Future Challenges and Requirements for Open Source Intelligence in Law Enforcement Investigations:
Results from a horizon scanning exercise

Petra Saskia Bayerl
Babak Akhgar
Alice Raven
Helen Gibson
Tony Day
CENTRIC, Sheffield Hallam University

Abstract
Open Source Intelligence (OSINT) is a well-established, time- and resource-efficient method in modern-day policing. At the same time, OSINT is not immune from technological, legal and societal developments that affect the ways and contexts in which it operates. This paper examines the key challenges and requirements that OSINT as a policing capability needs to address to remain viable long-term. The results are based on a horizon scanning exercise conducted with operationally active OSINT-investigators across eight countries. Findings identify core application areas, new capabilities and essential innovations. Results further define the organisational, ethical and legal requirements enabling the integration of Artificial Intelligence into OSINT-investigations as well as the handling of 'bad actors' and citizens' increasing privacy concerns. Collectively, the results provide vital guidance for police organisations and policy makers for future investments into OSINT-tools and practices.

Keywords: *Open Source Intelligence (OSINT), police investigations, Artificial Intelligence, organisational recommendations, horizon scanning*

Introduction[1]

Open Source Intelligence (OSINT) is a well-established method to acquire actionable intelligence for law enforcement agencies' investigations. As an important element of intelligence-led policing it can support law enforcement agencies in the prevention and identification of crimes (e.g., Capellan & Lewandowski, 2019; Hayes & Cappa, 2018), assist digital forensics (Quick & Choo, 2018) and critically enhance situational awareness (Akhgar & Wells, 2018). Although some debate exists whether OSINT can in fact be classified as 'intelligence' (Miller, 2018), OSINT's ability to find new or validate existing information makes it a valuable, time-effective and resource-efficient method for modern-day policing (Staniforth, 2016).

At the same time, OSINT investigations are continuously exposed to changes in its technical and societal environment. This requires a re-assessment of where OSINT as a discipline has innovation needs as well as an investigation of upcoming challenges that need to be addressed on an operational, organisational and policy level. This paper highlights the upcoming challenges and requirements to enable the formulation of practical and strategic guidance for OSINT-professionals, police organisations as well as policy makers on concrete operational challenges as well as future directions and investments. Valuable insights have been gained from literature reviews (e.g., Evangelista *et al.*, 2021; Ungureanu, 2021). Our approach is the exploration of expert perspectives by OSINT-investigators, which offer unique insights into the operational realities and complexities as well as the organisational and policy requirements for future investments into OSINT-tools and practices.

OSINT in Law Enforcement Investigations

OSINT is characterised by three aspects: "1) [it] consists of data collected from 'publicly available sources', 2) it is data to be used in an 'intelligence context', and 3) the data collection can be performed in an overt manner" (Akhgar & Wells, 2018, p. 68). OSINT possesses several desirable features for LEAs. It is a highly flexible technique that can support the full investigative cycle from first indications of criminal behaviour to presenting supporting evidence in court (Sampson, 2016). Social network information, for instance, can assist in the identification of radicalisation and terrorist activities (Cohen, 2014; critically: Lane *et al.*, 2018), provide vital situational awareness for the assessment of threats or during protests and crises (Capellan & Lewandowski, 2019; Stern, 2017) or alert of developing community tensions (Waddington, 2019). Further, OSINT-data can validate and enrich the operational picture (MoD, 2011; Staniforth, 2016) as well as corroborate information obtained through other means such as closed and protected sources, which can safeguard them from being revealed in court (Wells & Gibson, 2017). OSINT, moreover, is a relatively low-risk ac-

1 Our research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

tivity compared to physical deployments, which considerably reduces the dangers and resources needed for intelligence work (Akhgar & Wells, 2018; Hassan, 2019). According to some estimates, OSINT underlies up to 90% of available and relevant intelligence in police investigations (Hill, 2018).

Developing Challenges: AI, societal reactions, malicious actors

OSINT-investigations face a number of challenges, some of them well known and inherent in the discipline, some of them emerging more recently. To the former belong questions about reliability and validity as crucial aspects of OSINT-practices, as OSINT-activities are generally characterised by a high degree of access to data but an often low (or unknown) degree of trustworthiness (Gottschalk, 2009). Big data crawling and social media API harvesting tools, for instance, are able to perform mass data collection, yet often offer only limited measures to refine the volume of data returned (Whitler, 2018). This means that whilst OSINT-tools have the capacity to gather vast volumes of data, the data can contain a significant amount of noise from irrelevant information which can raise concerns around collateral intrusion and the proportionality of the investigation (Sheptycki, 2004).

OSINT-investigations are further exposed to new, fundamental changes in its technical and societal environment. For instance, LEAs have begun to employ Artificial Intelligence (AI) in a drive to increase the efficiency of data processing and decision-making (cp. Evangelista *et al.*, 2021). In future, OSINT may thus increasingly be supported by (semi-) automatic collection and analysis capabilities (Pastor-Galindo *et al.*, 2020). This means, OSINT-investigators can expect to obtain increasingly diverse data and more powerful technologies to enhance the capturing and scrutiny of large, diverse data streams, challenging the notion of what 'open data' refers to (e.g., newer data sources such as smart sensors, gaming platforms, Internet of Things devices, etc. which promise additional avenues to obtain more and disparate types of OSINT).

From a societal perspective, OSINT shares traditional intelligence challenges, in that it maintains "a suggestion of subterfuge, as clandestine and covert activity conducted by officers of a shady disposition involving a degree of moral ambiguity" (Ratcliffe, 2008, p. 263). Well-publicised events such as the 2018 Facebook-Cambridge Analytica or the more recent NSO Pegasus-Software scandals only exacerbate such concerns. They dramatically sharpen public perceptions about data privacy, leading to calls for moderation in police surveillance powers and stricter rules for the private sector such as social media giants (Sanders & Patterson, 2019; Wong, 2019). Public privacy awareness and the subsequent increase in privacy consciousness can complicate the availability of (reliable) open source information; not only because people move to closed and (better) encrypted services or consciously aim to avoid surveillance (e.g., Bayerl & Akhgar, 2015; Makin & Ireland, 2020), but also because data access has been greatly reduced by platform providers. For in-

stance, Twitter's policy regards 'surveillance' as a breach of usage conditions,[2] while Facebook has limited the possibility to view the information of 'unfriended' users and graph search functionalities which allowed complex search terms across users (Shu, 2019). In combination, these movements alter the quantity and quality of open-source information available to OSINT-investigators (Walden, 2018).

Compounding these challenges are observations that malicious actors are using OSINT-techniques for their own aims (Appel, 2011). The UK Financial Conduct Authority (2018), for instance, highlighted the dangers of OSINT-use by criminals for phishing attacks, whilst notorious trolling groups such as 4chan employ OSINT-techniques to harass, bully and intimidate other websites and personal accounts (Bonser, 2019). The same techniques are also used against LEAs. Knowledge about OSINT-techniques by 'malicious actors' do not render the method useless of course, but certainly means that LEAs' OSINT-process needs adaptations and safeguards.

Together these developments alter the playing field for OSINT-investigations. This observation motivated our investigation into how OSINT as a professional practice and the organisations using OSINT need to adapt. More precisely our investigation aims to explore the nature of trends as well as what these trends mean for OSINT-practitioners and how to adjust them going forward on operational, organisational and policy levels.

Methodology

Sample

To understand upcoming challenges and innovation requirements, we conducted a horizon scanning exercise with 31 active OSINT investigators (61.3% men, 38.7% women, June 2019). The experts stemmed from twelve organisations in eight countries (Belgium, Germany and US representing 8.7% of participants each; Italy, Romania and Spain representing 4.3% of participants each; UK representing 39.1% and Netherlands representing 17.4% of participants) operating on local (43.5%), national (34.8%) and international levels (17.4%). They were recruited as participants in a three-day expert workshop hosted by the authors' research group and conducted under the umbrella of a law enforcement organisation. Participants represented disparate areas of OSINT-work (counter-terrorism, human trafficking, financial crime, smuggling, support of central and local police investigations). The workshop's objective was the demonstration of and training for emerging OSINT-techniques using classified material on real-life cases and investigation techniques. The selection of participants into the workshop was restricted to serving police officers who use OSINT actively and consistently in their professional capacity. This stringent se-

2 Cp. developer.twitter.com/en/developer-terms/agreement-and-policy.html

lection ensured that participants had extensive professional experience, area knowledge and insights into developments, trends and challenges of OSINT-use in police investigations. The authors participated in this workshop as non-police (scientific) observers and moderators (details see below).

Data collection

A vital part of the workshop was a horizon scanning exercise to gather future OSINT requirements, trends and challenges. The exercise used an exploratory, concurrent mixed-method approach (Creswell & Plano Clark, 2011) combining quantitative data collection by survey and qualitative data collection by focus group. The survey captured four main areas:

1. *Areas for which OSINT be most relevant in the next two years:* Ranking of 11 pre-defined areas from 'most' to 'least relevant' with the option to add additional areas.
2. *Most important technical capabilities for OSINT-investigators in two years:* Raking of 13 pre-defined capabilities from 'most' to 'least important' with the option to add additional capabilities.
3. *'Next big' innovation for OSINT – given money and resources are unlimited:* This question used an open-ended format to allow unrestricted collection of ideas.
4. *Role of technologies for OSINT in the future:* Participants were asked to provide their perception on 1) predictive modelling, 2) Artificial Intelligence, 3) Internet of Things, 4) big data analytics and 5) face recognition on a Likert-scale from '1:no role at all' to '4:a very big role'.
5. *Impact of people moving to 'less open platforms' for the feasibility of OSINT-investigations:* Rated from '1: no impact at all' to '4: very high impact'.
6. *Concern about 'bad actors' exploiting OSINT capabilities:* Rated from '1:not at all concerned' to '4:very much concerned'.

Instructions to participants emphasised that answers were collected anonymously without requesting personal information about individuals or organisations to remove barriers for participation. Three people declined participation, while one person had to leave before the survey was handed out, which led to 27 completed surveys.

For in-depth qualitative insights, we further conducted three focus-groups including all 31 participants. The overall group was split into three sub-groups (allowing self-selection), each of which was moderated by one of the authors. Each focus group discussed one of three topics: (1) the role of predictive analytics and AI for OSINT, (2) the increasing use of closed networks/technologies for investigators' OSINT work, and (3) dealing with the use of OSINT by bad actors. After 30 minutes, each sub-group presented a summary of their discussion to the full plenum. In a second round, each sub-group took on one of the other questions, including a reflection on the summary of the previous debate. After

30 minutes, the sub-groups again summarised their results for the plenum. This process resulted in six focus-group discussions, two for each question, including a reflection of previous results. The three moderators took detailed notes during both rounds of discussions and the two plenum sessions which formed the basis for analysis.

Data analysis and validation

Survey information was analysed using the software package R. Next to descriptive statistics (mean ranks and top rankings), multidimensional preference scaling was used to determine similarities across ranking profiles (Lee & Yu, 2013) using the R package *pmr* (specialist package for ranking data analysis; Lee & Yu, 2015). Answers to the open questions were analysed in NVivo using thematic coding (Gibbs, 2007). Thematic coding was also used for the detailed notes taken during the focus-group discussions and summaries. Open codes from the first round of coding were reviewed and grouped into higher-order themes in a second round of analysis leading to overarching categories describing (e.g., 'challenges of AI', 'mitigation strategies' for dealing with bad actors, 'adaptations' required to handle privacy-driven changes in online behaviours). The qualitative findings were used to explain, extend and detail quantitative results. An external validation of findings was conducted by a senior police officer with a national remit for security, who had not been part of the original participants (October 2019). This person confirmed our results as well as their relevance for informing the future strategic direction of OSINT in policing.

Results

Future application areas and capabilities

OSINT-experts in our group had very decided views about the areas for which OSINT will be most relevant over the coming years: across all 11 areas *counter-terrorism* (CT) and *child-sexual exploitation* (CSE) achieved the highest average ratings (indicated by lowest mean ranks in Table 1; ranked by 63% of participants in top-3 future areas). Next came *serious and organised crime* (SOC; ranked by 41% in top-3), *trafficking in human beings* (THB) and *frontline policing* (both ranked by 33% in top-3). As least relevant (highest mean ranks in Table 1) emerged OSINT-use for *community policing, money laundering* and *fraud*. Only two experts added further areas addressing *riots* and *counterfeiting*.

We conducted multidimensional preference scaling (MPS) to investigate the underlying logic of these ranking decisions, positioning experts' preference rankings along two dimensions.[3]

3 The objective of multidimensional preference scaling is to cluster responses according to their similarity and represent the degree of similarity along dimensions in space. Respondents that rank objects in fundamentally different ways will be placed at opposite sides, while respondents that rank objects in similar ways will be placed close together. In this way, multidimensional preference scaling provides insights into the underlying structure of ranking data within a group of respondents.

The first dimension suggests that experts differentiate areas according to their impact as either *low versus high visual impact*[4] – with *CT*, *SOC* and *CSE* positioned at the high end and *CP*, *frontline policing*, *fraud* and *money laundering* on the lower end of the dimension. The second dimension seems to differentiate whether the nature of OSINT-investigations is mostly *reactive* – i.e., triggered by specific events such as *fraud*, *drug trafficking* or *money laundering* – or *proactive/preventive* such as in *community* and *frontline policing*.

Table 1. Mean ranks and number of top/bottom ratings across all 11 areas

Area	Mean rank	# of times in top-3 (% of answers)	# of times in bottom-3 (% of answers)	# of times in top half (ranks 1-5) (% of answers)	# of times in bottom half (ranks 6-11) (% of answers)
Counter-terrorism (CT)	3.00	17 (63%)	1 (4%)	24 (89%)	3 (11%)
Child-sexual exploitation (CSE)	3.74	17 (63%)	2 (7%)	20 (74%)	7 (25%)
Serious organised crime (SOC)	4.22	11 (41%)	2 (7%)	19 (70%)	8 (30%)
Trafficking in human beings (THB)	5.41	9 (33%)	6 (22%)	15 (55.5%)	12 (44%)
Frontline policing (FP)	6.07	9 (33%)	10 (37%)	14 (52%)	13 (48%)
Cybercrime (CC)	6.93	3 (11%)	8 (30%)	8 (30%)	19 (70%)
Illegal migration (IM)	6.81	5 (18.5%)	7 (26%)	8 (30%)	19 (70%)
Drug trafficking (DT)	7.33	1 (4%)	9 (33%)	6 (22%)	21 (78%)
Community policing (CP)	7.37	6 (22%)	14 (52%)	9 (33%)	21 (78%)
Money laundering (ML)	7.37	1 (4%)	10 (37%)	6 (22%)	18 (67%)
Fraud (FR)	7.74	2 (7%)	12 (44%)	6 (22%)	21 (78%)

Ranking reaching from 1: most relevant to 11: least relevant.

CT and *SOC* are at the neutral point of this dimension, probably because such OSINT-investigations tend to require both approaches. *CSE* emerged as somewhat of an anomaly as it appears at the proactive/preventive side of the dimension. A possible explanation is that CSE-cases generally require longer-term strategies and resources to effectively unearth the underlying criminal structures. Whilst the expert rankings indicate that OSINT will be most relevant for areas with high visible impact, some experts foresaw preventive OSINT-use and areas of lower visible impact such as *frontline policing* and *CP*. One expert

4 We use 'visual impact' instead of 'impact' since the actual ('objective') impact of these crimes is difficult to quantify.

explicitly mentioned *'OSINT for frontline officers'* in the survey's open question, thus broadening its use beyond traditional application areas.

Table 2 presents experts' rankings for the most important capabilities for OSINT-investigators in the coming two years. Most experts agreed that *social media analysis* will remain one of the most important capabilities in an investigator's arsenal (52% in top-3), followed by ensuring the *quality of intelligence* and *data visualisation* (both 41% in top-3). In contrast, handling *games*, *multilingual content* and support for *reporting* were seen as least important.

Table 2. Mean ranks and number of top/bottom ratings across all 13 OSINT capabilities

Capability	Mean rank	# Top-3 (% of answers)	# Bottom-3 (% of answers)	# Top half (ranks 1-5) (% of answers)	# Bottom half (ranks 6-11) (% of answers)
Social media analysis (SMA)	4.00	14 (52%)	0 (0%)	21 (78%)	6 (22%)
Quality of intelligence (QI)	4.96	11 (41%)	2 (7%)	16 (59%)	11 (41%)
Data visualisation (DV)	5.44	11 (41%)	1 (4%)	13 (48%)	14 (52%)
Data fusion (DF)	6.22	10 (37%)	4 (15%)	11 (41%)	16 (59%)
Dark-web analysis (DWA)	6.37	3 (11%)	2 (7%)	12 (44%)	15 (56%)
Compatibility w/ emerging social networks (CSN)	6.44	8 (30%)	6 (22%)	12 (44%)	15 (56%)
Mobile phones (MP)	6.48	7 (26%)	3 (11%)	11 (41%)	16 (59%)
Image processing (IP)	6.93	4 (15%)	3 (11%)	8 (30%)	19 (70%)
Analysis of chat rooms (ACR)	7.63	3 (11%)	6 (22%)	9 (33%)	18 (67%)
Covering own footprint (CFP)	7.78	3 (11%)	7 (26%)	9 (33%)	18 (67%)
Games (GMS)	8.70	4 (15%)	13 (48%)	7 (26%)	20 (74%)
Multilingual capabilities (MLC)	9.04	2 (7%)	13 (48%)	6 (22%)	21 (78%)
Reporting (REP)	10.48	0 (0%)	19 (70%)	1 (4%)	26 (96%)

Ranking reaching from 1: most important to 13: least important.

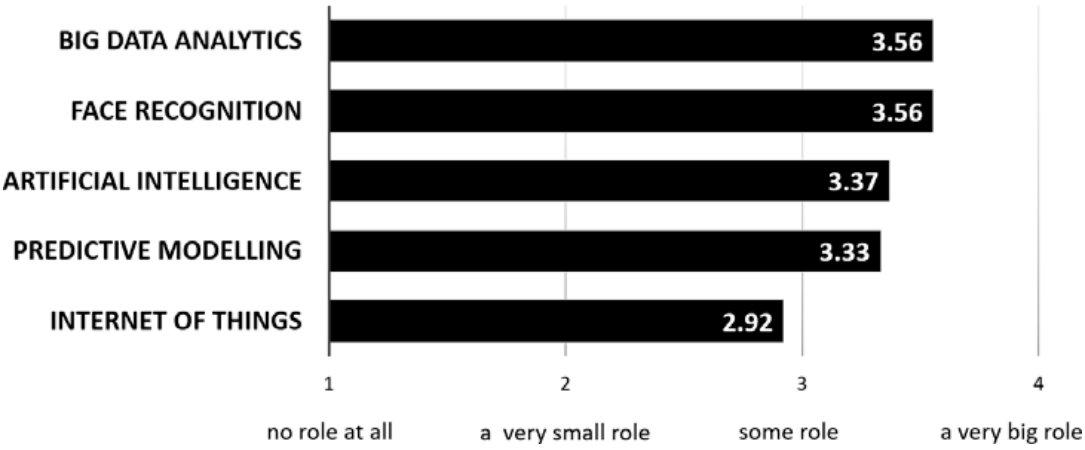
Overall, findings of our MPS-analysis suggest two disparate logics to explain disparities across ranking decisions. Firstly, experts seem to differentiate between *core* versus *supporting elements* in OSINT-investigations. Secondly, experts seem to differentiate between capabilities addressing the *OSINT-process* versus *potential data sources*. Perhaps unsurprisingly, capabilities supporting current core investigative activities such as *social media analysis*, *data visualisation, data fusion* and ensuring *quality of intelligence* were considered to remain relevant, more so than capabilities supporting *reporting* or the handling of *multilingual content*. The wide spread of profiles across core elements suggests, however,

that experts disagreed about the type of future capabilities to invest into. 37% focused on capabilities supporting the OSINT-process (*data fusion*, *visualisation,* enhancing *quality of intelligence*), while the majority (63%) indicated that the handling of disparate data sources will become most relevant. Next to investing in current core sources such as social media and images, *darkweb analysis* emerged as an important future capability, whilst one expert focused on the *analysis of chat rooms*. Interestingly, the handling of *game* content was seen as largely irrelevant, despite an increase in game-related criminal activities (Brewster, 2019).

Asked about the role of specific technologies in future OSINT-investigations, experts rated two technologies as highly relevant: *big data analytics* and *face recognition*. These were followed by *predictive modelling* and *Artificial Intelligence* (AI). We found the lowest relevance for *Internet of Things* (IoT), although it still was envisioned to play 'some role' in the future (Figure 1).

Figure 1. Average ratings for the future role of technologies for OSINT

In future, how big of a role will the following technologies play for OSINT?



Expectations for future capabilities

The quantitative results were mirrored in experts' answers to the 'wish-list' question in the survey, i.e., in their answers about the OSINT-innovations investigators would like to have. As the overview in Table 3 demonstrates, the majority of desired OSINT-innovations focuses on either the handling of additional data types and sources (e.g., 'blockchain analysis', 'darknet scraper', 'facial recognition tool') or on facilitating work across multiple platforms and data integration (e.g., 'centralised collection and data fusion', 'sharing of databases', 'platform-independent scraping'). Experts also require capabilities to make the investigation process more powerful, for instance, through automation or extra support for covert investigations such as 'total anonymity' or 'fake profile management'. In-

terestingly, experts rarely mentioned other aspects such as the groups who should use OSINT-techniques (two mentions) or organisational conditions (three mentions; e.g., 'professional LEA structures', 'senior management buy-in'). This suggests experts' preoccupation with the OSINT-process itself to the detriment of conditions that make OSINT-use successful within a broader environment. Still, focus-group discussions demonstrated that investigators are aware of organisational, legal and societal challenges surrounding LEAs' OSINT-use (see next section).

Table 3. Complete list of answers to open question about "what 'next big' innovation for OSINT would you wish you have"[5]

AUTOMATION	SUPPORT FOR COVERT INVESTIGATIONS
– Automated social media crawling – A red button in which you have an input (telephones, names...) and it gives you the most accurate result – Overview of most useful leads for manual OSINT	– Absolute online anonymity – Not just misattributed internet access, but the ability to choose a specific IP address, OS, web browser to the online host – Fake profile management, audit and development – Ability to access closed accounts/friends lists, etc.
HANDLING MULTIPLE PLATFORMS/DATA INTEGRATION	**CAPABILITIES FOR SPECIFIC DATA SOURCES**
– Centralised coordination/collation data fusion across platform – Capacity to record and capture on any platform to any evidential standard – The possibility to manage many profiles on different social platforms automatically populated with contents and credible information (for observation and covert operations) – Platform independent scraping and handling of the structured/unstructured data – Shared databases (secured) across/accessible to multiple jurisdictions – Single point of access to all management tools – emulators – A tool which gathers all databases available (phone numbers, emails, name, address, etc.), so that you can query on these items – Super-server where all the world's data come in and be categorised as a massive archive	– Big data analytics -> open source data on internet + police data + administrative data – Free & exhaustive blockchain analysis for Monero – Face recognition tool!!!; Face recognition tools (better & more reliable ones); Facial recognition software; Facial recognition capabilities* – Video recognition & detection; audio recognition – "Graph-search" functions working on Instagram, etc. – Functional social network analysis tool – Darknet - ongoing training and capabilities; Darknet scraper (Solis for all darknet/onion sites); Darknet - ongoing training and capabilities
MULTILINGUAL CONTENT	**GROUPS TO USE OSINT**
– Translation tool; Area/trustable translation solution	– OSINT for frontline officers – To allow victims to record their own OSINT in police database as evidence, e.g., hate crime

5 Number of answers does not add up to 27 as some experts provided more than one answer.

OTHER CAPABILITIES	ORGANISATIONAL CONDITIONS
– Offline plagiarism software – Effectively removing the "noise"	– Professionalised LEA structure, dedicated roles – Senior management understanding and buy-in – Tighter link between analysts and tech developers

* Answers from different experts with the same content were grouped together in one bullet point, separated by semicolons.

The role of Artificial Intelligence in OSINT-investigations

Given the frequently cited benefits of AI and predictive modelling for police work (e.g., McCarthy, 2019; Wulff, 2018), the (comparatively) low ratings for these two techniques seem surprising. The focus-group discussions revealed a somewhat ambiguous stance towards these technologies which may help explain the ratings. On the one hand, experts saw a clear potential for AI and predictive models to enhance OSINT-investigations by increasing efficiency through automation: AI may take over 'grind' work such as the automatic identification of indicators in social media content, accounts linked to the same person, removal of false positives and keeping accounts active to avoid their removal because of prolonged idleness. AI may further facilitate covert investigations utilizing automated web-scripts and bot-networks to collect large volumes of data through both reactionary (capturing data based on specific target activity) or proactive (continually capturing data in set time periods or based on user specified parameters) approaches. By automating 'menial tasks' OSINT-investigators should be able 'to handle many more investigations' than they are able today. The main future benefits of AI are seen as a 'force multiplier' by allowing police forces to increase efficiency and decrease workload.

However, experts were also vocal about challenges that limit the usefulness of AI for OSINT-investigations. Three types of challenges emerged:

a) *Technical and developmental challenges:*

- AI developers are believed to lack advanced knowledge of policing and more specifically insider knowledge about the processes and standards guiding the presentation of data and decisions in legal proceedings. AI applications therefore are often unable to produce evidence that is legally valid to be submitted to court. To help matters, experts requested a closer link between AI developers and OSINT-investigators starting during the preliminary stages of development (cp. Table 3).
- Participants claimed that research into AI innovations and algorithmic models cannot use real data from police investigations. Instead, development and testing rely on data specifically created for research and testing purposes (or 'fake data' in the words of our experts). They thus question whether AI applications and algorithms can be trusted for use in such a critical domain – and without trust in the data for AI-training and decision-making the results will not be trusted either.

- Severe events such as terrorist attacks are extremely rare which means there is very little data to train AI-models, thus jeopardizing their accuracy. Hence, participants see AI-support as inappropriate for OSINT-investigations concerning (very) rare threats.
- Experts further questioned whether social and psychological factors that influence criminal behaviours can be modelled with sufficient accuracy. Factors and relationships are deemed too complex for AI to capture and replicate realistically, particularly with current methods. The same is suggested for complexities inherent in language material as language detection and translation tools often struggle with specific dialects or concepts such as sarcasm. Experts were uncertain whether these issues can be resolved in the near future to a level adequate for police use.

b) *Procedural challenges:*

- Keeping predictive models up-to-date and relevant over time can be a challenge, as predictive models are often not updated fast enough to reflect changes in communication or behavioural trends (e.g., the use of specific hashtags is highly volatile; yet models often fail to remove/change such hashtags in a timely manner).
- Experts further observed that social media companies are becoming increasingly restrictive about accessing and harvesting their data, which creates constraints and negatively affects the feasibility of automating data collection using AI as such attempts may be blocked by platform providers.
- Some experts raised the possibility that reliance on AI can lead to the de-skilling of human analysts and investigators, threatening the expert basis of police work long-term.

c) *Ethical/legal challenges:*

- Given the often 'black box' nature of AI applications and models (i.e., lacking transparency of parameters and decision-making rules), experts questioned whether AI is able to create justifications that will be acceptable in courtrooms. They therefore want the OSINT-process to be overseen by human investigators with an understanding of AI-programming as well as knowledge in legal and ethical constraints.
- AI developments and deployments generally move faster than the discussions about their use in police forces and the development of legal and ethical frameworks. This creates consistent gaps between 'what is technically possible' and 'what is legal or ethical' which experts feared can lead to a legitimacy deficit in the perception of the public as well as legal challenges for LEAs.

For the above reasons, experts requested that the human analyst needs 'to be kept in the loop' stating that AI can never be 'a replacement' of human experts. In their view, human investigators accumulate experiences that create important intuitions or 'gut feelings' which 'sets humans apart' from AI-algorithms. Experts moreover suggested that in the

near future AI should be trained only to detect and/or remove generic content instead of training algorithms on domain-specific content. Also, AI should be restricted to the investigation of generic trends rather than specific cases.

Is the move to closed platforms an issue for OSINT-investigations?

Survey results indicate that experts are at least somewhat concerned about the development (m=3.30, sd=.54), which also acknowledged in focus groups in that experts proposed that behavioural changes may make their OSINT-work more difficult. Specifically, the distinction between overt and covert investigations can become dangerously blurred, when 'users move underground'. In consequence, OSINT-investigators may have to increasingly adopt covert techniques and therefore breach open source frameworks or pass investigations to other parts of the organisation to maintain legal and best practice standards. Although it will remain possible to collect intelligence, the quantity and detail of information collected through OSINT may thus decrease. Conversely, experts pointed out that with new platforms also new opportunities emerge to enhance investigations. LEAs should thus increase their presence on new platforms and investigators remain informed of developments to avoid 'playing catch-up', whilst ensuring not to neglect older media (e.g., Facebook).

Some experts also saw considerable 'scaremongering' in the public discussion around privacy which make new platforms appear more encrypted and secure than they really are. Most experts agreed that typical human characteristics will continue to play out on emerging platforms opening the doorway for future OSINT-investigations (e.g., users' need to post, link, like and share information to enhance their own ego, and individuals leaving their profiles open because they are inattentive about their digital security and privacy). Moreover, they expect that crime groups such as terrorist organisations will continue to require a public presence (e.g., for recruitment or to enhance their image), whereas offenders trying to groom children will still have to establish contacts over platforms that are popular with children. These activities will leave traces OSINT-investigators expect to follow and continue exploiting in future.

Threats from 'bad actors'

'Bad actors' refers to individuals or groups that aim to exploit OSINT-methods for criminal or malicious intent. According to survey results bad actors are a concern, although only to a moderate degree (m=3.00, sd=0.83). Experts highlighted the dangers of 'sharing too much', particularly by 'more senior officers'. Oversharing can create vulnerabilities to entire police departments; as one expert recounted it was possible to map 'their whole force from top to bottom' using free OSINT-tools. Whilst officers cannot be expected to live without an online presence, experts emphasised that keeping a minimal digital footprint is essential, especially as social media companies constantly modify privacy settings with potential implications for the exposure of private material. A growing challenge is

that new police recruits often have a long-standing social media presence, which is almost impossible to erase. Experts emphasised the need for prevention by raising the general level of awareness about digital footprints and 'how to stay private online' including training at all levels of police organisations. They suggested that OSINT-investigators should regularly conduct OSINT on themselves to obtain a picture of their own (and/or their colleagues') online exposure.

Discussion and Implications

Our results offer important insights for police organisations, policy makers as well as the status of OSINT as a discipline. Starting with the areas for which OSINT-investigations will be relevant, we found that high-visual impact areas (CT, CSE, SOC) emerged as primary future applications. Given that OSINT-specialisations across participants are quite broad our findings on areas seems to showcase a consensus across investigators on the large topic areas. At the same time, the question was raised whether OSINT should be retained as a 'specialist profession' located within expert teams. Some experts suggested that OSINT should be opened up to others such as frontline and community policing officers, which indicates a shifting understanding of OSINT as an investigation method. OSINT is already increasingly interwoven with other areas such as DMI or forensics. Experts saw value in an even broader approach that applies OSINT across all policing areas. In this perspective, OSINT would – and should – become a generalist tool instead of a specialist capability. For LEAs, this would require breaking down organisational and cultural barriers that often exist between specialist OSINT-experts and other policing disciplines as well as making trainings, tools and OSINT-resources available to staff not yet involved in OSINT-efforts.

Chief amongst highlighted challenges and their consequences for OSINT-use emerged securitisation/privacy movements resulting in the potential blurring between overt and covert procedures. Handling these challenges well is critical for the long-term validity and reliability of investigations (Bayerl & Akhgar, 2015; Walden, 2018). The UK has started this process, re-labelling OSINT as 'III' (Internet Intelligence and Investigations).[6] This deployment model incorporates overt and covert investigations, presenting a considerable change into how OSINT is understood and positioned. Addressing this issue alters and widens again the remit of OSINT, although in a different way than above: It results in breaking down the traditional demarcation between OSINT and covert investigations, in the process challenging existing legal and ethical frameworks. This calls for rapid and fundamental answers from policy and law makers.

6 https://www.uk-osint.net/documents/Internet_Intelligence_&_Investigations_Strategy_v13.pdf (Accessed: 20. September 2022)

Experts' wish-list of future OSINT-capabilities can be seen as a reflection of this increasing difficulty to access online data, combined with its growing volume and fragmentation. The wish-list focused strongly on efficiency gains (e.g., through automation and platform integration) and the handling of additional data sources. New data sources and new capabilities such as those requested by experts in our study require updates to ethical guidelines and legal regulations. Experts identified a number of pertinent legal and ethical questions that still need clarification, not only addressing 'how much' and 'in which ways' data should be gathered in investigations, but also the balance between human versus machine in decision-making following the envisioned automation of OSINT-processes.

Especially with respect to AI, our findings unearthed highly differentiated perspectives that identified significant potential but also considerable challenges to its large-scale implementation on technological, procedural and legal/ethical grounds. Experts made concrete recommendations about how to manage human and technological inputs in OSINT-investigations and the imperative of keeping humans 'in the loop' to avoid unexpected negative results of automation. In addition, police organisations should make efforts to be involved in the development and design of OSINT-related technologies such as predictive models and AI, to avoid the 'generic', 'black box' applications dreaded by our experts. This would help ensure that police organisations are not only users of OSINT-related technologies but can crucially shape systems to adhere to policing principles and effectively support the investigative process from source identification to evidence in court.

The 'wish-list' of capabilities and challenges identified in our study also clearly requires additional resources, training and support. OSINT-investigators, for instance, acknowledged a lack in awareness and training concerning threats by malicious actors. Such calls for more training are common across expert areas (e.g., Burcher & Whelan, 2018). Yet, training needs may also lay beyond the one's experts identified. For instance, the concern that research on and development of AI-applications and algorithmic models cannot use actual police data may reflect public opinions rather than the state-of-the-art in AI. To ensure that OSINT-investigators remain up-to-date with emerging technologies (e.g., IoT, AI, darkweb, blockchain), it is crucial that technological knowledge of investigative staff keeps pace with technological advancements. Strategic levels should equally request regular updates and trainings to guide decisions about which innovations to invest in and whether and how to adapt organisational procedures, as staying abreast of technological and societal changes requires continuous organisational awareness and flexibility to scope and react to technological, legal as well as societal developments.

Limitations and future studies

Our observations are based on evidence from an international group of experienced OSINT-investigators to achieve a broad view on future developments and challenges. While they probably played into discussions, country-specific issues were not in the scope

of our study and will require more targeted investigations; especially as there is yet to emerge an inter-organisational or even international consensus about OSINT-principles. Future investigations should also be conducted into how police organisations and policy makers together will react to the issues and recommendations outlined in this paper and the long-term effectiveness of such measures.

References

- Akhgar, B. & Wells, D. (2018) 'Critical success factors for OSINT driven situational awareness', *European Law Enforcement Research Bulletin*, 4, pp. 67-74.
- Appel, J.E. (2011) *Internet Searches for Vetting, Investigations, and Open-Source Intelligence*. Boca Raton, FL: Taylor and Francis.
- Bayerl, P.S. & Akhgar, B. (2015) 'Surveillance and falsification implications for open source intelligence investigations', *Communications of the ACM*, 58(8), pp. 62-69.
- Bonser, J. (2019) '*Capture the flag using OSINT technique*', Netwatch Global. Available at: https://www.netwatchglobal.com/case-studies/capturetheflag/
- Brewster, T. (2019) "*Discord: The $2 billion gamer's paradise coming to terms with data thieves, child groomers and FBI investigations*", Forbes. Available at: https://www.forbes.com/sites/thomasbrewster/2019/01/29/discord-the-2-billion-gamers-paradise-coming-to-terms-with-data-thieves-child-groomers-and-fbi-investigators (Accessed: 04 June 2022)
- Burcher, M. & Whelan, C. (2018) 'Intelligence-led policing in practice: Reflections from intelligence analysts', *Police Quarterly*, 22(2), pp. 139-160.
- Capellan, J.A. & Lewandowski, C. (2019) 'Can threat assessment help police prevent mass public shootings? Testing an intelligence-led policing tool', *Policing: An International Journal*, 42(1), pp. 16-30.
- Cohen, K., Johansson, F., Kaati, L. & Clausen Mork, J. (2014) 'Detecting linguistic markers for radical violence in social media', *Terrorism and Political Violence*, 26(1), pp. 246-256.
- Creswell, J.W. & Plano Clark, V.L. (2011) *Designing and conducting mixed methods research* (2nd edition). Los Angeles: Sage Publications.
- Evangelista, R.J.S., Romero, M. & Napolitano, D. (2021) 'Systematic literature review to investigate the application of Open Source Intelligence (OSINT) with Artificial Intelligence', *Journal of Applied Security Research,* 16(3), pp. 345-369.
- Gibbs, G.R. (2007) 'Thematic coding and categorizing', Gibbs, G. R. (ed.), *Analyzing qualitative data*, SAGE Publications, Thousand Oaks, pp. 38-55.
- Gottschalk, P. (2009) 'Information sources in police intelligence', *The Police Journal*, 82(2), pp. 149-170.
- Hassan, N.A. (2019) *Digital forensics basics*. Berkeley, CA: Apress.
- Hassan N.A. & Hijazi, R. (2018) *Open source intelligence methods and tools*. Berkeley, CA: Apress.

- Hayes, D.R. & Cappa, F. (2018) 'Open-source intelligence for risk assessment', *Business Horizon*, 61, pp. 689-697.
- Hill, S. (2018) *Open source investigations – building your toolkit*, City of London Police.
  Available at: https://academy.cityoflondon.police.uk/blog/introduction_open_source_investigations_stephen_hill
- Lee, P.H. & Yu, P. (2013) 'An R package for analyzing and modelling ranking data', *Medical Research Methodology*, 13(65), pp. 1-11.
- Lee, P.H. & Yu, P. (2015). *Package 'pmr'*.
  Available at: https://www.maths.bris.ac.uk/R/web/packages/pmr/pmr.pdf (Accessed: 04 June 2022)
- Makin, D.A. & Ireland, L. (2020) 'The secret life of PETs. A cross-sectional analysis of interest in privacy enhancing technologies', *Policing: An International Journal*, 43(1), pp. 121-136.
- McCarthy, O.J. (2019) *AI and Global Governance: Turning the Tide on Crime with Predictive Policing. Digital Technology and Global Order,* United Nations University Centre for Policy Research.
  Available at: https://cpr.unu.edu/ai-global-governance-turning-the-tide-on-crime-with-predictive-policing.html
  (Accessed: 04 June 2022)
- Miller, B.H. (2018) 'Open source intelligence (OSINT): An oxymoron?', *International Journal of Intelligence and CounterIntelligence*, 31, pp. 702-719.
- MoD (2011) *Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations* (3rd edition), UK Ministry of Defence.
- Quick, D. & Choo, K.-K. (2018) 'Digital forensic intelligence: data subsets and open source intelligence (DFINT+OSINT): A timely and cohesive mix', *Future Generation Computer Systems*, 78, pp. 558-567.
- Ratcliffe, Jerry H. (2008) 'Intelligence-led policing', in Wortley, R. & Mazerolle, L. (eds.), *Environmental Criminology and Crime Analysis*. Routledge, pp. 263-282.
- Sampson, F. (2016) 'Intelligent evidence: using open source intelligence (OSINT) in criminal proceedings', *The Police Journal*, 90(1), pp. 55-69.
- Sanders, J. & Patterson, D. (2019) 'Facebook data privacy scandal: a cheat sheet', *Tech Republic*.
  Available at: https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet (Accessed: 04 June 2022)
- Sheptycki, J. (2004) 'Organisational pathologies in police intelligence systems: some contributions to the lexicon of intelligence-led policing', *European Journal of Criminology,* 1, pp. 307-332.
- Shu, C. (2019) 'Changes to Facebook graph search leaves online investigators in a lurch', *Tech Crunch*.
  Available at: https://techcrunch.com/2019/06/10/changes-to-facebook-graph-search-leaves-online-investigators-in-a-lurch (Accessed: 04 June 2022)
- 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*. Cham: Springer, pp. 21-31.
- Stern, E.K. (2017) 'Crisis management, social media and smart devices', in Akhgar, B., Staniforth, A. & Waddington, D. (eds), *Application of Social Media in Crisis Management*. Cham: Springer, pp. 21-33.
- UK Financial Conduct Authority. (2018) 'Don't let a scammer enjoy your retirement - FCA and TPR 60 Second TV Ad', *UK FCA*.
  Available at: https://www.youtube.com/watch?v=NeFvYtCaykI (Accessed: 04 June 2022)

- Ungureanu, G.-T. (2021) 'Open source intelligence (OSINT). The way ahead', *Journal of Defense Resources Management,* 12(1), pp. 177-200.
- Walden, I. (2018) "The sky is falling!' – Responses to the 'going dark' problem', *Computer Law and Security Review*, 34, pp. 901-907.
- Wells, D. & Gibson, H. (2017) 'OSINT from a UK perspective: considerations from the law enforcement and military domains', in *Proceedings Estonian Academy of Security Sciences*, pp. 84-113.
- Wong, J.C. (2019) 'The Cambridge Analytica scandal changed the world – but It didn't change Facebook', *The Guardian Online*.
  Available at: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook (Accessed: 04 June 2022)
- Wulff, J. (2018) 'Artificial intelligence and law enforcement', *Australasian Policing*, 10(1), pp. 16-23.