
Image search engine	Bing Images	One of the most popular image searches besides Google Images. The search results of this tool are really good, which is due to its very large database of images. This image search engine also has many advanced filters, which can be very helpful during the investigation. A significant advantage is the ability to search only for an element of a given photo. Bing images are often integrated with other Microsoft products, like the Edge web browser. Currently, it is one of the best tools for finding images.	Very good results can be obtained by searching for image fragments.	Only for reverse image search.

Maps	satellites.pro	This map aggregates views from different sources (Apple Map, OpenStreetMap, Google Map, and Yandex Map) into one web application. This tool makes it easy to switch between maps from different sources and compare results and sources quickly. It has built-in weather and measures the distance between points.	Very good efficiency by comparing results from different maps.	Some maps do not have full functionality from this site.
Network	Shodan	Specialised web application with a search engine focused on searching networked devices and collecting information about them. The website is gathering much information. For example, IP address, open ports, domains, geographic location, etc. It depends on the type of device and how much-publicised information it has [37].	The most effective engine for searching information about network and network devices.	It does not have a free version.
Metadata	Exiftool	It is a small tool which extracts metadata from different types of files like JPEG, TIFF, PNG, MP3, MP4, AVI, PDF and many others. Metadata is additional information on the file. They can include much information like date and time, creator information, device information, GPS coordinates, resolution, frame rate, codec and others. It depends on the file type and with which the software and hardware were made. This tool can also remove or edit the metadata information. The creator of these tools is Phil Harvey [38].	Allows you to get information on metadata from many different file extensions.	Only for extracting metadata from file.
SocMINT	WhatsMyName Web	A powerful tool for finding usernames and logins in various applications and services WhatsMyName has a large database. The tool allows us to search for sites where the same username also appears. Which helps associate a person with various applications. The more unique the username, the better the result.	Very effectively searches multiple sites for the same usernames.	Only for searching usernames.
OSINT Automation	TheHarvester	Open-source tool written in Python focuses on finding and analysing information about companies and organisations, including nonprofits. It is used not only for open-source intelligence but also for scientific research or penetration testing. The tool provides modules such as Bing, duckduckgo, Anubis, brave, Rocket Reach, Hunter or GitHub-code. In 2022, the Google module was blocked and removed from the tool. The best alternatives for Google are Bing or Rocketreach. The tool can gather information like e-mail addresses, subdomains, and IP addresses. The results depend on the available information and used modules and limits. Some modules of this tool require API keys, and some are paid. Christian Martorella created the tool.	Very good at finding information about companies.	Additional paid API tokens are required for full functionality of this tool. Does not work well for finding information about people.
OSINT Automation	Maltego	One of the most popular OSINT Automation tools. It is a sophisticated tool that searches multiple data sources and presents the results in graphical form. The result of the investigation can be presented in the report version. The tool is free for the community version. A higher version of this product requires a paid license. The tool also has a special license for companies.	The best link analysis software used for OSINT and forensics.	Limited free version, and very expensive paid versions.

OSINT RESEARCH OPPORTUNITIES AND SOLUTIONS

As mentioned, OSINT is used in many domains [39]. Gordon in [40] highlights the impact of OSINT methods in criminal investigations (also, to evaluate wildlife crimes [41]. Even though these methods help to find criminals, they also cause data privacy problems. Thus, Osterritter et al. in [42] highlighted the importance of using dynamic network analysis and social network analysis because such analysis might show people and organizations trying to advance or shape narratives in ways that might not be immediately apparent to casual observers.

Alquwayzani et al. in [43] focused on the connection between the dark web and OSINT. Mainly, the dark web creates anonymous discussion forums, websites, e-commerce stores and blogs. The dark web includes legal and illegal content [44]. Alquwayzani et al. highlighted that we can find many interesting information for OSINT investigations on the dark web. Law enforcement and security experts can monitor the dark web to learn more about illicit activity and take the necessary precautions to stop or lessen it. Monitoring the dark web, however, has some drawbacks and difficulties. The main obstacle is the requirement for specific knowledge and technical proficiency to efficiently and safely explore the dark web. Additionally, those people or organizations who are unfamiliar with the nuances of the dark web run the risk of being exposed to potentially harmful or unlawful content. Also, OSINT techniques can be used to gather Tor onion addresses [45] or to research terrorism [46][47][48].

Also, Wangchuk et al. in [49] focused on the dark web. The authors proposed a Python-based framework for investigating the dark web. This tool is used to gather information from the dark web and turn it into intelligence that can be used with OSINT tools for further research. The proposed tool successfully scraped the hidden service URLs in the experimental implementation of the framework, harvested the email addresses of dark web users, and fed suspicious email addresses into OSINT tools for gathering intelligence to de-anonymize. The authors summarized that investigators can efficiently use the proposed framework to identify and de-anonymize suspect users from the dark web.

Yu in [50] focused on SOCMINT, which stands for social media intelligence, composed of computer forensic techniques used for intelligence gathering on social media platforms. The author used these techniques for cyber profiling and prediction of political orientation. Yu concluded that people's political opinions are not always consistent, and their political orientation might not be unchangeable. When analyzing SOCMINT, it is crucial to note any inconsistency and shift in attitude, which is impossible to capture when analyzing aggregate data.

Sasaki et al. in [51] used OSINT-based profiling to identify individual attackers visiting honeypots of connected infrastructure. Their method identifies attackers. These attackers were IT and security experts or employed by security, IT consulting, or engineering companies. The attackers publicize vulnerability exploits and malware, engage in aggressive activities, and have a particular interest in the system. The study concluded that it is possible to identify and profile these honeypot visitors. Lohar et al. in [52] proposed AutOSINT. This cutting-edge footprinting software uses artificial intelligence and machine learning techniques to extract valuable information about target victims using OSINT APIs. The software provides a user-friendly GUI, allowing users to interact and input requirements to obtain essential details like location, phone numbers, and domain information. AutOSINT streamlines information gathering by automating data retrieval from various sources, saving time, effort, and resources. This OSINT tool enhances intelligence gathering and investigation processes.

Dale et al. in [53] proposed an AI-based scheme to automatically extract information from Twitter, filter out security-irrelevant tweets, perform natural language analysis, correlate tweets, and validate information. This scheme can help security operators prioritize vulnerabilities and provide insight into ongoing events. Similar research was provided by Reyes et al. [54].

Suryotrisongko et al. in [55] used OSINT and explainable artificial intelligence methods for botnet domain generation algorithm (DGA) detection. They evaluated five machine learning methods using 55 botnet family datasets. Based on this research, the authors proposed a new model for botnet DGA detection. To combat doubt about the model's output and improve system confidence, open-source intelligence and explainable artificial intelligence approaches like SHAP [56] and LIME [57] were merged. The temporal

complexity of generating the features and the model's weak susceptibility to attacks from Mask botnets were further drawbacks of the offered frameworks. Fauziyyah et al. in [58] combined steganography and OSINT methods to analyze and decode images in social media to uncover hidden messages and protect sensitive information. Their tool can be used for intelligence gathering and secure communication. Also, they analyzed malware and OSINTs to determine the best OSINT for detecting malicious URLs and files.

Duitsman et al. in [59] employed OSINT tools to locate radioactive sources outside regulatory control. They noticed that open-source data could be a priceless addition to national inventories of radioactive sources, even though it cannot wholly replace more conventional techniques. An organizational centre for data and analysis is located at a place where radioactive sources are allegedly present. Several forms of data are used to learn about the facility, including satellite and ground truth imaging, academic and grey literature, news reports, and press releases, while social media details present and former staff. Guo et al. in [60] [61] noticed that cyberattacks have become more sophisticated and challenging to solve. They presented a framework for threat intelligence extraction and fusion that combines cybersecurity entity-relation triples from structured and unstructured data, constructing the Cyber Threat Kit. The joint model uses deep learning techniques to extract entities and relations simultaneously, outperforming traditional pipeline models. The lightweight method optimizes features of the cybersecurity corpus. A similar research was conducted by Shamunesh et al. [62].

Melshiyan et al. in [63] demonstrated how OSINT techniques can conduct an information security audit and potentially find weaknesses in an organization's information and telecommunication networks. The authors showed the possibility of finding restricted access information hidden within the organization's information resources and inaccessible through regular search techniques. Thanks to the mentioned methods, we can locate non-indexed files that include personal information or know-how and are not meant for open access by unauthorized individuals. They can be used in addition to standard audit methods to offer information on routes of sensitive information leakage that are difficult to identify during a company's routine audit process for information security needs. Based on the findings, suggestions were made to enhance the procedures for auditing businesses' information security by using information-finding techniques. Also, Decusatis et al. in [64] focused on auditing using open-source intelligence.

Al Mahmeed et al. in [65] proposed the Eagle-Eye tool, an Open-Source Intelligence tool for detecting IoT devices. The authors integrated this tool with the Shodan search engine. Companies, clients, and researchers can use this application to automate finding and looking for various IoT device statics that can be used and studied to harden these devices.

Saraswathi et al. in [66] noticed that ethical hackers become lazier and stop manually conducting each check, so recon automation is becoming more and more necessary. They provide a recon framework to improve the recon penetration testing process and make it simple and quick. The mentioned tool automates the time-consuming process of information gathering. It only requires the primary top-level domain of the organization as input. The output of this framework is created in the format and can be handled by other tools to further filter the data under the ethical hacker's requests and needs. Marinho et al. in [67] employed MITRE ATT&CK framework and OSINT methods for characterization and profiling the identified threats, including their intentions and goals. The authors proposed an automated cyber threat identification and profiling system based on the natural language processing of Twitter messages. The goal is to extract valuable information about emerging threats on time by mapping tweets to real threats described in the MITRE ATT&CK knowledge base. The system uses this evolving knowledge base to train machine learning algorithms, leveraging the efforts of the cybersecurity community to profile identified threats in terms of their intents.

Also, San Biagio et al. in [68] noticed that social media platforms enable interaction between individuals and organizations, allowing them to share knowledge, interests, and ideas while integrating them into daily life. Thus, they can be valuable tools for criminals to commit various crimes, including terrorism and cybercrime. The authors proposed a framework for threat intelligence that uses artificial intelligence methods to analyze open-source intelligence data and extract practical threat intelligence. Elmas et al. in [69] noticed that malicious users called trolls use social media to become famous. So they publish disparaging remarks

under YouTube videos, on forums, and posts on blogs and other social media sites to intentionally insult, annoy, or actively assault others. The authors proposed an OSINT-based tool for determining why an account has gained popularity. This tool helps users identify rogue accounts that have unnaturally amassed a large following and separate these accounts from those that obtained popularity and followers legitimately.

Similar research was provided by Mahaini et al. in [70]. The authors focused on detecting cybersecurity-related Twitter accounts and different sub-groups. They proposed a set of machine learning-based classifiers for identifying accounts related to cybersecurity on Twitter. These classifiers include a baseline classifier for identifying accounts related to cybersecurity generally and three sub-classifiers for identifying accounts related to individuals, hackers. Nobili et al. in [70] focused on European violence against workers. They noticed that this problem requires a combination of safety and security perspectives. The authors proposed a framework to collect evidence from multiple sources, including mass media and social networks, to provide a consolidated overview of the phenomenon. The mixed strategy combines qualitative and quantitative information, including Internet data.

Daskevics et al. in [72, 73] considered testing OSINT sources to detect their vulnerabilities. The authors proposed a non-intrusive tool for testing open data sources to detect vulnerabilities. This tool inspects predefined data sources like MySQL, PostgreSQL, MongoDB, Redis, Elasticsearch, CouchDB, Cassandra, and Memcached to assess their vulnerabilities and extent. It analyzes unprotected data sources and IP ranges, allowing for a comprehensive analysis of potential threats. The tool covers 8 data sources, including rational databases, NoSQL databases, and data stores, and is easily scalable. Karthika et al. in [74] proposed that NoRegINT. This tool is used to compile data regarding the Pulwama attacks [75] in an organized way and make deductions about data volume, general public opinion, and the influence of a specific hashtag.

Abdullah et al. in [76] proposed a methodology for determining which OSINT tools best address particular issues. The suggested framework offers tools based on MIME types or sophisticated search capabilities and is user-friendly. Subject matter experts have examined the framework, showing it to be a priceless source for tool recommendations for end users. Grine et al. in [77] proposed a method for accessing website material specific to a particular domain by leveraging social media networks as a portal. It starts by locating pertinent profiles, gathering links posted in posts to associated web pages, and then extracting and indexing the data acquired. The tool created using this methodology was tested for a case study in the area of human trafficking, specifically in sexual exploitation, and the findings were encouraging and suggested that it might be used in a real-world situation.

Seo et al. in [78] tried to improve the efficiency of defensive deception technology within organizations by proposing an open-source intelligence-based hierarchical social engineering decoy (HS-Decoy) strategy. The strategy considers the organization's fingerprint and proposes a loosely proactive control-based MTD strategy based on competitive exposure of OSINT between defenders and attackers. The proposed deception concepts reduce total attack efficiency by 287%, artificial deception efficiency by 382%, and increase deception overhead rate by 174%. The combination of HS-Decoy and LPC-MTD is introduced for organizational-specific optimization. The study aims to advance the HS-Decoy and LPC-MTD-based combined model into an international standard-based complex architecture characterized as game theory. Drichel et al. in [79] focused on phishing prevention techniques. They proposed a new pipeline that addresses this issue by monitoring Certificate Transparency logs during website preparation. The pipeline includes dataset creation, training, and classification of Certificate Transparency logs, allowing easy exchange of classifiers and verification sources. The pipeline has been tested on various classifiers and has potential for future improvements.

Khan et al. in [80] noticed that open-source intelligence is a rapidly growing field in security and intelligence involving collecting and transforming internet-based data into actionable intelligence. They proposed the system to manage open-source intelligence data and provenance information, enhancing efficiency and supporting intelligence-led security decision-making. The system allows for tracking requests, ownership, analysis, and delivery of intelligence products, reducing costs and improving operations. The authors suggested that the open-source intelligence company involved in this project must understand its data holdings and comply with General Data

Protection Regulation obligations. Also, many researchers (for example [81–85]), used OSINT methods and tools for emotional analysis, risk perception and mental health analysis during COVID-19 pandemic. This research was mainly based on social media analysis.

RECAPITULATION

Table 2 summarises OSINT's applications and solutions. The *Type* column refers to the areas into which we have divided all solutions. Column *Applications* refers to the issue solved using OSINT methods and tools. Column *References* points to cited publications.

We divided the research into four groups. CRD means cyberattack recognition and defence. This group refers to research focusing on cyberspace problems, threats, vulnerabilities and attacks. SMP means social media-based profiling. This group refers to research that uses OSINT techniques to collect social media user data. OM means OSINT management. This group refers to research that focuses on OSINT's tools verification. The last group, Other, refers to the rest of the discussed research that can not be included in other groups. Figure 4 summarises the number of articles related to OSINT in 2020–2023 prepared using the google.scholar.com database. The summary includes the division into the previously mentioned categories. We can observe an increase in interest in OSINT from 2022.

Open-source intelligence has many opportunities in which it can be applied. We observed that most OSINT solutions are connected with cyberattack recognition and defence. Also, we noticed that these solutions had a strong connection with

Table 2. Summary of OSINT's research applications and solutions

Type	Application	References
CRD	Dark web monitoring	[43][49]
	Gather Tor onion addresses	[45]
	Identify individual attackers visiting honeypots	[51]
	Domain generation algorithm detection	[55]
	Threat intelligence extraction and fusion	[60][61][62]
	Conducting an information security audit and potentially finding weaknesses	[63][64]
	Penetration testing automation	[66]
	Characterization and profiling the identified threats	[67]
	Detecting cybersecurity-related Twitter accounts and different sub-groups	[70]
	Compile data regarding the Pulwama attacks	[74]
	Phishing prevention	[79]

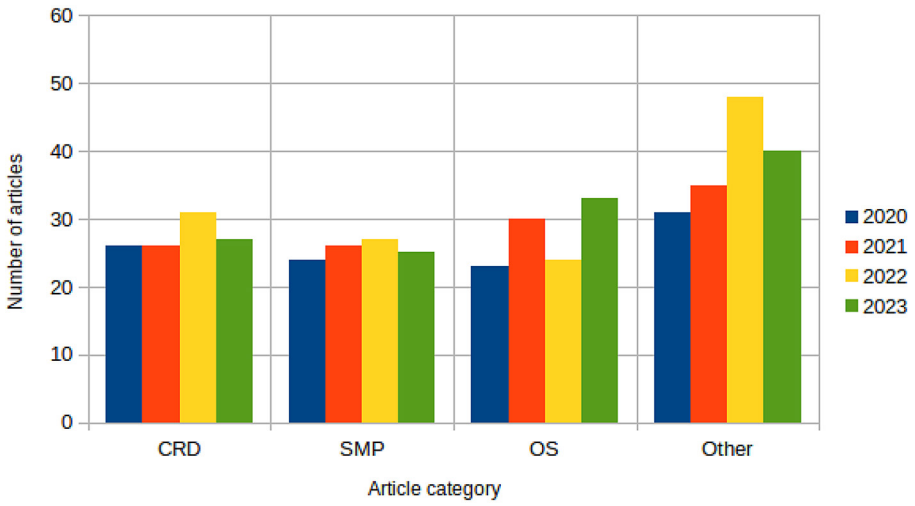

Figure 4. Summary of the number of articles related to OSINT in 2020–2023

Social Media group solutions. The first group was concerned with detecting and solving cyberspace problems to increase Internet users' security. However, these solutions used social media to gain the necessary knowledge, for example, about hackers. The solutions from the Social Media group are also aimed at security because they focus on the dangerous activities of other users, which may result in human trafficking or users' loss of privacy. The solutions from the other two groups were connected with security, but in different aspects, for example, OSINT source, environmental, and mental or employment security.

In security, OSINT plays an important role, enabling the collection of essential data for threat analysis, monitoring competitors' activities, and supporting investigative activities. Based on the overviewed research, we can assign the following trends related to OSINT security. The first is connected with automation and Artificial Intelligence. The rise of automation and Artificial Intelligence enables more efficient processing of large volumes of OSINT data. Artificial Intelligence algorithms can help identify patterns, classify information, and respond more quickly to potential threats. Next, due to the vast amount of OSINT data available, big data analysis tools and techniques are becoming increasingly important. They allow for more effective filtering, analysis and extraction of valuable information from large data sets. Also, over time, more and more information becomes available online. Therefore, OSINT monitors and analyses social media, online forums, blogs, and other publicly available sources and possesses a lot of data. As mentioned, OSINT plays a key role in monitoring the activities of cybercriminals. Analysis of cybersecurity threats using information obtained from open sources is an important element of the incident prevention and response strategy. With increasing threats from cybercrime and other attacks, OSINT education is becoming increasingly important. Organizations and individuals increasingly invest in staff training to use publicly available information sources more effectively. As technology advances and the online environment changes, OSINT security will likely continue to evolve, adapting to new challenges and taking advantage of new opportunities. On the other hand, it also comes with challenges and privacy concerns. OSINT can lead to collecting large amounts of personal information about individuals, which may constitute an invasion of privacy. OSINT also may lead to the collection of sensitive data, such as medical, financial or sexual orientation information, which may be ethically and legally problematic. Next, companies often worry that OSINT may help competitors obtain sensitive information about business strategies, customers or products. Cybercriminals can use collected information to launch attacks on individuals or companies. Also, collected information can be misinterpreted or used in the wrong context, leading to incorrect conclusions and reputational damage. Finally, the lack of uniform ethical standards regarding OSINT may lead to different practices in different cases and contexts. To minimize the risk of privacy breaches, it is crucial to work under applicable legal regulations, respect ethical principles and take appropriate precautions when collecting, storing and processing information. Whenever information is collected, consideration must be given to individuals' rights to privacy and data security.

CONCLUSIONS

In this manuscript, we surveyed papers that presented research using open-source intelligence. We collected papers focusing on different OSINT applications and resolutions. Also, we discussed the theoretical aspects of OSINT methods and attacks that can be performed using these methods. We highlighted the features of OSINT methods and tools. We use these methods and tools to investigate and learn about the functioning of employers, criminal groups, terrorist organizations, or specific people. OSINT investigations can help us find kidnapped persons or publicly available information about us. Also, criminals can use them to gain knowledge about a specific person in the organisation and then perform phishing attacks.

We looked at various scientific solutions that use OSINT methods for legitimate purposes. These solutions were associated with security, mostly cybersecurity, but with other security aspects like OSINT source, environmental, and mental or employment security. Also, these solutions widely use data from social media. This data makes predicting users' behaviour, intentions or political orientation possible. After such analysis, the other tools can block some users (who may cause problems or unnecessary confusion in social media).-OSINT offers numerous opportunities for

government organizations, security services, and companies, particularly law enforcement agencies, to gather evidence and verify information in the era of fake news. Future tools may improve social media content analysis, sentiment analysis, geospatial data integration, and cybersecurity. Blockchain technology can enhance the security and immutability of OSINT data.

Upon analyzing the present condition of open-source intelligence knowledge, we can set ourselves further research goals. We noticed that OSINT solutions for cybersecurity are extremely necessary because the dynamic development of network technologies also brings the development of attacking methods. Our future works will focus on OSINT's investigations around Advanced Persistent Threats (APT) groups. These groups carry out advanced, long-term cyber attacks that sophisticated and determined criminal or state groups carry out. APT groups are organized, highly capable and persistent in pursuing their goals. Preventing and detecting APTs is a difficult task that requires complex cybersecurity solutions, including appropriate protection tools, network traffic monitoring, user behaviour analysis, and IT security training for staff. If there is a suspicion that an organization may be a victim of APTs, it is necessary to take immediate action to identify and neutralize the threat. We will focus on preventing and detecting APT groups in the network.

REFERENCES

1. Lee, Soon L., Cai Lian T., Sivakumar T. Facebook depression with depressed users: The mediating effects of dependency and self-criticism on facebook addiction and depressiveness. Computers in Human Behavior, 2023; 139: 107549.
2. Govers J., Feldman P., Dant A., Patros P. Down the Rabbit Hole: Detecting Online Extremism, Radicalisation, and Politicised Hate Speech. ACM Comput. Surv. 2023; 55(14): 1–35. https://doi.org/10.1145/3583067
3. Kutschera S. Incidental data: observation of privacy compromising data on social media platforms. International Cybersecurity Law Review. 2023; 4(1): 91–114.
4. Pattnaik N., Li S., Nurse J.R.C. Perspectives of non-expert users on cyber security and privacy: An analysis of online discussions on twitter. Computers & Security. 2023; 125: 103008.
5. Downing J. Social Media, Digital Methods and Critical Security Studies. Critical Security Studies in the Digital Age: Social Media and Security. Cham: Springer International Publishing. 2023; 71–108.
6. Govardhan, D., Krishna, G.G.S.H., Charan, V., Sai, S.V.A., Chintala, R.R. Key Challenges and Limitations of the OSINT Framework in the Context of Cybersecurity. In 2023 2nd International Conference on Edge Computing and Applications (ICECAA). IEEE 2023; 236–243.
7. Manohari, D., Adithya E.S., Vijayakumar K. Information Retrieval using OSINT and GHDB." 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI). IEEE 2023.
8. Kim K., Youn J., Yoon S., Kang J., Kim K., Shin D. Study on Cyber Common Operational Picture Framework for Cyber Situational Awareness. Applied Sciences. 2023; 13(4): 2331.
9. Grigaliūnas Š., Brūzgienė R., Venčkauskas A. The Method for Identifying the Scope of Cyberattack Stages in Relation to Their Impact on Cyber-Sustainability Control over a System. Electronics. 2023; 12(3): 591.
10. Block L. The long history of OSINT. Journal of Intelligence History. 2023; 1–15.
11. NBC Philadelphia. https://www.nbcphiladelphia.com/news/national-international/instagram-etsy-sale-tattoo-how-fbi-found-woman-accused-of-torching-ppd-cars/2436832, Accessed 22nd November 2023.
12. Evangelista J.R.G., Sassi R.J., Romero M., Napolitano D. Systematic literature review to investigate the application of open source intelligence (OSINT) with artificial intelligence. Journal of Applied Security Research. 2021; 16(3): 345–369.
13. Hassan, Nihad A., Hijazi R. Open source intelligence methods and tools. New York, NY: Apress, 2018.
14. Nobili M. Review OSINT tool for social engineering. Frontiers in Big Data 6(2023).
15. Li X., Li D., Yang Z., Zhao H., Cai W., Lin, X. 2022. ND-NER: A Named Entity Recognition Dataset for OSINT Towards the National Defense Domain. In International Conference on Neural Information Processing. Singapore: Springer Nature Singapore. 2022; 361–372.
16. Black I.S., Fennelly L.J. Investigations and the art of the interview. Butterworth-Heinemann, 2020.
17. Böhm I., Samuel Lolagar S. Open source intelligence: Introduction, legal, and ethical considerations. International Cybersecurity Law Review. 2021; 2: 317–337.
18. Qusef A., Alkilani H. The effect of ISO/IEC 27001 standard over open-source intelligence. PeerJ Computer Science. 2022; 8: e810.
19. The Police1. https://www.police1.com/investigations/articles/using-webint-and-osint-to-tackle-extremist-groups-Fvy2So5OzaAoNLTC/, accessed 17th November 2023.

20. The Telegraph. https://www.telegraph.co.uk/world-news/2022/07/04/celebrity-ukraine-volunteer-soldier-exposed-fraud-internet-sleuths/, accessed 17th November 2023.
21. Kowta A.S.L., Bhowmick K., Kaur J.R., Jeyanthi N. 2021. Analysis and overview of information gathering & tools for pentesting. In 2021 International Conference on Computer Communication and Informatics (ICCCI) IEEE, 2021; 1–13.
22. Herrera-Cubides, J.F., Gaona-García P.A., Sánchez-Alonso S. Open-source intelligence educational resources: a visual perspective analysis. Applied Sciences; 2020; 10(21): 7617.
23. Yamin M.M., Ullah M., Ullah H., Katt B., Hijji M., Muhammad, K. 2022. Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security. Mathematics. 2022; 10(12): 2054.
24. Inc. Barracuda Networks. https://assets.barracuda.com/assets/docs/dms/Spear-phishing-vol7.pdf, accessed 22nd November 2023.
25. Microsoft. https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/what-is-spear-phishing-how-to-keep-yourself-and-your-data-above-water, accessed 18th November 2023.
26. Distler, V. The Influence of Context on Response to Spear-Phishing Attacks: an In-Situ Deception Study. Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. 2023.
27. Butt U.A., Amin R., Aldabbas H., Mohan S., Alouffi B., Ahmadian A. 2023. Cloud-based email phishing attack using machine and deep learning algorithm. Complex & Intelligent Systems. 2023; 9(3): 3043–3070.
28. Birthriya S.K., Ahlawat P., Jain A.K. An Efficient Spam and Phishing Email Filtering Approach using Deep Learning and Bio-inspired Particle Swarm Optimization. International Journal of Computing and Digital Systems. 2023; 13(1): 189–199.
29. Nalini Priya G., Damoddaram K., Gopi G., Nitish Kumar R. 2023. Phishing Attack Detection Using Machine Learning. In International Conference on Emerging Trends in Expert Applications & Security. Singapore: Springer Nature Singapore. 2023; 301–312.
30. Pro-tibetan activists become victim of spear phishing. https://thehackernews.com/2012/04/pro-tibetan-activists-become-victim-of.html, accessed 26 September 2023.
31. Tyagi S., Tyagi R.K., Dutta P.K., Dubey P. 2023. Next Generation Phishing Detection and Prevention System using Machine Learning. In 2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC). IEEE, 2023; 1–6.
32. Sonowal G., Sonowal G. Types of Phishing. Phishing and Communication Channels: A Guide to Identifying and Mitigating Phishing Attacks. 2022; 25–50.
33. Maniscalco P.M., Holstege C.P., Cormier S.B. Operations Security, Site Security, and Incident Response. In Ciottone's Disaster Medicine. Elsevier. 2024; 573–581.
34. Yamin M.M., Ullah M., Ullah H., Katt B., Hijji M., Muhammad K. 2022. Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security. Mathematics. 2022; 10(12): 2054.
35. OSINT framework, https://osintframework.com/, accessed 28th February 2024.
36. Awesome OSINT, https://github.com/jivoi/awesome-osint, accessed 28th February 2024.
37. Alsmadi I., Dwekat Z., Cantu R., Al-Ahmad B. Vulnerability assessment of industrial systems using Shodan. Cluster Computing. 2022; 25(3): 1563–1573.
38. Phil Harvey. Exiftoolgui for windows v12.62. https://exiftool.org/exiftool_pod.html}, accessed 25 August 2023.
39. Pastor-Galindo J., Nespoli P., Mármol F.G., Pérez G.M. 2020. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. IEEE Access, 2020; 8: 10282–10304.
40. Reider-Gordon M. Too Much Information: OSINT in Criminal Investigations and the Erosion of Privacy. Regulating Cyber Technologies: Privacy Vs Security. 2023; 145.
41. Katzner, T., Thomason, E., Huhmann, K., Conkling, T., Concepcion, C., Slabe, V., Poessel, S. Open-source intelligence for conservation biology. Conservation Biology. 2022; 36(6): e13988.
42. Osterritter L., Carley K.M. Conversations around organizational risk and insider threat. In Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. 2021; 613–621.
43. Alquwayzani A., Aldossri R., Rahman M.H. 2023. How dark web monitoring can be used for osint and investigations. Journal of Theoretical and Applied Information Technology, 101(10).
44. Connolly K., Klempay A., McCann M., Brenner P. Dark Web Marketplaces: Data for Collaborative Threat Intelligence. Digital Threats: Research and Practice. 2023; 4(4): 1–12.
45. Pastor-Galindo J., Mármol F.G., Pérez G.M. On the gathering of Tor onion addresses. Future Generation Computer Systems. 2023; 145: 12–26.
46. Chaudhary M., Bansal D. Open source intelligence extraction for terrorism-related information: A review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2022; 12(5): e1473.
47. Lakomy M. Open-source intelligence and research on online terrorist communication: Identifying ethical and security dilemmas. Media, War & Conflict. 2023; 17506352231166322.
48. Gianluigi, M. E., & MUCCI, M. F. (2023). Countering Daesh Cognitive and Cyber Warfare with

OSINT and Basic Data Mining Tools. In International Conference on Cybersecurity and Cybercrime. 2023; 10: 71–80).

49. Wangchuk T., Rathod D. Opensource intelligence and dark web user de-anonymisation. International Journal of Electronic Security and Digital Forensics. 2023; 15(2): 143–157.
50. Yu, S. Cyber profiling: Predicting political orientation with SOCMINT. Telematics and Informatics Reports. 2023; 10: 100058.
51. Sasaki T., Yoshioka K., Matsumoto T. Who are you*f* OSINT-based Profiling of Infrastructure Honeypot Visitors. In 2023 11th International Symposium on Digital Forensics and Security (ISDFS). IEEE, 2023; 1–6.
52. Lohar S., Kolte J., Zambare P. AutOSINT: GUI-Based Foot printing Software with AI and OSINT. EPRA International Journal of Multidisciplinary Research (IJMR), 2023; 9(5), 301–305.
53. Dale D., McClanahan K., Li Q. AI-based Cyber Event OSINT via Twitter Data. In 2023 International Conference on Computing, Networking and Communications. IEEE. 2023; 436–442.
54. Reyes J., Fuertes W., Arévalo P., Macas M. An Environment-Specific Prioritization Model for Information-Security Vulnerabilities Based on Risk Factor Analysis. Electronics. 2022; 11(9): 1334.
55. Suryotrisongko H., Musashi Y., Tsuneda A., Sugitani K. Robust botnet DGA detection: Blending XAI and OSINT for cyber threat intelligence sharing. IEEE Access. 2022; 10: 34613–34624.
56. Zheng G., Zhang Y., Yue X., Li K. Interpretable prediction of thermal sensation for elderly people based on data sampling, machine learning and SHapley Additive exPlanations (SHAP). Building and Environment. 2023; 242: 110602.
57. Li X., Xiong H., Li X., Zhang X., Liu J., Jiang H., Dou D. G-LIME: Statistical learning for local interpretations of deep neural networks using global priors. Artificial Intelligence. 2023; 314: 103823.
58. Fauziyyah A.K., Adrian R., Alam S. Analyzing Image Malware with OSINTs after Steganography using Symmetric Key Algorithm. Sinkron: jurnal dan penelitian teknik informatika. 2023; 8(2): 818–824.
59. Duitsman M., Kalinina-Pohl M. Open Source Intelligence and Investigative Techniques for Locating Radioactive Sources. 2013.
60. Guo Y., Liu Z., Huang C., Liu J., Jing W., Wang Z., Wang Y. CyberRel: Joint entity and relation extraction for cybersecurity concepts. In Information and Communications Security: 23rd International Conference, ICICS 2021, Chongqing, China, November 19–21, 2021, Proceedings, Springer International Publishing. 2021; I23: 447–463.
61. Guo Y., Liu Z., Huang C., Wang N., Min H., Guo W., Liu J. A framework for threat intelligence extraction and fusion. Computers & Security. 2023; 132: 103371.
62. Shamunesh P., Vinoth S., Srinivas L.N.B. Cybercheck–OSINT & Web Vulnerability Scanner. In 2023 2nd International Conference on Edge Computing and Applications (ICECAA). IEEE, 2023; 275–279.
63. Melshiyan M.A., Dushkin A.V. Information Security Audit Using Open Source Intelligence Methods. In 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). IEEE, 2022; 379–382.
64. DeCusatis C., Peko P., Irving J., Teache M., Laibach C., Hodge J. A Framework for Open Source Intelligence Penetration Testing of Virtual Health Care Systems. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference. IEEE, 2022; 0760–0764.
65. Al Mahmeed Y., Elmedany W., Sharif M.S. Eagle-Eye: Open-Source Intelligence Tool for IoT Devices Detection. In 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT) IEEE, 2022; 526–530.
66. Saraswathi, V.R., Ahmed I.S., Reddy S.M., Akshay S., Reddy V.M., Reddy S.M. Automation of recon process for ethical hackers. In 2022 International Conference for Advancement in Technology (ICONAT) IEEE, 2022; 1–6.
67. Marinho, R., Holanda, R. Automated Emerging Cyber Threat Identification and Profiling Based on Natural Language Processing. IEEE Access, 2023.
68. San Biagio, M., Acquaviva, R., Mazzonello, V., La Mattina, E., Morreale, V. A new SOCMINT framework for Threat Intelligence Identification. In 2021 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2021; 692–697.
69. Elmas T., Ibanez T.R., Hutter A., Overdorf R., Aberer K. WayPop Machine: A Wayback Machine to Investigate Popularity and Root Out Trolls. In 2022 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) (pp. 391–395). IEEE, 2022; 391–395.
70. Mahaini, M.I., Li, S. Detecting cyber security related Twitter accounts and different sub-groups: a multi-classifier approach. In Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. 2021; 599–606.
71. Nobili M., Faramondi L., Setola R., Ghelli M., Persechino B., Lombardi M. An OSINT platform to analyse violence against workers in public trasportation. In 2021 International Conference on Cyber-Physical Social Intelligence (ICCSI) IEEE, 2021; 1–6.
72. Daskevics A., Nikiforova A. ShoBeVODSDT: Shodan and Binary Edge based vulnerable open data sources detection tool or what Internet of Things

Search Engines know about you. In 2021 second international conference on intelligent data science technologies and applications (IDSTA). IEEE, 2021; 38–45.

73. Daskevics A., Nikiforova A. IoTSE-based open database vulnerability inspection in three Baltic countries: ShoBEVODSDT sees you. In 2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS). IEEE. 2021; 1–8.
74. Karthika S., Bhalaji N., Chithra S., Sri Harikarthick N., Bhattacharya, D. NoRegINT—A Tool for Performing OSINT and Analysis from Social Media. In Inventive Computation and Information Technologies: Proceedings of ICICIT 2020 Springer Singapore. 2021; 971–980.
75. Jan S.A., Barclay F.P. Conflict and Conflicting News Discourses: An Analysis of Newspaper Coverage of Pulwama Attack. Journalism Practice. 2023; 1–19.
76. Abdullah A., Laghari S.A., Jaisan A., Karuppayah S. OSINT Explorer: A Tool Recommender Framework for OSINT Sources. In Advances in Cyber Security: Third International Conference, ACeS 2021, Penang, Malaysia, August 24–25, 2021, Revised Selected Papers. Springer Singapore. 2021; 3: 389–400.
77. Griné T., Teixeira Lopes C. A Social Media Tool for Domain-Specific Information Retrieval-A Case Study in Human Trafficking. In Joint European Conference on Machine Learning and Knowledge Discovery in Databases Cham: Springer Nature Switzerland, 2022; 23–38.
78. Seo S., Kim D. (2021). OSINT-based LPC-MTD and HS-decoy for organizational defensive deception. Applied Sciences, 11(8), 3402.
79. Drichel, A., Drury, V., von Brandt, J., Meyer, U. Finding phish in a haystack: A pipeline for phishing classification on certificate transparency logs. In Proceedings of the 16th International Conference on Availability, Reliability and Security. 2021; 1–12.
80. Khan S., Wallom D. A system for organizing, collecting, and presenting open-source intelligence. Journal of Data, Information and Management. 2022; 4(2): 107–117.
81. Garzia F., Borghini F., Bruni A., Lombardi M., Minò L., Ramalingam S., Tricarico G. Sentiment and emotional analysis of risk perception in the Herculaneum Archaeological Park during COVID-19 pandemic. Sensors. 2022; 22(21): 8138.
82. Li T., Wang X., Yu Y., Yu G., Tong X. Exploring the Dynamic Characteristics of Public Risk Perception and Emotional Expression during the COVID-19 Pandemic on Sina Weibo. Systems. 2023; 11(1): 45.
83. Qing H., Bang Z., Agostini M., Bélanger J.J., Gützkow B., Kreienkamp J., Reitsema A.M., van Breen J.A. PsyCorona Collaboration, N. Pontus Leander. Associations of risk perception of COVID-19 with emotion and mental health during the pandemic. Journal of affective disorders. 2021; 284: 247–255.
84. Savadori L., Lauriola M. Risk perceptions and COVID-19 protective behaviors: A two-wave longitudinal study of epidemic and post-epidemic periods. Social Science & Medicine. 2022; 301: 114949.
85. Garzia F., Borghini F., Makshanova E., Lombardi M., Ramalingam S. Emotional analysis of safeness and risk perception of cybersecurity attacks during the COVID-19 pandemic. In 2022 IEEE International Carnahan Conference on Security Technology (ICCST). IEEE, 2022; 1–6.