OPEN SOURCE INTELLIGENCE

WHAT IS REALLY "OPEN SOURCE INTELLIGENCE"? A CONCEPTUAL ANALYSIS OF THE DIFFERENT NOTIONS OF OSINT

Ainara BORDES PEREZ*

Abstract:

The recent Ukrainian conflict has spurred innovative uses of Open Source Intelligence (OSINT) and nurtured several academic articles on the topic. It is just the last example of an overall rapid evolution of OSINT since the emergence of the Internet in the '90s, the arrival of smartphones, and the flourishing of social media and other openly available sources online in the early 21st century.

This fast evolvement has encouraged researchers and practitioners to study the validity, significance and legitimacy of this type of intelligence (OSINT) coming from openly accessible sources. However, in spite of the increased use and investigation of OSINT, its rapid evolution has hindered any universal definition of it. While practitioners and scholars have tried to conceptualise it since the beginning of its institutionalisation, different definitions shaped over the course of OSINT's expansion are ambiguous at times, vague, or incomplete. The latter has an impact on the creation of procedures for practitioners, recruitment needs, development of regulations and research.

This article studies those nuances in terminology and extracts the main conceptual differences present in some of the most prominent definitions offered by practitioners, oversight bodies and academics on OSINT. It does so through a comparative analysis of the definitions presented, which are not limited to one jurisdiction or body. Offering a structured taxonomy of the different shades of OSINT is the novelty of this article, which is a necessary first step towards a potential universal definition of the term.

Keywords: *Open Source Intelligence, OSINT, definitions, conceptual nuances, Intelligence Services, Law Enforcement*.

Introduction

Open source intelligence (OSINT) as a concept has rapidly evolved in the last decades. While open source information has supported

* A dual Ph.D. candidate at "Mihai-Viteazul" National Intelligence Academy & University of Malta, email: ainara.bordes.17@um.edu.mt.

governmental decisions since the beginning of intelligence (Schaurer & Störger, 2013), OSINT as a concept was first coined during the Cold War in the '60s and it was not until the '90s that, due to the emergence of the Internet, it started to be mentioned more regularly in publications due to the emergence of the Internet (Hatfield, 2023, pp. 6-7). Until then, monitoring and translating media was the main part of OSINT practices (Pallaris, 2008).

Advances in information technology at the end of the 20th and beginning of the 21st century with the wide spread of the Internet, the arrival of smartphones and the creation of social media, enabled new open sources to flourish and multiply, exponentially boosting the amount of openly available data. These, coupled with the opening of democracies, several geo-political changes, and some intelligence *failures* – expression used by Chris Pallaris (2008) – at the beginning of the 21st century (US 9/11, Madrid 2004, London 2005), pushed the intelligence community (IC) and law enforcement authorities (LEAs) towards stronger OSINT capabilities, and a feeling of urgency spurred its use (Hatfield, 2023, pp. 10–11). The latter, and advanced developments in data-mining and analytic software,[1] both in public and private sectors, shaped and re-shaped the notion of OSINT in the last couple of decades. The conflict in Ukraine and the various innovative ways of OSINT exploitation within it are the last examples of its changing nature (Freear, 2023).

This fast evolution has hindered any universal definition of OSINT. Practitioners and scholars have tried to conceptualise it since the beginning of its institutionalisation. However, different definitions shaped over the course of OSINT's evolution can be considered ambiguous, vague or incomplete (Wells & Gibson, 2017, p. 86).

The importance of defining any intelligence discipline (INT)[2] is diverse. From an operational perspective, prioritisation of collection efforts often follows the classification of intelligence disciplines. When collected data or information are later analysed by all-source analysts, credibility and validity are also often evaluated in accordance with the requirements per intelligence discipline (Williams & Blum, 2018, p. 21).

[1] For the purposes of this study, "data-mining software" or "data mining tools" encompasses all tools used to collect, extract and analyse large amounts of data.
[2] Whether OSINT is or should be an intelligence discipline will be discussed below.

In terms of recruitment purposes, hiring and organizing data scientists involves understanding the expertise and needs required for each intelligence discipline. Having a vague or ambiguous concept of OSINT does not help in drafting a job description, nor in assessing appropriate candidates for it (Hatfield, 2023, p. 6; Williams & Blum, 2018, p. 53). Also, from a legal perspective, intelligence practices are assessed according to their impacts on human rights (specified in international and national regulation) and in accordance with other applicable laws. These laws are usually later granulated by sectorial policies, guidance and procedures, which can sometimes be internal and classified by the institution.[3] Where OSINT as a concept is ambiguous, regulation and subsequent internal policies may become disparate regarding its feasible uses and regulatory and oversight needs. As a consequence, OSINT practices may have different legal and procedural protection in diverse security and intelligence services (SISs) and LEAs, despite prompting similar impacts on human rights and society as a whole (Omand et al., 2012, p. 820; Rønn & Søe, 2019, p. 11). Lastly, the interest in defining intelligence disciplines is also relevant for research purposes. Currently, studying the various endeavours related to OSINT requires defining the material scope of the concept by the researcher. Due to a lack of a universal definition of OSINT, published material might cover different activities, which makes it difficult to advance in this research area smoothly. Having an accepted international definition of OSINT would facilitate the study of this topic from all potential angles.

This article aims to illustrate, describe and analyse the different conceptualisations, descriptions, and opinions of the notion of OSINT, offered by the most prominent academics and practitioners on the topic throughout its evolution. For this, the study adopts a qualitative research method of a comparative nature, where it first exposes existing definitions of OSINT through a literature review of academic articles, institutional reports and policies, and studies their differences thereafter. Whilst most of the definitions may share similar characteristics, there are several disparities among them, some characteristics appear only

[3] See for example the UK National Police Chief's Council's (NPCC) Guidance on Open Source Investigation/Research (National Police Chief Council, 2015).

in some of the definitions, and many of the features need further understanding. Addressing the lack of a universal definition and structuring the differences in concept is the novelty of this article. Tackling and exposing those differences is the first step towards a debate around a potentially commonly accepted notion of OSINT.

Bearing this in mind, the article starts with a sequence of well-known OSINT definitions proposed by practitioners, scholars and policy-makers. It continues with the analysis of those definitions, divided into six different sections where the notion of OSINT is or can be interpreted differently in accordance with the definitions exposed. The study finalises with a section on conclusions on the differences encountered.

Defining Open Source Intelligence

Practitioners, scholars and policy-makers have tried to define Open Source Intelligence since the beginning of its institutionalisation in the '60s, until today. The following section encompasses a non-exhaustive list of the most prominent definitions of OSINT proposed by experts in the field over the years. These definitions are the benchmark for a later analysis of the similarities, divergences and unknowns of the notion of Open Source Intelligence.

Starting from the perception of OSINT by experts in the United States (US), the OSS Academy, a corporation founded by Robert David Steele to promote the understanding and opportunities of the use of OSINT, offered the following definition in 1998: "OSINT results from the integration of legally and ethically available multilingual and multimedia sources, with the heretofore largely secret processes of national intelligence: requirements analysis, collection management, source validation, multi-source fusion, and compelling presentation." (R. Steele & Lowenthal, 1998)

In parallel, Joseph Nye, Head of the National Intelligence Council in the US between 1993 and 1994, stated that "Open source intelligence provides the outer pieces of the jigsaw puzzle, without which one can neither begin nor complete the puzzle. But they are not sufficient of themselves. The precious inner pieces of the puzzle, often the most expensive to obtain, come from traditional intelligence disciplines. Open source intelligence is the critical foundation of the all-source intelligence

product, but it cannot ever replace the totality of the all-source effort." (Sands, 2005)

A decade later, the United States Congress adopted the Defence Authorization Act for Fiscal Year 2006, which considered that "Open Source Intelligence [is] produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement." (National Defence Authorization Act for Fiscal Year 2006 - Intelligence Community Directive Number 301, n. d.)

The Central Intelligence Agency (CIA) stated in 2010 that "information does not have to be secret to be valuable [and conceptualised open source intelligence as the] information that can be gathered from open sources, including the Internet, traditional mass media (newspapers, TV, radio broadcasts), specialized journals, conference proceedings, think tank studies, photos, maps and commercial imagery products." (Central Intelligence Agency, 2010)

Some years later, in 2018, the RAND Corporation[4] introduced the dilemma of the rapid evolution of technology and the creation of new online open sources into their definition (Williams & Blum, 2018, p. 9). While the high-level conceptualisation of OSINT proposed by them remained plain and generic – "we define OSINT as publicly available information that has been discovered, determined to be of intelligence value, and disseminated by a member of the IC," they acknowledged a lack of universal notion for OSINT and the difficulties for it due to the rapid evolution of the Internet and technology overall. With this in mind, they worked on a new taxonomy of current types of open-source information (OSINF) and data mining methods to create the notion of a "second generation of OSINT". According to them, open sources should be classified between institutionally generated content (news media and grey literature) and individually driven online content (long-form social media content such as blogs, and short-form social media content such as Facebook and Twitter content with little intelligence value individually). Moreover, they also described existing open-source analytic methods (i.e., lexical analysis, social network analysis, geospatial analysis) as part of the characterisation of the second-generation OSINT. Finally, they

[4] A widely US-based respected nonpartisan and nonprofit research organisation that aims at developing solutions to public policy challenges through research and analysis.

suggested a near-future emergence of a "third generation of OSINT", where evolution to Web 3.0 would include direct and indirect machine processing of data, machine learning and automated reasoning (Williams & Blum, 2018, p. 39). Figure 1 below shows the characteristics of the proposed OSINT generations by RAND Corporation:

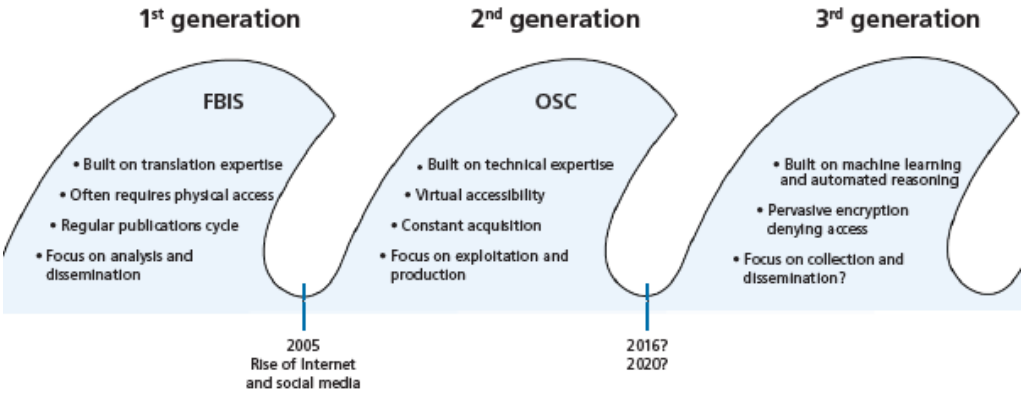

Figure 1: Characteristics of OSINT generations by RAND Corporation (Williams & Blum, 2018, p. 40)

To conclude, the last US-based definition of OSINT exposed in this article is the one provided this year (2023) by Joseph M. Hatfield, a US Naval Intelligence Officer and Assistant Professor at the US Naval Academy. As he explicitly exposes in the title of his article "There is no such thing as Open Source Intelligence", he argues that OSINT "is a fundamentally incoherent concept that should be abandoned" (Hatfield, 2023, p. 1). He challenges the underlying criteria used to demarcate OSINT as a stand-alone INT and considers that it had had its validity to help scholars and practitioners appreciate the new unclassified information that emerged with the creation of the Internet in the '90s, but this value no longer exists. He considers the term should be discarded altogether, and that openly derived sources of information should be reclassified within traditional INTs (Hatfield, 2023).

If we move to the European landscape, diverse voices have also tried to conceptualise Open Source Intelligence over the years. One of the examples is the Ministry of Defence in the UK, which defined OSINT

in 2011 as "intelligence derived from publicly available information, as well as other unclassified information that has limited distribution or access." (Ministry of Defence (UK), 2011, p. 12)

The National Police Chiefs Council (NPCC) Guidance on Open Source Investigation/Research in the UK provided a more extensive and specific definition in 2015 where they mentioned that "[Open Source Research is the] collection, evaluation and analysis of materials from sources available to the public, whether on payment or otherwise to use as intelligence or evidence … ." (National Police Chief Council, 2015).

Switching to a more recent definition, the German think tank Stiftung Neue Verantwortung analysed the notions and practices related to commercial and publicly available data within the different European intelligence agencies. According to this think tank, "OSINT comprises openly accessible data from sources such as the media, social media, and other public data" (Wetzling & Dietrich, 2022). The report also offers a non-exhaustive summary of non-legally compelled intelligence services' access to personal data, where voluntary submissions of data by the private sector, commercially available data, and OSINT are included (see Figure 2 below).

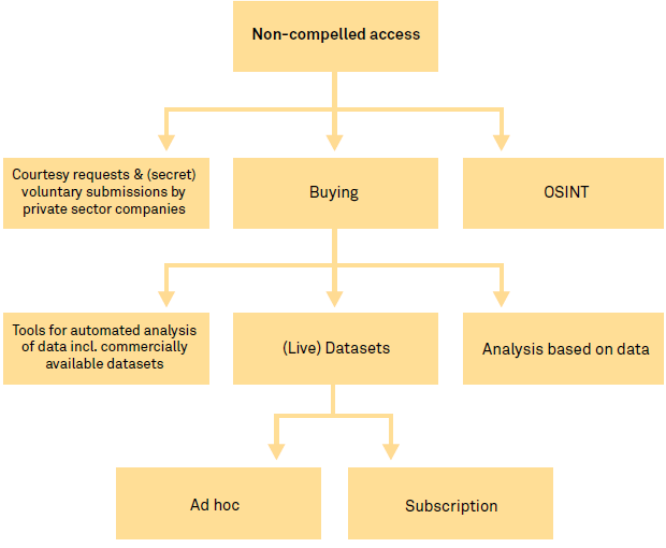

Figure 2: Modes of non-legally compelled access to data by SISs (Wetzling & Dietrich, 2022)

According to this report, the three non-compelled access modes can be understood as OSINT practices in some national regulations. The report emphasises the ambiguous terminology surrounding OSINT within SIS legislation (Wetzling & Dietrich, 2022, p. 34).

Finally, the last definition analysed is the one offered by Arno Reuser[5] in 2018, who mentioned that "Open Source Intelligence is a collaborative, integrated methodology and production process where customers' intelligence requirements are met by providing them with actionable intelligence that is produced through a process of synthesis and analysis based on a representative selection of open source information that is validated, reliable, timely, and accurate". According to this notion "… Open Source information or open sources, is all information in any format that can be acquired by anyone without any restrictions, whether for free or commercial, in a legal and ethically acceptable way" (Reuser, 2018). This notion takes relevance in today's uses of OSINT within the conflict of Ukraine as it is explained below.

Whilst most of the definitions share similar characteristics, (1) there are several disparities among them, (2) some characteristics appear only in some of the definitions, and (3) many of the features need further understanding. For example, is OSINT "information that can be gathered from open sources", as the CIA's definition states, or is it instead an "intelligence product"? Can OSINT be a stand-alone intelligence product as Arno Reuser, the NCPP and the US Congress suggest, is it just the foundation for other intelligence products, as the OSS Academy and Joseph Nye propose, or is it a concept that should disappear as Hatfield suggests? At the same time, some of the OSINT characteristics need further explanation: What is the meaning of *open sources* and where are the boundaries? What does "openly available information" mean? And finally, is OSINT open (overt) intelligence or does the openness refer only to the sources? The following sections attempt to answer those questions.

[5] Founder of the Open Source Intelligence Unit at the Dutch Defence Intelligence and Security Service (DISS) and founder of Reuser's Information Services in the Netherlands.

OSINT: Data, information, or intelligence?

The difference between data, information and intelligence is a basic one for all INTs, however, some of the different definitions exposed above seem to use these three terms interchangeably when defining OSINT.

Looking at the CIA's definition, OSINT is conceptualised as *information* that can be gathered from open sources. *Intelligence* and *information* are, nevertheless, two terms that cannot be equated. OSINT is indeed generally considered the output or the *intelligence product* derived from the processing of data and information that are accessible in open sources.[6] In other words, open source data (OSD) and open source information (OSINF) are the raw material for the creation of OSINT. NATO's Open Source Intelligence Handbook (NATO, 2001) offers a good explanation of these concepts, delimiting the notions of OSD and OSINF from OSINT, and describing the notion of *validated-OSINT*.

OSD consists of openly accessible raw material that has not been processed or edited. These primary data may comprise a photograph, a commercial satellite image, a debriefing of a government official, or technical data such as meta-data. When raw data are put together, analysed, edited, filtered and validated up to a certain level – in accordance with the requirements or needs at each moment, they become OSINF.

Likewise, open sources can also contain published OSINF that has already gone through editing and analysis and offers a clear understanding of a situation or a phenomenon. Usually, OSINF material is available from sources that have wider and easier distribution mechanisms. These sources can be traditional media, academic journals or government reports (Minas, 2010, pp. 8–11; NATO, 2001, pp. 2-3). OSINF material has received a variety of names over the years, such as: *non-secret information, overt information, unclassified information, and public information*. Likewise, the words *information* and *intelligence* have sometimes been used interchangeably, and terms like *overt intelligence* and *white intelligence* have inaccurately been employed to name both OSINF and OSINT (Saunders, 2000, pp. 12-13).

[6] The term 'open sources' is analysed in the following section.

Whilst OSINF is already a refined product providing a comprehensible story, it cannot be considered OSINT yet. OSINT is created when different OSINF and OSD materials are carefully selected, analysed, filtered, and validated, creating a compressed assessment that addresses a specific question, at a specific time, for a specific user. When OSD and OSINF materials, together with the OSINT product are analysed in terms of credibility, relevance and utility, the final product can be named *validated-OSINT* (Minas, 2010, pp. 8–11).

Thus, to summarise, OSINT does not equal *information*. It is instead an intelligence product or assessment that addresses a specific requirement of a user, on a specific topic and timing, through the processing of OSINF and OSD.

***Open sources*: what does it mean?**

The concept of *open sources* is one of the pillars of OSINT, and most of the definitions provided emphasise this. However, none of these definitions details its meaning *per se*. For instance, Arno Reuser equates *open source information* with *open sources*. However, these two terms may not represent the same thing. *Information* usually refers to the content that is found on a supporting platform, which is "the source". While the two terms are interconnected, the concepts differ.

As an alternative, the CIA, while it does not strictly define *open sources*, offers a list of sources that can be considered as *open sources*. More specifically, it conceptualises OSINT as the "information that can be gathered from open sources, including the Internet, traditional mass media (newspapers, TV, radio broadcasts), specialized journals, conference proceedings, think tank studies, photos, maps and commercial imagery product." (Central Intelligence Agency, 2010)

The CIA's definition provides an interesting point to analyse regarding the dynamism of the sources. To begin with, it offers a first glimpse of the main open sources available today, while it emphasises the dynamism of those sources with the use of the word *including*, which leaves an open door to other sources to be included in the list. Indeed, the NATO Open Source Intelligence Handbook (NATO, 2001) adds a few more sources to the CIA's list: commercial online databases (according to the Handbook, stand-alone sources separated from the Internet),

overt human experts (i.e. journalists)[7] and grey literature. The latter is a sub-group of open sources that needs special requirements, such as physical attendance or specific timing to acquire the information. Governmental reports, conferences, pre-prints and in-house letters are some examples of grey literature according to the NATO Handbook. The recent digitalisation of most of the grey literature has, nevertheless, increased the accessibility of these sources and has consequently narrowed down the number of sources included in this sub-group.

The more recent definition provided by the RAND Corporation (2018) is already focused on a digitalised world and assumes that most if not all open sources and the variety of data/information derives from this digital environment. In consequence, RAND Corporation offers a new taxonomy of open sources, distinguishing between institutionalised sources (mass media and grey literature) and sources that are individually content-driven (social media, blogs, etc.). Digitalisation is taken for granted, and there is a big emphasis on the analytic methods and the inferred data that can be extracted from those digitalised sources. Social media is the main new addition to the more classic taxonomy here, which is understandable as previous definitions were created prior to its existence. The Internet is removed from the list, and digital sources are instead sectioned in accordance with their characteristics. Commercial online databases are not addressed in RAND's definition though, creating a doubt to the reader as to whether these are considered open sources or not. Lastly, the definition provided by Stiftung Neue Verantwortung in 2023 assumes the digital world as a fact. However, after providing a generic definition of OSINT where social media is present, the think tank openly expresses that commercially available data and, furthermore, voluntary submissions of data by the private sector can also be considered open sources for some organisations.

From the analysis of the four definitions, we can realise that the term 'open sources' lacks a universally recognised definition, and that the boundaries of the notion can sometimes be difficult to establish. In

[7] NATO defines "overt human experts and observers" as people who have direct experience on a specific situation or a specific terrain. In many places of the world, it is difficult to obtain published information and some official communications may rely on second-hand reports. In those cases, an expert with experience on the ground can be valuable to get the needed insight of the situation.

particular, the rapid evolution of information technology in the last decades has created new sources that can be challenging to assess. For example, while it is generally accepted that paid-for sources such as commercial databases are *open sources* because *anyone* who pays the fee can have access to them (Koops, 2013, p. 660), this can be challenged by the RAND Corporations definition – which does not mention it as an open source, and by several private self-taught organisations (think tanks, NGOs, specialist teams) who are exploiting OSINT and collaborating with governmental institutions with seemingly no access to those databases (Freear, 2023; Wise, 2023).[8] The reasons behind a lack of access to those commercial databases can be varied. For instance, the budget cannot be sufficient. Also, commercial entities providing the datasets can delimit their services to governmental institutions only. Finally, commercial datasets are usually a mix of openly and non-openly available data provided by individuals who accepted the trade of their data by consenting to the terms and conditions and privacy notices. Can this still be called open source?

Another controversial area is the creation of fictitious identities on social media by SISs and LEAs to access specific forums or *befriend* individuals. Different organisations and oversight bodies differ as to whether those forums/profiles requiring covert access methods can still be considered open sources. The NPCC Guidelines for instance say that "contacting [in an undercover manner] individuals using social media websites" is part of the "[o]nline covert activity" of OSINT (Wells & Gibson, 2017, p. 90). Similarly, a Canadian study that interviewed several police officers in 2011 (Frank et al., 2011, p. 12) stated that typical OSINT gathering could encompass the creation of fake accounts to befriend the individual of interest or someone in their surroundings. In contrast, other voices such as the Committee for Intelligence and Security Services in the Netherlands (CTIVD) have stated the opposite. According to this Committee, the creation of a fictitious identity on social media goes beyond the mere use of an alias and must be regarded as a covert action, outside the scope of open source operations (Koops et al., 2016). This Committee, nevertheless, does not specify the differences between a *fictitious identity* and a *mere alias*. Overall, to date, there is still no universal consensus on this topic.

[8] The Ukrainian conflict is the best example of this collaboration.

A last example where the boundaries of *open sources* are blurry involves sources that are *open* or accessible only to SISs and LEAs. These sources could include, for instance, government driver and vehicle registration databases, criminal records or financial data. Several authors and practitioners have considered these databases to be *open sources* for OSINT purposes within SISs and LEAs (Layton & Watters, 2016, p. 3). However, this conceptualisation of *open sources* is open to interpretation (Wells & Gibson, 2017, p. 88).

In practice, nevertheless, LEAs and SISs often use advanced software to combine internal datasets with open sources information to get a better understanding of a situation or to enhance the predictive capabilities of the institution. Regardless of the source's nomenclature, these practices are commonly considered part of their OSINT capabilities.

Publicly available information

"Publicly available information" is a term commonly used as a synonym to OSINF as mentioned above. For example, the US Congress and the Ministry of Defence of the UK use this term in their definitions when referring to OSINF. However, the terms *open* and *available* may not always mean exactly the same thing. Indeed, it is widely accepted among practitioners and scholars that several legal and ethical limitations restrict the *availability* of information, even when this information is *open* to everyone (Lowenthal, 1998; Reagan, 2014; Reuser, 2018; Tylutki, 2018).

Some of these limitations relate to copyright and commercial requirements of vendors and are barely controversial (Lowenthal, 1998, p. 1). Others, instead, consist of human rights (especially privacy and data protection) and ethical boundaries and are still open to debate. Arno Reuser offers a good perspective on the differences between *open* and *available* information and his view about the ethical boundaries of using OSINF. Reuser states that information that is openly accessible but not intended to be open, should not be considered "publicly available information". As an example, he cites the information dumped by WikiLeaks, stating that in the absence of a clear intention by the author for publication, the material should not be considered "openly available information", and should not be used for OSINT purposes (Reuser, 2018). This was actually the way the information leaked by WikiLeaks was

treated in the US Library of Congress during 2010-2011. The SISs in the US were prohibited from using the material for their own assessments because it was still considered classified. Yet, contradictorily, this information was open and accessible to anyone with an Internet connection and of course to any foreign intelligence services (Dover et al., 2014, p. 123).

Other authors stress the legal and ethical boundaries of the uses of OSINF from a privacy and data protection perspective (Edwards & Urquhart, 2016; Nissenbaum, 2018; Rønn & Søe, 2019). As an example, Helen Nisenbaum states that making content publicly accessible is not the same as making it available for all purposes. According to her, respecting the context in which communications happen is key to assessing privacy and data protection needs (Nissenbaum, 2009).

These are only two tiny examples of the ongoing legal and ethical discussion about the uses and availability of different OSINF. However, they are enough to reflect that *openness* and *availability* do not necessarily go hand in hand.

Overt or covert intelligence?

Overt and *covert intelligence disciplines* are terms used by SISs to classify the collection methods for the production of intelligence products. *Covert intelligence disciplines* refer to practices that need clandestine means to acquire information (Saunders, 2000, p. 22). Human intelligence (HUMINT) and signals intelligence (SIGINT) are two examples that have traditionally required covert collection methods for their production. On the other hand, *overt intelligence disciplines* embrace collection methods that require no clandestine or secret means for information acquisition. Collection methods for OSINT are generally perceived as the latter (Kent, 1949, pp. 214-215; Minas, 2010, p. 9; Saunders, 2000, pp. 12–13).

Traditionally, the decision to use overt or covert collection methods has depended on whether the information sought was secret. When the information is openly accessible, it might seem reasonable to assume that no clandestine method needs to be involved to acquire it. Applying this logic to OSINT, whose raw material (OSINF) is openly accessible to everyone, OSINT has always been considered a product derived from an overt intelligence discipline.

However, as Dover *et al.* state, the *overt* notion is a misconception in regard to OSINT collection methods (Dover et al., 2014, p. 128). While some traditional information sources (e.g., radio, newspapers, etc.) allow an *overt* collection, most of the current OSINT collection methods rarely occur in an overt way despite the accessibility of the information. Collectors "may hide their interest in a conference, mask their intentions in the academic papers read or anonymize their IP address when interrogating websites" (Dover et al., 2014, p. 128). Especially in the Internet era, minimising the digital footprint and masking the collector's presence has become usual practice. Hence, the traditional notions of *overt* and *covert* may not properly represent today's differences in collection methods. While the notion *overt* can still characterise the openness of some OSD and OSINF, even the latter can be challenged in accordance with the discussion above (section "*Open sources*: what does it mean?").

In parallel, Hatfield's view of OSINT also relates to the overt vs. covert collection methods and questions the need for this distinction. As he mentions, the overall INT taxonomy is defined "in terms of its informational source – its origin's medium of transmission or acquisition" (Hatfield, 2023, p. 3). Human intelligence (HUMINT) is sourced from humans; imagery intelligence (IMINT) from images; signals intelligence (SIGINT) from signals; measurement and signature intelligence (MASINT) from specific technical sensors such as acoustic, infrared, and spectrographic. This taxonomy tries to impose order and clarity to the intelligence community and helps to understand the technical, organisational and human resources required per INT.

OSINT, nevertheless, falls outside of this order, and it is not classified according to the transmission or acquisition needs. Instead, OSINT is demarcated by a negation, as it is considered intelligence derived from information that is not under any production or distribution limitation and requires no covert action. According to Hatfield, the creation of OSINT as a stand-alone INT had been useful for practitioners to appreciate the influx of unclassified overtly available information at the brink of the Internet. However, the distinction between overt and covert is no longer valuable in today's digital environment and, in the author's view, OSINT should therefore disappear as a separate "INT". Hatfield suggests the recategorization of overtly

available sources of information into their traditional homes (INTs) to regain conceptual and analytical benefits from it. "Intelligence acquired via an image is IMINT, regardless of its degree of availability. Using commercial capabilities to measure the presence of nuclear radiation on a piece of paper is MASINT, whether it was covertly placed or originated as a publicly available newspaper in whatever remote country. Human-derived information is HUMINT, whether it was spotted, assessed, cultivated, and reported by the CIA, the BBC or any other human source" (Hatfield, 2023, p. 16). Again, the need to have distinguished overt and covert methods is questioned here.

Stand-alone intelligence vs. foundation for multi-source intelligence

Moving towards the concept of OSINT in practice, this section analyses OSINT as a stand-alone final product versus the foundation material for multi-source intelligence.

To start, the definitions provided by the OSS Academy and Joseph Nye describe OSINT as the foundation of a multi-source (also named *all-source*) intelligence product. This means that OSINT is not considered a final intelligence product, but instead, it is seen as a product integrated into an all-source process, together with other intelligence products such as SIGINT or HUMINT. The outcome of this process is an all-source actionable product that meets the requirements of users. Many practitioners and scholars support this opinion, stating that OSINT is useful as foundation material upon which other types of intelligence rest, or as material that serves to fill the gaps of fragmented covert intelligence (De Borchgrave et al., 2006, p. 12; Norton & Weaver, 2008, p. 5; Schaurer & Störger, 2013, p. 260).

However, other definitions provided by the US Congress, NPCC and Arno Reuser suggest something different. According to them, OSINT can be a final intelligence product by itself (also called "single-source intelligence"), disseminated in a timely manner, to an appropriate audience, for the purpose of addressing a specific intelligence requirement. Current technological developments and the emergence of social media networks have eased this. For example, OSINT is prioritized and used as actionable intelligence for quick responses such as for the management of natural disasters or real-time monitoring of an event (e.g. demonstrations,

international conflicts) (Backfried et al., 2012; Freear, 2023; Hogue, 2023; LCDR & USN, 2003). Furthermore, open sources might be the only directly accessible sources for actors such as international organisations (i.e. NATO, Europol, Interpol), journalists and non-governmental organisations who, beyond SIS and LEAs, are seeking intelligence (Freear, 2023; Muhammad Idrees, 2019). OSINT may play an important role as single-source actionable intelligence in these cases.

In light of the above, we can deduce that OSINT can be a final single-source intelligence product, as well as part of a multi-source intelligence process. Whether it is used one way or the other may be decided on a case-by-case basis.

OSINT as a collaborative, integrated methodology

To conclude the study of definitions, Arno Reuser offers a distinct notion of OSINT which is interesting to analyse. In his online course on open source intelligence, he defines OSINT as a "collaborative, integrated methodology and production process" (Reuser, 2018). This definition can be interpreted in two ways: (1) OSINT as a tool for institutional collaboration, and (2) OSINT as an outcome of societal collaboration.

The first interpretation is linked to institutional collaboration. SIS and LEAs are currently confronting complex threats that go beyond regional and national borders. Collaboration between and among SIS and LEAs has therefore become essential (Akhgar et al., 2015, p. 29; Martin, 2016, p. 25). In this context, being an intelligence product created through accessible information, OSINT is often considered the safest sharing option. This option allows LEAs and especially SISs to keep their inherently classified covert intelligence secret, while sharing OSINT for collaborative efforts (NATO, 2001, p. 33). Several international organisations (e.g., NATO, Europol) already use OSINT for collaboration, and the EU has also supported several projects aimed at creating a common platform for LEAs to share, exploit and analyse OSINF together (MIRROR Project; VIRTUOSO Project). However, OSINT sharing might also face some limitations. Indeed, some OSINT products, regardless of the accessibility of their sources, "may provide details of interests or intentions and should therefore be restricted in their dissemination" (NATO, 2001, p. 34)

The second of the interpretations is even broader and could go in line with R. D. Steele's understanding of OSINT which states that OSINT is a revolutionary intelligence process that allows the creation of a self-governance structure of society where all individuals take part. "All humans have access to all information all the time", and through the use of open sources, each individual can contribute to the creation of a *human mosaic* or *World Brain*. This *World Brain* allows the construction of a bottom-up structured intelligence, where publicly available information that individuals all around the world publish thanks to the Internet, can provide a continuous understanding of the world, and human interests and capabilities (R. D. Steele, 2010, p. 45).

This understanding of OSINT offers a wider view of the process and product involving OSINT in comparison with other definitions. First, it maximises the capacities of the Internet (to a utopian degree, perhaps) – something unimaginable in a definition of OSINT provided 30 years ago. Second, it includes the participation of the whole society (and each individual) in the creation of intelligence, a characteristic that none of the other definitions mention. While it sounds utopian to a degree, we can already taste this notion of OSINT through the so-called *crowdsourcing*, where individuals voluntarily collaborate and report incidents to LEAs, and the latter ask for help from citizens through social media. The London Riots in 2011 were one of the first examples of crowdsourcing (Couts, 2011; Hobbs et al., 2014). However, the best example is probably the currently ongoing conflict in Ukraine and the expanded, even revolutionised OSINT practices seen through the year and a half of war, where civil collaboration and grassroots initiatives have transformed the way OSINT was conceived until now, giving credit to Steele and Reuser's notion of it (Hogue, 2023; Perrot & Cadenza Academic Translations, 2022; Wise, 2023).

Conclusions

This article showed the difficulties academics, regulators and practitioners have in achieving a commonly accepted definition of OSINT today, largely due to the challenges of keeping pace with the digital revolution and its subsequent advances in OSINT technologies and practices.

After clarifying a terminological confusion of several OSINT definitions in regard to *information* and *intelligence* terms, the article analysed the dynamism of several core features of OSINT such as *open sources* and the *availability* of the so-called "publicly available information". The need to quickly adapt to the changing digital environment creates nuances around these terms and generates differences in opinion regarding what OSINT should involve. For instance, deciding whether sources such as commercially available datasets and some social media activities (e.g., befriending someone on FB and creating a fictitious identity to join certain forums) are *open sources* is open to discussion. Similarly, understanding the ethical and legal boundaries of some of the data/information extracted from *open sources* such as leaked data or personal data are topics that are still under debate among scholars and practitioners.

The digital revolution has also impacted the more practical *overt* notion of OSINT. Today's collection methods leave footprints that require removing and masking the collector's presence from the digital world. Hence, the traditional differentiation of *overt* and *covert* intelligence may not properly represent today's collection methods any longer. At the same time, OSINT is considered by (mainly) traditional conceptions as the foundation of a multi-source intelligence product. However, OSINT has also proved to be valuable as a final product by itself, and this perspective is now gaining ground thanks to the revolutionised OSINT practices seen in the Ukrainian conflict. The latter is perhaps proof of OSINT's potential as envisioned by Reuser and Steele, where each individual start contributing to the creation of a *World Brain* that allows the construction of a bottom-up structured intelligence.

All these nuances in the understanding of OSINT have multi-dimensional implications at a practical, legal and oversight level. To start, they bring uncertainty to practitioners regarding internal procedures to follow and recruitment purposes. As a solution, Hatfield advocates for the elimination of OSINT as an INT and the reclassification of openly derived sources of information within traditional INTs for certainty. Second, these nuances also make it difficult for regulators to understand the scope and impact of OSINT practices. As the German think tank

Stiftung Neue Verantwortung and the Dutch oversight body CTIVD showed, a lack of concrete material scope of OSINT can result in legal uncertainties and a lack of proper oversight. Finally, the vagueness in terminology also affects the overall research in the field, since it is harder to study a concept that is not fully established. Tackling and exposing these differences through this article is needed first step towards a debate around a potentially commonly accepted definition of OSINT.

References:

1. 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*. Oxford, UK: Elsevier.

2. Backfried, G., Schmidt, C., Pfeiffer, M., Quirchmayr, G., Glanzer, M., & Rainer, K. (2012). *Open Source Intelligence in Disaster Management*. 2012 European Intelligence and Security Informatics Conference, 254-258. https://doi.org/10.1109/EISIC.2012.42

3. Central Intelligence Agency. (2010). *INTelligence: Open Source Intelligence. Historical Document*. https://web.archive.org/web/20200303002208/https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html.

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

5. De Borchgrave, A., Sanderson, T., & MacGaffin, J. (2006). *Open Source Information: The Missing Dimension of Intelligence*. Centre for Strategic and International Studies (CSIS) - Transnational Threats Project.

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

7. 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. https://doi.org/10.1093/ijlit/eaw007.

8. European Union Funded H2020 Project, Grant Agreement No 832921. (n. d.). MIRROR Project. https://h2020mirror.eu/.

9. EUROSINT Forum, European FP7-funded project. (n. d.). VIRTUOSO Project. https://www.eurosint.eu/virtuoso-project.

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

11. Freear, M. (2023, March 14). *OSINT in an Age of Disinformation Warfare*. RUSI.Org.

12. Hatfield, J. M. (2023). "There Is No Such Thing as Open Source Intelligence." *International Journal of Intelligence and Counterintelligence*, 1-22. https://doi.org/10.1080/08850607.2023.2172367.

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

14. 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.

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

16. Koops, B. J. (2013). "Police Investigations in Internet open sources: Procedural-law issues." *Computer Law & Security Review*, 29, 654–665.

17. Koops, B. J., Roosendaal, A., Kosta, E., van Lieshout, M., Oldhoff, E., & Hildebrandt, M. (2016). TNO 2016 R10150-rapport – Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdienstein 20XX (p. 186). TNO innovation for life, Report for the Dutch Ministry of Internal Affairs.

18. Layton, R., & Watters, P. A. (Eds.). (2016). *Automating open source intelligence: Algorithms for OSINT*. Elsevier/Syngress.

19. LCDR, T. N., & USN, P. (2003). *Open Source Intelligence – Doctrine's neglected child*. Rhode Island, US: Naval War College.

20. Lowenthal, M. M. (1998). *Special Reports – Open Source Intelligence: New Myths, New Realities.* Washington D.C., US: Defence Daily Network Special Reports.

21. Martin, S. (2016). *Spying in a Transparent World: Ethics and Intelligence in the 21st Century*, 19/16 Research Series. GCSP. https://dam.gcsp.ch/files/2y10IFJfn5WfxlznHTeypxCeKNqdi9ptdONTckNIjqiSTuxCdF8PFXy

22. 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.

23. Ministry of Defence (UK). (2011). *Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations*. Ministry of Defence Development, Concept and Doctrine Centre. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf.

24. Muhammad Idrees, A. (2019, June 10). "Bellingcat and how Open Source Reinvented investigative journalism." *The New York Review*. https://www.nybooks.com/daily/2019/06/10/bellingcat-and-how-open-source-reinvented-investigative-journalism/.

25. National Defence Authorization Act for Fiscal Year 2006 – Intelligence Community Directive Number 301, Pub. L. No. 109–163, ICD 301.

26. National Police Chief Council. (2015). NPCC Guidance on Open Source Investigation /Research. Police Forces in England and Wales.

27. NATO. (2001). Open Source Intelligence Handbook.

28. Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* California: Stanford University Press.

29. Nissenbaum, H. (2018). *Respecting Context to Protect Privacy: Why Meaning Matters. Science and Engineering Ethics*, 24(3), 831-852. https://doi.org/10.1007/s11948-015-9674-9.

30. Norton, R. A., & Weaver, G. S. (2008). *Open Source Intelligence and Technology – A Natural Nexus for Academia and the Intelligence Community*. Auburn, Alabama, US: Auburn University.

31. Omand, D., Bartlett, J., & Miller, C. (2012). "Introducing Social Media Intelligence (SOCMINT)." *Intelligence and National Security*, 27(6), 801-823. https://doi.org/10.1080/02684527.2012.716965.

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

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

34. Reagan, C. M. L. (2014). *Terms & Definitions of Interest for Counterintelligence Professionals – Glossary (Unclassified).* Department of Defense (DoD) of the US.

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

36. 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. https://doi.org/10.1080/02684527.2019.1553701.

37. Sands, A. (2005). "Integrating Open Sources into Transactional Threat Assessments." In J. E. Sims & B. Gerber (Eds.), *Transforming U.S. Intelligence*. Georgetown, US: Georgetown University Press, p. 64.

38. Saunders, K. (2000). *Open Source Information – A True Collection Discipline* [Master Thesis]. Master of Arts (War Studies) – Royal Military College Canada.

39. Schaurer, F., & Störger, J. (2013). "The Evolution of Open Source Intelligence (OSINT)." *Journal of U.S. Intelligence Studies*, 19(3), 4.

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

41. Steele, R., & Lowenthal, M. (1998). *Open Source Intelligence: Private Sector capabilities to Support DoD Policy, Acquisitions, and Operations.* Defence Daily Network Special Report. https://fas.org/irp/eprint/oss980501.htm#N_1. Accessed 27 May 2020.

42. Tylutki, K. (2018). "The information of a mass destruction range – OSINT in intelligence activities." *Internal Security Review* 19/18, 384-404.

43. 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.

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

45. Williams, H. J., & Blum, I. (2018). *Defining second generation open source intelligence (osint) for the defense enterprise*. Santa Monica, US: Rand Corporation.

46. Wise, J. (2023, March 4). "The DIY Intelligence Analysts Feasting on Ukraine Meet the would-be Jack Ryans of OSINT." *New York Intelligencer*. https://nymag.com/intelligencer/2022/03/the-osint-analysts-feasting-on-ukraine.html.