**JOURNAL OF ANTI-CORRUPTION LAW**

**2024 Volume 8 Pages 159 – 174**

**HARNESSING OSINT TO ENHANCE THE INVESTIGATION OF** **ECONOMIC CRIME**

**Claire** **Adionyi[[1]](#footnote-1)\***

**ABSTRACT**

Economic crime is considered one of the fastest-growing global threats. As noted by the United Nations Office on Drugs and Crime (UNODC), this threat is increasingly enabled by technological advancements such as electronic banking and expanded internet access. While these advancements facilitate economic crime, this paper argues that they also provide new avenues for economic crime investigators to harness the power of open-source intelligence (OSINT). Defined as publicly available information that is accessible to any member of the public without the need for special legal status or authorisation, OSINT offers a wealth of untapped evidence that can enhance traditional investigative methods significantly. This paper explores how OSINT can be leveraged to supplement and transform traditional approaches to economic crime investigations. By relying on the hypothesis that OSINT can significantly augment the range and accessibility of available evidence, this research proposes that the integration of OSINT into conventional investigation techniques will result in a more efficient and comprehensive economic crime investigation. Based on a desk study of both primary and secondary data, this paper aims to demonstrate how OSINT tools and strategies can provide innovative solutions to bolster the ongoing fight against economic crime.

1. **INTRODUCTION** 
   1. **OSINT in legal context**

The Berkeley Protocol defines Open-Source Intelligence (OSINT) as “a subcategory of open source information that is collected and used for the specific purpose of aiding policymaking and decision-making, most often in a military or political context”.[[2]](#footnote-2) Open-source information refers to information that is publicly available and can be observed, purchased or requested by any member of the public without requiring special legal status or utilising unauthorised access.[[3]](#footnote-3) Therefore, according to this Protocol, OSINT is open-source information that is collected, exploited, and disseminated for the purpose of addressing a specific intelligence requirement.[[4]](#footnote-4) Various other definitions of this phenomenon exist but they all appear to mirror each other. For example, Pastor-Galindo, Nespoli, Mármol & Pérez define it as consisting of “the collection, processing and correlation of public information from open data sources such as the mass media, social networks, forums and blogs, public government data, publications, or commercial data”.[[5]](#footnote-5) The emphasis is on the process of collection from open sources, and the analysis process which utilises open-source software. Based on the foregoing, OSINT techniques can therefore be defined as the use of open-source information for the purpose of collecting information that can consequently be used as evidence.

There are multiple OSINT tools, a phenomenon that is increasingly enabled by rapid technological evolution such as advancements in machine learning capabilities and computing power. A few examples are provided for demonstrative purposes. These include: Maltego, an application that automatically finds publicly available information about certain targets within different sources such as search engines, social networks and the metadata of files;[[6]](#footnote-6) Spiderfoot, which automatically assesses public data sources from input such as IP addresses, subnet, domain names, e-mail addresses, among others, to compile information that is represented in a graph of nodes with all the entities and relationships found;[[7]](#footnote-7) and Fingerprinting Organisations with Collected Archives (FOCA), a tool that extracts and analyses metadata present in electronic documents and can be used for both local files present in computers and external documents that are downloaded from specified webpages;[[8]](#footnote-8) to name a few examples.

As expected, there are various iterations of OSINT techniques that are available to an economic crime investigation. Similarly, this list is not exhaustive but demonstrative of the available techniques. The most prevailing iteration of these techniques is social media investigation which entails collecting and analysing information from social media platforms such as Facebook, X (formerly Twitter), and YouTube, among others. Social media investigation entails the use of techniques such as, inter alia, tracking geolocation tags from videos and images, and using hashtags to collect information.[[9]](#footnote-9) Metadata analysis, a technique that encompasses the extraction of metadata content, can be used to, for instance, identify where an image was taken in the course of an investigation.[[10]](#footnote-10) Another important technique that actually leverages the negative aspects of the internet against criminals, is mining the deep web for data by utilising special browsers such as Tor. Deep web data mining can thus be used to gather intelligence on illicit activities such as money laundering. Other techniques include geospatial analysis, media and news monitoring, and so forth.[[11]](#footnote-11)

Evidently, the ultimate choice of techniques to be employed during a specific investigation would be dictated by the particularities of the subject matter of each investigation.

* 1. **Overview of economic crimes and their complexity**

Economic crime, defined as any “illegal act committed by an individual or a group of individuals to obtain a financial or professional advantage”, is considered to be one of the fastest growing global threats.[[12]](#footnote-12) The UNODC conceives the term “economic crime” as relating to any non-violent crime which has financial gain as its end-product.[[13]](#footnote-13) Various illegal activities fall under this ambit and these include fraud, money-laundering, corruption, tax evasion, and the like.[[14]](#footnote-14) The prosecution of economic crime is encumbered by many complexities, some of which arise from a “lack of a clear and accepted” definition of the term.[[15]](#footnote-15)

However, this paper focuses on the impact that rapid and continuous technological advancement has on economic crime. By creating a new informational landscape that has transformed the flow of information globally and changed the way of doing business, technological advancements are creating an enabling environment in which economic crime thrives. These advancements are also making the process of collecting and preserving evidence that relates to economic crime more challenging. As opined by the UNODC, this threat is increasingly being enabled by technological advancements such as electronic banking and internet expansion.

While these advancements facilitate economic crime, it is contended that they can also provide new opportunities for economic crime investigators to leverage the potential of OSINT by providing access to a wealth of untapped evidence that can significantly enhance traditional economic crime investigative methods.

Accordingly, this paper explores how OSINT techniques can be leveraged to supplement and transform traditional approaches to economic crime investigations. By relying on the hypothesis that OSINT can significantly augment the range and accessibility of available evidence, this research proposes that the integration of OSINT into conventional investigation techniques will result in a more efficient and comprehensive economic crime investigation.

Based on a desk study of both primary and secondary data, this paper aims to demonstrate how OSINT tools and strategies can provide innovative solutions to bolster ongoing efforts that are directed towards combatting economic crime, by supplementing traditional methods. The paper therefore contains an assessment of the role that OSINT tools and techniques can play in complementing the various phases of a traditional investigation cycle. Cognisant that OSINT is not unencumbered, the paper simultaneously discusses the various challenges and limitations that surround the usage of these tools and techniques and provides possible solutions on how they can be mitigated.

1. **THE ROLE OF OSINT IN COMPLEMENTING TRADITIONAL METHODS OF INVESTIGATION**

In light of the central thesis of this paper that an economic crime investigation can benefit by leveraging OSINT techniques, this section assesses the role of OSINT in complementing traditional methods of investigation. Accordingly, an assessment of how this can occur in the context of an investigation cycle is conducted. This thesis is buttressed by the recognition that traditional repressive methods of crime prevention and control are not very adequate. For instance, a Council of Europe’s Manual on Criminal Prosecution noted that “traditional methods do not represent the most adequate instruments for combatting crime”. This conclusion is based on the assessment that these methods have failed to provide any significant results in that regard.[[16]](#footnote-16)

Before delving into an in-depth discussion of how this integration can be achieved, it is important to highlight some of the challenges that traditional methods face. One of the well-recognised challenges of traditional methods is that despite the availability of data relating to these crimes, investigations are hampered by the inability to effectively interpret this data in order to define the problem and to identify the targets that are to be prioritised.[[17]](#footnote-17) Based on its capabilities to analyse large volumes of data in an automated manner, OSINT can very easily be harnessed to bridge this gap. The second challenge relates to the skills and resource gap. As observed by Wood, combatting economic crime requires a tailored solution and a different set of tools and techniques to be developed under what she terms a proper workforce strategy.[[18]](#footnote-18) Furthermore, traditional methods are sometimes encumbered by physical access restrictions resulting from, for instance, security concerns and denial of permission by relevant authorities.[[19]](#footnote-19) This paper contends that this challenge can similarly be addressed through OSINT, primarily due to its capacity for automation and conducting a larger volume of analytics as compared to manual methods.

It is however important to reiterate that the aim of this paper is not to advocate for a complete replacement of traditional methods of investigating economic crime, but rather it is a proposal that OSINT should be used to complement these methods. The following section assesses how these tools and techniques can be incorporated in the context of an investigation cycle.

An OSINT investigation cycle contains various phases as outlined below:

1. the identification of information that may be potentially useful from open data sources;

1. validation of the collected information to ensure that it is detailed, comprehensive and valuable;
2. analysis of the validated information to ascertain whether it is what it purports to be; and
3. incorporation of the information for use as evidence in a court of law.[[20]](#footnote-20)

The investigation cycle can therefore be summarised into four phases: the direction phase; the collection phase; the processing and analysis phase; and the verification and dissemination phase, which ideally reflects the traditional investigation cycle.[[21]](#footnote-21) The benefits that potentially accrue from integrating OSINT techniques into an economic crime investigation are significant mainly because these methods rely on information that is already publicly available, eschewing the challenges faced by the traditional methods such as restricted accessibility. And given the proliferation of smartphones and internet-enabled devices, technological advancements such as artificial intelligence and consequent machine-learning capabilities, there is an informational gold mine from which any modern legal investigation can benefit from by leveraging OSINT.

* 1. **The direction phase**

The direction phase is the stage whereby the planning and preparation for the actual investigation takes place.[[22]](#footnote-22) The Berkeley Protocol refers to this stage as the online inquiries’ stage. Two processes take place at this stage: searching, defined as the process of discovering information and sources of information using general or advanced search methodologies; and monitoring, which entails discovering new information through consistent and persistent review of a set of constant sources.[[23]](#footnote-23) These processes can benefit from OSINT in multiple ways. The first benefit relates to the vast amount of information that is available from open sources that can be available to an investigator through the use of specific OSINT tools.[[24]](#footnote-24) Identically, due to advancements in computing power, OSINT can be applied to a vast amount of publicly-available information and by relying on these advanced processes and analysis techniques, a high number of data sets can ably be mixed to clarify relationships and patterns from different types of open sources.[[25]](#footnote-25) By relying on the multitude of data analysis and data mining as a result of big data and machine-learning algorithms, an economic crime investigation can be automated resulting in a more intelligent output.[[26]](#footnote-26)

The Berkeley Protocol provides an in-depth outline on how an investigator can conduct these processes. For instance, during the search process, a structured search can be conducted on social media platforms and the Protocol emphasises the importance of ensuring that the methodology is documented as necessitated by laws of procedure and evidence.[[27]](#footnote-27) If integrated into a search for information in the context of a financial fraud investigation, for example, OSINT can be used to track digital footprints to reveal fraudulent financial transactions and can equally be used to analyse publicly available financial data to identify any suspicious patterns. In terms of combatting money laundering, OSINT tools and techniques can reveal money laundering operations, through for instance, cross-referencing public data such as real estate ownership, offshore accounts, and the like, to detect the money laundering. It is important to emphasise the need of ensuring that this entire process is structured, right from the monitoring stage. This can be accomplished through making “use of lists of known and previously evaluated online sources, such as websites or social media accounts, as well as search queries that are run on an ongoing basis against defined targets”.[[28]](#footnote-28) The benefit of conducting a structured search is that it enhances the evidence dissemination stage by enabling an arbiter to be able to follow the process of evidence gathering.

Another crucial value that OSINT adds to an investigation cycle that an economic crime investigation can benefit from is its ability to actively counterbalance bias – both the cognitive bias, that is, the investigator’s bias; or the technical bias, that is, “bias in the machine”.[[29]](#footnote-29) This can be achieved by taking advantage of the vast amount of open-source information thus enabling the broadening and diversification of an online inquiry.[[30]](#footnote-30) Similarly, the ability to ascertain the *prima facie* relevance and reliability of a piece of information is a benefit that accrues from these tools and techniques. Regarding the assessment of *prima facie* reliability, for instance, by using OSINT tools and techniques, an investigator will be able to ascertain the original source of open-source material by checking its embedded metadata to trace the data’s online provenance and its uploader, author, or both.[[31]](#footnote-31)

Therefore, an economic crime investigator can develop, amongst others, an investigative plan, develop a reporting plan, track the investigation progress, by relying on these tools and techniques resulting in the enhancement of this formative stage through ensuring accuracy and effectiveness.[[32]](#footnote-32) Furthermore, there is the added effect of safeguarding these investigations from the onset as the processes are embedded with steps that enable an investigator to abide by legal requirements such as the procedural requirement of maintaining the chain of custody, as this is the very essence of conducting a structured search process.

* 1. **The collection phase**

The second phase, that is, the process of identifying potentially relevant information and evidence can similarly leverage OSINT tools and techniques.[[33]](#footnote-33) By relying on tools such as social media information, media articles and reports, among others, an economic crime investigator has access to a vast berth of publicly available information. Beyond the increase in the amount of potentially relevant information, this phase of the investigation can equally be made more effective by applying technology. These benefits primarily relate to the fact that OSINT can be applied to “strike a balance between comprehensive data collection and the targeted identification of relevant information”.[[34]](#footnote-34) This is especially important keeping in mind the huge volumes of information that exist in the current digital/informational era. Specifically, these tools and techniques can allow an investigator to conduct searches across different platforms simultaneously by using a key search term.[[35]](#footnote-35) A process that would be both extremely cumbersome and would also increase the chances of errors if it were conducted manually.

* 1. **The processing and analysis phase**

The process of managing and preserving the collected evidence can also benefit from OSINT tools and techniques. At this stage, processes such as the categorisation, logging and filtering of the gathered data are conducted. Equally, by relying on OSINT, it has been observed that automation can transform the effectiveness and efficiency of these processes.[[36]](#footnote-36) Various OSINT tools and scripts can be used to automate the collection process and to ensure that the probative value of the information is maintained.[[37]](#footnote-37) In order to support the process of proving the authenticity of such information during a judicial process, these tools and techniques can identically be leveraged to ensure that the information collection process is thorough and entails a sound method of capture.[[38]](#footnote-38) A recommended best practice is utilising these tools to automatically collect foundational information such as, inter alia, the target web address (URL), the source code, embedded media files and metadata, hash value, and contextual data.[[39]](#footnote-39) Eventually, the same tools and scripts can be used to generate the technical report that would be used to establish the authenticity of the collected information in a legal process.[[40]](#footnote-40)

As opined by Pherson and Heuer Jr, the process of analysis within this context is continuously evolving from a mental activity done by an individual analyst to a collaborative effort due to various reasons such as the growing complexity of crimes.[[41]](#footnote-41) Pastor-Galindo, Nespoli, Mármol & Pérez hold a similar view as they propose that a key distinguishing factor between human-driven and intelligence-led analysis is that by incorporating OSINT, the process of collection and analysis improves significantly, resulting in accurate investigations thus emphasising the importance of OSINT.[[42]](#footnote-42) The use of OSINT techniques such as the structured analytic technique can facilitate such transitions by “guiding the exchange of information and reasoning among analysts in ways that identify and eliminate a wide range of cognitive biases and other shortfalls of intuitive judgment”.[[43]](#footnote-43)

Identically, a forensic analysis that utilises OSINT can be conducted on the retrieved evidence to ensure that the information is what it purports to be. On the other hand, OSINT tools and techniques can also be used to conduct data enrichment and review because they provide the possibility of integrating complementary types of data. Pastor-Galindo, Nespoli, Mármol & Pérez further observe that OSINT can be much more effective as due to its nature there is room for an investigator to add external pieces of information to complement the data from open sources.[[44]](#footnote-44) For example, by conducting a geospatial analysis, recollected data from social networks can be analysed from a location-based perspective thus enhancing the ability to extract meaningful connections between the data-set.[[45]](#footnote-45) This analysis can further be augmented by conducting a social media analysis to bolster the findings of an investigation by providing various collaborative data-sets.[[46]](#footnote-46) Thus, information that is to be used as evidence in a legal process can be processed, its reliability and relevance can be assessed and packaged into a report by using OSINT tools.[[47]](#footnote-47) It is also during this stage that “investigation-specific issues” such as preserving the chain of custody, can be assured by utilising digital preservation systems.

* 1. **The verification and dissemination phase**

As information collected in the investigation of economic crime will ultimately feed into a judicial process, the verification aspect of the evidence processing phase is important. The significance of the verification stage is further heightened given the nature of open-source information – its high susceptibility to manipulation. Defined as the process of establishing the accuracy or validity of information that has been collected online, OSINT tools and techniques can be used to verify the collected information by analysing: the source of the information, the digital information itself, and the content of the information.[[48]](#footnote-48)

OSINT processes such as social network analysis, which involves the “mapping and measuring of relationships between people, groups, organisations, computers, URLs and other connected information/knowledge entities” can easily be undertaken as part of the verification process by utilising an analytics software.[[49]](#footnote-49) Actor mapping can equally be conducted to understand key actors, identify power relations and channels of influence and consequently map out the relationship between these aspects.[[50]](#footnote-50) Given the interconnected nature of some economic crimes such as money laundering, it would be necessary for an investigator to establish such linkages in order to prove criminal responsibility.

The final step comprises of the process of producing and presenting the evidence in a format that can be used by competent judicial authorities as evidence in legal proceedings. By relying on OSINT, the evidence can be adapted into a visual and interactive format to enhance clarity and the ability of judicial actors to synthesise and effectively interact with this type of evidence.[[51]](#footnote-51) This is because most OSINT tools contain visualisation capabilities that support an investigator to synthesise large volumes of information thus enhancing the dissemination process.[[52]](#footnote-52) Other benefits that may accrue from these tools and techniques at this stage of the investigation cycle include enhancing consistency, standardisation, and enhancing information-sharing.[[53]](#footnote-53)

1. **CHALLENGES AND LIMITATIONS OF OSINT IN ECONOMIC CRIME INVESTIGATIONS**

Due to its nature, OSINT is encumbered by various challenges and limitations. It is therefore important to address some of these concerns to ensure that the open-source information that finds its way into legal proceedings as evidence is not prejudicial. The first challenge, as highlighted in the foregoing, arises from the fact that open-source information is highly susceptible to manipulation.[[54]](#footnote-54) As advancements in computing power continue to grow rapidly, artificial intelligence and machine-learning capabilities are continually increasing the ease of such manipulation through applications such as Photoshop, ChatGPT, to name a few.[[55]](#footnote-55) This susceptibility inevitably raises questions regarding the reliability of the collected information. It is for this reason that it is crucial that the investigation stages adhere to the rules of procedure and evidence. To wit, Freeman and Llorente observe that

it is more necessary than ever before to collect and preserve digital material in a forensic manner, maintain and document a clear chain of custody, ensure secure storage of originals offline, and engage technical experts in the handling of digital evidence at all stages.[[56]](#footnote-56)

Furthermore, the inclusion of the “verification phase” as a stand-alone phase of the investigation cycle – a non-traditional approach – is an attempt by this paper to respond to this challenge. Recognising this weakness, the paper proposes that the presence of a strong verification process is necessary in order to safeguard the authenticity of the information that eventually makes its way to court as open-source evidence.

Closely connected to the first challenge, is the risk of disinformation, misinformation and false information.[[57]](#footnote-57) As observed by Murray, McDermott & Koenig, disinformation or manipulation is a problem that every OSINT investigator has to contend with.[[58]](#footnote-58) This is due to the fact that, one of the biggest dangers of the rapid advancements in technology is the increase in the ability of digital content to be manipulated creating a very real risk for falsification. For instance, the advancement in machine learning capabilities makes it easy for virtually any internet user to develop hyper-realistic deep-fake content using open-source applications such as Vidnoz Flex and Leonardo.Ai, amongst others.[[59]](#footnote-59)

The second challenge relates to the fact that due to the proliferation of smartphones, internet connectivity and advancement in technology, there exists a vast volume of data which can potentially overwhelm an investigation. To exemplify how significant the volume hurdle is, Freeman and Llorente observe that a simple burglary case could produce terabytes of data from sources such as mobile devices and GPS data.[[60]](#footnote-60) Amplifying this to the level of an economic crime investigation means that the volumes increase exponentially, further complicating the challenge of filtering the relevant information. These large volumes of data can inevitably strain the investigation process. However, the presence of guidelines such as the Berkeley Protocol provides recourse by proffering recommendations on how an OSINT investigator can manage this challenge. The Protocol for instance advises that a preliminary assessment of any identified material should be conducted before it is collected in order to reduce the volumes.[[61]](#footnote-61) Specifically, the Protocol advises that “open source investigators should conduct a preliminary assessment of any material that they identify in order to avoid over-collection and to comply with the principles of data minimisation and focused investigation”.[[62]](#footnote-62)

The third challenge arises from the transnational nature of most economic crimes, on the one hand, and the borderless nature of the internet on the other, which create the potential for jurisdictional issues to arise when collecting open-source data across borders. To minimise this issue, the Berkeley Protocol advises that an OSINT investigator should strive to collect and preserve the information in a way that maximises its ability to be used in the widest range of potentially relevant jurisdictions.[[63]](#footnote-63)

Ethical and legal considerations in the usage of OSINT tools and techniques is another challenge that must be contended with. The pertinent question here being how to strike a balance between legal boundaries while also ensuring that there is effective intelligence gathering. Millet notes that despite its benefits, OSINT has the potential of negatively impacting various individual rights such as fair trial rights, the right to privacy and data protection rights.[[64]](#footnote-64) In order to ensure that the impact on these rights is mitigated, it is recommended that an investigator employs a “human rights based” approach in their investigation. Various actors have developed guidelines to enable investigators to be mindful of these considerations in their processes. These include a report on “Ethical Considerations for Open-Source Investigations” by the University of Essex, and the Berkeley Protocol.[[65]](#footnote-65) Koenig takes it a step further by proposing a three-step process, which she estimates would facilitate the decision-making process for an investigator, regardless of the investigation’s context. She suggests that the investigator should:

1. identify what the law says they can or cannot do according to their professional identity, intended purpose, and relevant jurisdiction;
2. solicit guidance from their professional code of ethics (if they have one); and
3. weigh their options against the values of safety, accuracy, and dignity.[[66]](#footnote-66)

Accordingly, even in the context of an economic crime OSINT investigation, these challenges may arise. Investigators must remain aware of them and take active steps to minimise their impact on the collected information, thereby enhancing its reliability as evidence in legal proceedings.

1. **CONCLUSION**

The role of OSINT techniques in combatting economic crime has proven to be indispensable in the modern digital era as they are a powerful tool. By leveraging publicly available data and advanced techniques, law enforcement and regulatory bodies now possess the ability to track and uncover illicit activities more efficiently. This paper has highlighted several OSINT tools and techniques that can be effective in detecting crimes such as fraud and money laundering, largely due to the increasingly interconnected nature of financial systems. To demonstrate the value of integrating OSINT into comprehensive economic crime-fighting strategies, this paper has compared traditional investigative approaches with OSINT.

However, the application of OSINT is not without its own set of challenges. These include privacy concerns, potential bias, and the legality of certain data collection which could arise from jurisdictional complexities. Therefore, for an economic crime investigation to fully benefit from OSINT, it is imperative that a balanced approach is employed keeping in mind the relevant legal and ethical considerations.

To conclude, while OSINT is not a panacea for all investigative needs, its role in complementing traditional methods of investigating economic crime cannot be overstated. It would therefore be prudent to integrate OSINT techniques into these investigations to enhance both their efficiency and effectiveness.

1. **\*** Claire Adionyi, LLD, Lecturer, Strathmore Law School, Nairobi,

   Email: [cadionyi@strathmore.edu](mailto:cadionyi@strathmore.edu) ORCID ID: <https://orcid.org/0000-0001-8684-2433> [↑](#footnote-ref-1)
2. Human Rights Center UC Berkeley School of Law & Office of the United Nations High Commissioner for Human Rights (OHCHR) (2022) *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*, available at <https://digitallibrary.un.org/record/3973652?ln=en&v=pdf> (visited 20 December 2024) at 7. [↑](#footnote-ref-2)
3. Human Rights Center UC Berkeley School of Law & OHCHR (2022) at 6. [↑](#footnote-ref-3)
4. Human Rights Center UC Berkeley School of Law & OHCHR (2022) at 7. [↑](#footnote-ref-4)
5. See, Koenig A (2024) “Ethical Considerations for Open-Source Investigations into International Crimes” 118 *AJIL Unbound* 45 – 50; See also, Pastor-Galindo J, Nespoli P, Mármol FG & Pérez GM (2020) “The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends” 8 *IEEE Access* 10282 – 10304 at 10282. [↑](#footnote-ref-5)
6. Maltego, available at http://bit.ly/4gAURcG (visited 3 October 2024). [↑](#footnote-ref-6)
7. Intel471, available at <https://intel471.com/solutions/attack-surface-protection> (visited 3 October 2024). [↑](#footnote-ref-7)
8. Telefónica Tech, available at <https://cybersecuritycloud.telefonicatech.com/en> (visited 3 October 2024). [↑](#footnote-ref-8)
9. UNODC *Open Source Intelligence Investigations*, available at <https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/investigation/OSINT.html> (visited 3 October 2024). [↑](#footnote-ref-9)
10. Frank E, Hall MA & Witten IH. The WEKA workbench. Online appendix for" Data mining: Practical machine learning tools and techniques" (2016) *Data Mining: Practical Machine Learning Tools and Techniques* 4th ed Elsevier at 503 – 532. [↑](#footnote-ref-10)
11. Pastor-Galindo, Nespoli, Mármol & Pérez (2016) at 6. [↑](#footnote-ref-11)
12. Europol *Economic Crime*, available at <https://www.europol.europa.eu/crime-areas/economic-crime> (visited 3 October 2024). [↑](#footnote-ref-12)
13. UNODC *Open Source Intelligence Investigations*. [↑](#footnote-ref-13)
14. UNODC (2005) “Economic and Financial Crimes: Challenges to Sustainable Development” UN Congress on Crime Prevention and Criminal Justice, Fact Sheet 5. [↑](#footnote-ref-14)
15. UNODC (2005). [↑](#footnote-ref-15)
16. Huremagić R, Penko B & Tegeltija M (Spring 2004 – Spring 2006) *Manual on* *Criminal Prosecution of Corruption and Economic Crime Offences*  Council of Europe: PACO at 72. [↑](#footnote-ref-16)
17. Wood H (11 July 2022) “Five Problems with Economic Crime Policing – And How to Solve Them” *Royal United Service Institute (RUSI)*, available at <https://rusi.org/explore-our-research/publications/commentary/five-problems-economic-crime-policing-and-how-solve-them> (visited 3 October 2024). [↑](#footnote-ref-17)
18. Wood (11 July 2022). [↑](#footnote-ref-18)
19. Abrahams F & Murray D (2020) “Open Source Information: Part of the Puzzle” in Dubberley S, Koenig A & Murray D (eds) *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation and Accountability* Oxford University Press at 85 – 105. [↑](#footnote-ref-19)
20. UNODC *Open Source Intelligence Investigations*. [↑](#footnote-ref-20)
21. See generally, Böhm I & Lolagar S (2021) “Open Source Intelligence: Introduction, Legal, and Ethical Considerations” 2 *International Cybersecurity Law Review* 317 – 337; See also, Blackdot Solutions *The OSINT Handbook: How to Use Open Source Data to Transform Investigatory Best Practice*, available at <https://blackdotsolutions.com/wp-content/uploads/2021/11/The-OSINT-Handbook_.pdf> (visited 3 October 2024). [↑](#footnote-ref-21)
22. Böhm & Lolagar (2021) at 323. [↑](#footnote-ref-22)
23. Human Rights Center UC Berkeley School of Law & OHCHR (2022) at 56. [↑](#footnote-ref-23)
24. Wong BLW (2016) “Fluidity and Rigour: Addressing the Design Considerations for OSINT Tools and Processes” in Akhgar B, Bayerl PS & Sampson F (eds) *Open Source Intelligence Investigation: From Strategy to Implementation* Springer International Publishing 167 – 185. [↑](#footnote-ref-24)
25. Pastor-Galindo, Nespoli, Mármol & Pérez (2016) at 4. [↑](#footnote-ref-25)
26. Gandomi A & Haider M (2015) “Beyond the Hype: Big Data Concepts, Methods, and Analytics*”* 35(2) *International Journal of Information Management* 137 – 144. [↑](#footnote-ref-26)
27. Human Rights Center UC Berkeley School of Law & OHCHR (2022) at 56. [↑](#footnote-ref-27)
28. Human Rights Center UC Berkeley School of Law & OHCHR (2022) at 56. [↑](#footnote-ref-28)
29. Zarmsky S & Mionki J (10 February 2023) “Symposium on Fairness, Equality, and Diversity in Open Source Investigations: Out in the Open: Fair Trial Rights and Open Source Evidence at the ICC” *Opinio Juris*, available at <https://opiniojuris.org/2023/02/10/symposium-on-fairness-equality-and-diversity-in-open-source-investigations-out-in-the-open-fair-trial-rights-and-open-source-evidence-at-the-icc/> (visited 3 October 2024); See also, Human Rights Center UC Berkeley School of Law & OHCHR (2022) at 57. [↑](#footnote-ref-29)
30. Human Rights Center UC Berkeley School of Law & OHCHR (2022) at 57. [↑](#footnote-ref-30)
31. Human Rights Center UC Berkeley School of Law & OHCHR (2022) at 57. [↑](#footnote-ref-31)
32. Blackdot Solutions *The OSINT Handbook* at 13. [↑](#footnote-ref-32)
33. Blackdot Solutions *The OSINT Handbook* at 13. [↑](#footnote-ref-33)
34. Blackdot Solutions *The OSINT Handbook* at 13. [↑](#footnote-ref-34)
35. Böhm & Lolagar (2021) 317 – 337. [↑](#footnote-ref-35)
36. Blackdot Solutions *The OSINT Handbook* at 14. [↑](#footnote-ref-36)
37. Human Rights Center UC Berkeley School of Law & OHCHR (2022). [↑](#footnote-ref-37)
38. Human Rights Center UC Berkeley School of Law & OHCHR (2022) at 58. [↑](#footnote-ref-38)
39. Human Rights Center UC Berkeley School of Law & OHCHR (2022) at 58 [↑](#footnote-ref-39)
40. Human Rights Center UC Berkeley School of Law & OHCHR (2022) at 58 [↑](#footnote-ref-40)
41. Pherson RH & Heuer RJ Jr (2021) “Structured Analytic Techniques for Intelligence Analysis” 3ed *Sage Publications*. [↑](#footnote-ref-41)
42. Pastor-Galindo, Nespoli, Mármol & Pérez (2016) at 4. [↑](#footnote-ref-42)
43. Pherson & Heuer Jr (2021). [↑](#footnote-ref-43)
44. Pastor-Galindo, Nespoli, Mármol & Pérez (2016) at 4. [↑](#footnote-ref-44)
45. Pastor-Galindo, Nespoli, Mármol & Pérez (2016) at 5. [↑](#footnote-ref-45)
46. Pastor-Galindo, Nespoli, Mármol & Pérez (2016) at 6. [↑](#footnote-ref-46)
47. Blackdot Solutions *The OSINT Handbook* at 16. [↑](#footnote-ref-47)
48. Human Rights Center UC Berkeley School of Law & OHCHR (2022) para 176. [↑](#footnote-ref-48)
49. Orgnet *Social Network Analysis: An Introduction*, available at <http://www.orgnet.com/sna.html> (visited 3 October 2024). [↑](#footnote-ref-49)
50. OHCHR (2011) *Manual on Human Rights Monitoring* Chapter 8 at 24. [↑](#footnote-ref-50)
51. See for instance, the use of digital platforms as demonstrative evidence by the ICC OTP in *Prosecutor v Ahmad Al Faqi Al Mahdi* ICC-01/12-01/15. [↑](#footnote-ref-51)
52. Blackdot Solutions *The OSINT Handbook* at 16. [↑](#footnote-ref-52)
53. Blackdot Solutions *The OSINT Handbook* at 16. [↑](#footnote-ref-53)
54. Freeman L & Llorente RV (2021) “Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age” 19 *Journal of International Criminal Justice* 163 – 188 at 169. [↑](#footnote-ref-54)
55. Browning JG (2013) “Burn after Reading: Preservation and Spoliation of Evidence in the Age of Facebook” 16 *Science and Technology* 273 – 308; Durrant R (2005) “Spoliation of Discoverable Electronic Evidence” *Loyola of Los Angeles Law Review* 1803 – 1834; See also, Freeman & Llorente (2021) at 171. [↑](#footnote-ref-55)
56. Freeman & Llorente (2021) at 171. [↑](#footnote-ref-56)
57. Murray D, McDermott Y & Koenig KA (2022) “Mapping the Use of Open Source Research in UN Human Rights Investigations” 14(2) *Journal of Human Rights Practice* 554 – 581 at 569. [↑](#footnote-ref-57)
58. Murray, McDermott & Koenig (2022) at 569. [↑](#footnote-ref-58)
59. Murray, McDermott & Koenig (2022) at 569. [↑](#footnote-ref-59)
60. Freeman & Llorente (2021) at 169. [↑](#footnote-ref-60)
61. Human Rights Center UC Berkeley School of Law & OHCHR (2022) para 147. [↑](#footnote-ref-61)
62. Human Rights Center UC Berkeley School of Law & OHCHR (2022) para 147. [↑](#footnote-ref-62)
63. Human Rights Center UC Berkeley School of Law & OHCHR (2022) para 48. [↑](#footnote-ref-63)
64. Millet E (5 December 2023) “Deploying OSINT in Armed Conflict Settings: Law, Ethics, and the Need for a New Theory of Harm” *ICRC Humanitarian Law & Policy Blog*, available at <https://blogs.icrc.org/law-and-policy/wp-content/uploads/sites/102/2023/12/Deploying-OSINT-in-armed-conflict-settings_-law-ethics-and-the-need-for-a-new-theory-of-harm.pdf> (visited 3 October 2024). [↑](#footnote-ref-64)
65. Dubberley S & Ivens G (2022) “Outlining a Human-Rights Based Approach to Digital Open Source Investigations: A Guide for Human Rights Organisations and Open Source Researchers” University of Essex, Human Rights; Human Rights Center UC Berkeley School of Law & OHCHR (2022) paras 61 – 66. [↑](#footnote-ref-65)
66. Koenig (2024) at 46. [↑](#footnote-ref-66)