The role of Open Source Intelligence in the Fight against Transnational Organized Crime – A European Perspective

Ricardo Ehe

75142548

Presented in partial fulfilment of the requirements for the Degree of International Master in Security, Intelligence and Strategic Studies

Word Count: 23881

Supervisor: Dr. Eamonn Butler McIntosh
Date of Submission: 06.08.2020

CHARLES UNIVERSITY

Abstract

While terrorism and the internet, especially social media, has received substantial recognition in literature, this paper will address the research question of how Open Source Intelligence (OSINT) can be utilized to combat Transnational Organized Crime (TOC). As the fight against transnational organized groups is primarily a government concern, the perspective of European Law Enforcement Agencies (LEAs) and the methodology of intelligence-led policing is placed in the center of the analysis. The link between vendors and consumers of illegal goods and services will also be investigated as it is a particularly valuable access point for OSINT given that the attention of consumers is generally captured publicly. One of the most promising applications could be identified in the context of combating human trafficking, as sexual exploitation of victims is often linked to a rich source of images which can provide specific traces. Even if the illegal business of TOC is conducted in anonymous places such as the darknet, new technological solutions of machine learning and web crawling constitute promising ways forward. Due to its unique characteristics as an intelligence discipline, OSINT, does not only provide opportunities regarding TOC, but it also has a positive impact on interagency collaboration and intelligence sharing. Open source intelligence products can be easily shared and do not have the same restrictions as closed-source products which demonstrates the potential impact it can have in this domain.

Contents

Abstract **2**

1 Introduction **4**

1.1 Research Aim, Question, and Structure *4*

1.2 Literature Review: Identifying the Gap *8*

1.3 Research Design and Methodology *9*

2 Contextualizing Open Source Intelligence (OSINT) **11**

2.1 Definition, Concept and Methodology *11*

2.2 OSINT and its value transformation in the 21st century *16*

3 The Manifestation of Transnational Organised Crime (TOC) **18**

3.1 Definition and Typology *18*

3.2 Modus Operandi, Networks and Markets *21*

3.2.1 Illicit Networks and Supply Chains 22

3.2.2 The modus operandi and logic of TOCGs 24

3.2.3 Digital Markets and new technologies 25

4 Combatting TOC in the 21st Century **27**

4.1 European Policies and Regulations *27*

4.2 European Security Architecture and Interagency Cooperation: Synergies and Challenges *29*

4.3 Intelligence-led Policing (Methodology and Practice) *33*

5 The digital Footprint of Transnational Criminal Groups (Vulnerabilities) **37**

5.1 Social Media Presence *37*

5.2 Darknet and virtual marketplaces *39*

5.3 Case Study: Geolocating and Tracing Children Trafficking and Sexual exploitation *41*

6 OSINT Approaches and Tools – Understanding, Interrupting, Reducing TOC **46**

6.1 On the Strategic Level: The ePOOLICE Project *46*

6.2 On the Tactical Level: The CAPER Project *52*

6.3 Satellite Images and Remote Sensing Approaches *55*

6.3.1 Environmental Crimes 56

6.3.2 Slavery from Space 58

6.3.3 Drug Cultivation 59

7 Implications and Discussion: OSINT and the European Security Architecture **62**

7.1 The Future of OSINT *62*

7.2 Opportunities in the Public Sector: Police Cooperation and Intelligence Sharing *64*

7.3 Emerging Private Sector and Public Private Partnerships *67*

8 Conclusion **71**

9 Bibliography **73**

1 Introduction

1.1 Research Aim, Question, and Structure

In 2018, a young military student noticed that Strava, a social fitness tracking app, could be used to reveal 'the apparent locations of secret military bases owned by the US and other governments in places like Russia, Afghanistan, and Turkey' (Romano, 2018).[1] The running app created an openly accessible heat map which compiles all tracking-data into one map in order to visualize the activity of other athletes in specific areas. What they hadn't anticipated is that 'Strava members in the military, humanitarian workers and others living abroad may have shared their location in areas without other activity density and, in doing so, inadvertently increased awareness of sensitive locations' (blog.strava.com).[2] As this example shows, the world of open sources, particularly in the internet age, has become extraordinarily rich in various kinds of data. This aspect illustrates how information, when publicly shared, can be used or repurposed for intelligence purposes in such a way that the value of open source intelligence (OSINT) rather depends on someone's creativity of how to use those sources, than on the actual lack of it. In response to this new finding, the Washington Post stated that 'the rapid development of new and innovative information technologies enhances the quality of our lives but also poses potential challenges to operational security and force protection' (Sly, 2018). While this is factual and the challenge of data privacy in the modern world is widely acknowledged, a different opportunity also rises: the use of open sources to target and counter malicious actors such as terrorists and criminals. As Simeone (2008) points out,

> *criminals and terrorists have become increasingly networked and have leveraged the Internet to achieve an unprecedented capacity to plan and conduct their criminal enterprises and operations,* [likewise] *local law enforcement agencies must do the same in order to keep their communities safe.*[3]

While terrorism and the internet, especially social media, has received substantial recognition in the literature, this paper addresses the research question of how open data can be utilized to combat transnational organized crime (TOC) and to what extent it can add value to existing

[1] https://www.vox.com/technology/2018/2/1/16945120/strava-data-tracking-privacy-military-bases
[2] https://blog.strava.com/press/a-letter-to-the-strava-community/
[3] https://core.ac.uk/display/36718253?source=3

challenges in this context. As the EU Security Union Strategy (2020-2025) emphasized, 'organized crime comes at a huge economic and personal cost' (EU Strategy, 2020: 12). Furthermore, it highlights the fact that those types of crime increasingly operate across borders 'including from the immediate neighbourhood of the EU' (EU Strategy, 2020: 17). Hence, TOC will remain a high-priority security challenge for the European Union (EU) which will require both political and academic attention to focus on possible solutions and countermeasures. While there certainly are several ways to address TOC (see an overview in chapter 4.1), this paper addresses the particular role of OSINT and its value in understanding, disrupting and reducing TOC. As combating crime is primarily a government concern, the focus is placed on European law enforcement agencies (LEAs) and regional institutions, such as Europol and Frontex. To that end, the role and use of OSINT within LEAs is discussed within the framework of intelligence-led policing (see chapter 4.3). In contrast to terrorism, most types of TOC are inherently clandestine and do not dependent on public responses or recognition. Therefore, this research takes a more nuanced perspective by analysing various types of TOC individually to evaluate how they may be connected possibly with OSINT opportunities (see Figure below). Furthermore, as different types of TOC are engaged in different operational activities, such as smuggling, recruiting or marketizing, these aspects will also be addressed individually. As these particular activities can be placed differently on the hidden-public spectrum, each one theoretically provides different OSINT opportunities or limitations.

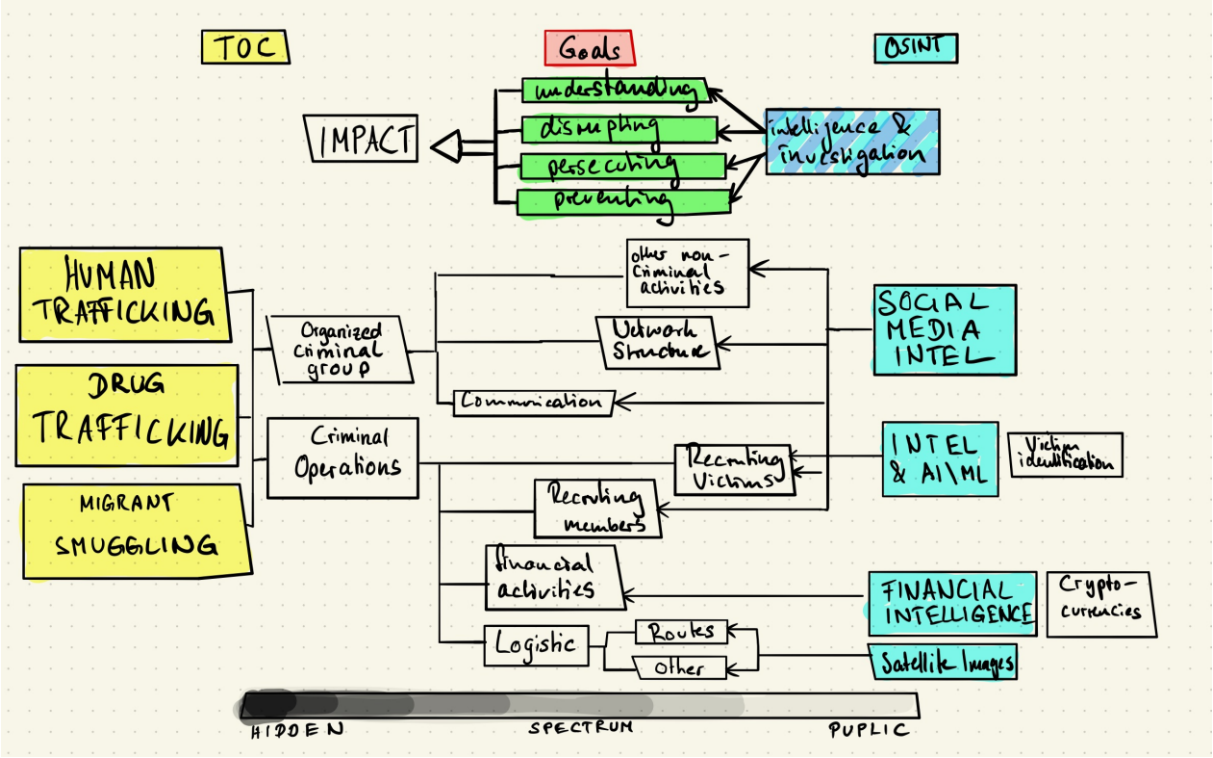

Figure 1: exemplary illustration of linkages between OSINT and TOC along a hidden-public spectrum

In order to assess sufficiently these aspects, the behaviour, markets and networks are addressed in chapter 3.2. Besides a rather minor social media presence, the darknet is a particularly central place for OSINT opportunities. Among various types of transnational organized crime groups (TOCGs) using the darknet, the most promising OSINT opportunity can be seen in businesses which require strong marketization of their illegal commodities and services. Human trafficking is highlighted as a particular example in which OSINT can have strong applications. Due to its complex operational process of recruiting and attracting victims as well as advertising their services, several more digital traces can be noticed in comparison to different types of illicit material, such as drugs or firearms.

On the basis of this analysis, and after contextualizing and discussing the OSINT capabilities nowadays in chapter 2, chapters 5 and 6 assess the digital traces of TOCGs and analyse how specific OSINT tools and methods can leverage the TOCs. This analysis is separated into strategic (chapter 6.1) and tactical OSINT applications (chapter 6.2), as both differ in the way they utilize open source information. This paper argues that strategic intelligence can leverage open source information more effectively as it is less dependent on the personal and detailed one. In contrast, tactical intelligence is rather prone to obstacles such as dis-/misinformation, lack of verification possibilities as well as privacy constraints particularly when scanning through social media networks. In this research, the focus is on the question of *what OSINT can*

do rather than on *should it be used*. This is a notable mention, as there are certainly valid concerns towards the increasing engagement of LEAs in intelligence functions and technologies which provide capabilities of vetting digital private information of individuals. Along with tactical and strategic intelligence, applications of satellite technology are discussed in chapter 6.3. Due to its increasing commercialization, satellite imagery can be considered as OSINT. The chapter provides several example usages of this technology highlighting its opportunities and limitations.

Chapter 7 discusses the future of OSINT and its implications for the European security architecture and interagency cooperation among LEAs combatting TOC. This paper argues that artificial intelligence (AI) and machine learning (ML) are increasingly part of OSINT platforms and tools. While this does not replace human analysis, it is an important task to oversee large amounts of data for specific insights. AI and ML will most likely continue to shape future OSINT approaches and applications. Due to the open nature of OSINT, this paper further argues that OSINT provides a particularly promising opportunity to facilitate interagency collaboration both nationally and across borders with other European LEAs. Intelligence products programmed from open sources do not have the same sharing restrictions as closed-source products do, thus they can easily be shared. Moreover, the increasing value of open sources increases the autonomy of the EU's security institutions similarly. EU institutions, such as Europol, were strongly dependent on member state's input in the past – as they have no secret intelligence collection mandate – which means they can now leverage on their own input, deduced from open sources. This aspect has become particularly noticeable when looking at the quality and acknowledgement of Europol's regularly published strategic serious and organised crime trend reports (SOCTA). The paper ends by discussing the increasingly important role of the private sector, both as a contributor of OSINT technology and as a valuable assistant in the form of private intelligence agencies. As the paper argues, public-private partnerships (PPP) are a central opportunity not only to enhance anti-crime capabilities in general but also specifically in the realm of OSINT.

As TOC is a particularly complex security challenge with many elements and factors at play, the goal of this research is to provide a foundational analysis which provides further research opportunities to assess specific types of TOC in more detail and how OSINT can add value. Furthermore, this paper aims to facilitate further interdisciplinary research as other academic fields, such as computer science, criminology or law could have a beneficial contribution to subsequent research questions that address the nexus between OSINT and TOC.

1.2 Literature Review: Identifying the Gap

After reviewing the literature on TOC and OSINT, there is only a very limited number of papers addressing intelligence and its connection to TOC. There is, for instance, Larsen et al. (2017), who provide in their book 'Using Open Data to Detect Organized Crime Threats: Factors Driving Future Crime' a detailed analysis on how open data can be used for the purpose of strategic law enforcement intelligence. They specifically address recent approaches of how open data can be used to identify emerging organized crime threats. However, the book does not specifically refer to the phenomenon of TOC but rather focuses on organized crime in general. While their analysis is valuable for both further research in crime science and computer science (data mining, AI/ML), it also does not specifically address the social science perspective of OSINT and TOC. As authors who do take this perspective, the work of Hobbs et al. (2014) and Williams and Blum (2018) need also to be mentioned. In the book 'Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities', Hobbs et al. (2014) contextualize OSINT with contemporary security issues like proliferation, counterterrorism, humanitarian crises, or cybersecurity. The other authors address OSINT in the context of conflict resolution or the defence industry. While their approach fits well into the field of social science, the nexus between OSINT and TOC is left unaddressed. As their work has only limited value for this research question, it clearly highlights the need to reassess and evaluate the role and value of OSINT in the light of 21st-century challenges. The transnational element of crime is intentionally chosen as it opens the discussion around law enforcement cooperation and intelligence sharing. This is particularly relevant in the EU and, therefore, constitutes the regional focus point in this research. Another worth mentioning research approach, which is closely related to this paper, is offered by Coyne (2014) who analyses the role of strategic intelligence in the context of Australia's law enforcement community. However, in contrast to Coyne (2014) and Larsen et al. (2017), this paper does not only look at strategic intelligence alone but on the whole intelligence collection discipline (OSINT) considering both strategic and tactical purposes. This paper also takes a step further by discussing its implications on the European security architecture and its mechanisms of intelligence sharing. As the previous section has already highlighted, terrorism and particularly radicalization has become a huge academic topic in which the nexus to social media and OSINT frequently was made. As TOC has generally received viewer public attention and is in its logic inherently different to terrorism (see Table below), a distinct academic contemplation on the nexus between OSINT and TOC was considered as both necessary and relevant.

	Terrorism	Drug Trafficking	Human Trafficking
Degree of using the internet for their primary purposes	**High** (spread of fear, political agenda, etc.) sometimes even live video footage	**Low** as the whole business is conducted clandestinely However, **Medium-High** when the process is linked to Darknet markets.	**Medium** to attract victims or customers Although high if images of sexual child abuse is taken into consideration)
Secondary operational use of the internet	**High** (e.g. recruitment, communication with foreign fighters)	**Medium-High** (communication, supply chain management, deterrence)	**Medium**

Table 1: comparison between Terrorism and TOC

As the research method of this paper is primarily built on literature analysis, this section is held comparably brief and only aims to highlight the particular literature gap. Chapter 2, 3, and 4 will continue to highlight and discuss literature findings which build the foundation for the subsequent analysis. Drawing on the literature throughout the dissertation provides the opportunity to effectively contextualize both OSINT (chapter 2), TOC (chapter 3), and EU policies (chapter 4) with the specific thematic analysis and discussion.

1.3 Research Design and Methodology

Equivalent to Coyne's approach (2014), this research is explanatory in design aiming to develop theoretical knowledge in the field of law enforcement intelligence. The research follows the approach of inductive reasoning. Deductive theory testing was not seen as a valuable way of addressing this topic. Neither the literature on TOC nor on intelligence has much theory to offer. As Hillebrand and Hughes (2017) point out, there is no scientific theory in the field of intelligence and this should also not be the objective. Both TOC and intelligence lack quantitative analysis. Within intelligence studies, there is the inherent problem of secrecy, which makes the access of classified and sensitive data very difficult. Similarly, TOC does hardly allow any kind of quantification as the phenomenon is very complex bearing definitional challenges and most importantly a lot of unknowns as criminal groups predominantly operate clandestinely. Usually, crime statistics only show the tip of the iceberg, not displaying meaning and unreported or undetected crimes. Still, research in this field is significant as TOC is a major threat to the democratic values of the EU. New approaches and opportunities that support the understanding and persecution of TOC need to be explored and developed. This research,

therefore, contributes to the development of new conceptual methods and explores the practical value of applying OSINT tools for this purpose and its potential value in the future. By predominantly looking at novel approaches in the context of OSINT, both limitations and opportunities are addressed.

As the beginning of the research process had been affected by the Covid-19 pandemic, a short statement of its impact on the research design is considered as important. The pandemic crisis unfolded in the early stages of the research process in mid-March of 2020. At this point, first pre-arrangements were made to conduct qualitative semi-structured expert interviews. This was considered as beneficial, as expert knowledge could supplement the literature analysis process of this research and add a practical and novel insight into the use of OSINT within LEAs. On the 23rd of March, the School of Social and Political Science at the University of Glasgow officially changed its policies in regards to permissible research methods during the crisis. Referring to the high risk of face-to-face interviews and data collection, the University asked all students to conduct desk-based research. As a result, this research shifted its focus exclusively towards document and web analysis. Specifically, this included primary literature from relevant agencies, such as Europol or SatCen, extensive analysis of the academic literature and occasionally the analysis of expert publications on blogs or as interviewees within podcasts. In hindsight, the change has not materially limited the research as a considerable amount of literature coverage on OSINT applications and tools could be identified (see chapter 6: CAPER, ePOOLICE, satellite remote sensing). While often covered for different research purposes, it still gave reasonable insights into complex OSINT applications designed for LEAs. The limitations with this method bear in the fact that those tools could neither be directly tested nor could practitioners of those tools be interviewed. However, as this research does not aim to conduct an analysis of one specific tool but rather wants to discuss the general usability of OSINT, this research strategy could still be pursued.

2 Contextualizing Open Source Intelligence (OSINT)

2.1 Definition, Concept and Methodology

To understand the value of OSINT and to analyse its role in the fight against TOC, it is important to start by contextualizing and explaining the overall concept of intelligence itself. Predominantly, the term *intelligence* is used in the context of national security and the military. The most original and classic example of intelligence usage is a situation of war. At war, military leaders are continuously required to make strategic and tactical decisions about how to deploy their military capabilities in the field. To make those decisions, information about the opponent's military capabilities, location, and plans can crucially improve those decisions. The historical and most reasonable inference of this was to use spies.

> *Thus, what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is FOREKNOWLEDGE. Now this foreknowledge cannot be elicited from spirits; it cannot be obtained inductively from experience, nor by any deductive calculation. Knowledge of the enemy's dispositions can only be obtained from other men. Hence the use of spies [is needed].* (The Art of War by Sun Tzu Online Book, n.d.)

Today, spies are only one of several ways to receive valuable intelligence. The typical intelligence collection capabilities, or disciplines, comprise along with human sources (human intelligence or HUMINT), also the interception of communication or other electronic emissions (signals intelligence or SIGINT), the use of satellite imagery (geospatial intelligence or GEOINT), measurement and signature intelligence (MASINT), and last but not least intelligence collected from open sources (OSINT) (Lowenthal, 2009).

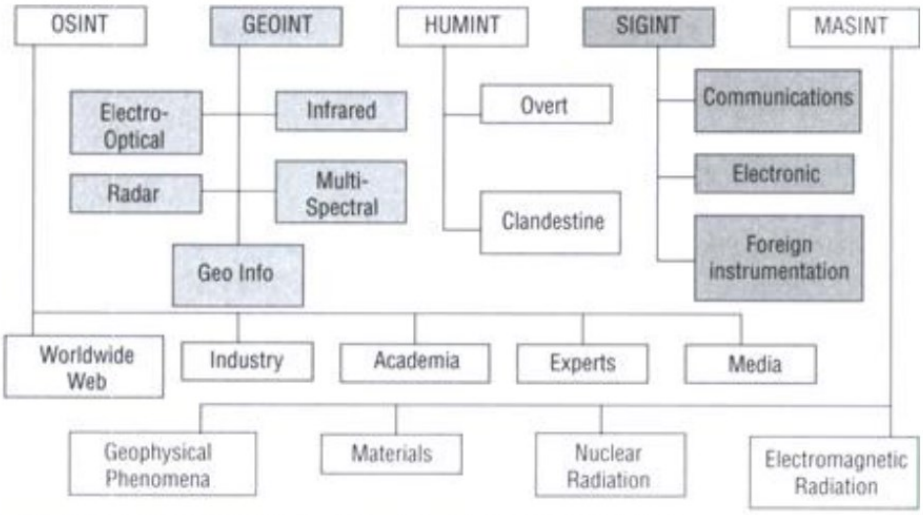

Figure 2: Collection Disciplines (Lowenthal, 2009)

Furthermore, the aim of using intelligence and the actors who use it have, also, gone way beyond the mere military application. Today, intelligence is employed by a diverse range of actors, ranging from LEAs to businesses. Intelligence is integrated into police work, crisis or conflict management, the private sector and several other forms of operational settings in which informed and accurate decision-making is required. However, as the example of war importantly points out, intelligence does not have its purpose in itself but in its dissemination on which basis decision makers can act upon. Indeed, intelligence is best understood as a process in which several actors, such as collectors, analysts and policymakers are involved. This process is conceptualized and is now predominantly accepted in the literature as the *intelligence cycle*.

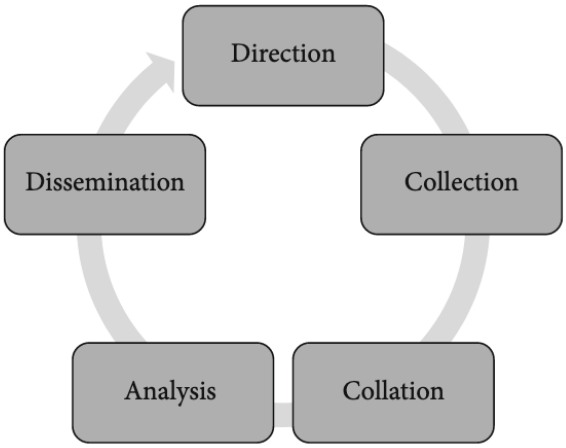

Figure 3: Intelligence Cycle (Coyne & Bell, 2015: 138)

At each step, intelligence goes through the process of being collected as mere (raw) data or information, processed and collated with other input, analysed and contextualized to develop knowledge and finally disseminated to clients which directed the process beginning. It is the most accurate conceptual depiction of the intelligence practice in reality, as it displays a holistic picture of all elements, actors and steps that are included in the intelligence business. It perfectly highlights that intelligence is more than just information as it first needs to be systematically analysed and targeted towards decision makers' requests and direction. Hence, Kleiven (2007: 264) defines intelligence as 'information that has been given some added value after being collated and assessed'. Yet, the literature of intelligence studies shows certain inconsistencies on how a holistic definition should look like. Harfield and Harfield (2008, cited in Staniforth, 2017: 23), for instance, defines intelligence as the 'systematic and purposeful acquisition, sorting, retrieval, analysis, interpretation and protection of information'. Although both definitions are valid, they differ as Kleiven rather emphasizes intelligence as a product, while Harfield and Harfield depict intelligence as the process. Lowenthal (2009) even adds another perspective defining intelligence as both the means 'by which certain types of information are required and requested, collected, analysed, and disseminated', as the product of this process and as the organization or unit which carries out the various functions of the intelligence process. So when this paper analyses the role and value of OSINT, the collection of intelligence is significant but always considered in the context of the whole intelligence process. Therefore, an appropriate definition of OSINT includes the same elements as the definition of intelligence itself:

> *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 Open Source Enterprise, 2006: 8)

'Open sources' can be defined as information provided by any person or group 'without the expectation of privacy' (Staniforth, 2016: 26). In other words, 'the information, the relationship, or both is not protected against public disclosure' (Staniforth, 2016: 26). The latter is more precise as expectations can be subjective and not all published information is expected to reach a wider audience. Especially when it comes to social media, where information is primarily expected to be seen by friends or colleagues but theoretically can be seen by all if privacy settings are not adjusted accordingly. The fact that information is publicly available does not

necessarily mean that it is free or easily accessible. There are several publicly available information platforms which require certain registration, authentication or payment (e.g. compliance database *LexisNexis* or identity verification search engine *pipl*). The provided intelligence of those commercial platforms and service providers do count as open source since the word *open* refers to the absence of classification or privacy barriers not to the absence of costs or registration (Gibson, 2017: 89). Practically, it is, however, not always clear what should be considered open source and whatnot. Certain grey areas exist. For instance, actively approaching an individual on social media to get information would for the one still count as OSINT while others would call it HUMINT, or virtual HUMINT (Wilson, 2019).

Still, as OSINT has increasingly been used in several distinct settings, the agreement over an all-encompassing definition has become challenging. The consensus is generally found that it 'must be systematically collected and should constitute an essential component of analytical products' (Best and Cumming, 2007). A more complex definition from a rather military perspective, provided by Burke (2007, cited in Casanovas, 2016: 143), defines OSINT as

> *unclassified information obtained from any publicly available source in print, electronic, or verbal form (radio, television, newspapers, journals, internet, commercial databases, and video). The process to gather intelligence in this way begins with raw information from primary sources assembled through filtering and editing processes. OSINT is then "constructed". Only after the process has been completed, OSINT is created.*

All these mentioned sources of Figure 2 are generally collected clandestinely, covertly or secretly which requires certain intelligence tradecraft which is, from a legal point of view, exclusively available to mandated governmental agencies. OSINT, however, is distinct to those disciplines, as the use of open sources for gathering information does not require secret means. Therefore, it is not limited to state authorities but to everyone who has the means to access open sources (e.g. computer with internet access, library card, radio, TV, etc.). The implication of this for the European security architecture will be discussed in chapter 7. Due to this difference, some have argued that OSINT should not even be seen as an intelligence discipline as it is not covertly collected. Lowenthal (2014: 61, cited in Williams and Blum, 2018: 8) provides an alternative view by stating that OSINT should anyway not be understood separately but as a 'facet of each of the various other intelligence disciplines'. He hints toward the concept of *all-*

source-fusion which is an important step during the collation and analysis process (see Figure 4). This research agrees to Lowenthal's position and understands OSINT as a legitimate and increasingly important intelligence discipline. Even though OSINT is distinct, it follows the same process and goal as other intelligence disciplines. In the words of Stephen Mercado (2007), open source intelligence are the 'open versions of the covert arts'.

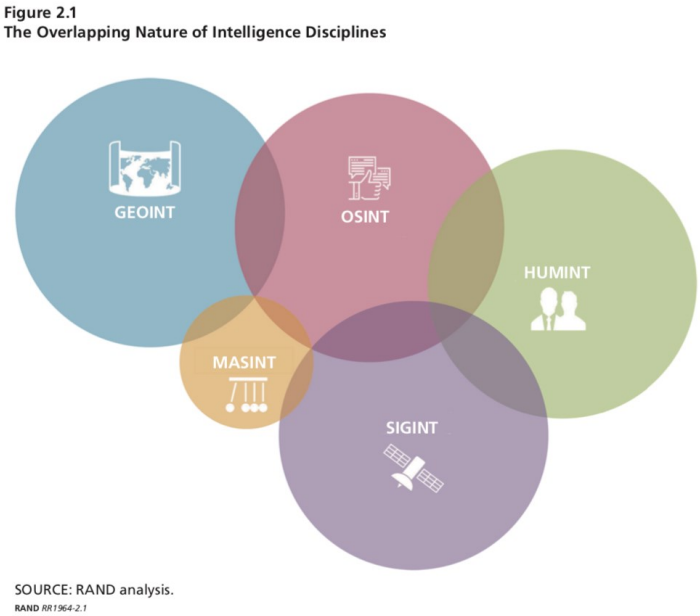

Figure 4: intelligence fusion and overlap of various collection disciplines (Williams and Blum, 2018: 9)

Elements such as misinformation, intentional disinformation or the simple lack of information require the intelligence analyst to incorporate as many distinctive sources as possible to sufficiently verify the information and to enhance the resulting assessment and recommendations. Intelligence from different sources can each add a certain puzzle piece to the overall picture the intelligence consumer wants to look into. In that sense, OSINT can be understood as the 'glue which binds, compliments and increasingly corroborates and confirms other […] intelligence functions' (Staniforth, 2016: 27). This is important to highlight as it is often believed that the main intelligence business consists of clandestine activities such as espionage. However, considering the centrality of OSINT as a non-clandestine activity, this is not the case. Indeed, former CIA Director Allen Dulles estimated the amount of OSINT used within intelligence agencies to be as high as 80 percent (Gibson, 2014: 9). While this certainly highlights today's centrality of OSINT, the remaining 20 percent of secret activity often provide the missing puzzle piece that contributes critical meaning to all other open source input. As Salisbury (2014: 82) argues, the value of open sources is often depicted as 'background and

contextual information', there is, however, also 'a clear potential for open source to fulfil a real-time operational role'.

2.2 OSINT and its value transformation in the 21st century

Although most of today's OSINT is conducted via the internet, the collection discipline existed already long before those technological advancements. In 1942, after the attack on Pearl Harbor, General William J. Donovan was entitled to lead the newly founded US Office of Strategic Services (OSS) which was the predecessor of the CIA. One of its five branches, the so-called Research and Analysis (R&A) Branch was entirely assigned to conduct open source intelligence on the Axis powers using libraries, newspapers, and government and industry information as a resource. The branch quickly received high recognition and significantly contributed to critical missions such as the allied bombings on oil facilities in Europe by pinpointing the Nazi's oil production as a key vulnerability (OSS, 2010). Donovan's assessment on the value of OSINT is as true today as it was during the second world war: 'Even a regimented press will again and again betray their nation's interests to a painstaking observer (Waters, 2018). Although the Cold-War time is generally known for glamorous HUMINT and SIGINT operations, OSINT was not at sleep. As one CIA veteran recalls in the context of the Soviets suppression of the Hungarian uprising: 'there often comes a time when public political activity proceeds at such a rapid and fulminating pace that secret intelligence, the work of agents, is overtaken by events publicly recorded' (de Silva, 1978, cited in Mercado, 2007). The events of the Iranian Green Revolution in 2009 and the Arab Spring in 2011 are prime examples which highlight his statement. Indeed, those two examples were key events which significantly changed the perception of OSINT capabilities within the intelligence community. During the Iranian election protest, the Green Revolution, thousands of Iranians used social media to organize and mobilize demonstrations and for communication exchange. During those protests, social media accounts turned into real-time intelligence sources including valuable images and videos which provided multiple first-hand accounts on what was happening (Colquhoun, 2016). Since that event, CIA's Open Source Center – which was created in response to 9/11 attacks and mainly tasked with counterterrorism and counterproliferation – started to shift its focus and began to track up to 5 million tweets daily (Keller, 2011). After the Arab Spring, deputy director of the Defense Intelligence Agency David Shedd admitted that they had underestimated the value of open-source information and focused too much on spies 'collecting information from power elites, not opposition groups' (Dilanian, 2012). As Shedd further states, the event 'had

led to a lot more discussion in the intelligence community on how to take advantage of the enormous amount of open-source information that is out there, and draw inferences of where a trend may be' (Dilanian, 2012). Today, OSINT is a well-established collection discipline which even transcended from the public NIA to other actors such as private intelligence companies, LEAs, NGOs, or investigative journalists. However, as Mercado argues, OSINT has actually not changed as a discipline, but rather in its scale and ease in which open sources can now be utilized. As he states, 'the revolution in information technology, commerce, and politics since the Cold War's end is only making open sources more accessible, ubiquitous, and valuable' (Mercado, 2007). Still, this had a significant impact on the intelligence community. As NGA Director Robert Cardillo has stated, 'classified sources, methods and networks will always have value in our agency and to our customers, but we cannot always view unclassified information as supplemental,' rather, 'moving forward the reverse is more likely to be true – that which is exquisite, but classified will supplement an ever broader and richer unclassified base' (NGA, 2015). Similarly, Lowenthal (2009) places the ratio of open sources in comparison with other sources in a ratio of 80:20. A ration which was quite the opposite during cold-war times. During the early 2000s, the aftermath of the information revolution further expanded in its complexity. With Web 2.0 and 3.0, the internet has changed significantly in its original character. Information on the internet was no longer a static flow between information providers and receivers but dynamic with multiple ways to engage with, discuss, and share information (Chauhan and Panda, 2015: 19). On the one hand, this has increased the value of OSINT dramatically, however, on the other hand, it has brought along significant challenges from an ethical and legal point of view. How open sources, and particularly the internet will further expand and either set the way for more or fewer OSINT opportunities, will be discussed inter alia in chapter 7.1.

The following chapter gives now a clear account and context of the phenomenon of TOC. Both the emergence, the definition and typologies, as well as the practice of TOCGs will be addressed. This sets the ground to analyse OSINT opportunities for combatting TOC in a holistic and better context.

3 The Manifestation of Transnational Organised Crime (TOC)

TOC, as it is known today, has only emerged around 30 to 40 years ago. Glenny describes two key events which triggered the rapid growth and the global connectedness of OCGs. Firstly, he identifies the 'deregulation of controls on capital movement in the Anglo-American sphere' (Glenny, 2018). In contrast to the post-World War II economic order, industrial states moved around 1980 towards neoliberal policies of deregulation to limit short-term capital movements across borders and to embrace the development of international financial markets and the opportunities that come along with global business (Goodman and Pauly, 1993). Shortly after in 1985, European Member States signed the first version of the Schengen Treaty which provided the way for the Single Market of the EU in 1993 allowing the free movement of goods, services, money and people (Europol, n.d.). It did not take long until 'crime and terror groups […] exploited the enormous decline in regulation, lessened border controls, and greater freedoms to expand their activities across borders and to new regions of the worlds' (Shelley, 2014: 13). From the criminal's perspective, the essential benefit of conducting crime transnationally is the exploitation of legal, political and economic differences and resulting opportunities that come along with different regions in the world. TOCGs 'travel to regions where they cannot be extradited, base their operations in countries with ineffective or corrupted law enforcement, and launder their money in countries with bank secrecy or few effective controls' (Shelley, 2014: 13). In essence, the emergence of transnational organized crime became the 'unintended consequence […] of the development of common economic markets' (Lemieux and Gerspacher, 2013: 62).

Secondly, the collapse of communism in 1989 left many central and eastern European states as poorly regulated and lawless zones (Glenny, 2018). The entire region witnessed increasing levels of crime in general and activities of organized criminal groups operating across borders in particular. As Hignett (2010: 71) puts it, the 'post-communist transition has facilitated a fundamental reshaping of organized crime in terms of its structure, composition and activities.' Something which became a major issue of concern as the EU wanted to incorporate this region between 2004 and 2007.

3.1 Definition and Typology

Transnational Organized Crime , as the term says, is a form of Organized Crime (OC) including the element of transnationality – the crossing of borders. As the Palermo Convention (2000) on

TOC states, the inherent challenge of TOC is that 'the rule of law is undermined not only in one country but in many'. Therefore, combatting TOC requires transnational cooperation as 'those who defend [the rule of law] cannot limit themselves to purely national means' (Palermo Convention, 2003). One important step for addressing TOC collaboratively is to find an agreed definition on which basis collective anti-TOC instruments can be developed. However, as TOC comprises a great 'diversity of activities carried out by criminal groups' with 'differences in their structure', this task turned out to be very difficult (Bakowski, 2013). Facilitated by the United Nations (UN), the Palermo Convention eventually was the first international agreement and until today constitutes an important milestone on how to define and collectively approach the emerging phenomenon of TOC. The definition is constructed around the definition of an organized criminal group and the criteria of transnationality. Article 2 of the Palermo Convention defines an organized criminal group as a

> *structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit.* (Palermo Convention, 2000)

The definition highlights the elements of group size, financial motive, and illegal nature. Albanese further separates illegal activities conducted by those groups in three major categories. The 'provision of illicit goods', such as drugs, stolen properties, human organs or environmental goods; the 'provision of illicit services', such as prostitution, labour or gambling; and the 'infiltration or abuse of legitimate business', such as labour racketeering or money laundering (Albanese, 2001). In accordance with Article 3, a criminal group can be considered as TOCG if an offence is committed

(a) 'in more than one state;
(b) In one state but a substantial part of its preparation, planning, direction or control takes place in another state;
(c) In one state but involves an organized criminal group that engages in criminal activities in more than one state; or
(d) In one state but has substantial effects in another State.' (Palermo Convention, 2000)

The convention is signed by 147 Member states and was ratified by forty states which highlights the wider international consensus of the definition and was therefore used as the basis for this research (un.org). While some see it as successful as it offers a homogenous agreement on the phenomenon, critiques see the convention and the global fight against organized crime as an instrument to foster the political hegemony by the US using it for the 'control and imposition of economic and financial rules' as a form of 'soft power' (Nyer, 2004, cited in Pascual, 2017: 26). For the purpose of this research, this debate is not particularly relevant. However, on the positive side, the Palermo convention perfectly highlights the inherent entanglement of TOC with other important elements such as money laundering and corruption. Adding terrorism to the list, Shelley (2014) argues that those elements 'will remain critical security challenges in the twenty-first century as a result of globalization, technological advances, economic and demographic inequalities, ethnic and sectarian violence, climate change, and the failure of nineteenth- and twentieth-century institutions to respond coherently to these challenges when they emerged.' What she importantly points out is that TOC is not only a matter of law enforcement and state prosecution, it is a phenomenon which interconnects and impacts social, economic and political dynamics. Indeed, TOC can be even a significant driver to state failure and institutional erosion as it often intersects with terrorism and generally flourishes in situations of conflict (Comolli, 2018). Furthermore, TOC is particularly challenging as its illicit practices often blend into the legitimate economies making it extremely difficult to combat. Indeed, money laundering – a pivotal element in the illicit economy of TOC – flourishes in a close entanglement of crime and the legitimate economy (Klerks, 2007, cited in Coyne and Bell, 2011).

As already mentioned, TOC can take various forms of crimes. This section briefly explains the most prominent types of TOC. Generally, illegal trafficking of goods is 'TOC's most lucrative manifestation' (Comolli, 2018). Such illegal goods can range from drugs, arms, and antiques to counterfeited pharmaceuticals and protected environmental goods (Comolli, 2018). However, trafficking is not only limited to illicit goods, a very lucrative type of TOC is the trafficking of human beings. What has been referred to as *human trafficking* needs to be further explained as there is often a certain misconception or disagreement around this term both in academic and public discourse. In contrast to most other types of TOC, the UN created the Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children as a supplement to the Palermo Convention. In this document, trafficking in persons is defined as

> *the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs.* (ohchr, n.d.)

Human trafficking is a serious human rights violation and is, therefore, a particularly serious form of TOC. As the definition of human trafficking involves a wide range of criminal forms, there is a certain overlap and confusion with other terms such as modern slavery, bonded labour or forced prostitution. Often human trafficking has a strong connotation to sexual exploitation, in particularly forced prostitution. As Katona (2020) points out, this is highly problematic because it often leads to a wrong understanding of the actual problem and its solution, misleading statistics, and the undermining or marginalization of efforts addressing forced labour, debt bondage and slavery which received less attention. For the purpose of the subsequent analysis, it is therefore helpful to define subcategories of human trafficking, which are: labour-related exploitation, sexual exploitation, and physical exploitation (removal of organs). In practice, those types might be easily separated as a trafficked human can potentially encounter all of these crimes along the way or simultaneously. A further related type to human trafficking is migrant smuggling. In this case, a person is generally not a victim but the recipient of a service. However, this does not mean that during the smuggling process, a person cannot become a victim of crimes such as violence, threatening, document theft etc. Also, in many cases, the service of smuggling results in human trafficking as people are often very vulnerable during the smuggling process and particular dependent on the smuggler (Katona, 2020). Similar to human trafficking, there is a supplementing protocol in the annexe of the Palermo Convention specifically addressing smuggling of migrants.

3.2 Modus Operandi, Networks and Markets

The analysis of networks, markets and the modus operandi of TOCGs is essential for identifying vulnerabilities and subsequently assessing opportunities for OSINT. However, there is an inherent challenge when it comes to creating knowledge on TOCGs. Firstly, it is difficult to detect. Secondly, it is difficult to study. TOC ‘is not stagnant, but is an ever-changing industry,

adapting to markets and creating new forms of crime' (UNODC, 2012). So when talking about their modus operandi and network dynamics, those limitations need to be considered. Still, there are certain insights which give important value and context to the scientific discourse. The Palermo Convention is very clear when they picture the general behaviour of TOCGs. As Kofi Annan stated, TOCGs 'take advantage of the open borders, free markets and technological advances […]. They thrive in countries with weak institutions, and they show no scruple about resorting to intimidation or violence' (Palermo Convention, 2000). In the following analysis, the underlying and well established illegal enterprise theory is used to provide a better theoretical understanding of how TOCGs operate. The theory points out the underlying similarities between legal and illegal business activities. Both are essentially profit-driven activities operating by the same principles of supply and demand, seeking profit maximization. This theory is especially important when thinking about countermeasures.

3.2.1 Illicit Networks and Supply Chains

One central deduction of this logic is that 'restrictions on supply do not eradicate demand, instead only alter market conditions for illegal entrepreneurs' (Glenny, 2009). It further highlights that similar to legal business companies, criminal networks often operate in a hierarchical network of decision makers, enforcement and those which Kleemans (2014) describes as facilitators. The latter has an essential position in a criminal organisation as they provide services such as financial and legal advisory, money exchange and money laundering, as well as document forgery. Still, there are certainly various kinds of network structures in criminal groups. A traditional mafia group focusing on racketeering is differently structured than a human trafficking network which is often rather web-like in structure, consisting of strong family ties rather than rigid and hierarchical (Katona, 2020). Similar to many legitimate businesses, TOC operates with supply chains including zones of production (in drug trafficking, typically Colombia or Afghanistan), zones of distribution (e.g. the Balkans, or Mexico) and zones of consumption (e.g. USA, Europe or Russia) (Glenny, 2009). As an example of illegal wildlife trafficking, Figure 5 highlights this process by linking all contributing actors to the specific zones of the supply chain.

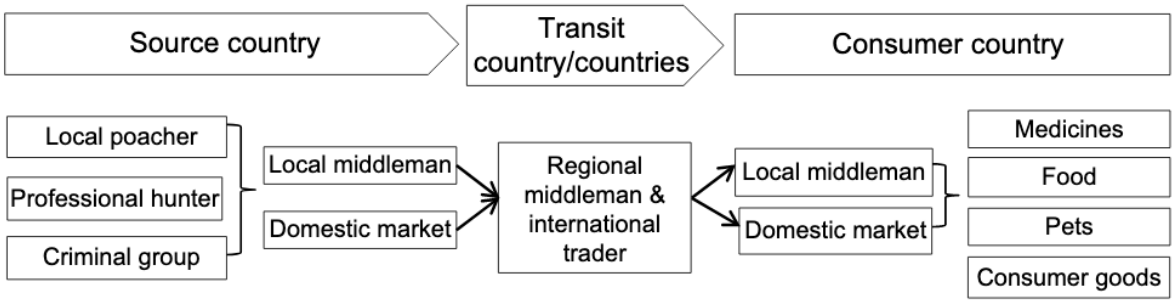

Figure 5: Supply Chain Network of a TOCGs engaged in illegal wildlife crime (Polner and Moell, 2016: 62)

Generally, the first link in every supply chain is built in the zone of production (source country). Depending on the type of crime, this can be the production of counterfeit goods, the recruitment of victims, the cultivation of poppies or the poaching of protected wildlife. The second link in the supply chain includes those actors who facilitate the transportation of those goods or people. They do this either in person or supervise the smuggling from a distance, focusing on departure and arrival of goods (e.g. illicit placement of goods in a container of legitimate shipments) (Sellar, 2016). This certainly varies depending on the specific type of TOC. There are, however, two essential business risks along the supply chain which are common among all types: the detection and arrest by LEAs and the competition by other groups. In contrast to the legal business, they obviously do not have any legal protection by authorities and therefore need to facilitate their own protection measures. Traditionally, this can be the bribery of corrupt police officers and customs, or the use of violence to spread fear to deter competitors. Depending on the risk and the costs, criminal groups can further decide to either keep the whole supply chain internal or to outsource certain supply chain links. Outsourcing is the contracting of an external actor who then facilitates a certain part of the supply chain. Those external partners are especially beneficial if they have established themselves in a certain region or market over time with trusted couriers and corrupt officials. As Canales (2013) notes, this is certainly common practice among TOCGs. The illustration of Figure 5 further helps to think about various entry points for investigations and OSINT approaches. It is important to understand that TOC-related incidents should not be approached isolatedly but with the notion that it probably only constitutes a certain piece in a larger network of crimes. At each stage, there are usually several related crimes taking place, such as violence as a form of maintaining control of the victims; the falsification of documents to move victims across borders; or forced prostitution. Those crimes can be described as ‘instrumental criminal activities’ or ‘secondary crimes’ and are often performed by the aforementioned facilitators (OSCE, 2010). To successfully prosecute TOC, it is important to recognize and link those secondary crimes to primary crimes. Usually, the

linkage requires effective police cooperation and intelligence sharing among EU member states (MS) and third parties (e.g. Interpol). A deeper analysis of this topic and how OSINT can impact this collaboration is discussed in chapter 7.

3.2.2 The modus operandi and logic of TOCGs

The manifestation of TOC is generally fostered and generated by so-called 'opportunity factors', which consist of economic factors (e.g. poor living standards; governmental conditions (weak government or corruption); law enforcement factors (degree of training, equipment and capabilities, payment and corruption); and social or technological changes (Internet crime and anonymous payment such as Bitcoin) (Albanese, 2001). Depending on the criminal environment in a certain area or entire country, opportunity factors are more likely to be exploited than in others (e.g. higher acceptance of organized crime due to the history of a certain area). As opportunity factors alone do not necessarily lead to people engaging in (transnational) organized crime, special access or skills are sometimes crucial factors for criminals to exploit opportunities (Albanese, 2001). Such factors are important to keep in mind as they can potentially explain certain crime hotspots and contribute to assess or estimate the future of TOC. This also constitutes the basis for strategic law enforcement intelligence (see chapter 6.1). These factors explain why weak states outside the EU can still have an important impact on criminal products or services ending up in Europe. Western countries are generally the countries of demand and consumption while weak and failed states (e.g. Libya) currently function as key transit or production countries.

Core activities in almost any TOCG are corruption, violence, the penetration of the legal economy through money laundering (Framis, 2017). The most essential part of TOC is the smuggling of goods which are prohibited to transport across borders, controlled or taxed. Focusing on the activity of smuggling allows covering a whole range of TOC types since smuggling is essentially almost always a crucial element in TOC. While production and distribution may take place in different settings and contexts, the crossing of borders comes with generally one elementary concern: how to avoid customs controls and the detection of the illicit activity? As Von Lampe (2011) points out, TOC networks need to engage in complex strategic decision making in order to reach that goal. The change of modus operandi can be boiled down in 'switching their means of transportation', 'moving their smuggling routes', or 'increasing their level of sophistication' (Von Lampe, 2011). A second or additional method is to change the scale of the operation. Depending on the client, the time frame or the degree of

establishment of certain processes or generally the risk smugglers want to take, they can choose whether they want to smuggle the goods in bulk or whether they split the goods into multiple shipments or couriers to diversify the risk and maximize the chances that at least some goods will successfully arrive instead of being seized, lost or destroyed. It can be even a strategic decision to give up 'mules' as bait in order to divert the attention of customers away from other mules (Von Lampe, 2011). As customs agencies and LEAs will usually try to find patterns in smuggling routes and activities, one challenge is that TOCGs continuously try to change their modus operandi. This allows TOCGs to make their operations less predictable and less detectable, especially in light of new technologies and techniques which LEAs increasingly try to deploy for such purposes (e.g. x-ray scanning of containers) (Freeman, 2017). In the words of Von Lampe (2011), it is a 'constant game of cat and mouse' in which smugglers continuously need to adjust. Indeed, the reason for the difficulties in detecting illicit goods is the deliberate blending between legal and illegal business routes and processes. This practice becomes especially central when TOCGs are trying to disguise their financial profits, better known as money laundering. The Palermo Convention (2000) defines the criminal act of money laundering as 'concealing or disguising […] the true nature, source, location, disposition, movement or ownership' of criminal proceeds. Generally, it is the goal to use criminal proceeds in the legitimate economy for reasons such as pleasure, further investments, or luxury etc. If these proceeds would not be laundered, LEA would have a comparably easy job to identify crime through following back the money trail to its origin. Sophisticated money laundering techniques, such as the use of offshore banking, shell companies etc. make it particularly difficult for LEAs to do just that.

3.2.3 Digital Markets and new technologies

As Buckley points out, the internet has fundamentally changed crime in two ways. Firstly, it has changed the type of crime that can be committed. A particular example is the distribution of illegal sexual child abuse material. Using the words of the EU Security Union Strategy on Child Abuse (2020), the 'exponential development of the digital world has been abused making this crime a truly global one, and has unfortunately facilitated the creation of a global market for child sexual abuse material'. Generally, cybercrime began in its earliest form in the nineties, as young hackers, sometimes referred to as 'script kiddies', began to for example deface websites for fun or getting respect among like-minded people (Glenny, 2018). Today, criminal cyber syndicates have reached new dimensions in which revenues of a single attack can result in millions of euros. Their activities have gone beyond traditional identity or credit card number

theft towards large-scale targets such as critical infrastructure of states or large industries. An extraordinary example of such attacks is the hacking of the Central Bank of Bangladesh which created a loss of 81 Million Dollar (Hammer, 2018). Interestingly, it was not until recently, that cybercriminals and traditional TOCGs discovered the mutual benefit of their business and joint forces. Originally, cyber criminals and TOCGs evolved in parallel, as their criminal methodology or culture is fundamentally different. Traditional mafia groups, for instance, who are involved in trafficking or racketeering have to protect their business from competitors or the police. To do this, they have usually had to use violence to spread fear, show their power and credibly deter competitors. Cybercriminals, on the other hand, do not have to use violence as they mostly operate virtually but are still able to achieve similar high revenues. When a more organized form of cybercrime developed at the beginning of the 21st century, traditional OCGs perceived it with disdain. However, as a new generation of 'digital natives' appears, today's emerging bosses of TOCGs are more likely to perceive the cyber realm as a beneficial facilitator or market for their operations, a trend which can be described as the 'digitization of organized crime' (Glenny, 2018).

Secondly, the internet has changed the way OCGs can interact with each other for operational purposes and to facilitate the commission of other crimes. This is particularly true for illegal darknet markets and forums. Indeed, the darknet has revolutionized the way the seller and buyer engage with each other. Facilitated by cryptocurrencies such as Bitcoin, the darknet provides an anonymous and borderless virtual space which is the perfect breeding ground for the illegal business of TOCGs. Chapter 5.2 provides further details on how the darknet is used by TOCGs and how it might facilitate opportunities for OSINT. Still, as the EU Security Union Strategy emphasizes, technological advancements which are exploited for criminal purposes go beyond the darknet. As the case of EncroChat illustrates, a large-scale encrypted phone network used by OCGs, criminals constantly assess how new technologies can benefit their business. This does also include technologies such as 3-D printing of weapons, artificial intelligence or robotics (EU Strategy, 2020: 4)

4 Combatting TOC in the 21st Century

This chapter explains the main attributes of the security architecture in the EU and countermeasures in regards to TOC. The European security architecture is used as a term to describe all actors, partnerships or agreements which are directly or indirectly relevant for the fight against TOC. Chapter 4.2 will explain this architecture in more detail by addressing some central European institutions individually. Before discussing specific applications and possibilities in chapter 5, this section is necessary to contextualize the role of OSINT within the whole framework of countermeasures, strategies, and possibilities in the EU. The chapter follows a top-down approach by first describing policies and regulations at EU level and then continues by explaining specific law enforcement principles and strategies. This chapter also constitutes the foundation for discussing how OSINT is impacting the European security architecture (chapter 7).

4.1 European Policies and Regulations

As already mentioned, the foundational framework for combating TOC on the policy level was the UN Palermo Convention in 2000. It was an important milestone for defining the phenomenon of TOC and to set out guiding definitions and recommendations. The convention highlighted that TOC isn't something which states can effectively handle alone. As already pointed out in the previous chapter, an effective response on TOC requires international collaboration as TOCGs do not respect national boundaries. In that sense, collaboration policies are required as LEAs can only operate in the boundaries and framework the state provides for them. While theoretically, this finds consensus among MS, practically, European policies and regulations in this context have only slowly found its way into effective implementation. Furthermore, this development did not take place without some seeing it with certain concern. As Carrapico (2012, cited in Olley, 2019) points out, TOC effectively went through a process of securitization within the EU. As it initially was only considered as a criminological phenomenon or as economic harm, it is meanwhile considered a threat to national security. Tellingly, the EU has placed cross-border crime among the main priorities on its agenda (2019-2024) in order to ensure the protection of EU citizens and freedoms (European Council, 2019). While it is important to question whether the securitization of TOC is justified, this paper argues that political action at the EU level is crucial. As Olley (2019) points out, TOC is a real threat as it results not only in high numbers of civilian deaths, but also has a serious impact on states

economy and political stability. Therefore, policy responses on high levels such as the EU are considered both as legitimate and necessary. However, whether those policies are effective is certainly debatable.

There are generally three types of responses on the EU level. Firstly, there are several legal measures. With the Council Decision 579 of 2004, the EU introduced and approved the Palermo Convention to the EU Community. However, due to the diverse legal environment within the EU, the legal consensus remained challenging. Legal efforts to overcome this challenge, such as the EU Framework Decision of 2008, have not led to the hoped success. Currently, strong attention is placed on Anti-Money Laundering (AML) legislation. On May 7th 2020, the EU has published a new action plan to combat money laundering and terrorism financing more effectively. Among six pillars, the action plan includes 'better use of information to enforce criminal law' which is particularly relevant for this research (see chapter 7) (European Commission, 2020).

Secondly, the EU has implemented a policy cycle to address TOC within a strategic framework. While the EU had already implemented certain action plans and strategies on OC since the 1990s, often in context to specific types of crime, in 2010 they introduced a new four-steps policy cycle. The first cycle was initiated in 2014 after its decision in the EU Internal Security Strategy of 2010. Since 2018, a second cycle takes place which finishes in 2021. The overall goal is

> *to tackle the most important threats posed by organised and serious international crime to the EU in a coherent and methodological manner through improving and strengthening co-operation between the relevant services of the Member States, EU institutions and EU agencies as well as third countries and organisations, including the private sector where relevant. (EMPACT, n.d.)*

Figure 6: EMAPCT Policy Cycle (EMPACT, n.d.)

In its first step, Europol conducts an extensive threat assessment (SOCTA) using various sources (including open sources) on serious and organized crime in the EU, setting out priorities, recent development, and changes in the criminal environment. On this basis, the EU develops the so-called multi-annual strategic plans (MASPs) to specifically address the identified threats. In the third step, an EU multidisciplinary platform (EMPACT) produces operational action plans (OAPs). Those action plans are cooperatively implemented by MS and relevant institutions. Finally, the results on the OAPs are sent back to Europol for assessment and priority adjustment (EMPACT, n.d.). This not only highlights that the EU is actively engaged in fostering strategic collaboration, but it also shows that with Europol's SOCTA, open sources have an important role to play even on such high-level strategic dynamics.

Thirdly, the EU has built institutions which facilitate and support police cooperation among MS. Central among those are Europol, as the main European police body; Eurojust, as the judicial cooperation unit; and CEPOL, as the European police academy. The mandate of those institutions reflects the balance between both MS awareness of the benefit of cooperation and its desire to protect their state sovereignty. This tension is inherent to all EU efforts to combat TOC (Bakowski, 2013). How those institutions are collaborating to combat TOC will be explained in the subsequent section.

4.2 European Security Architecture and Interagency Cooperation: Synergies and Challenges

a. Europol

The European police office *Europol* is the central European institution for combating TOC. Their mission and mandate are set out in Article 88(1) of the Treaty on the Functioning of the European Union:

> *Europol's mission shall be to support and strengthen action by the Member States' police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy.*[4]

Their mission can be generally divided into two main tasks. Firstly, Europol acts as a centralised information hub and intelligence provider. By fusing open sources and information from national LEAs and occasionally third parties they produce regularly thematic-specific threat assessment reports such as the already mentioned SOCTA, the Internet Organised Crime Threat Assessment (iOCTA) or the EU Terrorism Situation and Trend Report (TE-SAT). Their intelligence products and reports are therefore not only for specific clients such as the European Commission and member states' LEAs, but are publicly available to everyone. Still, there are certainly also products which are exclusively for specific clients. For instance, Europol has agreed to deliver 'reports on threat evaluation, risk analysis, on development of technologies, types of crime or methods of organised crime and statistical summaries' to the European Commission (2003).

Secondly, they act as a facilitator of bilateral and multilateral police cooperation between MS. Through joint investigation teams (JITs), MS can make use of this platform to establish a judicial or law enforcement cooperation for a 'limited duration' and a 'specific purpose', to set up an investigation 'in one or more of the involved States' (JITs, n.d.). In Europol's recently published *strategy 2020+* (2018), they highlighted their role as a platform for policing solutions and their ambition to 'be at the forefront of innovation and research for law enforcement'.

b. Eurojust

Closely related to the work of Europol is the work of Eurojust. In the recently established EU regulation (2018/1727), Eurojust's function is defined as a 'Union body with legal personality, to stimulate and to improve coordination and cooperation between competent judicial

[4] https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_2&format=PDF

authorities of the Member States, particularly in relation to serious organised crime'.[5] Weyemberg, Armada & Brière describe both as 'sister agencies' with Europol as the 'mega-search engine' and Eurojust as the 'control tower'. Both are designed to 'maintain close cooperation […] in order to increase their effectiveness in combating serious forms of international crime' (Weyemberg et al., 2014: 11-15). As Weyemberg et al. further point out, the collaboration among those two agencies has not been without its challenges. Among other concerns, there is a certain 'risk of duplication' and an 'increase in competition between the two agencies' (Weyemberg et al., 2014: 15).

c. CEPOL

What is interesting to note about European's police academy CEPOL, is that its recently published assessment on the EU's strategic training needs for 2018-2021, it repeatedly emphasizes the importance of teaching OSINT to police officers. For instance, they mention the use of OSINT in the context of undercover online investigations to combat organised property crime, OSINT in the darknet to investigate drug or arms trafficking. Generally, they depict the use of OSINT as a valuable technique for digital investigations in the open web which helps to get a better 'intelligence picture' on online trade sellers and buyers (CEPOL, 2018). This is an important finding, as it highlights that on EU level, the value of OSINT in the context of TOC is well recognized. Additionally, the assessment emphasizes that cooperation with the private sector is increasingly important but at the same time difficult, 'as they are not always open to disclosing information' (CEPOL, 2018). This is a particular challenge where this paper argues that the use of open source for intelligence purposes could serve as a beneficial bridge between the public and the private sector. This argument is further elaborated in chapter 7.2.

d. OLAF

A further EU agency which is relevant to TOC – especially for fraud, and corruption – is the European Anti-Fraud Office OLAF. Without going into much detail, it is important to mention that the nature differs from Europol and Eurojust. While the latter operate primarily upon MS request, OLAF operates autonomously and primarily serves the interests of the EU (Weyemberg et al., 2014: 34). For this particular research, OLAF is not as relevant as it does

[5] http://eurojust.europa.eu/doclibrary/Eurojust-framework/EurojustRegulation/Eurojust%20Regulation%20(Regulation%20(EU)%202018-1727%20of%20the%20European%20Parliament%20and%20of%20the%20Council)/2018-11-21_Eurojust-Regulation_2018-1727_EN.pdf

not operate with open sources, but rather starts its investigations on the basis of whistle-blowers and informants or as a request by other EU institutions (OLAF, 2013).

e. Further relevant EU institutions

Lastly, European institutions such as Frontex, MS' FIUs, INTCEN, and SATCEN need to be briefly mentioned even though their primary focus is not particular on TOC and their structure and logic varies significantly from institutions such as Europol. The EU Intelligence Analysis Centre INTCEN and the EU's Satellite Centre SATCEN, for instance, are European intelligence agencies and, strictly speaking, do not count as a 'police cooperation body, since it is a Directorate of the European External Action Service (EEAS) and only deals with strategic analysis' (Bux, 2020). Still, their intelligence products can occasionally be relevant for LEAs or other institutions such as Europol or Frontex. Among the sources of INTCEN, are inputs from NIA's, LEA's, the military, and diplomats (Bux, 2020). SATCEN primarily uses satellite imagery form commercial providers and is, therefore, less dependent on governmental input. Both INTCEN and SATCEN work with open sources. The latter particularly states that the 'essential additional information underpinning and complementing the imagery analysis is acquired from open sources and from users of SatCen services' (SatCen, 2020: 15). The particular implications of this are discussed in chapter 7.2. While these are all European institutions, it should not be overlooked that important interagency collaboration also takes place internationally with third parties. Relevant international institutions are for instance the United Nations Office on Drugs and Crime (UNODC), the Financial Action Task Force (FATF), the Egmont Group, the G8, Interpol or the Organisation for Economic Co-operation and Development (OECD). Whether they act as specific investigators or cooperation facilitators, they are all to various degrees engaged in combating TOC.

While the need for law enforcement cooperation and intelligence sharing is increasingly recognized in the EU, there are fundamental challenges to implement these goals. Generally, regional police cooperation can bring up a number of problems. Those can relate, for instance, to different laws and mandates, different rules of starting investigations or using evidence, unequal technological advancement or financial capabilities (Brady, 2008). Among these, one particularly stands out and is essential to this research: the reluctant sharing behaviour of intelligence with other agencies. Or as Svendsen (2013: 196) calls it 'the ever-present secrecy-sharing dilemma that exists with regard to multilateral arrangements'. This 'dilemma' is primarily related to the issue of trust. In particular, intelligence agencies or intelligence units within LEAs are highly concerned that their methods and sources are revealed, leaked or

generally get in the wrong hands once intelligence has been shared. In some sense, methods and sources are the lifeblood of successful intelligence and therefore requires careful consideration of what exactly and with whom classified intelligence products are shared. To various degrees, effective intelligence sharing can be a challenge within states, between LEAs and NIAs, between national agencies and regional agencies (e.g. Europol), and between agencies working under certain agreements, both bilateral and multilateral. The first relationship (LEA-NIA), is treated very differently among MS as there is no clear common position in the EU. While some have overlapping structures, others have strict boundaries law enforcement and national intelligence. The latter is comparably more established within the EU (bilateral intelligence liaison). The sharing of intelligence with Europol has been rather challenging and a central weakness in Europol's early history until today. As Bures points out, 'efforts aimed at encouraging a more intense and effective exchange of criminal information and intelligence had not yielded the expected results, mostly due to the lack of unanimity and the deficit of trust among Member States' (Gruszczak, 2016). As examples in history have shown (e.g. FBI and CIA), effective intelligence sharing requires a process of developing mutual trust which certainly needs time to develop. As the aftermath of terrorist attacks in the EU (e.g. the London or Madrid bombings) had certainly an impact on intelligence sharing in the context of terrorism, there is little reference to intelligence sharing within other domains such as TOC. While the issue of European law enforcement cooperation and intelligence sharing is a topic for its own, structural challenges among EU institutions are important as it constitutes the basis to discuss the opportunities of OSINT as a possible benefit (chapter 7.2). As this section focused on interagency collaboration and synergies, the subsequent section addresses the role of intelligence within LEA when combatting TOC. The practice of using intelligence within LEAs has become known as *intelligence-led policing*.

4.3 Intelligence-led Policing (Methodology and Practice)

Although intelligence-led policing (ILP) often seems like a recent phenomenon, as it is often related to terrorist attacks in the early 2000s, the basic concept of it is quite old. In 1881, Metropolitan Police Assistant Commissioner Howard Vincent stated:

> *Police work is impossible without information, and every good officer will do its best to obtain reliable intelligence, taking care at the same time not to be led away on false issues. Information must not be treasured up, until opportunity offers for action by the*

> *officer who obtains it, but should be promptly communicated to a superior, and those who are in a position to act upon it. Not only is this the proper course of action to task in the public interest, but it will be certainly recognised by authorities and comrades, prompting esteem and confidence, which will bring their own reward.* (Cook et al., 2013, cited in Staniforth, 2016: 22-23)

Along with the benefits of targeted and informed action, as mentioned by Howard Vincent, the underlying idea of ILP is that it serves to identify patterns and structures in criminal activities as those activities are rarely random. Criminal patterns are essential opportunities which provide LEAs with the key to identify vulnerabilities and appropriate options for intervention. Patterns may include communication, movement, lifestyle, or intend (Staniforth, 2016: 23). Intelligence-led policing can be therefore defined as

> *an information-organizing process that allows police agencies to better understand their crime problems and take a measure of the resources available to be able to decide on an enforcement tactic or prevention strategy best designed to control crime.* (Ratcliffe and Guidetti, 2008)

Practically, this means that LEAs either have 'special intelligence analysis units to support extended investigations against organised crime' or police officers perform dual functions (Aliprandi et al., 2014: 151). There is, however, certainly a trend towards the former model, as the intelligence business requires adequate training. In the literature, the term *criminal intelligence* is often used to separate intelligence practices by LEAs with the practice by NIAs. However, as NIAs often also collect intelligence on OCGs, a better term might be *law enforcement intelligence* (LEI) which is subsequently used to refer to intelligence activities conducted by LEAs. Initially, academia often lagged behind the reality of law enforcement practices. As Coyne and Bell (2011) point out, the expansion of ILP within LEAs 'occurred despite the distinct absence of law enforcement intelligence definitions and theories'. The terrorist attacks of 9/11 are further mentioned by them as an important turning point in the shift of LEAs towards a strong ILP methodology increasingly focusing on matters of national security. While today, several authors have made efforts to discuss the theoretical methodology of ILP, there is still only little practical academic coverage on its implementation and effectiveness (Burcher and Whelan, 2019).

A central contribution in the body of literature is the 3i Model of ILP by Ratcliffe (see Figure below). The model conceptualizes three processes which are at play when combating crime in an intelligence-led approach. The intelligence unit within an LEA *interprets* the criminal environment which then serves as a foundation (*influence*) for decision-makers to *impact* the criminal environment through their strategic, operational or tactical decisions.

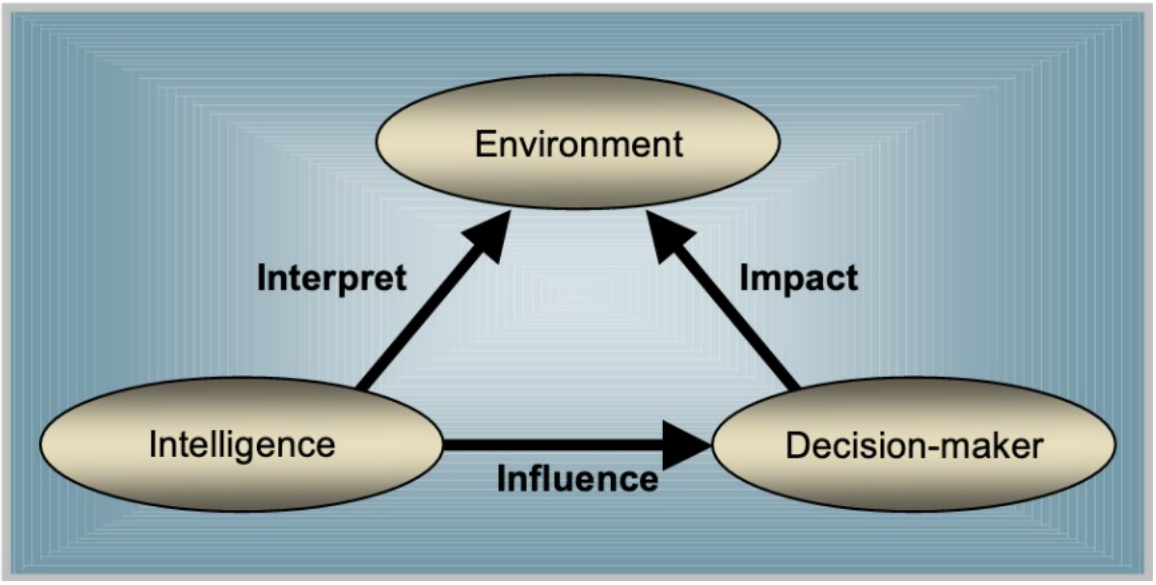

Figure 7: 3i model contextualizing ILP (Simeone, 2008: 3, adopted from Ratcliffe, 2003)

In many ways, the recognition of ILP by LEAs is closely related to the value transformation of OSINT as both have emerged out of the information revolution. In the context of this research, ILP can be understood as the bridge between OSINT and TOC as it encourages LEAs to use intelligence methods (of which one is OSINT), in order to fight crime (of which one is TOC). As it was explained in chapter 2, intelligence itself is usually used by NIAs or in the Military. LEAs were generally not tasked with intelligence and, still today, it is not its primary function. However, the evolving complexity of crimes, the crossings of borders and the formation of criminal networks created the need for a more proactive approach than conventional police control and response. Hence, the use of openly accessible information was a logical step to address this problem. Even if they are usually not described as intelligence, the police certainly can also make use of other collection methods, such as the use of informants (HUMINT), the use of CCTV cameras or even telephone interception techniques. Further information sources accessible to LEAs can include medical or criminal records. When it comes to closed source social media data, such as private messages, LEAs have shown an increasing interest but are dependent on the platform providers to grant them access.

The particular difference to NIAs is that LEAs usually need a special warrant to use particular privacy-sensitive means. The access granting on social media platforms specifically requires proof of an ongoing official investigation. Hence, the use for future-oriented intelligence gathering is very limited. Indeed, the distinction between investigations and intelligence is important to discuss. As LEAs are primarily tasked with investigations and evidence-gathering, the question arises how intelligence corresponds with investigations. Indeed, especially tactical intelligence may support or initiate investigations. There is only a fine line separating those tasks. In contrast, strategic intelligence is quite distinct to investigations as it does not focus on individuals nor on timely information. An specific explanation of strategic and tactical intelligence is provided in chapter 6. Generally, investigations are initiated whenever a crime has occurred or has been reported to the police. The aim of an investigation is to find evidence for the particular committed crime and potentially to uncover related crimes or people involved. In contrast, intelligence is done on an ongoing basis. As explained in chapter 2, the intelligence business works through a cycle of planning, collection, collation, analysis and dissemination. It aims to support decision makers or specifically for LEAs, it contributes to informed action on the ground. Hence, a further difference between investigation and intelligence is that intelligence generally focuses on the future while investigation deals with events in the past. Still, one can initiate the other as it is the case when intelligence uncovers certain suspicious activities (payments, movement, networking) which then provides the basis for an official investigation. Furthermore, intelligence might be particularly beneficial in cases where quick investigative responses are essential for its success. For instance, when someone is abducted and there are indicators that the person has been kidnapped by human traffickers, it is utterly important to quickly respond before the person is trafficking across borders and traces are lost. In such cases, having intelligence on certain human trafficking groups already available would significantly help investigators to respond fast and informed. As Staniforth (2016: 27) points out in this context, ‘the rise and availability of OSINT has served to inform and dramatically improve the very beginning of police action and response which is vital to save lives, prevent disasters and respond effectively to unfolding events.’

5 The digital Footprint of Transnational Criminal Groups (Vulnerabilities)

Digital footprints, or to be precise *digital open source footprints*, include both intentional activities and unintentional activities leaving behind certain traces. Indeed, those traces do not even have to be left behind in the digital sphere. With openly accessible satellite imagery or Google Street View, possible insights into criminal operations might become visible even though no specific traces have been left behind. OSINT leverages on the increasing transcendence of the virtual and physical world. Most newspapers, TV-news or libraries can be accessed through the internet. This chapter analyses several access points which can be used to identify digital footprints of TOCGs. As the example of Strava in the introduction has shown, digital traces can be found at various places and are certainly not limited to the subsequent examples.

5.1 Social Media Presence

Especially for tactical intelligence on individual suspects and their social links to other people, social media platforms are the logical go-to. As social media has extensively evolved in complexity and quantity of data, some consider social media as an independent intelligence discipline (SOCMINT). Even though it is not very likely to find high profile actors of TOCGs on Facebook or Twitter, there is always a chance to identify low-level criminals bragging with expensive cars, stolen goods, or money. In the best case, this directly reveals certain insights into criminal activities and allows the police to take direct action. If this is not possible, opportunities may relate to information about the target person's aliases, whereabouts or other information which can generally be traced back to certain criminal groups. Even if an account does not reveal much of such information at all, there is always the chance that minor traces lead to other places in the realm of open sources (e.g. other social media accounts) that provide further insights. The motive behind criminals who reveal information on social media is manifold. First, it is important to note that members of TOCGs are not just criminals. They may have a non-criminal past or are part of a visible 'non-criminal' social or business environment. Sometimes it is enough to be tagged by someone else on a picture which preserves a person's location at a given time which reveals certain clues during investigations. In other cases, in which members of TOCGs intentionally give away certain information on social media, they either underestimate the value of information they are revealing, feel secure enough and

untouchable by LEAs, or simply cannot resist to share their criminal successes with others for public attention (e.g. posting pictures with expensive cars). Not to mention that some criminals commit crime only for the purpose of getting attention. Generally, the intelligence analyst should not underestimate that people make mistakes. Indeed, there are quite a number of cases which indicate that social media played an important role and provided specific leads to e.g. find missing people, solve murders or other crimes (drunk driving, animal cruelty, hate crime, etc.). However, these are often not linked to organised crime. Generally, it is reasonable to assume that established criminal networks and high-ranking players are not very likely to have a large social media footprint. On the contrary, some key actors might even employ a specialist to disguise their internet presence. Still, it depends on the type of TOC. So-called *Outlaw Motorcycle Gangs* (OMCGs) and Mafia-like groups might rather and intentionally post on social media than others. Typically, such postings would show them with firearms and their gang logo to communicate their power to the public (McGovern and Milivojevic, 2016).

Generally, social media provides manifold opportunities. Sometimes, it is not about the information certain criminals are giving away on social media but the social media community which provide hints to the police. One example of this is the aftermath of the Boston Marathon Bombing in 2013, where the FBI requested the public's help on social media (Bruinius, 2014). However, this does not necessarily count as OSINT, but is rather a timely and potentially anonymous way of online reporting. Also, social media can be used by LEAs not to find evidence directly but use it to 'acquire probable cause for a search warrant' (Encartele, 2018). Hence, social media might not necessarily be the place to find important leads, but certainly provides a good starting point for further investigations. At this point, it should also be mentioned that LEAs have the possibility to request private information on social media accounts. However, depending on the country, social media providers do not necessarily need to cooperate with the police. As such information would not count anymore as open source, this topic is not further discussed in this research.

Lastly, it is important to state that criminals might actively use social media for their purposes. Instead of bragging, they might spy on potential victims or to share their public appearance (e.g. spreading fear among rivals). The latter is a phenomenon which particularly has been observed with Mexican drug cartels. As Muggah (2015) correctly notes, the use of social media by OCGs seems 'counterintuitive' as those groups 'traditionally thrive[] in the shadows, far from public gaze' trying to minimize their 'public profile, not amplifying it'. The purpose is to 'shape opinion and elicit respect, fear and terror' (Muggah, 2015). Much of the elements a terrorist organisation has on its agenda. In Mexico, the infamous and powerful Sinaloa cartel

used to have a twitter account with ‘more than 34,000 followers’ and it's now imprisoned leader, El Chapo, had an account with ‘almost 400,000 followers’ (Muggah, 2015). Meanwhile, both accounts have been blocked by twitter. Along with the rather obvious content of images with ‘girls, guns and gore’, drug cartels have used social media to publish so-called ‘narcomensajes’[6] or ‘narcovideos’ (Muggah, 2015). These messages were placed on social media pages of murdered individuals stating the motive and publicly threatening ‘that this is what happens when you work with such and such a rival cartel’ (Muggah, 2015). Arguably, this phenomena might be limited to drug cartels who constantly have to protect their markets by demonstrating power and control to deter law enforcement and rival gangs. It is less likely to be a trend which can be expected for TOCGs in other domains, such as human trafficking or smuggling of cultural goods. O’Neil, an expert on Latin America, contributes a valid perspective by stating that the use of the internet by TOCGs can also be linked to demographic change. Young members of drug cartels have grown up with the internet and are therefore much more comfortable using it (Gittens, 2015). Similar shifts have also been witnessed by members of traditional mafia groups who are increasingly shifting their business into the digital domains of organised crime.

5.2 Darknet and virtual marketplaces

Apart from social media, a primary and increasingly important place for criminal operations is the darknet. During the last decades, the darknet has shown its significance for TOCGs. It is not only an anonymous illegal marketplace between the end-user and supplier of illegal goods, but it is also a platform which facilitates crime as a form of business to business (B2B). In comparison to the surface web, the darknet is not indexed. Hence, LEAs need to know where to look at and sometimes even gain access to restricted sites in order to collect intelligence. The darknet is the primary example where OSINT quickly turns into virtual HUMINT. To access the more restricted parts of the darknet and to collect actionable intelligence, law enforcement officers need to lure themselves into criminal networks which arguably leaves the realm of open sources. Other possibilities, for instance, the encryption of protected areas, require the use of enhanced technology such as supercomputers which are usually limited to some NIAs and are usually not available for LEAs. The main opportunity for OSINT collection is placed in the intersection between customer and vendor. As the darknet vendor needs to describe and/or illustrate the product, they are potentially giving away certain clues about their whereabouts.

[6] mensajes (spanish) = messages; ‘narcos’ are criminals in the illegal narcotic business

This is particularly the case of human related material. As pictures of victims advertised for prostitution are commonly photographed in hotel rooms, the background (etc. hotel decoration) might indicate the exact name or branding of the hotel. Hence, the important bridge from victims to locations is made possible. This approach, for instance, is pursued in the project Hotels-50K. The project created an extensive data set of 1 million hotel room images from 50.000 hotels around the world. Those images were partly sourced from openly accessible travel websites and partly crowdsourced by hotel guests who uploaded images of the hotel room into a mobile application *TraffickCam*. The latter was particularly necessary as those unprofessional images were more likely to match with those images involving trafficked victims (see Figure below) (Stylianou et al., 2019).

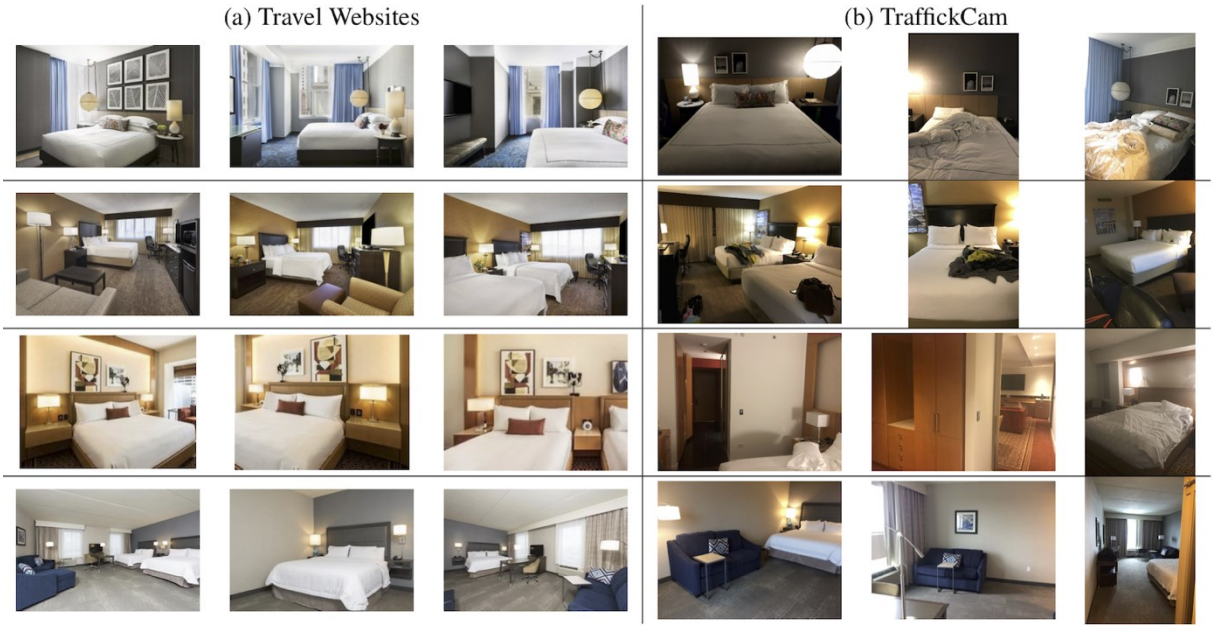

Figure 8: Comparison between the source images of Hotels-50 (Stylianou et al., 2019: 728)

Through the use of this data-set and machine learning (ML) algorithms, darknet vendor images could be automatically queried and potentially matched with one of the hotels in the Hotels-50K data-set (see Figure 9). Importantly, the matching process functions by comparing the background of those images. This allows the use of censored images on which the victim's identity is protected. Even though this approach might only allow LEAs to identify places at which trafficking has taken place, it still might contribute to the identification of further leads or patterns and potentially gives the opportunity to intervene in future crimes (Stylianou et al., 2019).

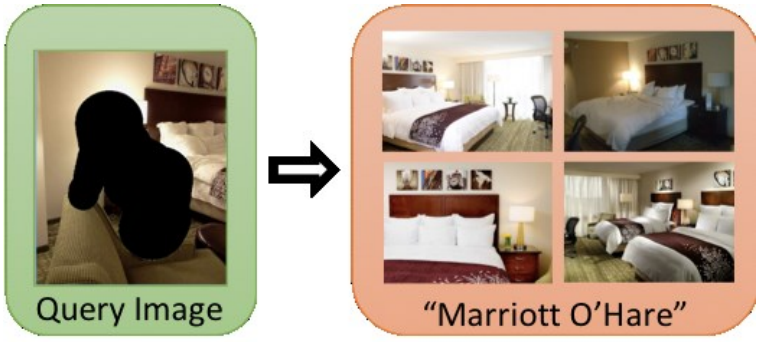

Figure 9: matching open source images with the Hotels-50K data-set (Stylianou et al., 2019: 726)

Using similar ML-technology, the UK Home Office has created a 'Child Abuse Image Database' form both surface and darknet distribution places (open source) which can be used to query images from suspect computers or phones and to potentially 'recognise specific victims or abusers' (Day et al., 2016).

5.3 Case Study: Geolocating and Tracing Children Trafficking and Sexual exploitation

Indeed, sexual abuse in relation to human trafficking and exploitation bears a significant opportunity for OSINT. Similar to the approach with Hotels-50K, Bellingcat – an investigative journalism initiative specialized on OSINT – has geolocated the crime scene where child sexual abuse material (CSAM) was produced by a TOCG. As the investigation revealed, the group was running a 'child modelling studio' in which they produced CSAM exploiting children who were trafficked from Moldova to Ukraine (Gonzales, 2019). Bellingcat started its investigation based on an image published by Europol in its crowdsourcing campaign *Stop Child Abuse – Trace and Object*. In this campaign, Europol publishes on its website certain censored parts of images (objects) which could be identified on the background of 'sexual explicit material involving minors' (see Figure 11, subsequently called 'imageC5') (Europol, n.d.). Europol notes that those objects relate to cases in which 'every other investigative avenue has already been examined' (Europol, n.d.). Therefore, they are calling the general public to support them by providing tips which help to identify the origin of those images.

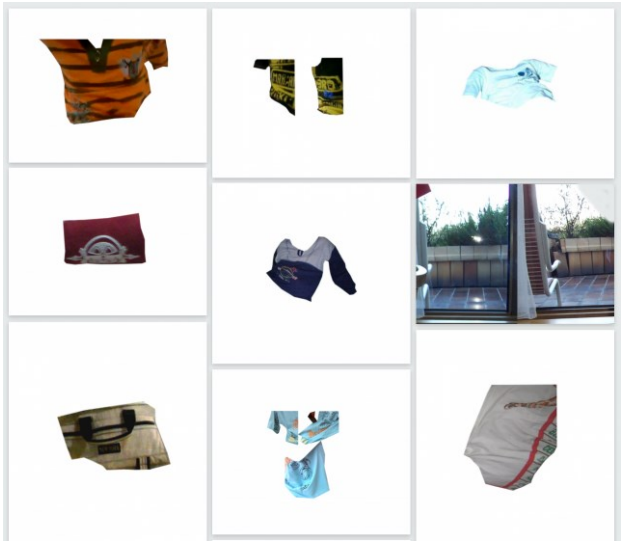

Figure 10: Europol's 'Stop Child Abuse - Trace an Object' campaign (Europol, n.d.)

Figure 11: Published CSAM ImageC5 (Background) by Europol and starting point for Bellingcat's OSINT investigation (Gonzales, 2019)

According to BBC, Europol 'holds more than 40 million images of child sexual abuse' (BBC, 2019). Since the launch of the campaign in June 2017, Europol has generated 21.000 leads on 119 published objects in the very first year which resulted in 79 objects being identified and the geolocation of 32 places of production (Europol, 2018). As Europol generally does not provide any information on the investigation around those cases, Bellingcat has provided valuable insight into both how they used OSINT to geolocate the image and how it uncovered the crime story behind it. At first, they identified the buildings in the distance as likely former soviet buildings. From there, they tried to reduce the search area to those regions which best fitted to the vegetation displayed on the image below.

Figure 12: Vegetation map of the former Soviet Union (Gonzales, 2019)

Figure 13: initial area selection of West Maldova, Russia and East Ukraine (Gonzales, 2019)

As the images provided no distinctive landmarks which could further reduce the selection area, the Bellingcat analysts turned away from open satellite image analysis towards general web analysis, specifically targeting any kind of information which both related to the selected area and to reported cases of child abuse. Following those indicators, they found an open-source report about child exploitation in this region. While the report was not giving away any specific geolocations, it gave insight into the criminal modus operandi of the group producing CSAM in the region which narrowed down the search and led them to investigative files from an anonymous source.[7] Those files provided several more outdoor images of the same CSAM producer (Figure 14). The investigative files even included imageC5 published by Europol. From then on, the Bellingcat analysts geolocated all the images one by one, hoping that it would also reveal the location of imageC5. While not going into details about each image geolocation process, the approach of the image with the hole in the wall in one of the ruins (Figure 14, bottom) needs to be highlighted. The analysts presumed the hole to be possibly resulting from a projectile impact. As they studied possible conflicts in the region which could substantiate this theory, they identified two events which took place 'along the Dniester River and the Dniester Estuary' (Gonzales, 2019). Both World War Two and the Transnistria conflict could have been the cause of such damage. Precise open-source maps of those battles provided leads to where those ruins could be located

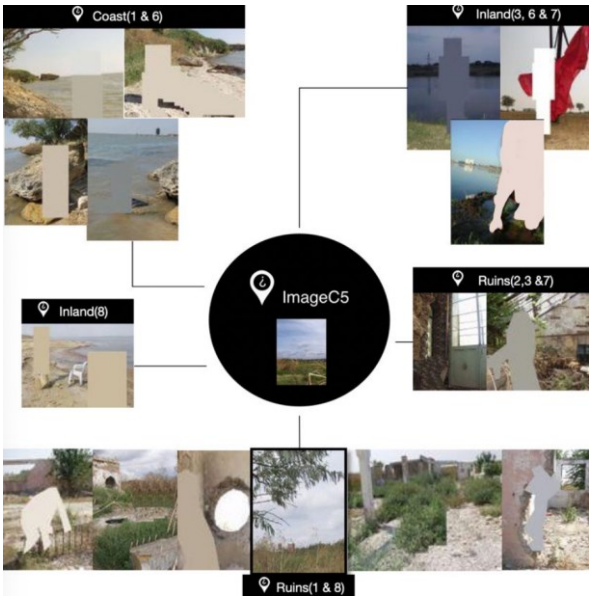

Figure 14: related images (censored) to initial

Figure 15: red pins show the geolocation of the images in figure 14 (Gonzales, 2019)

[7] Bellingcat only refers to 'investigative files' which were found following a lead from the report. They further state that the source is anonymous and the files were shared with Europol.
https://childhub.org/en/system/tdf/library/attachments/50_141_EN_original.pdf?file=1&type=node&id=6981

starting image (Gonzales, 2019)

After geolocating most of the images, the location was highly likely to be in the wider Odessa region (south Ukraine, see Figure 15). Still, the image set of 'Ruins(1 & 8)' and imageC5 were not found yet. The breakthrough was the geolocation of the red church (small building in the black encircled image of ruins(1 & 8)) which was found in a small village called Kalahliya (left bottom corner in Figure 15). From there one they only had to look for the ruins itself or the buildings in the background of imageC5 in close vicinity. As there was no Google Street View in the area, eventually, a YouTube drone video provided the missing images which were key to link and verify the elements of imageC5 (see Figure 16) (Gonzales, 2019). At the time of the investigation, the ruins were not there anymore. Still, the likely position of the photographer of imageC5 could be identified including a sketch of the ruins (see Figure 17).

Figure 16: Linking the elements in the drone video (top) and imageC5 (bottom) (Gonzales, 2019)

Figure 17: likely position of the photographer of image C5 considering all elements (bottom) and sketch of the ruins (top) (Gonzales, 2019)

This example perfectly illustrates how OSINT can indeed be used to have a real impact on TOC. In this case on a TOCG which trafficked children from Moldova from poor families to Ukraine disguising their activity as a modelling agency. While in this case, the impact of Bellingcat's investigative results cannot be evaluated as Europol does usually not provide feedback on tips from the public, it still illustrates how OSINT can be used to potentially rescue victims and prosecute members of TOCGs. Also, the example illustrated the variety of OSINT techniques, which included image and satellite analysis (e.g. algorithm-based image reverse search techniques), document and text analysis (report on CSAM in the region) and finally video analysis (YouTube drone video).

In total, it needs to be highlighted that with the image alone they wouldn't have found the location. The investigative files which included more images of the same case were essential. It highlights the need for a centralised database shared among LEAs in which images of such

cases are accessible by other LEAs or for the purpose of similar investigations in the future. Even if the geolocation process of images containing CASM (outdoor) does not necessarily result in rescued victims they might assist the 'preliminary geographical search […] creating leads for new cases (Gonzales, 2019). Recent approaches of such OSINT sharing platforms have been pushed forward and funded by the EU.

Looking at all those different perspectives and opportunities in the digital realm, Locard's claim (2010, cited in Pascual, 2017: 39), that 'every crime activity leaves a trace', is indeed at least as relevant today as it was in the past. The question is, however, whether you know where to look and how collected data fits into the bigger picture. In the next section, several approaches are explored which potentially help the criminal intelligence analyst to answer this question and to harness all available intelligence from open sources which contribute to the overall goal of understanding, disrupting, persecuting and preventing TOC.

6 OSINT Approaches and Tools – Understanding, Interrupting, Reducing TOC

Other than most other crimes, combatting TOC is particularly reliant on strategic measures. This is the case as LEAs are not just dealing with a temporary phenomenon but with large scale networks and markets. Whenever a TOCG is successfully prosecuted it is highly likely that they will be simply replaced by the next group. For this reason, strategic decisions are necessary which involve partnerships, specific resources and a certain response on the policy level. Nonetheless, tactical intelligence plays an important role too. Tactical intelligence comprises target focused intelligence activities to uncover criminal networks and operations. In contrast to market-focused strategic intelligence, tactical intelligence often involves the processing of personal data. Both forms also differ in their time focus. While strategic intelligence particularly informs long-term strategic decision-making, consumers of tactical intelligence (e.g. police chiefs and team leaders) often use it for instantaneous or short-term planning and decision-making. Subsequently, both forms will be addressed. The term *operational intelligence* is sometimes used to describe intelligence products between the tactical and the strategic level. In this research, however, operational intelligence is not analysed as an extra level as it is functionally quite similar to tactical intelligence.

6.1 On the Strategic Level: The ePOOLICE Project

Since strategic intelligence is especially interested in long-term and potential future developments, the following approaches will focus on the macro-perspective of TOC. That is, the crime trends, markets and emerging modi operandi. As Pascual rightly states,

> *a good product of strategic intelligence not only determines which is the current situation related to the phenomenon, but also provides explanations about the existence of that very phenomenon and sets likely evolutions or trends, defining possible and likely scenarios. It also enables the definition of objectives against organised crime and the establishment of policies and plans to implement and achieve the goals that have been set.* (Pascual, 2017: 36)

The ePOOLICE project as an example of strategic intelligence. ePOOLICE (2013-2015) is an EU funded project and stands for 'early Pursuit against Organized crime using environmental scanning, the Law and Intelligence systems' (ePOOLICE, 2016). It was designed to use open sources to analyse external factors in order to long-term trends in criminal markets. Similar to CAPER (see chapter 6.2), the result of the ePOOLICE project is a platform for law enforcement intelligence analysts. As ePOOLICE incorporates several important elements of (automated) OSINT techniques (e.g. web crawling or concept extraction), the project is used as an example to provide context when analysing and explaining them. Among those, the primary approach within the ePOOLICE project is Environmental Scanning (ES). While ES can be understood as the overarching concept of the project it also incorporates several sub-techniques to effectively manage data acquisition, structuring, and analysis. ES describes 'the art of systematically exploring and interpreting the external environment to better understand the nature of trends and drivers of change and their likely future impact on Organised Crime' (Pastor and Larsen, 2017: 48). Hence, ES does not directly look at crime factors and trends but on 'non-criminal drivers of change' which still have the potential to impact OC and may drive its activities in a certain direction in the future (Pastor and Larsen, 2017: 51). In this context, the environment refers to external factors in political, economic, social, technological, legal, and environmental dimensions, also known as the PESTLE dimensions. Among those dimensions, the focus is placed on all factors which have the potential to be crime relevant. 'Crime-relevant factors' (CRF) can be both factors which facilitate crime and inhibiting crime (Pastor and Larsen, 2017: 49). A basic example of this could be the opening of borders between two countries (primarily a political dimension). Without border controls, e.g. transnational traffickers of illegal goods have a decreasing risk to be caught by the customs authorities and might consider increasing their business between those countries. This would be an example of a 'crime-facilitating factor' (CFF) (Pastor and Larsen, 2017: 49). Another example and an important external factor which facilitates TOC are events that decrease state control (e.g. insurgencies and guerrilla warfare). Such situations often increase the susceptibility for corruption and ineffective law enforcement. Libya is a particularly good example in which the still-ongoing conflict has a huge impact on TOC (Williams, 2019).

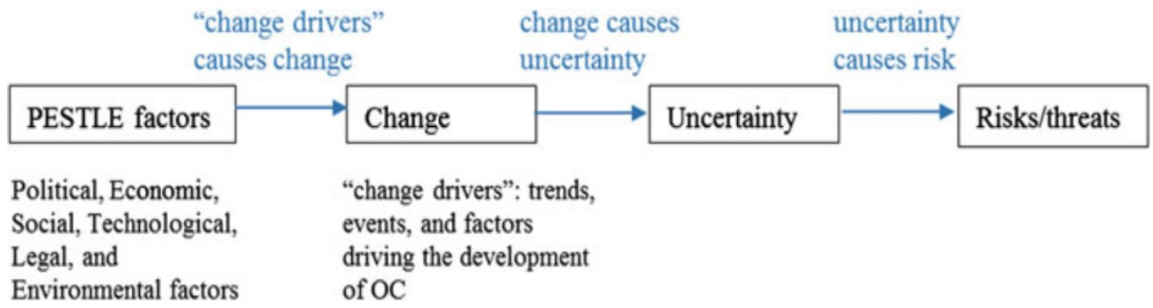

Figure 18: risk/threat identification process through PESTLE factors (Pastor and Larsen, 2017: 50)

As Figure 18 illustrates, identifying PESTLE factors is only the beginning of the process. They only direct the identification of changes or drivers which then result in uncertainties as it is not known how TOCGs will respond to those changes. Therefore the chain ends with the identification of risks and threats. From a strategic intelligence point of view, those risks can directly translate into building scenarios and producing estimates. A specific example of such a process is the already mentioned SOCTA produced by EUROPOL.

As the examples of opening borders or civil unrest are rather obvious CRFs, the focus in the environmental scanning process is additionally on so-called 'weak signals' (Pascual, 2017: 38). They are called weak signals as they have only little impact and value for intelligence purposes as an isolated signal (signals = events, news, etc). However, grouping and analysing isolated indicators 'under certain conditions, such as proximity to a certain location and type of activity, they can begin to provide insights into the presence or emergence of organised crime' (Pascual, 2017: 37).

Taking a closer look at the methodology of the ePOOLICE project, it gives a better understanding of how environmental scanning through open sources translates into actionable strategic intelligence. Open source text data is generally collected via web crawling techniques. Web crawling (or Spidering) is the process in which an automated tool (crawler) navigates through the internet from website to website until it finds the specific information it is looking for specific keywords. As websites on the internet (surface web) are all connected by hyperlinks, the web crawler can identify and follow them while searching through the content. They usually stop as soon as they have located all relevant content (Bhavsar, 2020). As Gibson (2017: 75) points out,

> *web crawlers provide a good starting point for an OSINT investigation if the investigator knows that there is a significant amount of information on the web about*

the subject they are interested in, but they do not have the time to follow links manually or read each page to identify whether it is relevant or not.

Classical examples of web crawlers are internet search engines such as Google, Bing or Baidu.

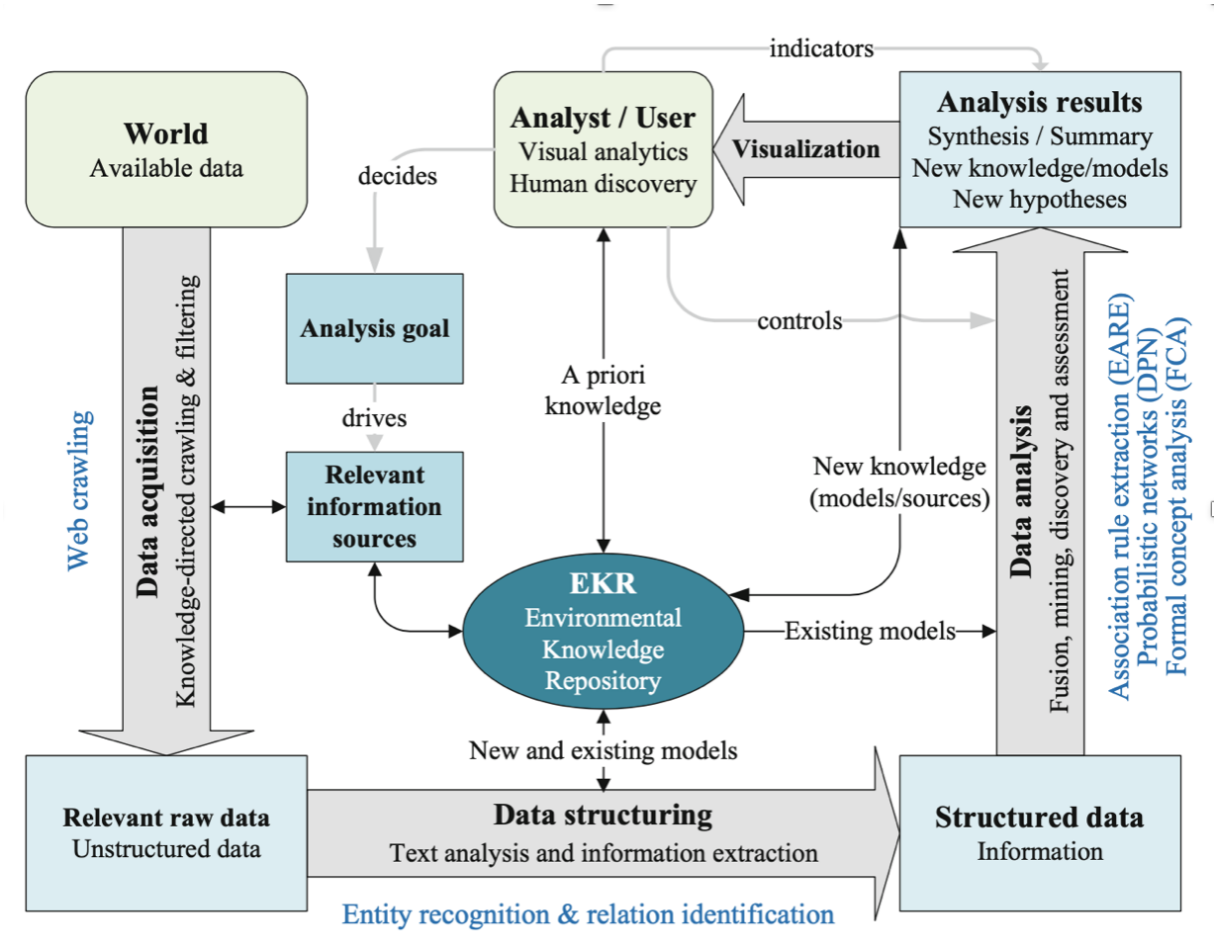

Figure 19: systematical structure of ePOOLICE (Pastor and Larsen, 2017: 57)

In the ePOOLICE process system, the crawled raw data undergoes a data-structuring-process via automated entity recognition and relation identification, also called *natural language processing* (NLP). NLP detects 'meaning from disparate content through the assessment of structure, linguistic patterns and concept references in the source data' (Brewster et al., 2014: 277). A good illustration of how NLP in the form of rule-based textual analysis can look like is illustrated in Figure 20. The concept of this example was extracted out of a Europol report on European drug markets.

<DATE>On 26 March 2012</DATE>, a highly organised <CRIME>drug trafficking</CRIME> network was brought to trial in <LOCATION>Sweden</LOCATION>. Eight members of the group faced criminal charges for trafficking multi-tonne shipments of high-quality <DRUG>cocaine</DRUG> from <ORIGIN>South America</ORIGIN> to <DESTINATION>Europe</DESTINATION>. Another trial on the <CRIME>money laundering</CRIME> .....

Figure 20: example for context extraction (Brewster et al., 2014: 278)

The words in brackets (<word>) describe the identified content categorization and can be used to build specific concept rules in order to receive the targeted information. For instance, if you are searching for human trafficking routes, you can apply the concept rules of destination and origin, as displayed in the graphic below.

Fig. 5. Concept Rule Matches

Upon arriving in <DESTINATION_LOC><LOCATION>Leeds</LOCATION></DESTINATION_LOC> traffickers were apprehended by police. The nail salon workers were identified as being trafficking victims originating from <ORIGIN_LOC><LOCATION>Vietnam</LOCATION></ORIGIN_LOC>.

Best Matches	
Concept	Matches
Top/LOCATION	2
Top/DESTINATION_LOC	1
Top/ORIGIN_LOC	1

Figure 21: Rule-based concept matches (Brewster et al., 2014: 10)

In this case, a simple open-source news article is used to demonstrate how concept extraction automatically turns unstructured data into structured results (concept matches) with meaning. Those results could then be transferred into geographical maps, visualizing human trafficking hotspots and frequent routes (Brewster et al., 2014: 277). This technique is especially helpful to identify weak signals. As mentioned above, weak signals have little value in itself but have a possibly strong impact in bulk. Figure 21 illustrates a content extraction from social media tweets with the keyword queries ‘nail salon’ and ‘nail bar’. Nail salons are often used for labour exploitation, money laundering, or human trafficking. Hence, although single tweets are only very limited (weak) indicators for OC trends when collected systematically through a specific filter, they can have an impact on strategic intelligence analysis.

Fig. 6. XML Document Markup

```
<?xml version="1.0" encoding="UTF-8"?>
<article>
<query>"Nail Salon" "nail bar"</query>
<authortimezone>London</authortimezone>
<doclang>en</doclang>
<body>The girls working at that new nail-bar in Leeds sure look young. I must ask them what their
secrets are for young looking skin!</body>
<LOCATION>Leeds</LOCATION>
<Categories>top\NailBar</Categories>
</article>

<?xml version="1.0" encoding="UTF-8"?>
<article>
<query>"Nail Salon" "nail bar"</query>
<authortimezone>London</authortimezone>
<doclang>en</doclang>
<body>Must have walked past 2 or 3 nail bars on the way to Elland Road this afternoon, they are
springing up all over the place!</body>
<LOCATION>Elland Road;Leeds</LOCATION>
<Categories>top\NailBar</Categories>
</article>
```

Figure 22: XML Tweet Content (edited by author, Brewster et al., 2014: 11)

Coming back to the process of the ePOOLICE tool, the now structured data is stored in the Environmental Knowledge Repository (EKR). The structured data, or information, is subsequently analysed via several data analysis techniques. Important to mention is that the whole process is not exclusively an automated process. The 'human in the loop' is especially important for controlling the data analysis and setting the indicators to receive the required analysis results (Akhgar and Wells, 2018: 11). The analyst or end-user of the ePOOLICE tool is provided with a graphical user interface which can, for instance, visualize the PESTLE factors per country or as a result of specific text mining techniques visualize certain illegal trafficking hot spots.

In total, the ePOOLICE project is a notable approach of how open sources can be used to provide strategic criminal intelligence on TOCGs and OCGs. It is an approach which can fully operate on the basis of open sources and is not dependent on closed source input. It makes use of several automated techniques which are incorporated into the ePOOLICE process (e.g. web crawling, textual analysis and concept extraction). The potential impact on TOC in total, especially compared to other techniques, is difficult to assess as it is a high-level approach with only long term effects. Positively, the approach of ePOOLICE does not depend on automated systems alone, but includes the human in the loop and makes effective use of 'technological resources and human actors that serves to improve the process of detecting and selecting new OC threats that warrant EU level analysis and EU-wide responses' (Pastor and Larsen, 2017: 48). Still, automated technology is an important component to process the huge amount of openly available data in which human resources are limited. As the tool does not primarily focus on the collection or the processing of personal data, it bypasses the otherwise often recognized limitation of privacy and legality of OSINT tools. Although the project itself was

only a prototype, it provided a good insight of how the application of such systems can look like. A possible limitation of this approach is that the 'big picture view' on criminal market trends and patterns can 'prevent analysts from seeing discrete pieces of information that make up the mosaic of intelligence' (Eldridge et al., 2018: 395). Especially within trend analysis, more is not always better as a lot of data can be relevant but are surrounded 'by ever increasing quantities of irrelevant data' (Eldridge et al., 2018: 395).

6.2 On the Tactical Level: The CAPER Project

After looking at an example of a strategic intelligence approach, this section analyses tactical intelligence approaches on the example of CAPER. CAPER is an EU-funded project (2011-2014) which aimed to 'support the automatic collection and analysis of unstructured text and audio-visual contents (video, audio, speech and images)' and the development of an automated tool to identify 'networks of entities and their relationships' (Aliprandi et al., 2014: 147-148). CAPER is the acronym for 'Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organised crime' (Aliprandi et al., 2014). It is a collaborative platform designed for European LEAs which facilitates the 'sharing, exploitation and linking of Open and Closed information Sources' (Aliprandi and Marchetti, 2011: 481). The CAPER platform is a novel approach of European intelligence sharing among LEAs which tries to overcome the challenge of intelligence sharing. The fusion of open and closed sources provides LEAs with the opportunity to, on the one hand, exploit OSINT form other European MS fostering interagency collaboration, and on the other hand, to integrate their own closed sources internally on the same platform allowing them to effectively fuse open and closed sources. Furthermore, CAPER's framework design also allows other participating LEAs to 'configure their own internal closed sources and control how and whom the data is shared' (Aliprandi and Marchetti, 2011: 484). While CAPER is addressing all types of OC, the transnational cooperation specifically adds value to the combatting of TOC. CAPER does not necessarily provide a new technological tool, rather it provides a new model of standardization which integrates existing state-of-the-art technology. As such, Aliprandi and Marchetti (2011: 485) argue that CAPER is especially beneficial as it can directly focus on the needs and 'functional specifications' of LEAs rather than on technical matters. In its framework design, there are six integrated technological pillars, as illustrated in the figure below: Open and Closed Sources (grey), Data Collection Services (orange), Information Analysis Services (light blue),

Information and Reference Repositories (white/black circles), CAPER Management Application (dark blue), and Visual Analytics (green).[8]

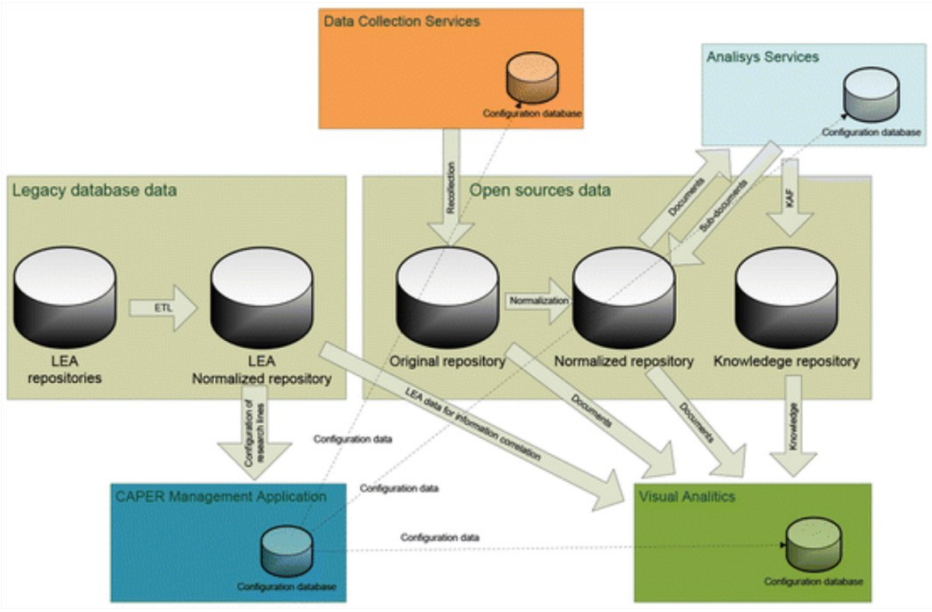

Figure 23: CAPER information flow (Casanovas, 2017)

At the collection phase, CAPER uses a multimedia crawler which is designed to 'manage huge collections of data coming from heterogeneous and distributed information sources' (Aliprandi et al., 2014: 149). Those sources can be either in text, audio, or video format. Using specific key-words, the user can direct the crawler towards specific information. The crawler is able to systematically screen URLs, documents, and social media sites (APIs) and turns unstructured data into structured data. Once relevant data is collected, it is introduced into the CAPER data management and storage process, as illustrated in the figure below.

[8] https://link.springer.com/content/pdf/10.1007%2F978-3-642-22098-2_96.pdf

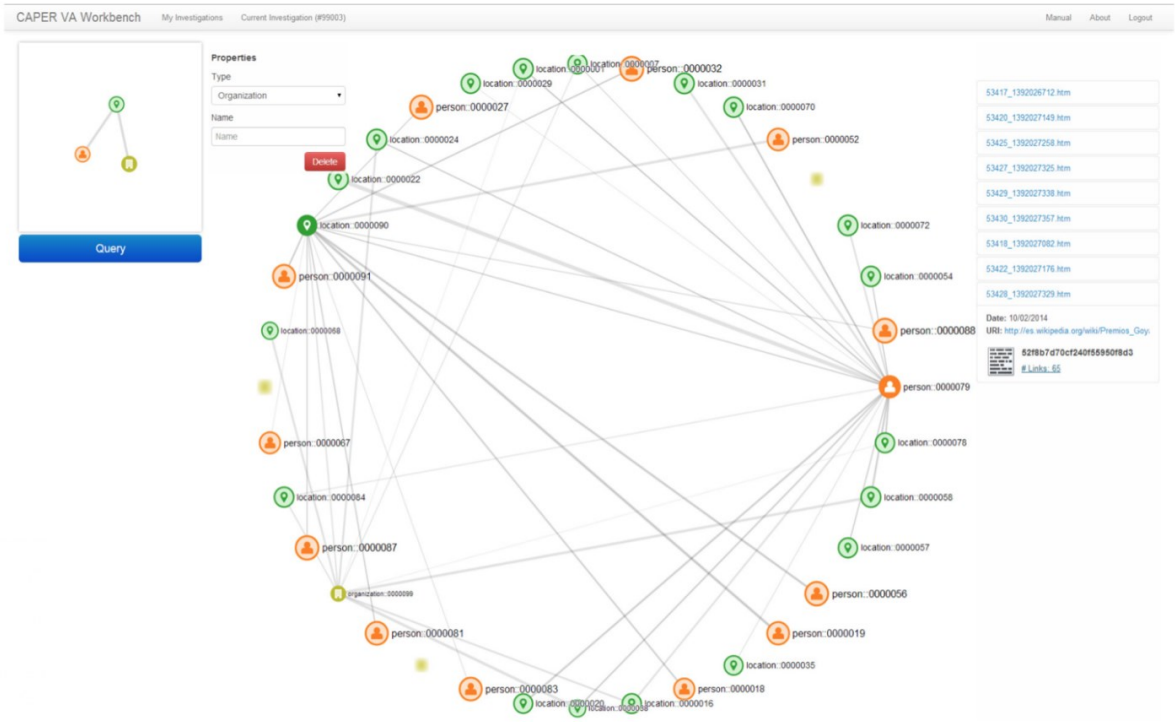

Figure 24: visual interface of CAPER (Aliprandi et al., 2014: 151)

At this step, collected open source information is saved in the original repository before it is normalized into a suitable format for the subsequent analysis (normalized repository). The central element during the analysis is the automated network screening which contextualizes entities and their relationships to each other. As Keim, Mansmann and Schneidewind argue, network and entity recognition is 'one of the most (if not the most important) objective of OSINT solutions when fighting crime' (Aliprandi et al., 2014: 150). It further illustrates the tactical nature of this approach. CAPER is not designed to identify crime relevant factors (CRFs) such as modus operandi of TOCGs, trafficking routes, money laundering or recruiting processes. Still, network insights into criminal groups might potentially result in insights which lead to further CRFs. Another limitation is that CAPER is not able to integrate AI-based Natural Language Understanding (NLU), and is limited when it comes to ambiguities of human communication (Aliprandi and Marchetti, 2011: 482).

However, on the positive side, it seems to be a strong technique for comparing and validating intelligence, especially identified entities and relationship networks. Through the crawling and analysis of multimedia and multilingual content, there is an increasing chance of not only discovering relevant entities but also validating them. The strongest element of the CAPER platform is that it does not only process open sources but also closed source intelligence from your own LEA (internal) and potentially also intelligence from other European LEAs (external) as it was mentioned at the beginning of this section. Hence, CAPER is a great example of how

European LEAs can effectively benefit both from open source itself and the resulting interagency collaboration as it is by nature less restrictive. A finding which will be further elaborated in chapter 7.2.

Ultimately, the focus on the whole project was rather on the feasibility of such a platform considering legal, ethical, and privacy (political) issues and less on its actual value on combating OC. Hence, there is little input in regards to the operational and tactical usability for ILP. However, this is not necessarily bad, as it still gives a clear insight into the issues around the use of OSINT for such purposes. In other words, even if OSINT shows great value in combating TOC but is practically not feasible due to legal and ethical constraints, there is little gain for LEAs. The CAPER project has shown that OSINT has its place in a European transnational police environment. It has the potential to bring added value to intelligence-driven LEAs combatting TOC without sacrificing citizens right for privacy.

6.3 Satellite Images and Remote Sensing Approaches

Although not often linked to OSINT, satellite images and remote sensing technology is an important asset when considering approaches of how to combat TOC via open sources. Satellite remote sensing (SRS) differs to regular satellite images, as it refers to the 'process of detecting and monitoring the physical characteristics of an area by measuring it's reflected and emitted radiation at a distance' (USGS, n.d.). This is typically done through the use of satellite or aeroplane sensory. It allows the analyst to receive other information and insights as from regular satellite images. Depending on the use case, SRS and regular satellite images each provide individual benefits. The main advantage of SRS is that it includes 'spectral, spatial and temporal resolutions' (ceinsys, n.d.). This specifically impacts the 'accuracy of ground objects' and allows scientists to identify detailed insights of selected areas, such as environmental and urban change (ceinsys, n.d.). Apart from environmental applications, SRS can also give insights into social, political and even criminological issues. One example of its application in a criminal context is for instance discussed by Bartel, as she analyses its use for monitoring and identifying the 'transgression to land clearance restrictions' which serves as a legitimate evidence in prosecutions in Australia's provinces of Queensland and South Australia (Bartel, 2018: 323). Meanwhile, a similar regulatory monitoring approach is also permissible in the EU (Purdy, 2010). While this adds to an increasingly diverse set of applications, Bartel also touches upon one very important aspect: 'the opening and commercialization of remote sensing technology' – a trend which has started in the early 1990s and thirty years later is still growing (Rothe, 2017:

341). In other words, satellite technology started to transcend from the 'monopoly of a few satellite superpowers' to the realm of non-state actors (Rothe and Shim, 2018: 415). What has been 'restricted to the defence and intelligence communities has been made available to a range of non-state actors' (Rothe and Shim, 2018: 414). This trend has especially empowered non-governmental organizations (NGOs) and activists to uncover human rights abuses and to make those findings better accessible to the general public. In other words, GEOINT is increasingly also OSINT (Williams and Blum, 2018: 8). Among others, Rothe and Shim (2018: 419) state in this context that NGOs using remotely sensed imagery have become 'quasi intelligence agencies reconnoitring the notorious secrecy of states'. This is an important point for the discussion in chapter 7, which focuses on the impact of OSINT on private and public sectors and its relation to each other.

In the next sections, several applications and approaches of regular satellite images and SRS technology in the context of TOC will be discussed. As those examples illustrate, satellite images can be understood as a hybrid approach as it can be used for both tactical and strategic intelligence purposes.

6.3.1 Environmental Crimes

Starting with the more prominent example in literature, satellite images can be not only used to analyse environmental trends such as climate change, but it can also specifically target criminal activities such as illegal deforestation and wildlife crimes. As Shelley points out, environmental crimes are on the brink in recent years and have significantly increased in its scale and focus among OCGs. Apart from cyber-related crimes, environmental crimes have 'the greatest rates of growth in illicit trade' particularly targeting 'the world's limited resources' such as water, timber, wildlife (e.g. rhinos), and fish (Shelley, 2018: 5). As the UNODC states, 'a global response for wildlife and forest crime is necessary as illicit trafficking in wild fauna and flora is transnational, supply consumption that often takes place thousands of kilometres from the source and transits several countries' (UNODC, n.d.).

An illustrative example of satellite technology for detecting environmental crimes is illegal deforestation. As the image below shows, even low-resolution satellite images without SRS technology are valuable tools to detect deforestation, especially when LEAs are not able to patrol large territories. The image below was used by an Australian State Enforcement Agency and displays illegal deforestation activities.

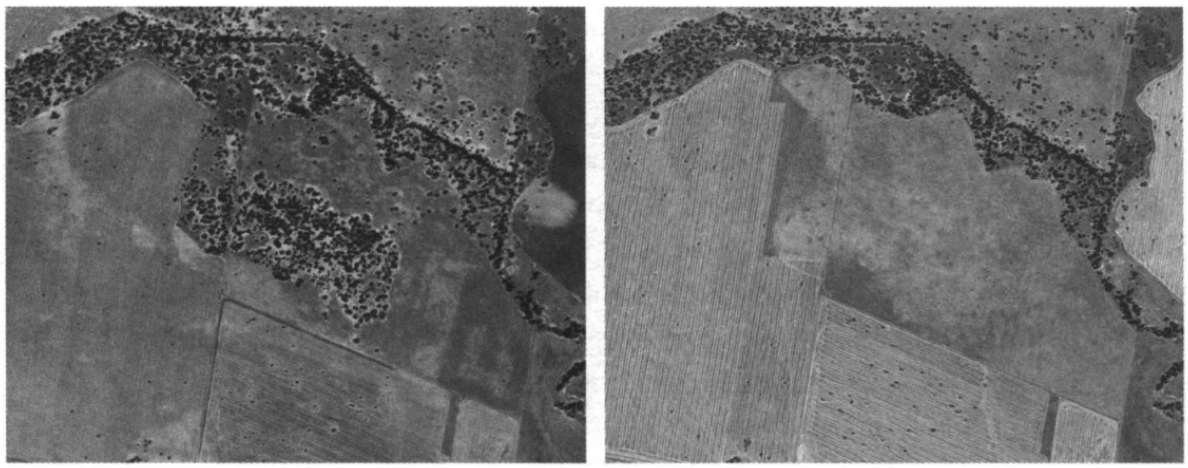

Figure 25: low-resolution image used by a State Enforcement Agency showing illegal deforestation in Australia (Purdy, 2010)

While these kinds of satellite images provide good insights if the analyst knows where to look at, gathering intelligence on environmental crime across large territories might be a time consuming and difficult process. Therefore, linking satellite images with machine learning (ML) algorithms for automatic change detections constitutes a very useful combination. As Figure 27 illustrates, specially trained algorithms are not only able to detect deforestation but also other specific characteristics such as forest gains (yellow), forest persistence (green), and non-forest areas (grey). The combination of high-resolution satellite imagery and ML is even able to detect the disappearance of individual trees (see Figure 17).

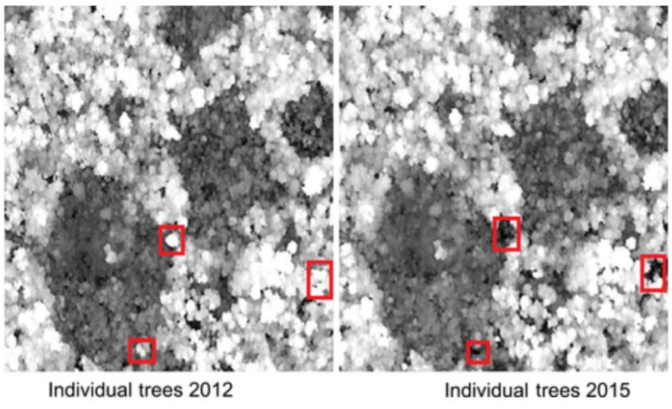

Figure 26: algorithm-based machine learning techniques

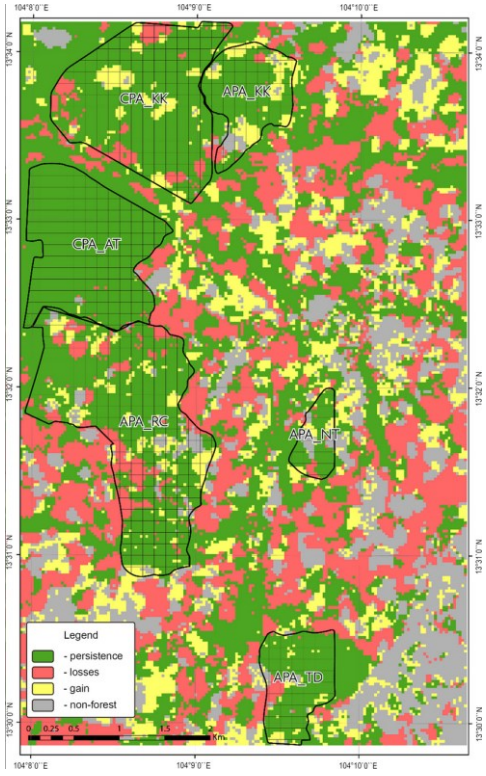

Figure 27: forest developments and trends (Singh et al., 2018)

6.3.2 Slavery from Space

The project *Slavery from Space* (SFS) is a rather novel approach of using SRS for the purpose of contributing to the United Nations Sustainable Development Goal 8.7: ending modern slavery and human trafficking by 2025. The project, led by the Rights Lab (University of Nottingham), utilizes both openly available satellite remotely sensed images and machine learning algorithms to identify brick kilns from space in South Asia. The researchers of the Rights Lab estimate that around 70% of those 23 million people manually working in brick kilns are victims of bonded and forced labour with many being trafficked into those situations (Boyd et al., 2018: 2). Thus, brick kilns give an important insight into both scale and location of forced labour – a form of TOC. As Loreen Boyd, the Director or the program, puts it, 'you can't see slavery directly, but you can infer it', referring to Rights Lab's goal of being the 'world's first Geospatial Slave Observatory' (Scoles, 2019). The concept behind this approach is twofold. In the first phase, the machine learning algorithm is trained by volunteers who manually click on brick kilns on selected satellite images on which basis the algorithm is subsequently trained on. In the second phase, the trained algorithms are applied on a much larger geographical scale to identify all other brick kilns in a selected region automatically. This approach is possible as brick kilns have a unique shape, size, and colour (see Figure 28). The search area primarily focuses on the brick belt, an area of clay fields across Pakistan, Nepal, Bangladesh, and India (around 1,551,997 km^2) (Boyd et al., 2018: 2). According to the researchers of the Rights Lab, first trials show a promising result in which the algorithm correctly identified '169 of 178 kilns in Google Earth data on one area of Rajasthan' in India (Scoles, 2019). The results of the project provided with 55,387 kilns the 'first rigorous estimate of the number of brick kilns present across the 1,551,997 km^2 area of south Asia' (Boyd et al., 2018: 8). This is especially powerful as it can be used to both direct political action to address this deeply rooted problem and to equip regional LEAs with the necessary intelligence to initiate coordinated investigations. It further provides important value for measuring and monitoring the effectiveness of prevention strategies and policies. To that end, the Rights Lab is researching opportunities to not only detect but monitor the behaviour of how and when these kilns operate (Zolli, 2018). On SRS imagery, indicators of brick kiln activities can be for instance deduced from the smoke they are creating (see Figure 29). In terms of slavery measuring, the SRS technology certainly also bears a limitation, as the reduction or inactivity of brick kilns does not necessarily imply the reduction of forced labour. The whole approach is

only effective as there is currently a high correlation between brick kilns and bonded labour (and human trafficking). However, if the percentage of currently 68% successfully decreases, it still provides a good monitoring tool of the brick industry in general. In this context, it is also important to note that brick kilns are not the only application of this approach. The Rights Lab themselves have tested their technique in the fishing industry (Lake Volta, Ghana) which likewise has strong correlations to forced labour in certain parts of the world. Furthermore, the approach can be transferred to other forced labour-affected industries such as mining or quarrying (Boyd et al., 2018: 8).

Figure 28: Brick kilns on satellite images (Boyd et al., 2018: 3)

Figure 29: brik kilns with emissions from the chimney stack (Boyd et al., 2018: 8)

Of course, such projects can be very time-consuming and costly if introduced within LEAs. Currently, this might not be feasible. Still, it highlights the importance of private-public partnership which bears strong potential for future OSINT work by LEAs combating TOC. While this is not primarily an issue of TOC affecting the EU, it still is relevant for this research question as it first highlights how OSINT can be used in a novel way to address forms of human trafficking and, second, it is relevant as European companies might have forced labour in their supply chains.

6.3.3 Drug Cultivation

The cultivation of narcotic plants is the first step in the often complex trafficking process of transnational drug trafficking. While the TOCGs try to disguise their trafficking activities, the cultivation of narcotic plants might be the most visible part considering SRS technology. Monitoring and detecting drug fields might provide significant leads to investigate the supply chain of transnational drug trafficking from early on. In its basic form, SRS technology can be used to target and monitor specific areas where drug cultivation is commonly known. In the

case below (Figure 30), for instance, satellite images show the behaviour of a well-known drug market in the Farah province of Afghanistan between mid-2018 until early 2019. The use of high resolution satellite images allows detailed activities become visible to the distant analyst. In this case, the image on the very right shows how several bags of Ephedra are loaded onto trucks. Ephedra is used for the production of methamphetamine (meth).

Figure 30: Afghan marketplace for meth production (Soderholm and Mansfield, 2019)

The image below shows how a meth laboratory is identified on the same day and later on (16th of August) targeted by US airstrikes. Through the use of high resolution satellite images, the impact of the strikes can be closely identified and the reaction behaviour analysed. On this basis, the London School of Economics and Political Science has recently conducted a detailed analysis, assessing the impact of the US air campaign targeting Afghan drug labs. It concludes that 'the campaign did not serve its primary purpose of denying revenue' as among several reasons some labs were inactive or quickly rebuilt within a short time (e.g. one month).

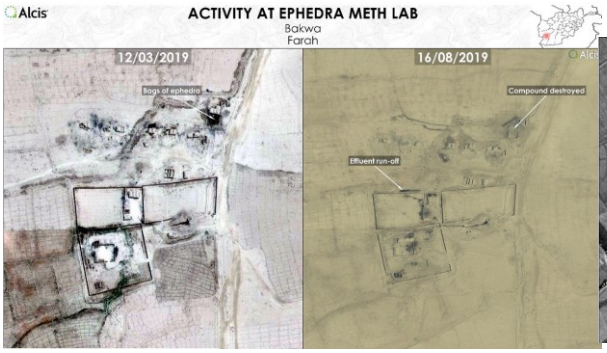

Figure 31: Examples of an Afghan Meth Lab with detailed analysis insights (Soderholm and Mansfield, n.d.)

Figure 31: post-airstrike developments (Mansfield, n.d.)

This perfectly highlights the strength and weaknesses of this approach. Firstly, the use of openly accessible satellite imagery helps non-governmental actors to hold governmental actors accountable. By carefully analysing the imagery before and after airstrikes they are able to assess the effectiveness of those strikes to a certain degree. Secondly, while SRS images might identify meth labs, it is difficult to assess whether they are active or not, and what role they have within TOC networks. Even as satellite imagery provides valuable insights, the most accurate intelligence is produced when fused with other intelligence collection disciplines, such as informants on the ground (HUMINT). Also, targeting meth labs with airstrikes is usually not relevant to the work performed by LEAs. Furthermore, the case mentioned above is certainly not the usual situation as NATO forces are currently involved in counterinsurgency operations in Afghanistan and would otherwise not be able to apply such heavy military responses to TOC. Still, it perfectly shows the tactical implications that satellite imagery can offer. However, there are certainly other responses to prevent the circulation of drugs in the transnational trafficking process.

On the one hand, SRS technology can give insights into trends which relate to TOC (an increase in the illegal fishing industry, deforestation patterns, or drug cultivation) and, on the other hand, for tactical/operational purposes when SRS images are timely analysed and disseminated they can be used for specific enforcement interference operations and prevention strategies.

7 Implications and Discussion: OSINT and the European Security Architecture

7.1 The Future of OSINT

Before looking at specific implications for the European security architecture, the chapter starts by discussing OSINT trends by assessing relevant drivers and events, how these have impacted OSINT in the past and how these might shape the future role and value of OSINT. This is important since only if OSINT continues to offer value to future European security agencies, it is worth discussing how the public and private sector can leverage on it. For this purpose, the three-generation model by Williams and Blum (2018: 40) is used, as it gives valuable context for analysing the evolution of OSINT in three waves. As chapter 2.2 has already described the evolution of OSINT in history, the section directly starts by discussing current trends and development without further explaining the first and second generation of OSINT.

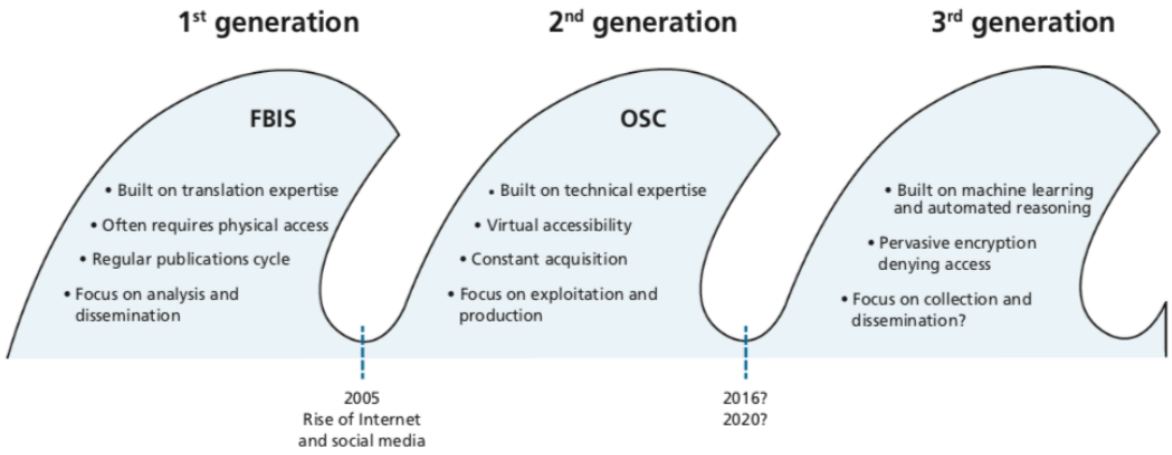

Figure 32: OSINT in three generations (Williams and Blum, 2018: 40)

Recently, some OSINT practitioners in the private sector have recognized a certain decline in the value of OSINT. Some do even proclaim that we are close to 'the end of the golden age of OSINT' (Wilson, 2019). Those claims were often made in the context of the Snowden leaks in 2013, the revelation of data breaches of Cambridge Analytica in 2018, the new General Data Protection Regulations (GDPR) of 2018 or the banning of facebook's graph search in 2019 – which enhanced users privacy (Wilson, 2019). These incidents certainly contributed to the decline of OSINT possibilities which were once common practice. For instance, the popular API graph search by Facebook allowed OSINT analysts to search extensive public user data

content (e.g. posts and likes) for keywords in a specific selected time-frame. In June 2019, Facebook eventually deleted the popular graph search feature placing more emphasis on user privacy (Cox, 2019). Despite these trends, this paper argues that what has been called the end of OSINT was only the end of 2nd generation OSINT and that recent technological trends contributed to what Williams and Blum (2018: 40) predicted as 3rd generation OSINT. Indeed, looking at the presented examples, it's reasonable to say that we are in the middle of wave three. To various degrees, almost all examples and case studies of chapters 5 and 6 included an element of machine learning and automated reasoning (or generally AI). Especially open source image analysis profits from machine learning technology. As the example of Hotels-50K illustrates, AI technology allows the analyst to reach far beyond human capabilities. The same is true for the assessment of huge data sets of remotely sensed satellite imagery. Furthermore, looking at recent EU projects, it is evident that most OSINT related projects research the application of AI/ML. As ML and AI is only starting to gain momentum, wave three is likely to persist and even expand in the near future. As discussed in chapter 6.3, advancements in SRS technology and the ongoing commercialization of satellite imagery certainly also contribute to the long-term value of OSINT.

The increasing application of automated technology, however, should not lead to the assumption that the 'human in the loop' loses in significance. As the case study of chapter 5.3 illustrates, human analysis capabilities are still central in the intelligence business. Much rather, automated technologies based on ML and AI should be understood as the longer arm of the human analyst. The examples show that AI/ML can both initiate the intelligence process (e.g. Hotels-50K, Slavery from Space, or text-crawling) or contribute to it in form of analytical and collection tools (e.g. reverse image searching).

Furthermore, it is important to highlight that the increasing development of new technologies might increase OSINT capabilities, but it does not necessarily increase the value of open source data itself. Especially the collection of personal information highly depends on individual behaviour on the internet. If a person is very careful or simply does not use the internet, the best technological tools cannot produce something valuable out of nothing. As discussed in chapter 5, individuals behaviour on the internet strongly depends on the dynamic of organized criminal groups (e.g. see biker gangs) or the overall cultural crime setting (e.g. narcomensajes in Mexico). However, as TOCGs increasingly use and depend on the internet (e.g. darknet markets), OSINT opportunities are likely to persist. However, the collection of personal information/data might become more difficult as privacy awareness generally increases and law enforcement's OSINT capabilities become more mainstream and noticed by the wider public.

As private-sector OSINT practitioner Matthias Wilson (2019) notes, 'we have shifted from the passive gathering of information to more active means of collecting data.' What he is referring to is sometimes described as digital or virtual HUMINT. It is about taking an active, often covert, role in social media or darknet forums to get the otherwise restricted information. This often requires the use of fake accounts to conceal your true identity and to blend in into a certain digital community or to engage with one specific target. Referring to the definition of OSINT in chapter 2, this practice does not count as OSINT.

Ultimately, there are various drivers which impact the future role of OSINT both in general and specifically in the context of TOC. It needs to be noted that mentioned factors have different impact on strategic intelligence than they have on tactical intelligence. For instance, as the GDPR regulates the use of personal information, this particularly affects the operational and tactical use of OSINT. The less personal data is relevant for intelligence purposes, the less OSINT is hampered by the GDPR. Hence, strategic intelligence produced from open sources is likely to remain valuable to LEAs despite increasing privacy regulatory barriers. In contrast, the value of OSINT on social media platforms (SOCMINT) is more prone to sudden changes. As it has been already mentioned, the behaviour of social media users has changed and has become more sensitive to personal data protection. This has also been the reason for the decline of wave two. However, as new generations appear which grew up with social media, trends can also quickly change. Furthermore, it also needs to be noted that these estimates might not be true globally. Indeed, there are trends which indicate considerable different internet behaviour in regions such as Africa (Marmon, 2017).

7.2 Opportunities in the Public Sector: Police Cooperation and Intelligence Sharing

Building on the elaboration on the European security architecture of chapter 4, this chapter now discusses the specific implications of OSINT. As chapter 4 has already pointed out, laws and organizational frameworks are highly diverse among EU MS. Therefore, it is generally difficult to make specific judgements of how OSINT is impacting the security architecture in the EU. However, some general implications can be made.

Firstly, the major benefit of open source intelligence products is that sources and methods generally do not need to be protected. Hence, OSINT could constitute the central element to facilitate better collaboration among relevant EU agencies. If the essential challenge among MS is related to lack of trust, a good first step is to collaborate on intelligence gathered from open

sources. This could improve interagency-collaboration and be the foundation for building closer relationships. When this collaboration is more established, further steps in European intelligence collaboration could follow. With the increasing value of open sources, there is likewise an increasing chance for better collaboration on an open source basis. Additionally, open sources bypass the problem of protecting sources and methods in criminal proceedings.
Of course, those opportunities also need to be recognized and exploited. However, looking at EU projects such as CAPER or ePOOLICE, the appetite for such collaborative OSINT platforms is certainly there and still growing. Indeed, Project VIRTUOSO (2010-2013), for instance, was specifically designed to facilitate 'cooperation of various European agencies […] by proposing a standard, open and interoperable toolkit, facilitating storage and sharing of information' (VIRTUOSO, 2019). The design of such platforms is certainly not an easy task as, on the one hand, they need to bring real added value to MS and on the other hand they need to comply with EU standards and recognize certain boundaries such as privacy requirements, especially in light of the recent GDPR. Apart from those OSINT platforms and taking into account that most intelligence products are based on multiple sources both open and closed, limitations certainly remain. Indeed, whenever open sources are fused with closed sources, the whole intelligence product effectively becomes classified and faces again the challenge of the secrecy-sharing dilemma. However, there is a potential work around for this problem. As Simeone (2008: 5) proposes, intelligence products could be produced for multiple consumers with varying degrees of confidentiality. Specifically, intelligence analysts could create one version for their own national law enforcement policy makers, another for general law enforcement, one via Europol for other MS LEAs and potentially even one for the private sector (Simeone, 2008). With strong input from open sources, these products could still bring important added value to the consumers at all levels. This practice has already been used, for instance, by US Special Forces when interacting with local actors. Instead of using classified satellite sources, they switch to open source Google Maps when sharing intelligence with third parties. Similarly, intelligence briefings for US presidential candidates which are classified as top secret are reduced to analytical judgments 'based on available evidence' without giving away details about sources, methods, or 'operational-level information about ongoing activities' (Chido, 2018: 56). This logic has already been emphasized by Rathmell (2002: 75-76) who argued in the early 2000s that 'the low level of classification required for [open] sources and methods also enables resources to be pooled between states. This further reduces costs and is likely to improve European coordination in a time of crisis.' Furthermore, the more strategic intelligence products are in nature, the less they involve sensitive operational

information about ongoing activities, specific people or events. The facts that Europol's intelligence products such as the SOCTA or TESAT which are, apart from AWS by MS, to a large degree based on open sources, show that they can bring significant added value. Apart from better information exchange, strategic intelligence reports are fostering an unified and strategic response, guiding the EU's law enforcement and intelligence community in a similar direction. Hence, OSINT can be an important source in which better collaboration among relevant EU agencies can take place.

Secondly, EU institutions gain in autonomy and significance. As the value of open sources increases, so does the value of European agencies. Without specifically referring to OSINT, Gruszczak recognizes the increasing internal intelligence capabilities of Europol focusing on strategic intelligence. Today, EU's agencies usually work both with the classified information from MS and with information from open sources. Particularly referring to Europol, past criticism often pointed towards the overreliance on 'criminal intelligence received form the member states' and its difficulties to provide real added value to national criminal investigations' (Brady, 2008). Often their input was considered as 'information rather than more serious intelligence' (Svendsen, 2013: 195). This has changed. Through the added value of OSINT, Europol and other agencies are less dependent on the input of MS, even though the quality certainly increases as more closed source input they receive. As Gruszczak (2016: 193) further remarks, 'recent years have seen increased use of qualitative and quantitative methods of data analysis and information management by competent EU agencies, most of all Europol and Frontex'. However, this is not only true for Europol or Frontex, emerging institutions such as EU's SatCen and IntCen have also received greater recognition. The role of SatCen has increased in significance as a result of both the commercialization of satellite technology and developments in the field of artificial intelligence as well as big data. SatCen itself uses the private sector services of *DigitalGlobe* for all their open source satellite imagery analysis. The relationship between Frontex and SatCen is a good example to point out that the increased significance of these agencies has fostered the collaboration among them. While they are both not primarily mandated with combating TOC, they have successfully collaborated in the context of cross-border crimes such as illegal migrant smuggling. As a matter of fact, Frontex was in 2019, with 586 requests, the third highest intelligence consumer of SatCen. Frontex uses SatCen's satellite images to identify illegal cross-border activities, such as smuggling routes and patterns and for several further non-TOC related threats (SatCen, 2020).

As Svendsen (2013: 194-195) points out, similar developments can be seen between IntCen and Europol. While this relationship mainly focuses on terrorism, the EU intelligence analysis

center IntCen originally only used OSINT for their activities. As the EUROSINT forum (cited in Hayes, 2010) highlights in one of their statements, 'OSINT provides EU institutions with the perfect platform to, quite legitimately, initiate intelligence cooperation'. In that sense, the increasing significance of EU's security agencies simultaneously increases the collaboration and trust discussed in the previous argument. Indeed, Svendsen (2013: 185) goes on to call recent developments of the 21st century in the EU as an increasing 'regionalisation of intelligence' in which OSINT is among other factors certainly one central driver.

> *Law enforcement needs the assistance of intelligence agencies, especially when it comes to transnational crime and in order to intercept communications. Effective legislation is needed to allow intelligence to be shared and to protect sensitive sources and methods. It is only through change that law enforcement can hope to keep up with the way organised crime has changed.* (Buckley, 2017: 144)

This paper argues that OSINT has positively contributed to that needed change as it makes LEAs to be less dependent on NIA and follow an intelligence-led approach. Furthermore, it allows NIAs to better share their intelligence products with LEAs as they could produce intelligence products solely based on OSINT.

7.3 Emerging Private Sector and Public Private Partnerships

As briefly presented in chapter 1, there are multiple ways of how the private sector uses OSINT for several business-oriented problems. This aspect can be noticed as especially common in sectors in which due diligence is necessary, such as the financial sector (money laundering and terrorist financing), the investment sector (integrity screenings of potential portfolio companies), or industries which need to protect their supply chains from corruption, human trafficking, environmental crimes etc. (ESG) and therefore need to engage in the so-called 'Know-Your-Customer' (KYC) process when OSINT becomes a valuable tool. While these are examples in which OSINT is used for the industries' own needs (compliance, integrity, reputation), the private sector is also a provider of public needs. This is best illustrated in the public sector of consulting and assisting (private intelligence firms, think tanks, institutes or academia) and as providers of technology which increases public sector capabilities of exploiting open sources. The realm of OSINT has an unique position in this field indeed.

Due to its unclassified nature and usability, OSINT-technology can be an advantage for both the private and the public sector. Hence, the market becomes larger as compared to other technologies solely used in the public sector (e.g. data retention). From a market perspective in which increasing demand generates enhanced supply, this can be a significant advance for research and development in the context of OSINT related technology from which public sector entities like LEAs and NIAs can profit from. One example illustrating this is the Darknet Search Engine *Memex*, developed by the Defense Advanced Projects Agency (DARPA). The tool was developed to provide a more sophisticated search engine that is able to crawl through data that are not indexed in the surface web. As a result, the search engine could be used to better monitor and detect various forms of online illicit trafficking in the darknet. The effectiveness of such crawlers lies especially on illicit industries which have an established presence in the web to attract potential customers (DARPA, n.d.). As illustrated in chapter 5.3, the primary example of this is human trafficking. Memex uses AI-based algorithms to conduct so-called 'deep monitoring' to detect the 'often hidden and covert networks' of human trafficking (DarkWeb Onion, 2020). The whole development process of Memex was accompanied by private sector experts and the use of private sector technologies and research knowledge. While the effectiveness of Memex is a question beyond this discussion, it certainly illustrates how PPP has developed in the realm of OSINT and how those partnerships can generate important value in the fight against TOC. While Memex is an example of PPP in the US, the benefit of such partnerships have certainly also been recognized in the EU. ASGARD (Analysis System For Gathering Raw Data) is a good example of an EU-led project. ASGARD is still an ongoing project specifically aiming to facilitate effective cooperation among all stakeholders, both public and private, to combat organised crime and terrorism though the development of a big data-analysis tool set. Among those stakeholders are academic and research institutions such as DCU or the KEMEA Centre for Security Studies, private technology companies such as IBM or 4iQ, and several European LEAs (ASGARD, n.d.). While these and similar projects are promising developments visible inside the EU, the challenge of implementing new features and opportunities in the national work of LEAs remains. As Trottier points out, 'the impact of OSINT on police work is tempered by an institutional culture that is comparatively unresponsive to emerging technologies, despite a perceived need among officers to be seen as embracing such technologies' (Trottier, 2015: 538). Apart from the private sector as a technological provider, OSINT has had significant implications of what has been called the *privatisation of intelligence*. In other words, intelligence agencies have started to outsource certain intelligence activities to the private sector which were originally purely restricted to

governments. This trend has started mainly in the US and as Van Puyvelde (2017: 300) argues, it can be traced back to the 'open source revolution in the 1990s' which has 'generated enthusiasm for the development of networks of experts bridging the public-private divide'. This enthusiasm was certainly fostered by the events of 9/11 and the global war on terror which had a significant impact on security policies beyond the US. While the practice of privatizing intelligence is continuously critically debated, it needs to be noted that the growing significance of open sources for intelligence purposes certainly was a central driver which facilitated this trend. As Rathmell (2002: 75) remarks, 'there is little reason to think that [OSINT] can be done better by in-house experts than by established private sector research institutes and companies. Crucially too, outsourcing will often relieve budgetary pressures.' Prominent private intelligence agencies (PIAs) are, for instance, Stratfor, Booz Allen Hamilton, and Control Risk. Most of them are based in the UK and the US but operating world-wide. Looking at their service portfolio, there was no indication found that their OSINT products focus on TOC or are specifically targeted towards LEAs. Booz Allen Hamilton (n.d.) indicated a law enforcement collaboration in regards to providing 'technical investigative tools and technologies', however, not referring to any kind of in-house analysis support. Generally, the primary focus of their analysis seems to be on geopolitical events and developments related to threats and risks for their individual clients (both public and private). Hence, when criminal incidents are monitored, the predominant focus – and this especially targeted to private sector clients – is on the question *does this impact my business and how can I mitigate the risk?* rather than *how does it help me to combat criminal actors and protect the society?*. The latter is certainly the leading question for governmental agencies. This is, however, only a limited observation since those PIAs predominantly communicate their services to private sector customers. If and how collaboration takes place with governmental actors, services are likely discussed individually and not publicly.

A third dimension in public-private relations is the one between LEAs and social media and communication providers like twitter, Facebook or Apple. Those providers basically function as information gatekeepers. Although it is an important and highly discussed PPP and relevant for combatting TOC, it is beyond definition of OSINT, and therefore not further elaborated in this research. Looking at the discussed opportunities of OSINT and its implications for European security architecture, we are today much closer to what Steele (1993: 21) was proposing in 1993 where he states:

> *Imagine an extended network of citizen analysts, competitive intelligence analysts in the private sector and government intelligence analysts, each able to access one another, share unclassified files, rapidly establish bulletin boards on topics of mutual interest and quickly pull together opinions, insights and multimedia data which is all the more valuable for being immediately available without restrictions.*

The implementation of this idea in the law enforcement intelligence domain is still lacking and there is potential to expand PPP further. However, the opportunities are there. While the EU has started to facilitate OSINT related networks via various projects, the process of implementing new approaches and opportunities in national LEAs is still a long and challenging way to go. The increasing participation of the private sector is nonetheless a promising step into the right direction.

8 Conclusion

The aim of this paper was to discuss the question of how open data can be utilized to combat TOC. As the fight against TOCGs is primarily a concern of the government, the perspective of European LEAs was placed in the center of the analysis. Conceptually, it has been shown that OSINT is most effective within LEAs that use the methodology of ILP. After contextualizing both the concept of OSINT (chapter 2) and the challenge of TOC itself (chapter 3), the following chapters were used to analyse how OSINT opportunities connect with the challenge of TOC. It has been highlighted that different types and elements of TOC provide to various degrees OSINT opportunities or generally leave behind digital footprints and traces. One of the most promising applications of it could be identified in the context of human trafficking. Specifically, against those TOCGs who are actively engaged in advertising sexual services of victims. It has been argued that the link between vendors and consumers of illegal goods and services is a particularly valuable access point for OSINT as the attention of consumers often needs to be 'publicly' attracted. Even if the illegal business of TOC is conducted in anonymous places such as the darknet, new technological solutions of text mining and concept extraction constitute promising ways forward. Automated ML-based applications in the context of image recognition, such as Hotels-50K, or in combination with satellite remote sensing, has been highlighted as a particularly effective solution. However, any of those technologies and tools are still in their initial stage of development and have not yet been used in mainstream law enforcement work. Therefore, it is highly important that the transfer of knowledge and tools is not only distributed to MS but also implemented. As this is often a financial question, political action to allow such investments is required. In regard to AI-based applications, there was no indication found that anytime soon automated intelligence tools make the work of the human intelligence analyst obsolete. Instead, it has been noted that new automated AI-based tools can help the analyst to better process the ever-increasing publicly available data. Evidence of the significance of human analysts has been presented with the case study of geolocating and investigating leads of a children trafficking case in Moldova (see chapter 5.3).

In light of projects such as CAPER or ePOOLICE, the EU has shown that it is willing to invest and develop new approaches for collaborative efforts among its MS. Looking at recent and ongoing EU projects, it is evident that there is a high appetite for public-private collaboration to use new technologies for the purpose of countering terrorism and organized crime in the EU. Not exclusively, but often, those projects specifically utilize open source data for the production of intelligence requirements. Closed-source intelligence continues to play an important role

when fighting TOC, however, OSINT does so increasingly too. It is the fusion of both closed and open source which makes intelligence products particularly effective and more reliable. As it was pointed out in chapter 7, OSINT does not only increase in its value isolatedly. Due to its unique characteristics it has positive impact on interagency collaboration and intelligence sharing. This is the case, as open source intelligence products can be more easily shared and do not have the same restrictions as closed-source products. In chapter three it was argued that intelligence sharing and police cooperation is essential not only to combat TOC but also to initially detect TOC. As TOC constitute itself through various secondary crimes, it is important not to see TOC-related crimes as isolate incidents. Only through effective interagency cooperation, the complex manifestation of TOC can be detected in all its facets. Furthermore, it has been pointed out that OSINT provides particular value and opportunities for strategic intelligence on TOC. As it is evident with Europol's SOCTA, OSINT has already been beneficially utilized on high level strategic decision making. It is critical that also EU member states recognise those opportunities and take specific action to implement OSINT methodologies beyond situational awareness (e.g. demonstrations) applications but in the context of TOC. New opportunities constantly need to be assessed so that the rapidly evolving TOCGs would not lack behind. This means also that LEAs need to become more open to the private sector and perhaps contribute both as a technology provider and as a strategic partner. Furthermore, LEAs need to consider the employment of external OSINT specialists or invest and adapt in their own training capabilities. Making use of CEPOL's training offerings or orienting on their training-needs-assessment could be particularly profitable. As the TOC would rather increase instead of ease in the near future, EU MS need to assess and evaluate all possible means to address this threat and find mitigation possibilities. The fact that TOC is often less visible to the public in comparison to terrorist attacks should not lead to an underestimation of this threat and result in political indifference. This paper has elaborated on OSINT opportunities as one promising way forward to strengthen LEAs and the wider European security architecture in the fight against this threat and its manifestation within European markets.

9 Bibliography

A Letter to the Strava Community [WWW Document], 2018. . Strava. URL https://blog.strava.com/press/a-letter-to-the-strava-community/ (accessed 8.5.20).

Action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, 2020.

Administrative Agreement on Co-operation between the European Commission and the European Police Office, 2003.

Akhgar, B., Wells, D., 2018. Critical success factors for OSINT Driven Situational Awareness.

Albanese, J., 2001. The Prediction and Control of Organized Crime: A Risk Assessment Instrument for Targeting Law Enforcement Efforts. Trends in Organized Crime 6, 4–29. https://doi.org/10.1007/s12117-001-1002-x

Aliprandi, C., Arraiza Irujo, J., Cuadros, M., Maier, S., Melero, F., Raffaelli, M., 2014. CAPER: Collaborative Information, Acquisition, Processing, Exploitation and Reporting for the Prevention of Organised Crime, in: Stephanidis, C. (Ed.), HCI International 2014 - Posters' Extended Abstracts, Communications in Computer and Information Science. Springer International Publishing, pp. 147–152.

Aliprandi, C., Marchetti, A., 2011. Introducing CAPER, a Collaborative Platform for Open and Closed Information Acquisition, Processing and Linking, in: Stephanidis, C. (Ed.), HCI International 2011 – Posters' Extended Abstracts, Communications in Computer and Information Science. Springer Berlin Heidelberg, pp. 481–485.

Analysing the Business Model of Trafficking in Human Beings to Better Prevent the Crime, 2010. . OSCE.

Anonymous, 2020. EU Security Union Strategy.

Anonymous, 2016. The history of the European Union [WWW Document]. European Union. URL https://europa.eu/european-union/about-eu/history_en (accessed 8.5.20).

Applications of Satellite Imagery & Remote Sensing Data | Ceinsys, n.d. URL https://www.ceinsys.com/blog/applications-of-satellite-imagery-remote-sensing-data/ (accessed 8.6.20).

ASGARD [WWW Document], n.d. URL http://asgard-project.eu/ (accessed 8.6.20).

Bakowski, P., 2013. The EU response to organised crime. Library of the European Parliament.

Bartel, R.L., 2018. When The Heavenly Gaze Criminalises: Satellite Surveillance, Land Clearance Regulation and the Human-Nature Relationship. Current Issues in Criminal Justice.

Best, R.A., Cumming, A., 2007. Open source intelligence (OSINT): issues for Congress.

Bhavsar, A., 2020. What Is a Web Crawler and How Does It Work? | Crawler, Spider, Bot. Hir Infotech. URL https://hirinfotech.com/what-is-a-web-crawler-and-how-does-it-work/ (accessed 8.6.20).

Boyd, D.S., Jackson, B., Wardlaw, J., Foody, G.M., Marsh, S., Bales, K., 2018. Slavery from Space: Demonstrating the role for satellite remote sensing to inform evidence-based action related to UN SDG number 8. ISPRS Journal of Photogrammetry and Remote Sensing 142, 380–388. https://doi.org/10.1016/j.isprsjprs.2018.02.012

Brady, H., 2008. Europol and the European Criminal Intelligence Model: A Non-state Response to Organized Crime. Policing 2, 103–109. https://doi.org/10.1093/police/pan014

Brewster, B., Andrews, S., Polovina, S., Hirsch, L., Akhgar, B., 2014. Environmental Scanning and Knowledge Representation for the Detection of Organised Crime Threats, in: Hernandez, N., Jäschke, R., Croitoru, M. (Eds.), Graph-Based Representation and Reasoning, Lecture Notes in Computer Science. Springer International Publishing, pp. 275–280.

Brewster, B., Polovina, S., Rankin, G., Andrews, S., 2014. Knowledge management and human trafficking: using conceptual knowledge representation, text analytics and open-source data to combat organized crime, in: Hernandez, N., Jäschke, R., Croitoru, M. (Eds.), Graph-Based

Representation and Reasoning. Springer International Publishing, pp. 104–117. https://doi.org/10.1007/978-3-319-08389-6_10
Bruinius, H., 2014. FBI asks Americans to help ID masked Islamic State jihadi. Good idea? Christian Science Monitor.
Buckley, J.F., 2017. Intelligence and Organised Crime – Paradigms and Paradoxes, in: Dover, R., Dylan, H., Goodman, M.S. (Eds.), The Palgrave Handbook of Security, Risk and Intelligence. Palgrave Macmillan UK, London, pp. 137–154. https://doi.org/10.1057/978-1-137-53675-4_8
Burcher, M., Whelan, C., 2019. Intelligence-Led Policing in Practice: Reflections From Intelligence Analysts. Police Quarterly 22, 139–160. https://doi.org/10.1177/1098611118796890
Bux, U., 2020. Police cooperation.
Canales, R., 2013. Transcript of "The deadly genius of drug cartels." TEDSalon NY 2013.
Casanovas, P., 2017. Cyber Warfare and Organised Crime. A Regulatory Model and Meta-Model for Open Source Intelligence (OSINT), in: Taddeo, M., Glorioso, L. (Eds.), Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative, Philosophical Studies Series. Springer International Publishing, Cham, pp. 139–167. https://doi.org/10.1007/978-3-319-45300-2_9
Chauhan, S., Panda, N.K., 2015. Open Source Intelligence and Advanced Social Media Search, in: Hacking Web Intelligence : Open Source Intelligence and Web Reconnaissance Concepts and Techniques. pp. 15–32.
Chido, D.E., 2018. United Nations Intelligence and Transnational Organized Crime Initiatives: Evolution and Lessons Learned, in: Chido, D.E. (Ed.), Intelligence Sharing, Transnational Organized Crime and Multinational Peacekeeping. Springer International Publishing, Cham, pp. 31–71. https://doi.org/10.1007/978-3-319-71183-6_3
Colquhoun, C., 2016. A Brief History of Open Source Intelligence. bellingcat. URL https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/ (accessed 8.5.20).
Comolli, V., 2018. Why fighting organized crime can unlock peace in conflict zones [WWW Document]. World Economic Forum. URL https://www.weforum.org/agenda/2018/05/how-fighting-organized-crime-can-unlock-peace-in-conflict-zones/ (accessed 8.5.20).
Cox, J., 2019. Facebook Quietly Changes Search Tool Used by Investigators, Abused By Companies. VICE. URL https://www.vice.com/en_us/article/zmpgmx/facebook-stops-graph-search (accessed 8.6.20).
Coyne, J., Bell, P., 2015. Conceptual Frameworks for the Integration of Strategic Intelligence, in: Coyne, J., Bell, P. (Eds.), The Role of Strategic Intelligence in Law Enforcement: Policing Transnational Organized Crime in Canada, the United Kingdom and Australia. Palgrave Macmillan UK, London, pp. 126–144. https://doi.org/10.1057/9781137443885_8
Coyne, J.W., 2014. Strategic intelligence in law enforcement : anticipating transnational organised crime.
Coyne, J.W., Bell, P., 2011. The role of strategic intelligence in anticipating transnational organised crime: A literary review. International Journal of Law, Crime and Justice 39, 60–78. https://doi.org/10.1016/j.ijlcj.2011.02.003
Day, T., Gibson, H., Ramwell, S., 2016. Fusion of OSINT and Non-OSINT Data, in: Akhgar, B., Bayerl, P.S., Sampson, F. (Eds.), Open Source Intelligence Investigation: From Strategy to Implementation, Advanced Sciences and Technologies for Security Applications. Springer International Publishing, Cham, pp. 133–152. https://doi.org/10.1007/978-3-319-47671-1_9
Dilanian, K., 2012. U.S. intelligence official acknowledges missed Arab Spring signs. LA Times Blogs - World Now. URL https://latimesblogs.latimes.com/world_now/2012/07/us-intelligence-official-acknowledges-missed-signs-ahead-of-arab-spring-.html

early Pursuit against Organized crime using envirOnmental scanning, the Law and IntelligenCE systems [WWW Document], 2016. . CORDIS EU research results. URL https://cordis.europa.eu/project/id/312651 (accessed 8.6.20).
Eldridge, C., Hobbs, C., Moran, M., 2018. Fusing algorithms and analysts: open-source intelligence in the age of "Big Data." Intelligence and National Security 33, 391–406. https://doi.org/10.1080/02684527.2017.1406677
EU Policy Cycle - EMPACT [WWW Document], n.d. . Europol. URL https://www.europol.europa.eu/empact (accessed 8.6.20).
EU SatCen Annual Report 2019, 2020. . SatCen.
EU Strategic Agenda for 2019-2024, 2019.
EU strategy for a more effective fight against child sexual abuse, 2020.
European Union Strategic Training Needs Assessment 2018-2021, 2018. . CEPOL.
Europol Strategy 2020+, 2018.
Framis, A.G.-S., 2017. Organised Crime as a Framework Concept, in: Larsen, H.L., Blanco, J.M., Pastor Pastor, R., Yager, R.R. (Eds.), Using Open Data to Detect Organized Crime Threats: Factors Driving Future Crime. Springer International Publishing, Cham, pp. 3–23. https://doi.org/10.1007/978-3-319-52703-1_1
Freeman, M., 2017. This company's scanning technology is a smugglers' nightmare [WWW Document]. URL https://phys.org/news/2017-05-company-scanning-technology-smugglers-nightmare.html (accessed 8.5.20).
Gibson, H., 2016. Acquisition and Preparation of Data for OSINT Investigations, in: Akhgar, B., Bayerl, P.S., Sampson, F. (Eds.), Open Source Intelligence Investigation: From Strategy to Implementation, Advanced Sciences and Technologies for Security Applications. Springer International Publishing, Cham, pp. 69–93. https://doi.org/10.1007/978-3-319-47671-1_6
Gibson, S.D., 2014. Exploring the Role and Value of Open Source Intelligence, in: Hobbs, C., Moran, M., Salisbury, D. (Eds.), Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities, New Security Challenges. Palgrave Macmillan UK, London, pp. 9–23. https://doi.org/10.1057/9781137353320_2
Gittens, H., 2015. El Chapo's "Official" Twitter Takes On Trump, Mexican President [WWW Document]. NBC News. URL https://www.nbcnews.com/news/latino/el-chapos-official-twitter-takes-trump-mexican-president-n391411 (accessed 8.6.20).
Glenny, M., 2018. Partners in crime: Why mafia groups and cybercriminals are joining forces [WWW Document]. World Economic Forum. URL https://www.weforum.org/agenda/2018/04/partners-in-crime-why-mafia-groups-and-cybercriminals-are-joining-forces/ (accessed 8.5.20).
Gonzales, C., 2019. Europol's Child Abuse Image Geolocated In Ukraine: A Forgotten Story Hidden Behind A Landscape. bellingcat. URL https://www.bellingcat.com/news/2019/09/11/europols-child-abuse-image-geolocated-in-ukraine-a-forgotten-story-hidden-behind-a-landscape/ (accessed 8.6.20).
Goodman, J.B., Pauly, L.W., 1993. The Obsolescence of Capital Controls?: Economic Management in an Age of Global Markets. World Politics 46, 50–82. https://doi.org/10.2307/2950666
Gruszczak, A., 2016. Criminal Intelligence in the EU, in: Gruszczak, A. (Ed.), Intelligence Security in the European Union: Building a Strategic Intelligence Community, New Security Challenges. Palgrave Macmillan UK, London, pp. 173–198. https://doi.org/10.1057/978-1-137-45512-3_7
Guidelines on Investigation Procedures for OLAF Staff, 2013.
Hammer, J., 2018. The Billion-Dollar Bank Job. The New York Times.
Hayes, B., 2010. Statewatch | Spying on a see through world: the "Open Source" intelligence industry, by Ben Hayes. Statewatch. URL https://www.statewatch.org/statewatch-

database/spying-on-a-see-through-world-the-open-source-intelligence-industry-by-ben-hayes/ (accessed 8.6.20).
Hignett, K., 2010. The Changing Face of Organized Crime in Post-Communist Central and Eastern Europe. Debatte: Journal of Contemporary Central and Eastern Europe 18, 71–88. https://doi.org/10.1080/09651561003732520
Hillebrand, C., Hughes, R.G., 2017. The Quest for a Theory of Intelligence, in: Dover, R., Dylan, H., Goodman, M.S. (Eds.), The Palgrave Handbook of Security, Risk and Intelligence. Palgrave Macmillan UK, London, pp. 1–24. https://doi.org/10.1057/978-1-137-53675-4_1
Hobbs, C., Moran, M., Salisbury, D. (Eds.), 2014. Introduction, New Security Challenges. Palgrave Macmillan UK, London. https://doi.org/10.1057/9781137353320_1
Homeland Security & Law Enforcement [WWW Document], n.d. . Booz Allen Hamilton. URL https://www.boozallen.com/markets/homeland-security-and-law-enforcement.html (accessed 8.6.20).
How Law Enforcement Uses Social Media as an Investigation Tool, 2018. . Encartele. URL https://www.encartele.net/2018/06/law-enforcement-uses-social-media-investigation-tool/ (accessed 8.6.20).
Joint Investigation Teams - JITs [WWW Document], n.d. . Europol. URL https://www.europol.europa.eu/activities-services/joint-investigation-teams (accessed 8.6.20).
Katona, N., 2020. Combating trafficking of Hungarian women to Western Europe: a multi-level analysis of the international law enforcement cooperation. Trends Organ Crim 23, 115–142. https://doi.org/10.1007/s12117-019-09358-7
Keller, J., 2011. How The CIA Uses Social Media to Track How People Feel. The Atlantic.
Kleemans, E.R., 2014. Theoretical Perspectives on Organized Crime. https://doi.org/10.1093/oxfordhb/9780199730445.013.005
Kleiven, M.E., 2007. Where's the Intelligence in the National Intelligence Model? International Journal of Police Science & Management 9, 257–273. https://doi.org/10.1350/ijps.2007.9.3.257
Lampe, K. von, 2011. The Practice of Transnational Organized Crime. Routledge Handbooks Online. https://doi.org/10.4324/9780203698341.ch12
Larsen, H.L., Blanco, J.M., Pastor Pastor, R., Yager, R.R. (Eds.), 2017. Using Open Data to Detect Organized Crime Threats: Factors Driving Future Crime. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-52703-1_1
Lemieux, F., Gerspacher, N., 2013. A market-oriented explanation of the expansion of the role of Europol: filling the demand for criminal intelligence through entrpreneurial initiatives, in: International Police Cooperation : Emerging Issues, Theory and Practice. Willan, pp. 62–78. https://doi.org/10.4324/9781843927624
Liu, X., Tian, Y., Yuan, C., Zhang, F., Guang, Y., 2018. Opium Poppy Detection Using Deep Learning. Remote Sensing 10, 1886. https://doi.org/10.3390/rs10121886
Lowenthal, M.M., 2020. Intelligence, 4th ed.
Mansfield, D., n.d. Despite claims to the contrary, US air raids against Afghanistan's drugs labs have had little to no impact. USAPP. URL https://blogs.lse.ac.uk/usappblog/2019/04/25/despite-claims-to-the-contrary-us-air-raids-against-afghanistans-drugs-labs-have-had-little-to-no-impact/ (accessed 8.6.20).
Marmon, B., 2017. The Uses and Abuses of Social Media in Africa | Democracy in Africa. URL http://democracyinafrica.org/uses-abuses-social-media-africa/, http://democracyinafrica.org/uses-abuses-social-media-africa/ (accessed 8.6.20).
McGovern, A., Milivojevic, S., 2016. Social media and crime: the good, the bad and the ugly. The Conversation. URL http://theconversation.com/social-media-and-crime-the-good-the-bad-and-the-ugly-66397 (accessed 8.6.20).
Memex (Domain-Specific Search) [WWW Document], n.d. . DARPA. URL https://www.darpa.mil/program/memex (accessed 8.6.20).

Memex High Speed Search Engine, 2020. . DarkWeb Onion. URL https://darkwebonion.com/memex-high-speed-search-engine/ (accessed 8.6.20).
Mercado, S.C., 2007. Sailing the Sea of OSINT in the Information Age. Studies in Intelligence 48.
Muggah, R., 2015. The rising threat of organised crime on social media [WWW Document]. World Economic Forum. URL https://www.weforum.org/agenda/2015/07/social-media-violence/ (accessed 8.6.20).
National Open Source Enterprise, 2006. Intelligence Community Directive Number 301.
NGA, 2015. NGA announces creation of unclassified lab to answer key intelligence questions [WWW Document]. URL https://www.nga.mil/MediaRoom/PressReleases/Pages/2015-07.aspx (accessed 8.5.20).
Olley, N., 2019. Transnational policing and organised crime, in: The Development of Transnational Policing. Routledge. https://doi.org/10.4324/9781351039543-11
OSS, 2010. The Office of Strategic Services: Research and Analysis Branch — Central Intelligence Agency [WWW Document]. URL https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/oss-research-and-analysis.html (accessed 8.5.20).
Pascual, D.S.-R., 2017. Measuring Organised Crime: Complexities of the Quantitative and Factorial Analysis, in: Larsen, H.L., Blanco, J.M., Pastor Pastor, R., Yager, R.R. (Eds.), Using Open Data to Detect Organized Crime Threats: Factors Driving Future Crime. Springer International Publishing, Cham, pp. 25–44. https://doi.org/10.1007/978-3-319-52703-1_2
Pastor, R.P., Larsen, H.L., 2017. Scanning of Open Data for Detection of Emerging Organized Crime Threats—The ePOOLICE Project, in: Larsen, H.L., Blanco, J.M., Pastor Pastor, R., Yager, R.R. (Eds.), Using Open Data to Detect Organized Crime Threats: Factors Driving Future Crime. Springer International Publishing, Cham, pp. 47–71. https://doi.org/10.1007/978-3-319-52703-1_3
Polner, M., Moell, D., 2016. Interagency Collaboration and Combating Wildlife Crime, in: Pink, G., White, R. (Eds.), Environmental Crime and Collaborative State Intervention, Palgrave Studies in Green Criminology. Palgrave Macmillan UK, London, pp. 59–75. https://doi.org/10.1007/978-1-137-56257-9_4
Press Release: With your help we are 21 000 steps closer to saving a child from sexual abuse [WWW Document], 2018. . Europol. URL https://www.europol.europa.eu/newsroom/news/your-help-we-are-21-000-steps-closer-to-saving-child-sexual-abuse (accessed 8.6.20).
Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime [WWW Document], n.d. URL https://www.ohchr.org/EN/ProfessionalInterest/Pages/ProtocolTraffickingInPersons.aspx (accessed 8.5.20).
Purdy, R., 2010. Using Earth Observation Technologies for Better Regulatory Compliance and Enforcement of Environmental Laws. J Environmental Law 22, 59–87. https://doi.org/10.1093/jel/eqp027
Ratcliffe, J.H., Guidetti, R., 2008. State police investigative structure and the adoption of intelligence-led policing. Policing: An International Journal of Police Strategies & Management. https://doi.org/10.1108/13639510810852602
Rathmell, A., 2002. The Privatisation of Intelligence: A Way Forward For European Intelligence Cooperation - “Towards A European Intelligence Policy,” in: NATO Open Source Intelligence Reader. pp. 74–79.
Romano, A., 2018. How a fitness app revealed military secrets — and the new reality of data collection [WWW Document]. Vox. URL https://www.vox.com/technology/2018/2/1/16945120/strava-data-tracking-privacy-military-bases (accessed 8.5.20).

Rothe, D., 2017. Seeing like a satellite: Remote sensing and the ontological politics of environmental security. Security Dialogue 48, 334–353. https://doi.org/10.1177/0967010617709399
Rothe, D., Shim, D., 2018. Sensing the ground: On the global politics of satellite-based activism. Review of International Studies 44, 414–437. https://doi.org/10.1017/S0260210517000602
Salisbury, D., 2014. Open Source Intelligence and Proliferation Procurement: Combating Illicit Trade, in: Hobbs, C., Moran, M., Salisbury, D. (Eds.), Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities, New Security Challenges. Palgrave Macmillan UK, London, pp. 81–100. https://doi.org/10.1057/9781137353320_6
Scoles, S., 2019. Researchers spy signs of slavery from space. Science | AAAS. URL https://www.sciencemag.org/news/2019/02/researchers-spy-signs-slavery-space (accessed 8.6.20).
Sellar, J.M., 2016. Intelligence-gathering: to question or not to question? That is the question. Global Initiative. URL https://globalinitiative.net/intelligence-gathering-to-question-or-not-to-question-that-is-the-question/ (accessed 8.5.20).
Shelley, L.I., 2018. Introduction:: THE FUNDAMENTAL TRANSFORMATION OF ILLICIT TRADE, in: Dark Commerce, How a New Illicit Economy Is Threatening Our Future. Princeton University Press, pp. 1–13. https://doi.org/10.2307/j.ctv346n56.4
Shelley, L.I., 2014. Dirty Entanglements: Corruption, Crime, and Terrorism. Cambridge University Press. https://doi.org/10.1017/CBO9781139059039
Simeone, M.J., 2008. Integrating Virtual Public-Private Partnerships into Local Law Enforcement for Enhanced Intelligence-Led Policing.
Singh, M., Evans, D., Chevance, J.-B., Tan, B.S., Wiggins, N., Kong, L., Sakhoeun, S., 2018. Evaluating the ability of community-protected forests in Cambodia to prevent deforestation and degradation using temporal remote sensing data. Ecology and Evolution 8, 10175–10191. https://doi.org/10.1002/ece3.4492
Sly, L., 2018. U.S. soldiers are revealing sensitive and dangerous information by jogging. Washington Post.
Soderholm, A., Mansfield, D., 2019. New US airstrikes obscure a dramatic development in the Afghan drugs industry – the proliferation of low cost methamphetamine. LSE US Center. URL https://blogs.lse.ac.uk/usappblog/2019/05/28/new-us-airstrikes-obscure-a-dramatic-development-in-the-afghan-drugs-industry-the-proliferation-of-low-cost-methamphetamine/ (accessed 8.6.20).
Soderholm, A., Mansfield, D., n.d. Long Read: The unknown unknowns of Afghanistan's new wave of methamphetamine production. LSE US Center. URL https://blogs.lse.ac.uk/usappblog/2019/09/30/long-read-the-unknown-unknowns-of-afghanistans-new-wave-of-methamphetamine-production/ (accessed 8.6.20).
Staniforth, A., 2016. Police Use of Open Source Intelligence: The Longer Arm of Law, in: Akhgar, B., Bayerl, P.S., Sampson, F. (Eds.), Open Source Intelligence Investigation: From Strategy to Implementation, Advanced Sciences and Technologies for Security Applications. Springer International Publishing, Cham, pp. 21–31. https://doi.org/10.1007/978-3-319-47671-1_3
Steele, R.D., 1993. National Security and National Competitiveness. Bulletin of the American Society for Information Science, Information Networks 21–22.
Stop Child Abuse – Trace an Object [WWW Document], n.d. . Europol. URL https://www.europol.europa.eu/stopchildabuse (accessed 8.6.20).
Stylianou, A., Xuan, H., Shende, M., Brandt, J., Souvenir, R., Pless, R., 2019. Hotels-50K: A Global Hotel Recognition Dataset. 1 33, 726–733. https://doi.org/10.1609/aaai.v33i01.3301726
Svendsen, A.D.M., 2013. On a "Continuum with Expansion"? Intelligence Cooperation in Europe in the Early 21st Century, in: Kaunert, C., Léonard, S. (Eds.), European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe, Palgrave Studies in European

Union Politics. Palgrave Macmillan UK, London, pp. 185–214. https://doi.org/10.1057/9781137314734_8
The Art of War by Sun Tzu Online Book [WWW Document], n.d. URL http://ancientmilitary.com/the-art-of-war-online.htm (accessed 8.5.20).
The Oxford Handbook of Organized Crime, 2014. . Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199730445.001.0001
Tracing child abusers: Where was this picture taken? [WWW Document], 2019. . BBC News. URL https://www.bbc.com/news/av/stories-47660347/tracing-child-abusers-where-was-this-picture-taken (accessed 8.6.20).
Transcript of "The real story of McMafia -- how global crime networks work," 2009.
Transnational Organized Crime – The Globalized Illegal Economy, 2012. . UNODC.
Trottier, D., 2015. Open source intelligence, social media and law enforcement: Visions, constraints and critiques. European Journal of Cultural Studies 18, 530–547. https://doi.org/10.1177/1367549415577396
UN CONVENTION AGAINST TRANSNATIONAL ORGANIZED CRIME TO ENTER INTO FORCE ON 29 SEPTEMBER [WWW Document], n.d. . un.org. URL https://www.un.org/press/en/2003/lt4373.doc.htm (accessed 8.5.20).
United Nations Convention against Transnational Organized Crime, 2000.
Van Puyvelde, D., 2017. Privatisation, in: Dover, R., Dylan, H., Goodman, M.S. (Eds.), The Palgrave Handbook of Security, Risk and Intelligence. Palgrave Macmillan UK, London, pp. 297–313. https://doi.org/10.1057/978-1-137-53675-4_17
Versatile InfoRmation Toolkit for end-Users oriented Open Sources explOitation - VIRTUOSO [WWW Document], 2019. URL https://cordis.europa.eu/project/id/242352 (accessed 8.6.20).
Waters, N., 2018. Google Maps Is a Better Spy Than James Bond. Foreign Policy. URL https://foreignpolicy.com/2018/09/25/google-maps-is-a-better-spy-than-james-bond/ (accessed 8.5.20).
Weyemberg, A., Armada, I., Briere, C., 2014. The interagency cooperation and future architecture of the EU criminal justice and law enforcement area. European Parliament.
What is remote sensing and what is it used for? [WWW Document], n.d. . USGS. URL https://www.usgs.gov/faqs/what-remote-sensing-and-what-it-used?qt-news_science_products=0#qt-news_science_products (accessed 8.6.20).
Wildlife and Forest Crime: Global Programme [WWW Document], n.d. . UNODC. URL //www.unodc.org/unodc/en/wildlife-and-forest-crime/global-programme.html (accessed 8.6.20).
Williams, H.J., Blum, I., 2018. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise: (Product Page).
Williams, M., 2019. Drugs and Smugglers: Libya has become a haven for transnational crime [WWW Document]. The Conflict Archives. URL http://theconflictarchives.com/transnational-crime/2019/5/29/drugs-and-smugglers-libya-has-become-a-haven-for-transnational-crime (accessed 8.6.20).
Wilson, M., 2019. The Golden Age of OSINT is over. Key Findings. URL https://keyfindings.blog/2019/01/04/the-golden-age-of-osint-is-over/ (accessed 8.5.20).
Zolli, A., 2018. Monitoring Human Rights from Space. Medium. URL https://medium.com/planet-stories/monitoring-human-rights-from-space-a07b0a8cb613 (accessed 8.6.20).