INTELLIGENCE AND SECURITY IN THE 21ST CENTURY

OPEN SOURCE INTELLIGENCE: AN OVERVIEW OF TODAY'S OPERATIONAL CHALLENGES AND HUMAN RIGHTS AFFECTED AS A CONSEQUENCE

Ainara BORDES PEREZ[*]

Abstract:

Open Sources Intelligence's (OSINT) landscape has gone through a rapid evolution in the information era. Volumes of open-source information have never been so broad and high, and today's technology is able to monitor interesting topics, contrast and match new data with old, spot early signs and discover previously unknowns, patterns and relationships at a level never seen before. This has not gone unnoticed by Law enforcement authorities (LEAs) and intelligence services (SISs), which, slowly but steadily, have embraced this new environment. OSINT is today exploited by LEAs and SISs for all types of intelligence needs, starting from (near) situational awareness, to investigatory and preventive purposes.

The rapid evolution has, nevertheless, created new, and exacerbated existing operational challenges. Assessing reliability against online data manipulation and disinformation has become a great challenge in the Internet era. While advanced technology is needed to extract and analyse the sheer volumes of data, measuring the outcome of these tools is not easy due to difficulties in traceability, pre-existing human and algorithmic bias, the institutions' need for secrecy and the existing opacity around the vendors and their products. All those challenges can result in inaccurate OSINT products being later used for decision-making. Those, when used by SISs and LEAs, can affect by extension human rights such as the right to freedom from discrimination and the right to a fair trial.

This article analyses those operational challenges and their subsequent impacts on human rights. It does so by doing a comprehensive literature review on the topic through academic articles, national and international institutional reports, and newspaper articles. The study focuses on concrete problematic activities involving the creation and use of current OSINT products and describes examples that are not limited to one jurisdiction. Structuring both the OSINT operational challenges and their

[*] Ainara Bordes Perez is a dual PhD candidate at "Mihai-Viteazul" National Intelligence Academy & University of Malta. Her primary research interests concern Open Source Intelligence and its impact on human rights, email: ainara.bordes.17@um.edu.mt

subsequent impacts on human rights is the novelty of this article. While some academics have addressed several of those challenges affecting advanced mining technologies overall, addressing the operational challenges and their impacts from a single focal point – OSINT, is novel. Addressing them in a structured manner is a necessary first step to carve up the landscape for a potential subsequent legislative evaluation of how to address those operational challenges and their impacts on human rights.

Keywords: *Open Source Intelligence, OSINT, human rights, Law Enforcement, Intelligence Services, operational challenges.*

Introduction

Open Source Intelligence (OSINT) has undergone a thorough and rapid evolution in the last decades within security and intelligence services (SISs) and law enforcement authorities (LEAs). Its role in the Ukrainian war is the latest example of it. From monitoring and translating foreign radio broadcasts and newspapers on the brink of World War II, OSINT capabilities have expanded exponentially over the last thirty years. The creation of the Internet and dynamic user-generated platforms have vastly increased the amount of openly available data online and have created a growing interest among the public and private sectors to approach these data for different purposes.

This interest has also stimulated technological developments aiming to exploit this data, and advances in software have enabled the processing[1] of openly available online data in unprecedented ways. Thanks to today's data mining and analytic tools, SIS and LEAs can collect high volumes of data and analyse them to discover previously unknowns, patterns and relationships at a level never seen before (Bernal, 2016, p. 5; Tavani, 2008, pp. 139-140). Furthermore, today's commercial off-the-shelf products (COTs) are able to offer customised toolkits to SISs and LEAs tailored to their needs, which usually may include multiple software functionalities together, impacting every step of intelligence creation. These toolkits can continuously feed datasets and monitor open

[1] This article uses the word "process" or "processing" in accordance with the definition provided by the European General Data Protection Regulation (GDPR). "Processing" according to the GDPR means any operation or set of operations performed on data or sets of data, such as collection, analysis, and sharing.

sources, contrast and match new data with old, and spot early signs in different areas of interest or targets. Also, these COTSs usually integrate further modelling, simulation, and visualisation techniques, allowing the OSINT analyst fluidly to transit between methods and reasoning strategies, interrogate data, and test hypotheses (Akhgar et al., 2015).

SISs and LEAs have – slowly but steadily – embraced these new technologies as today's OSINT capabilities have been perceived as valuable at all levels of intelligence (Rolington, 2013, p. 52; Wells & Gibson, 2017, p. 94). OSINT is currently being used by SISs and LEAs for (near) situational awareness, investigatory, and preventive purposes. It is also employed for the oversight of ongoing events and in evaluating their risks, gaining in-depth insight into a person of interest, group or a phenomenon, detecting early warnings, and combined with other sources, inferring patterns to make predictions on criminality and threats (Wells & Gibson, 2017, p. 94)

This rapid evolution of OSINT capabilities has nonetheless opened the debate surrounding the potential risks new means and uses of OSINT can involve for human rights. OSINT has traditionally been perceived as having no impact on human rights, and apart from information security and intellectual property issues, the (side) effects of OSINT have received little attention in the literature until recently (Eijkman & Weggemans, 2013, p. 289) However, the new OSINT setting is both qualitatively and quantitatively different from the "traditional" OSINT, and the potential impacts of the new techniques are also new.

This report aims at studying those impacts, focusing on the risks deriving from technical and practical challenges of the OSINT process as we know it today[2]. Challenges such as difficulties in assessing reliability and accuracy of the data, or bias in collection and analysis, can result in inaccurate OSINT products being later used for decision-making. When used by SISs and LEAs, these compromised OSINT products can affect, by extension, human rights such as the right to freedom from discrimination

[2] Other impacts on human rights are instead inherent in today's OSINT practices due to its nature as a surveillance mechanism. The mere fact of collecting, aggregating, analysing and taking decisions of the (OSINT) outcome can affect the rights of citizens by its very nature. The latter is however out of scope for this article due to constraints in space.

or the right to a fair trial. This article analyses those risks and subsequent impacts by focusing on concrete problematic activities involving the creation and uses of current OSINT products, and deploys examples that are not restricted to one state of jurisdiction. The methodology used for it is qualitative in its nature, focused on analysing existing literature review (academic articles and institutional reports) and several newspaper's articles on the topic. The novelty of this article resides in its structuring of the impact that operational OSINT has on human rights. While there exist, studies focused on single risks or impacts of some of the challenges mentioned in the article, having these impacts analysed from a single focal point (OSINT) is novel. Addressing them in a structured manner is a necessary first step to carve up the landscape for a potential subsequent legislative evaluation of how to address those operational challenges and their impact on human rights.

Bearing this in mind, this study starts with a brief overview of the dependencies of the OSINT environment and its evolution over time (section two). It continues with an analysis of the challenges in reliability and accuracy of today's OSINT products (section three and four). It later examines these challenges all together within the greater OSINT production process (section five) and the study finalises with an analysis of how human rights are affected as a consequence of all the aforementioned (section six).

Dependencies of a good OSINT product

The OSINT creation process is dependent on (i) the nature of its open sources, (ii) the environment in which these exist, and (iii) the state-of-the-art technical capability of transforming open-source data/information into intelligence. These three factors affect the way in which validation and reliability of sources are assessed, and they also impact in the analysis of accuracy of the content (NATO, 2001, pp. 23-24). Validation, reliability and accuracy assessments play an important role in the later analysis of the OSINT product, which ultimately impacts decision-making. Therefore, an analysis of the current challenges on source validation, reliability and accuracy is also an analysis of the current challenges of the final OSINT products and their uses.

If we think of the period prior to the Internet, the main open sources used for intelligence were traditional media (radio broadcasts, television and newspapers), together with limited published material from public institutions (e.g., censuses, cadastres when public), maps, journals, academic papers, and a few human experts and observers (usually) in the field (Minas, 2010, p. 11). These sources were usually limited, unidirectional, multilingual, and especially in the case of traditional media, widely spread. These characteristics posed (and some still pose) certain challenges to OSINT, and subsequently shaped the OSINT production process and its attributed value. For example, the unidirectionality and wide-reaching scope of traditional media often encouraged both state and non-state actors to use these sources to broadcast political propaganda (Mercado, 2004). By extension, this made it hard to ascertain the accuracy of the material, and generated a mistrust in open sources that still remains in certain minds (Pallaris, 2008, p. 3). Likewise, the multilingual nature of the sources has always posed difficulties in understanding foreign content (an important task in attempting to gain insights into a country/region from the local perspective). To overcome this challenge, language skills became very valuable among staff (Pallaris, 2008, p. 3).

The later development of the Internet significantly changed this scenario. The Internet not only brought an exponential increase in available sources, but also extended the type of sources and their characteristics. Advances in the Internet connection (3G, 4G and 5G), the blossoming of user-generated content platforms, and technological advancements such as smartphones, shifted open sources from offline, limited and unidirectional, to online, multi-directional and dynamic, from which today's individuals acquire information, share ideas and interact with each other daily (Hobbs et al., 2014, p. 1).

This new environment generated a new range of opportunities for SISs and LEAs, but it has also created new challenges for the OSINT process, and exacerbated the old ones. The large volumes of available data, the constant motion of online sources, and the ubiquitous nature of the information coming from everywhere and everyone, in all languages and language varieties, have become huge challenges for SISs and LEAs, where separating valuable data from "noise" or "misinformation" has become both difficult and time-consuming (Hogue, 2023, p. 110; Pallaris, 2008, p. 2; Perrot & Cadenza Academic Translations, 2022, p. 68). The following sections focus on those challenges using the changing nature of open sources and the evolving technical capacities as mainstay.

Difficulties assessing reliability

It can be said the Internet has given voice to all individuals around the world. Some academics call this phenomenon the "democratisation" of information (Tewksbury & Rittenberg, 2012). According to R.D. Steele and Arno Reuser, this "democratisation" enables the creation of a self-governance structure of society where all individuals take part, and where OSINT can be derived from the participation of the whole society (Reuser, 2018; Steele, 2010, p. 45). One of the most prominent outcomes of this concept is "crowdsourcing"[3], where individuals either voluntarily report to the authorities a specific ongoing situation, or the authorities ask for collaboration to citizens through online channels (Couts, 2011; Flacy, 2011; Hogue, 2023, pp. 108–109).

However, the outreach capacity of the Internet can also create several challenges. The "echo effect" is one of those, which can make it easy to misjudge the importance of a certain topic or the reliability of certain information (Akhgar et al., 2016, pp. 105–106) Indeed, the Internet allows individuals to distribute material widely through secondary sources. This can involve individuals replicating the news on other websites, and posting their views around the topic on social media, websites and blogs. The high volume of secondary sources can subsequently overshadow valuable material, and give priority to erroneous information within SISs and LEAs.

Secondly, the evolving cyberspace and associated technologies are also a great opportunity for different entities, organisations, and mainly states for strategic and military purposes (See Molander et al., 1996). Open sources are not free of it, and current open sources are being used to spread ideologies and versions of the truth in the so-called

[3] Used today as a common practice among LEAs in Europe and abroad. One of the most prominent examples is the one happening now in Ukraine, where the government set up a chatbot on Telegram (Stop Russian War) and an Android app "Bachu" where citizens were encouraged to share their information with the authorities.

"hybrid warfare"[4]. While the use of open sources for political propaganda is not new, today's online social media are the perfect environment to weaponize these sources to influence citizens through disinformation campaigns, political propaganda and even shaping war narratives (Gunneriusson, 2021; Hogue, 2023, p. 110; Perrot & Cadenza Academic Translations, 2022; Tolz & Hutchings, 2023).

While this report will not discuss hybrid warfare and the strategies to tackle it[5], from an OSINT perspective, current technological capacities allow different entities to spread disinformation that can involve a variety of different tactics. Some of these tactics are the use of bots to widely distribute a particular piece of news or fake news, the microtargeting of disinformation campaigns through aggressive profiling tactics, and the use of artificial intelligence (AI) techniques to create not only false written content, but also audio-visual content called "deep fakes" that can be used to imitate faces and mimic human behaviours (European Parliament. Directorate General for Parliamentary Research Services, 2021, pp. 7–8, 27, 129–130). OSINT practitioners are being challenged daily by these and other methods of manipulation where assessing reliability can become very difficult.

While there already exist several techniques to detect disinformation and its diverse ramifications, not every LEA or SIS possesses the same technical capabilities. Time constraints can also limit the useability of this technology (Babuta, 2017, p. 18). Moreover, some manipulation techniques such as deep fakes are relatively new and while there are now nascent techniques to verify their authenticity, these are still in their early stages (Masood et al., 2023). To give two examples of the impact deep fakes can make in the international context, in April 2021 several European Members of Parliament (MEPs) were targeted by deep fake video calls imitating the Russian opposition figure, Leonid Volkov. According to the real Volkov, this was an "attempt by the Kremlin to discredit protest leaders and Putin's number two enemy in Russia" (Roth, 2021). Additionally, on March 02, 2022, a deep fake of the

[4] For a deeper understanding of 'Hybrid Threats' see Giannopoulos et al., 2020.

[5] For an overview of what the European Commission is doing against disinformation see the European Commission's website on the topic: https://digital-strategy.ec.europa.eu/en/policies/online-disinformation (last accessed on 09 September 2023).

president of Ukraine, Volodymyr Zelensky, appeared in different social media channels announcing his surrender to Russia's invasion (Simonite, 2022; Wakefield, 2022). While this seems to be the first deep fake ever used in an armed conflict and was easily detected, it does show what is potentially to come in the open-source arena.

Difficulties assessing accuracy

Assessing accuracy of today's open source material is also subject to increased challenges for a number of reasons. To start, the fact that the Internet gives voice to everyone, everywhere, all time, has exacerbated the old challenges of multi-lingualism, while creating new ones on multi-contextuality. While some foreign languages are difficult to translate, beyond language, understanding culture-based and context-based nuances of user-generated content has become a greater challenge to LEAs and SISs. Much open source information (OSINF) is no longer articulated in a "neutral" or "journalistic" style made by a few experts in communication, and open sources are no longer used just for informative (or propagandistic) purposes. Instead, OSINF is now overwhelmingly generated by users with different backgrounds, contexts and feelings, and publications can easily go from informative purposes to opinion sharing, jokes, social interactions and expressions of personal feelings. As a result, sources such as social media, forums and blogs are today full of data/information where the context can vary enormously and meanings of the words and sentences can differ accordingly (Akhgar et al., 2016, pp. 96-98). Exaggerations, humour, sarcasm, irony, are in combination with dialects, slang, typos, non-standard grammar and erroneously-chosen automatically-corrected words. And the latter are only some of the existing resources and language alterations to be found online.

As a consequence, learning a foreign language is often not enough for an agent to be efficient in preventing, detecting and investigating crime/threats for national security within OSINT. Understanding the context in which this information is published is as essential as understanding the language itself. Understanding the context can however be challenging for agents. Diversity and inclusion among staff members could partially help to improve this within the organisation.

The challenge can partially be exacerbated by the use of Natural Language Processing (NLP) tools. The rapid evolution on information technology has been followed by a parallel blossoming of computer technologies aiming at exploiting the new online scenario, and a variety of software tools help today's SISs and LEAs collect large amounts of data, and process, monitor and analyse them. However, these tools can also create new challenges and exacerbate the old ones as explained below.

NLP tools can be very useful for the monitoring of large volumes of available sources, and today's LEAs and SISs already employ them for a variety of purposes such as to monitor ongoing events, to help detect anomalies that may lead to criminal offences or threats, and to improve the efficacy of border controls (Akhgar et al., 2016, pp. 96–103; Williams & Blum, 2018, pp. 23–27). However, accurately identifying meanings of words in context is not an easy task for these tools. The nuances/resources of language may go beyond the tools' design parameters and when an online post or comment is wrenched from its context and fed into a database, this can lead to mangled meaning and harmful consequences, especially when SISs and LEAs decision-making is involved (Edwards & Urquhart, 2016, p. 306). For instance, the word "rape" can mean something completely different in gaming and among hackers from the usual sexual offence meaning (Miller, 2014). If there is contextual confusion, this can lead to serious consequences for users and their police records or profiles (Edwards & Urquhart, 2016, p. 306). Although examples are difficult to go public, one that went viral is from 2012, when two British tourists were detained and deported for tweeting that they were going to "destroy America" during their holidays. According to the affected individuals, the word "destroy" meant "to get trashed and party" within the context. (Huffingtonpost, 2012). Another example is a teenager being arrested for a tweet taken out of context around Pink's concert in 2013. According to the teen, she wanted to make a reference to Pink's song "Timebomb" when she tweeted "I'm ready with my Bomb. Time to blow up #RodLaverArena Bitch" (SocialNewsDaily, 2013). Last but not least, an example of a mistranslation of an NPL tool is the one published by The Guardian in 2017. A Palestinian man got arrested by Israeli police after an artificial intelligence-powered translation tool erroneously translated an Arabic "good morning" into an

English “hurt them” and Hebrew “attack them”. According to The Guardian, no Arabic-speaking officer had read the actual post before the arrest (The Guardian, 2017).

Additionally, as pointed out above, the Internet is full of information which is in other than text format. Useful information can also be found in images, videos, audios, and more. While a proper understanding of text-format data can trigger challenges explained above, other formats can be even more challenging. A good example of these challenges is the technical difficulties faced by SIS and LEAs to accurately identify individuals from images disclosed in open sources.

SISs and LEAs may find it valuable to detect, recognise and verify a human face from a digital image or a video frame found in open sources. This can be done manually or by the use of emerging developments on Facial Recognition Technology (FRT). FRT has existed for decades, nonetheless, it has become more prevalent and innovative in recent years due to the integration of artificial intelligence (AI) within its systems. Some SISs and LEAs have already used COTs with FRT based on datasets filled with open-source images/videos or with the ability to scrape (near) real-time social media platforms (BuzzFeed News, 2021; The New York Times, 2021). However, the use of AI-based FRT raises significant concerns from an ethical, legal and accuracy perspective (European Data Protection Supervisor, 2022; European Parliament Resolution 2020/2016(INI), 2021; ClearView AI Inc Enforcement Notice, 2022). The following lines look into the concerns related to the accuracy of this technology.

Several studies have demonstrated that current AI-based FRT can have up to 20% error rate when images are captured from real world settings, against their advertised 0.1% error rate with high quality images obtained from settings such as cooperating subjects taking pictures in good lighting (Grother et al., 2019a). When results are broken down by gender and skin colour, numbers get even worse. Studies have concluded that today’s technology is significantly less accurate at recognising individuals with darker skin, especially dark-skinned women (Grother et al., 2019b; Najibi, 2020), where the error rate can go up to 34% (Buolamwini, 2017). If these erroneous outcomes are later used by LEAs and SISs, the implications for individuals’ fundamental rights can be profound. To give some examples, in the US there have been three reported instances of false arrest based in part on facial recognition technologies (Detroit Free Press, 2020; The New York Times, 2020a, 2020b). The three cases were later wrongly corroborated by witnesses, which leads to the investigation on the individuals' behaviour in regard to challenging automated decisions Another example is the one happened in the Rhode Island (US) of 2019, where a student suffered death threats due to a facial identification tool that wrongly flagged him as a suspect in the Sri Lanka bombings (Ivanova, 2020).

On the legal perspective, in Europe, facial recognition is considered biometric data[6] and falls under the special categories of data that require a restricted use and protection[7]. Nevertheless, in the legislative framework there is no specific provision for the uses of AI-based FRT and its potential harmful consequences to fundamental rights. The Council of Europe (CoE) issued guidelines on the uses of FRT in January 2021[8] but these have not yet been put onto an explicit legal basis in most of the signatory countries. In parallel, the European Commission (EC) has published a proposal for an Artificial Intelligence (AI) regulation (AI Act or AIA)[9], where remote biometric systems such as FRT using AI are a central concern. However, the proposal must still go through

[6] The definition of "biometric data" is understood in this article according to the definition provided by the GDPR, where it means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

[7] See Art. 6, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 2018; Art 9 GDPR; Art. 10, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016.

[8] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Convention 108, Guidelines on Facial Recognition, 2021.

[9] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, 2021.

consultations within the EU before its adoption, so there is no solid legal basis for this technology yet in the EU.

In the meantime, more research is needed to explore the specific reasons of FRT's gap in accuracy. One of the studied factors is the lack of diversity in training images and benchmark datasets, which leads to biased outcomes that can ultimately result in discrimination and abuse. This risk is indeed not unique to AI-based FRT, and bias (human and technical) is a central concern in any software.

All individuals have pre-existing knowledge, experiences and societal understanding of the world that affect their decision-making processes, either consciously or unconsciously. The design of data-mining/analytics is not different, and humans' subjectivity plays a role in the design of algorithms. This means that the outcome of a software is dependent on the humanly biased algorithms. In the case of AI-based software, after the initial design phase, AI tools are trained on pre-defined sample data that enables them to recognise relevant patterns from new data. However, the decision of which training data set to employ is also a human decision that is not risk-free from bias[10].

Regulatory bodies have tried to solve this problem adding several pre and post measures to automatic decision-making processes. One of the most prominent is including human oversight to the process[11]. This means that results of the software are later interpreted by an analyst, who should assess the tool's decision and adjust the outcome of the software if necessary. However, this solution may be missing a relevant factor: again, human bias. While the analyst might be able to adjust or "correct" technical errors or "algorithmic-bias" in the tool, it can introduce a second layer of human bias (Dencik et al., 2015, p. 52). This can be particularly relevant when referring to software outcomes. As mentioned by Lorna McGregor, the degree of deference granted to an automated recommendation is generally high, and individuals may be reluctant to go against it (McGregor et al., 2019, p. 317). There is a general perception (or "bias") that an algorithm is neutral or more accurate than a human being. This perception combined with the

[10] While training data can be chosen with unconscious human preconceptions or bias, other factors such as the availability of data can also affect.

[11] See Art. 22 GDPR an Art. 14 or the EU Proposal for the Artificial Intelligence Act.

difficulty in explaining why an algorithmic recommendation or decision is overturned may render human oversight ineffective.

Indeed, even ignoring the technical and human bias, understanding how advanced data mining/analytics (AI-based or not) work is difficult for analysts when data architecture systems become vast and highly interconnected. These difficulties to understand (and subsequently explain) the outcome of an algorithm is called the "black-box effect" (Dencik et al., 2015, p. 51). This, combined with the need for secrecy of SISs and LEAs, makes ensuring accountability (and accuracy) a challenging task (Eijkman & Weggemans, 2013, p. 293; Patel et al., 2019). If we combine the above with the fact that OSINT can sometimes be provided by private entities, other state agencies, and/or international partners, tracing the source and its subsequent modifications is a complex task making accuracy one of the greatest challenges for OSINT (Wetzling & Dietrich, 2022).

In conclusion, a diversity of factors affects the proper validation and reliability of sources, as well as the accuracy of OSINF and the OSINT outcome. Some of these challenges are specific to OSINT, others are not, and affect the technology used for it. The table below summarises those challenges:

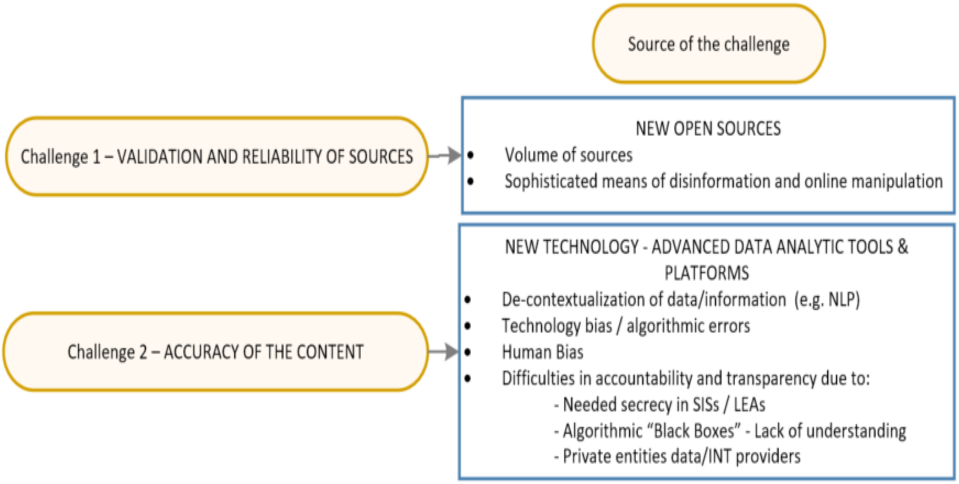
Source of the challenge
Challenge 1 – VALIDATION AND RELIABILITY OF SOURCES
NEW OPEN SOURCES
• Volume of sources
• Sophisticated means of disinformation and online manipulation
NEW TECHNOLOGY - ADVANCED DATA ANALYTIC TOOLS & PLATFORMS
• De-contextualization of data/information (e.g. NLP)
• Technology bias / algorithmic errors
• Human Bias
• Difficulties in accountability and transparency due to:
- Needed secrecy in SISs / LEAs
- Algorithmic "Black Boxes" - Lack of understanding
- Private entities data/INT providers
Challenge 2 – ACCURACY OF THE CONTENT

Figure 1: Today's OSINT production challenges (author's idea)

Challenges can be interconnected one to another, and some of them (e.g., disinformation and online manipulation) can affect both validation/reliability and the accuracy-assessment of the material. In addition, none of them are a new discovery of this report. They are all well documented, and experts in the field are trying to overcome them through technical, regulatory or ethical means. However, none of the challenges has a fully satisfactory solution yet, and all together create the biggest challenge from a human rights perspective: the use of a compromised OSINT product by law enforcement and/or intelligence services for decision-making impacting human rights as a result. The following section maps the challenges in the OSINT production cycle and the report finalises with an analysis of the human rights affected as a consequence.

Mapping the OSINT challenges within the greater intelligence cycle

The practical challenges analysed in the previous two sections can be found on each and every stage of the OSINT creation process. If we take the intelligence cycle[12] as benchmark to describe the OSINT production process, we can tell that the challenges on validation and reliability of sources occur in the collection phase, when a piece of material is considered valuable and is collected as a consequence of a compromised decision (human or technical).

[12] As aforementioned, the "intelligence cycle" is one of the best-known models describing the intelligence production process. It is an American model created in 1920s designed as a mechanical sequence similar to a manufacturing production-line principle and it consists of five main phases: (1) User's requirements and planning; (2) Collection and retention of raw material; (3) Processing of the material; (4) Analysis of processed material; and, (5) Dissemination or delivery of the end material to the users. In practice, the cycle is not always unidirectional and different phases can be interconnected one to another in different ways. However, the cycle represents a simplified version of the reality that allows us to analyse the challenges of OSINT from a human rights perspective. For further detailed information on the intelligence cycle see (Phythian, 2013).

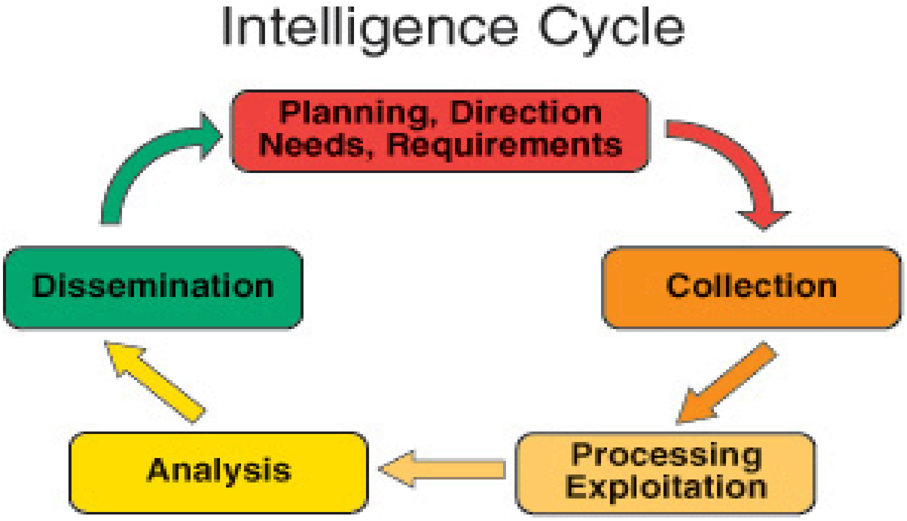

Figure 2: Basic Intelligence Cycle Structure (Source: https:// www.e-education.psu.edu/sgam/node/15, accessed on September 11, 2023)

By contrast, difficulties in assessing the accuracy of the material can happen either in the collection phase or in the later processing and/or analysis phases. The latter will depend on the context of the intelligence need and the technical and organisational capacity of each SIS and LEA. Depending on these factors, (i) time constrains might play a role in the ability to assess material (e.g., a (near) real-time situation vs. a strategic intelligence requirement (Dencik et al., 2018, pp. 1441–1443); (ii) OSINF can be treated by a human (OSINT agent) or software tools with their aforementioned bias; (ii) OSINF can be processed and analysed alone or together with other OSINF/INTs.; and, (iv) the (erroneous) inferred material/assumptions can be further processed and analysed together with other OSINT or non-OSINT for decision-making.

Indeed, SISs and LEAs operate in diverse manners depending on their capabilities and some of them focus more on manual OSINT production while others employ some or most of the existing advanced software functionalities (Akhgar et al., 2016, p. 89; Babuta, 2017, p. 17; CTIVD, 2021, p. 11; Williams & Blum, 2018, p. 36). If SISs and LEAs choose to use software technology, they are often not in-house built.

Openly available tools and COTSs assist them in the OSINT production. Consequently, a third party enters into play in the design of the software. If software tools are openly available, which LEAs are more prompt to use than SISs (Frank et al., 2011, p. 13), the organisation does not necessarily have the design behind it, therefore accountability becomes highly difficult. When those tools are customised for SISs and LEAs, they are parametrised according to the requirements of the institutions (Dencik et al., 2018, p. 1441). However, lack of knowledge regarding the software-design and possible pre-existing databases provided by the third-party as part of the tool can still present (McGregor et al., 2019, p. 317; Wetzling & Dietrich, 2022, p. 14). Moreover, regardless of whether the software is customized or not, bias in both the design phase and the later human-centric analysis are still present, impacting all phases of the OSINT production and resulting in potential unfair inequalities as explained in the following section (Fabre, 2022, pp. 217–227).

Complexity increases when multiple software functionalities are combined in an integrated OSINT platform that impacts on every step of the intelligence cycle[13]. The combination of software functionalities can scan, collect, process and analyse lexical, social, geospatial and other forms of data together. This can reveal new connections that officers/agents take longer or find impossible to uncover. Furthermore, it can detect unnoticed behaviours or leads that a human might not pick up because of lack of capacity. These tools in combination are able to cobble together a deep and comprehensive (but not necessarily accurate) picture of an individual. All these processes can be running simultaneously and the database can be continuously fed (Akhgar et al., 2016, p. 89; Staniforth, 2016) creating an "intelligence-net" rather than a "cycle" where discovered unknown unknowns can re-conduct the investigation and/or drive new requirements from policy-makers (Van Puyvelde, 2017, p. 1404). Ultimately, this technology converts the "cycle" into a vast "net" where an erroneous output/input in any of the phases is very difficult to detect[14].

[13] See for example the services offered by Maltego: https://www.maltego.com/products/ (accessed 11 September 2023).

[14] This technology not only converts the "cycle" into a vast" net", but it also inverts the intelligence cycle model itself, questioning the purpose specification of the investigation.

Some COTSs offer the possibility to further analyse OSINF with classified sources such as an organisation's own datasets (The Guardian, 2021)[15]. They can also include functionalities such as data storage, modelling, simulation, visualisation and sharing tools, allowing the data analyst to construct different explanations and explore hypotheses from previously and continuously processed data (Akhgar et al., 2016, p. 89). Keeping track of changes and recording the processes becomes essential to guarantee the reliability of data and reproducibility of results. However, detecting in a timely-manner human/technical bias and erroneous assumptions/inferred data in a highly interconnected and sophisticated platform is again vastly difficult, indeed almost impossible.

Human Rights affected due to practical challenges in OSINT production

The consequences of the aforementioned challenges are dual. On the one hand, compromised OSINT products can affect the decision-making of SISs and LEAs, consequently impacting on their efficiency. However, there is no "quantum" or international accepted performance-standard to measure efficiency in intelligence production, since precise identification of cause and effect of an intelligence product and the later outcome of the intelligence goal is highly difficult (Dover et al., 2014, p. 124; Herman, 1996, pp. 314-326; Rønn & Søe, 2019, p. 13) This report does not deal with this topic since it is outside its brief.

On the other hand, inaccurate OSINT products that are later used for decision-making can endanger a variety of human rights. These rights vary from case to case and will depend on the context of the intelligence requirement and on the nature of the compromised OSINT product. Unfortunately, obtaining an accurate picture of the rights affected and the number of individuals impacted per organisation is also very difficult. First, measuring the impact is not feasible when SISs/LEAs are not aware of all the inaccuracies in the OSINT process. Second, the opacity of these organisations around the processes and technology used renders the task even more complex (Bernal, 2016, p. 16). In order to provide a

[15] See again the options offered by Maltego in https://www.maltego.com/transform-hub/ (accessed 11 September 2023).

picture of the human rights involved, the following lines use pieces of news detailing several past SISs/LEAs errors in combination with studies that have analysed different data-mining and analytic technologies offered to SISs and LEAs.

The most visible human right impact is perhaps when the right of liberty (Art. 5 European Convention on Human Rights, "ECHR") is denied. On several occasions, media coverage has mentioned situations where erroneous OSINT outcomes have triggered the detention of individuals. The aforementioned example of two British citizens apprehended on arrival in Los Angeles due to a joke on Twitter is a good illustration of this, where figures of speech were misinterpreted (BBC News, 2012). The three false arrests based in part on facial recognition inaccuracies in the US are another example (Detroit Free Press, 2020; See The New York Times, 2020a, 2020b). In the latter, not all images/videos used to reach the arrest-decisions were based on open sources, however, the technology behind all of them is the same, hence the risk. Similarly, other difficulties assessing reliability and accuracy discussed above (e.g., online manipulation, de-contextualization of data, human and technological bias) could lead to an inaccurate OSINT product resulting in a false arrest.

At the same time, human input, both in designing algorithms as well as in the analysis and interpretation of the open-source data, remains central to data-driven policing. As analysed above, the latter opens up possibilities for pre-existing human biases to enter predictive policing and intelligence work in the guise of "neutral" data analysis, resulting in possible discriminatory implications (Dencik et al., 2015, p. 52; European Parliament Resolution 2020/2016(INI), 2021). For instance, targeting certain groups in the initial analysis due to preconceived ideas creates self-fulfilling prophecies[16] where the initial analysis raises the group's visibility in all future calculations and obscures the rest (Dencik et al., 2015, p. 10). The consequence of this is

[16] For this article, self-fulfilling prophecies are understood as the targeting of certain groups in an unconscious manner in the initial design of the software tools and the posterior analysis of the outcome by analysts. This unconscious targeting raises their visibility and can affect future calculations. At the same time, this unconscious focus on a target can obscure other forces of interest to be analysed.

over-policing and harassment of communities that have traditionally been the focus of policing/intelligence, impacting directly in the collective dimension of the right to equal treatment and non-discrimination (Art. 14 ECHR) (Council of Europe, 2017; Levinson-Waldman, 2019, p. 7). As Levinson mentions, this dangerous practice also magnifies the risk of accidentally monitoring individuals belonging to underrepresented minorities (Levinson-Waldman, 2019, p. 7).

Finally, we should mention the criminal procedural issues resulting from inaccurate OSINT products. While OSINT investigations will mostly be used as intelligence steering an investigation, there might be situations where OSINT is used as evidence in later criminal proceedings. However, if reliability and accuracy are difficult to assess, OSINT evidence might not be admissible in courts, or the right to a fair trial can be impacted (Art. 6 ECHR) (Bernal, 2016, p. 14).

The aforementioned are only three of the main impacts an inaccurate OSINT product can produce on individual's rights. These impacts need to always be balanced against a necessity and proportionality test, and in combination with the European and national legal frameworks for LEAs and SISs. State accountability is essential here, where SISs and LEAs can validate on a case-by-case scenario the actions taken and justify their decision through oversight mechanisms. Accountability is characterised by its focus on the rule of law and good governance. However, at the moment of writing this report, the legislator seems to be silence about OSINT practices in the data protection legal framework for both LEAs and SISs (Recommendation No. R (87)15; Modernised CoE Convention, 2018; Directive (EU) 2016/680, 2016; Framework Decision 2008/977/JHA, 2016). Moreover, different national LEAs' and SISs' regulations have a variety of differences regarding OSINT. OSINT as a concept is not uniform among member states[17], and practices around OSINT are also differently regulated. Spain and Romania for instance, have old regulations in place for SISs (2002

[17] For instance, the National Police Chiefs Council (NPCC) in the UK considers contacting individuals in an undercover manner using social media is part of the 'covert activity' of OSINT. The Committee for Intelligence and Security Services (CTIVD) in the Netherlands states the opposite instead, and considers these practices outside the scope of OSINT.

and 1991 respectively), and while their SISs legislations contain some reference to the collection and processing information using technical means, there is no mention to the need for safeguards for processing publicly available data. Other regulations such as the Law on Intelligence and Security Services in the Netherlands has instead introduced the systematic collection of open-source information in the law (Article 38), adding several safeguards to this processing activity. In the case of the UK, the Office of Surveillance Commissioner – nowadays replaced by the Powers Commissioner's Office, has emphasized in several occasions that the repeat viewing of "open source" sites should constitute directed surveillance and regulate it as such (Shere, 2020; The Intelligence and Security Committee of Parliament of the UK, 2018). However, neither the Regulation of Investigatory Powers Act of 2000, nor the new Investigatory Powers Act of 2016 have incorporated those suggestions into the law.

Further study is needed to assess whether the international and European legal framework on human rights and the surrounding European Union and Council of Europe's guidelines and regulations are sufficient to appropriately protect the impacts of today's OSINT practices in every stage of its production and its uses. Addressing current technical challenges of OSINT and their subsequent impacts for human rights is nonetheless a necessary first step to carve up the landscape for a subsequent legal evaluation.

Conclusions

The rapid development of new open sources and the successive advances in data gathering and analysis tools have created some new technical challenges in the OSINT production, which subsequently created a debate surrounding the potential risks new means and uses of OSINT have for human rights. Validating and assessing reliability has become highly challenging with the large volumes of available data online, the constant motion of online sources, and the ubiquitous nature of the information, coming from everywhere and everyone, and in all languages. Differentiating valuable material from "noise" has become more difficult than ever, partially due to the "echo effect" individuals create when sharing secondary sources information. Sophisticated means of disinformation and online manipulation techniques exacerbate this difficulty. The use of bots to spread disinformation and other hybrid warfare techniques such as "deep fakes" are already being deployed by states and other stakeholders to misinform, create confusion or make "noise" among the large volumes of data, making the work of OSINT agents more challenging than ever.

In parallel, assessing the accuracy of the collected and processed open-source material is also a challenge in the current online environment. While advanced data mining and analytic tools try to overcome the difficulties of finding valuable material in the large "sea" of the Internet, these tools have created new challenges and exacerbate the old ones. Natural Language Processing tools, which are currently being employed by LEAs and SISs for a variety of purposes have difficulties in identifying the nuances of language found in open sources. The "democratisation of information" has led to open-source information overwhelmingly generated by users with different backgrounds. The use of different resources of the language (e.g., exaggerations, humour, sarcasm), in combination with dialects, slang, and grammar errors confuse NLP algorithms, resulting in erroneous OSINT. Moreover, softwares are now switching to AI based technologies, raising additional concerns. Bias in the design of the algorithms, in the chosen benchmark datasets to train the software, and in the final human revision are an added risk to the OSINT production. AI based Facial Recognition Technologies (FRT) are a good example of this, where different studies have demonstrated their gap in accuracy, and the impact of erroneous outcomes when used by LEAs or SISs.

Difficulties in validation of sources affect mainly the collection phase of OSINT, but compromised material is dragged into the rest of the process. Challenges in the accuracy are instead present in every step of the intelligence cycle. While new OSINT environment has great disparities from one institution to another, difficulties in understanding the rationale behind the software decision and bias are an integral challenge of every OSINT process in every institution. Complexity increases when OSINT is provided by private parties, or is later merged with other intelligence and/or shared with other institutions.

The outcome of these technical challenges is compromised OSINT products that can be used in decision-making by LEAs and SISs, endangering a variety of human rights. Obtaining an accurate picture of the rights affected is a challenging task due to the difficulties in detecting compromised OSINT among SISs/LEAs, and due to a lack of transparency of the institutions. Nevertheless, studies show that one of the most visible impacts of inaccurate OSINT is the right to equal treatment and non-discrimination of article 14 ECHR. Bias both in designing algorithms as well as in the analysis and interpretation of the open-source data has resulted in targeting certain groups or minorities due to pre-conceived ideas, and creating self-fulfilling prophecies. The consequence of this is over-policing and harassment of communities that have traditionally been the focus of policing/intelligence, raising visibility of these groups in future calculations and obscuring the rest. Where OSINT is used in criminal proceedings, the right to a fair trial (article 6 ECHR) is also at stake. Compromised OSINT might be used as evidence in courts, where judges (and even OSINT practitioners) might be reluctant to dismiss the OSINT outcome as evidence, despite of the difficulties to understand the rationale behind the product. Finally, and in a case-by-case scenario analysis, other fundamental rights such as the right of liberty (article 5 ECHR) has been proved to be impacted due to compromised OSINT products. Several cases have been disclosed where NLP and AI based FRT have led to inaccurate OSINT products resulting in a false arrest.

These impacts need to be addressed through current regulation and state accountability. However, at the moment of writing this report, there is no specific mention to the collection and processing of digital open-source information by LEAs and SISs in the data protection frameworks, and different national LEAs' and SISs' regulations have a variety of differences regarding OSINT. Further investigation is needed to address the appropriateness of state accountability of today's OSINT practices. Addressing current technical challenges of OSINT and their subsequent impacts for human rights is nonetheless a necessary first step to shape the landscape for a subsequent legal evaluation.

References:

1. Akhgar, B., Bayerl, P. S., & Sampson, F. (eds.). (2016). *Open Source Intelligence Investigation: From Strategy to Implementation*. Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-319-47671-1

2. Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., & Saskia Bayerl, P. (Eds.). (2015). *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies* (Elsevier).

3. Babuta, A. (2017). "Big Data and Policing – An assessment of Law enforcement Requirements, Expectations and Priorities." *RUSI Occasional Paper.*

4. BBC News. (2012, March 8). "Caution on Twitter urged as tourists barred from US." *BBC News*. Retrieved from https://www.bbc.com/news/technology-16810312

5. Bernal, P. (2016). "Data gathering, surveillance and human rights: Recasting the debate." *Journal of Cyber Policy*, *1*(2), 243–264. Retrieved from https://doi.org/10.1080/23738871.2016.1228990

6. Buolamwini, J. (2017). *Gender shades: Intersectional phenotypic and demographic evaluation of face datasets and gender classifiers*. MIT Master's Thesis.

7. BuzzFeed News. (2021, August 25). "Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here." *BuzzFeed News*. Retrieved from https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table

8. *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-DP (2017)01 (2017).

9. *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, CM/Inf (2018)15-final (2018).

10. Couts, A. (2011, August 9). "London Riots: Police use Flickr to help catch looters." *Digital Trends*. Retrieved from https://www.digitaltrends.com/social-media/london-riots-police-use-flickr-to-help-catch-looters/

11. CTIVD. (2021). *Toezichtsrapport Automated OSINT: tools en bronnen voor openbronnenonderzoek* (No. 74).

12. Dencik, L., Hintz, A., & Carey, Z. (2015). *Managing 'threats': Uses of social media for policing domestic extremism and disorder in the UK. Project report.* Cardiff School of Journalism, Media and Cultural Studies.

13. Dencik, L., Hintz, A., & Carey, Z. (2018). "Prediction, pre-emption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom." *New Media & Society*, *20*(4), 1433–1450. Retrieved from https://doi.org/10.1177/1461444817697722

14. Detroit Free Press. (2020, July 10). *Controversial Detroit facial recognition got him arrested for a crime he didn't commit*. Retrieved from https://eu.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/

15. Dover, R., Goodman, M. S., & Hillebrand, C. (Eds.). (2014). *Routledge Companion to Intelligence Studies*. Routledge.

16. Edwards, L., & Urquhart, L. (2016). "Privacy in public spaces: What expectations of privacy do we have in social media intelligence?" *International Journal of Law and Information Technology*, *24*, 279–310. Retrieved from https://doi.org/10.1093/ijlit/eaw007

17. Eijkman, Q., & Weggemans, D. (2013). "Open source intelligence and privacy dilemmas: Is it time to reassess state accountability?" *Security and Human Rights*, *23*(4), 285–296. Retrieved from https://doi.org/10.1163/18750230-99900033

18. European Data Protection Supervisor. (2022). *EDPS Opinion on the possibility to use Clearview AI and similar services at Europol*. Retrieved from https://edps.europa.eu/system/files/2022-01/21-03-29_edps_opinion_2020-0372.pdf

19. European Parliament. Directorate General for Parliamentary Research Services. (2021). *Strategic communications as a key factor in countering hybrid threats.* Publications Office. Retrieved from https://data.europa.eu/doi/10.2861/14410

20. European Parliament resolution 2020/2016(INI), European Parliament, European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2021). Retrieved from https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

21. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, (2016).

22. Fabre, C. (2022). *Spying Through a Glass Darkly: The Ethics of Espionage and Counter-Intelligence* (1st ed.). Oxford University Press. Retrieved from https://doi.org/10.1093/oso/9780198833765.001.0001

23. Flacy, M. (2011, August 10). "NYPD creates unit to track criminals on social networks." *Digital Trends*. Retrieved from https://www.digitaltrends.com/social-media/nypd-create-unit-to-track-criminals-on-social-networks/

24. Frank, R., Cheng, C., & Pun, V. (2011). *Social Media Sites: New Fora for Criminals, Communication, and Investigation Opportunities* (021.2011). Public Safety Canada. Retrieved from http://publications.gc.ca/collections/collection_2012/sp-ps/PS14-5-2011-eng.pdf

25. Giannopoulos, G., Smith, H., & Theocharidou, M. (2020). *The Landscape of Hybrid Threats: A Conceptual Model* (PUBSY No. 123305). European Commission, Ispra, 2020.

26. Grother, P., Ngan, M., & Hanaoka, K. (2019a). *Face Recognition Vendor Test (FRVT) part 2: Identification* (NIST IR 8271; p. NIST IR 8271). National Institute of Standards and Technology. Retrieved from https://doi.org/10.6028/NIST.IR.8271

27. Grother, P., Ngan, M., & Hanaoka, K. (2019b). *Face recognition vendor test part 3: Demographic effects* (NIST IR 8280; p. NIST IR 8280). National Institute of Standards and Technology. Retrieved from https://doi.org/10.6028/NIST.IR.8280

28. Gunneriusson, H. U. (2021). Hybrid warfare & theory. *Revista ICONO14 Revista Científica de Comunicación y Tecnologías Emergentes*, *19*(1), 15–37. Retrieved from https://doi.org/10.7195/ri14.v19i1.1608

29. Herman, M. (1996). *Intelligence power in peace and war*. Royal Institute of International Affairs: Cambridge University Press.

30. Hobbs, C., Moran, M., & Salisbury, D. (Eds.). (2014). *Open Source Intelligence in the Twenty-First Century – New Approaches and Opportunities*. Palgrave Macmillan.

31. Hogue, S. (2023). "Civilian Surveillance in the War in Ukraine: Mobilizing the Agency of the Observers of War." *Surveillance & Society*, *21*(1), 108-112. https://doi.org/10.24908/ss.v21i1.16255

32. Huffingtonpost. (2012, January 30). "British Tourists Detained, Deported for Tweeting 'Destroy America'". *Huffingtonpost*. Retrieved from https://www.huffpost.com/entry/british-tourists-deported-for-tweeting_n_1242073

33. ClearView AI Inc Enforcement Notice, (2022).

34. Ivanova, I. (2020, June 12). "Why face-recognition technology has a bias problem." *CBS News*. Retrieved from https://www.cbsnews.com/news/facial-recognition-systems-racism-protests-police-bias/

35. Levinson-Waldman, R. (2019). "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media." *Oklahomw Law Review*, *71*(4), 997–1012.

36. Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2023). "Deep fakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward." *Applied Intelligence*, *53*(4), 3974–4026. Retrieved from https://doi.org/10.1007/s10489-022-03766-z

37. McGregor, L., Murray, D., & Ng, V. (2019). "International Human Rights Law as a Framework for Algorithmic Accountability." *International and Comparative Law Quarterly*, *68*(2), 309–343. Retrieved from https://doi.org/10.1017/S0020589319000046

38. Mercado, S. C. (2004). *Sailing the sea of OSINT in the information age* [dataset]. American Psychological Association. Retrieved from https://doi.org/10.1037/e741272011-005

39. Miller, C. (2014, January 21). *This is your Brain Online: How Twitter Changed the World 'Rape'*. Retrieved from https://www.politics.co.uk/comment-analysis/2014/01/20/this-is-your-brain-online-how-twitter-changed-the-word-rape/

40. Minas, H. (2010). "Research Paper No. 39: Can the Open Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the 21st Century?" *Research Institute for European and American Studies (RIEAS)*, 59.

41. Molander, R., Riddile, A., & Wilson, P. (1996). *Strategic Information Warfare: A New Face of War*. RAND Corporation. Retrieved https://doi.org/10.7249/MR661

42. Najibi, A. (2020, October 24). "Racial Discrimination in Face Recognition Technology." *Science in The News - Harvard University*. Retrieved from https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

43. NATO. (2001). *Open Source Intelligence Handbook*.

44. Pallaris, C. (2008). "Open Source Intelligence: A Strategic Enabler of National Security." *CSS Analyses in Security Policy*, *3*(32), 3.

45. Patel, F., Levinson-Waldman, R., DenUyl, S., & Koreh, R. (2019). *Social Media Monitoring – How the Department of Homeland Security uses Digital Data in the Name of National Security*. Brennan Centre for Justice.

46. Perrot, S. & Cadenza Academic Translations. (2022). "L'Open Source Intelligence dans la guerre d'Ukraine", *Politique Étrangère, Automne* (3), 63–74. Retrieved from https://doi.org/10.3917/pe.223.0063

47. Phythian, M. (Ed.). (2013). *Understanding the Intelligence Cycle*. Routledge.

48. Reuser, A. (2018, May 21). *Online course on Open Source Intelligence*. IntelHub. Retrieved from https://www.apus.edu/academic-community/intelhub/events#reuser

49. Rolington, A. (2013). *Strategic intelligence for the 21st century: The mosaic method*. Oxford University Press.

50. Rønn, K. V., & Søe, S. O. (2019). "Is social media intelligence private? Privacy in public and the nature of social media intelligence." *Intelligence and*

National Security, *34*(3), 362–378. Retrieved from https://doi.org/10.1080/02684527.2019.1553701

51. Roth, A. (2021, April 22). "European MPs targeted by deep fake video calls imitating Russian opposition This article is more than 6 mo." *The Guardian*. Retrieved from https://www.theguardian.com/world/2021/apr/22/european-mps-targeted-by-deepfake-video-calls-imitating-russian-opposition

52. Shere, A. R. K. (2020). "Now you [don't] see me: How have new legislation and changing public awareness of the UK surveillance state impacted OSINT investigations?" *Journal of Cyber Policy*, *5*(3), 429–448. Retrieved from https://doi.org/10.1080/23738871.2020.1832129

53. Simonite, T. (2022, March 17). "A Zelensky Deep fake Was Quickly Defeated. The Next One Might Not Be." *Wired*. https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/

54. Social News Daily. (2013, July 8). *'Timebomb' Tweet Taken Out of Context Gets Teen Arrested*. Retrieved from https://socialnewsdaily.com/timebomb-tweet/

55. Staniforth, A. (2016, July 19). *Big Data and Open Source Intelligence—A game changer for counter-terrorism?* Retrieved from http://trendsinstitution.org/big-data-and-open-source-intelligence-a-game-changer-for-counter-terrorism/

56. Steele, R. D. (2010). *Intelligence for earth: Clarity, integrity, & sustainability*. Earth Intelligence Network.

57. Tavani, H. T. (2008). "Informational Privacy: Concepts, Theories, and Controversies." In *The Handbook of Information and Computer Ethics* (Kenneth E. Himma&Herman T. Tavani (Eds.), pp. 131–164). Jhon Wiley & Sons.

58. Tewksbury, D., & Rittenberg, J. (2012). *News on the Internet: Information and Citizenship in the 21st Century*. Oxford University Press. Retrieved from https://doi.org/10.1093/acprof:osobl/9780195391961.001.0001

59. The Guardian. (2017, October 24). "Facebook translates 'good morning' into 'attack them', leading to arrest." *Alex Hern*. Retrieved from https://www.theguardian.com/technology/2017/oct/24/facebook-palestine-israel-translates-good-morning-attack-them-arrest

60. The Guardian. (2021, November 17). "Revealed: The software that studies your Facebook friends to predict who may commit a crime." *Johana Bhuiyan*. Retrieved from https://www.theguardian.com/us-news/2021/nov/17/police-surveillance-technology-voyager?CMP=Share_iOSApp_Other

61. The Intelligence and Security Committee of Parliament of the UK. (2018). *Annual Report 2017-2018*.

62. The New York Times. (2020a, June 24). *Wrongly Accused by an Algorithm*. Retrieved from https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

63. The New York Times. (2020b, December 29). *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*. Retrieved from https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

64. The New York Times. (2021, January 18). "The secretive company that might end privacy as we know it." *Kashmir Hill*. Retrieved from https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

65. Tolz, V., & Hutchings, S. (2023). "Truth with a Z: Disinformation, war in Ukraine, and Russia's contradictory discourse of imperial identity." *Post-Soviet Affairs*, *39*(5), 347–365. Retrieved from https://doi.org/10.1080/1060586X.2023.2202581

66. Van Puyvelde, D. (2017). "Beyond the buzzword: Big data and national security decision-making." *International Affairs*, *93*(6), 1397–1416.

67. Wakefield, J. (2022, March 18). "Deep fake presidents used in Russia-Ukraine war." *BBC News*. Retrieved from https://www.bbc.com/news/technology-60780142

68. Wells, D., & Gibson, H. (2017). "OSINT from a UK perspective: Considerations from the law enforcement and military domains." In *Proceedings Estonian Academy of Security Sciences, 16: From Research to Security Union* (pp. 84–113). Estonian Academy of Security Science.

69. Wetzling, T., & Dietrich, C. (2022). *Disproportionate use of commercially and publicly available data: Europe's next frontier for intelligence reform?* Stiftung Neue Verantwortung.

70. Williams, H. J., & Blum, I. (2018). *Defining second generation open source intelligence (OSINT) for the defence enterprise*. Rand Corporation.