OSINT from a UK perspective: considerations from the law enforcement and military domains

WELLS, Douglas <http://orcid.org/0000-0001-8877-039X> and GIBSON, Helen <http://orcid.org/0000-0002-5242-0950>

Published version

WELLS, Douglas and GIBSON, Helen (2017). OSINT from a UK perspective: considerations from the law enforcement and military domains. In: Proceedings Estonian Academy of Security Sciences, 16 : From Research to Security Union. Estonian Academy of Security Sciences, 84-113.

OSINT FROM A UK PERSPECTIVE: CONSIDERATIONS FROM THE LAW ENFORCEMENT AND MILITARY DOMAINS

Douglas Wells, MA Conflict, Development and Security Studies
CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research), Sheffield Hallam University, UK
Researcher

Helen Gibson, PhD
CENTRIC, Sheffield Hallam University, UK
Lecturer in Computing

Keywords: OSINT, law enforcement, military, intelligence

ABSTRACT

Both law enforcement and the military have incorporated the use of open source intelligence (OSINT) into their daily operations. Whilst there are observable similarities in how these organisations employ OSINT there are also differences between military and policing approaches towards the understanding of open source information and the goals for the intelligence gathered from it. In particular, we focus on evaluating potential similarities and differences between understandings and approaches of operational OSINT between British law enforcement agencies and UK based MoD researchers and investigators. These observations are gathered towards the aim of increasing interoperability as well as creating opportunities for specific strengths and competencies of particular organisational approaches to be shared and utilised by both the military and law enforcement.

1. INTRODUCTION

The value of intelligence, be it for law enforcement, the military, or businesses, cannot be understated. Intelligence gives an organisation some kind of advantage over another; this might be the vital intelligence that solves a crime, enables victory in a battle, or allows a company to return a better profit than their rivals. This intelligence may come from a wide range of sources: from people who have been interviewed, from internal data and logs, from crime scene evidence, from videos and imagery, from phone calls and communications, and many more besides. One intelligence discipline that is attracting more and more attention is open source intelligence (OSINT). Fuelled by the near ubiquitous nature of the internet and coupled with narcissistic tendencies that have accompanied the rise in the use of social media, OSINT has moved into the fore of the intelligence gathering disciplines. However, as we will see in this paper social media is not the only source of open source intelligence and nor does it exist in a vacuum from other intelligence sources. This study is built primarily upon a qualitative analysis but also references personal communications of interactions between the researchers and key informants of the military and police OSINT sector.

2. DEFINING OSINT

Open Source Intelligence will be shown throughout this paper to be a dynamic term that often consists of contradictory or ambiguous pre-requisites and thus one single definition does not exist. A good starting point is the definition provided by the CIA (2010) who make the claim that "information does not have to be secret to be valuable" and build on this tenet to describe OSINT as public information that can be retrieved from:

- The Internet
- Traditional mass media (e.g., television, radio, newspapers, magazines)
- Specialised journals, conference proceedings, and think tank studies
- Photography
- Geospatial information (e.g. maps and commercial imagery products)

However, they do not rule out the fact that other open sources may also be available as well as clarifying that this data collected from 'publically available' sources must be used in an 'intelligence context' and the collection of the subject data may be performed in an overt manner.

The Ministry of Defence (2011) in the UK provides a more specific definition of OSINT: "intelligence derived from publicly available information that has limited public distribution or access." In particular, they state that OSINT material is especially useful when "exploited by trained analysts to ensure the intelligence produced is unbiased and free of prejudice, open-source material is no less important than protectively marked material". This statement of OSINT being equal to other forms of intelligence is a recurring theme within official doctrine around OSINT; however, many of these reports also mention that it sometimes can have difficulty in being taken seriously.

Most intelligence domains (HUMINT, SIGINT, IMINT, etc.) have their roots in the military and in such a context; OSINT became an accepted term around the mid-90s (Steele, 1995). An early example of OSINT was the Foreign Broadcast Intelligence Service (FBIS), which monitored

foreign radio broadcasts, transcribed and translated them, beginning in 1941. In fact, as early as 1947, Allan Dulles (formerly Head of the CIA), and at that point working for the Office of Strategic Services, is reported as saying that 80 percent of the required intelligence during peace time could potentially be obtained through open sources and more recent estimates have continued to offer the same claim or even higher (Gibson, 2014).

The National Police Chiefs Council (NPCC) in the UK also provides two similar definitions of open source (2015). The first being on what is considered open source research:

> *"the collection, evaluation and analysis of materials from sources available to the public, whether on payment or otherwise to use as intelligence or evidence within investigation".*

The NPCC then go on to define open source information as being:

> *"Open source is defined as publically available information (i.e., any member of the public could lawfully obtain the information by request or observation). It includes books, newspapers, journals, TV and radio broadcasts, newswires, Internet WWW, and newsgroups, mapping, imagery, photographs, commercial subscription databases and grey literature (conference proceedings and institute reports).*

Thus we see that the police definition of open source is somewhat more extensive and specific than what is supplied by the MoD. It could be argued that the NPCC definition is more detailed due to a recent publication, additionally, following the Snowden and Assange leaks of 2013-2016 (Kwoka, 2015, p.1387), it may have been of interest to better define online investigation tactics to avoid potential controversy and increase public transparency (ISC, 2015, p.6). Therefore, because the NPCC definition is more recent and more developed, yet doesn't conflict or disagree with current UK military practices, this paper will use it as the primary definition of OSINT for subsequent comparisons.

Descriptions of OSINT, such as those cited from the CIA, MoD, and NPCC, characterise the range of definitions available of OSINT and their tendency to be rather broad and nonspecific. And while there may

be areas of agreement within these definitions and others; it is also clear that some of the generic criteria for defining OSINT may be somewhat ambiguous. As such there are at least three observable areas of potential dispute: (1) the use of the term *publically available;* (2) the extent to which the data is collected *overtly* and *covertly*; and (3) the requirement to practice good *cyber-hygiene* when conducting open source investigations. We now consider these points term-by-term.

Firstly, the phrase *'publically available'* is open to interpretation. Both military and law enforcement officers may, when authorised, draw upon 'open source' data that a non-service civilian could not gain access to. Two such examples include; driver and vehicle registrations (DVLA databases) and financial data including credit ratings and banking providers (Home Office Centre for Applied Science and Technology (CAST), 2016, personal communication, November 2016). Although such databases can be accessed by paying customers, local authorities and police organisations this information is not made available to the general public. Indeed, there may be some debate as to whether such access to data can reasonably be considered 'open source'. Whilst information stored by websites such as 192.com holds personal OSINT data behind 'paywalls', this is considered to be 'fair game' meaning anyone with the interest in purchasing details such as personal addresses, electoral and telecoms data may do so. Indeed, other databases, such as those maintained by large companies often host what is known as 'consented data'; and, while such data is only stored when someone gives their consent, the extent to which they are made aware of both how this data may be used in the future and opportunities to scrub data from these records are not expressly advertised. Arguably, police and military access to DVLA and financial databases are a step beyond 'paywalls', wherein the data is not available for the wider public under any circumstance.

Secondly, although many OSINT definitions describe that the data collection process *may* be done in an overt manner, in practice it is rarely done so (South Yorkshire Police, Digital Media Investigations Officer, 2017, personal communication, February 2017). This is especially true due to the dominance of the internet both for data storage as well as through its convenience to search and locate intelligence through social media and other publicly open sites, and while the NPCC defines five levels of open source research, only Level 1 is explicitly termed overt research (National Police Chiefs Council, 2015).

Social media especially is a minefield because of the personal nature of almost all information posted to such sites. For example, considering investigations that operate on Twitter and Facebook, users are not and cannot be notified if their profile content is being reviewed, screen-captured, directly downloaded by another user or through a specially designated OSINT software product such as Repknight (2017), Echosec (2017) and Cosain (2017). Interestingly, such OSINT products market themselves specifically for Policing, Home Office and MoD usage by making themselves on the G-Cloud (the UK government's digital marketplace (see e.g., Cosain[1] and Palantir[2])).

Historically and internationally, such methods of covert OSINT surveillance may be recognised as early as the 1930's, in which the aforementioned United States Foreign Broadcast Intelligence Service (FBIS) (Mercado, 2007) was established to begin monitoring overseas public radio frequencies, by 1941 it had begun to turn radio into a primary intelligence source during World War II. In a similar manner to the investigation methods of the contemporary era, this OSINT was accessing publicly available sources through covert technologies with trained analysts, the process was invisible to axis powers (Mercado, 2001) in the same manner modern social media collection may be undetectable to suspect user profiles.

Thirdly, often not stated is the responsibility of military and law enforcement (when operating at levels 2-5, see below) to act with high levels of 'cyber hygiene', minimising the digital footprint left behind on websites, or use services to mask such a presence. This approach is considered to be more of a counter-intelligence measure than clandestine exploitation. Indeed, it is often necessary to protect the anonymity of investigators, the organisation as well as the individuals or groups being targeted, which may in turn reveal details of the operation.

Additionally, UK law enforcement have specific guidance, via the College of Policing, detailing the requirements for level 4-5 OSINT investigations utilising social media account takeovers and covert human intelligence sources (CHIS) to obtain 'open source' social media evidence

[1] https://www.digitalmarketplace.service.gov.uk/g-cloud/services/945108024310388 (Cosain)

[2] https://www.digitalmarketplace.service.gov.uk/g-cloud/services/388738118169964 (Palantir Front Line Policing and Intelligence)

or intelligence (Cleveland Police, 2014). This may be a particularly contentious issue, due to the high-level covert tactics taken to impersonate or infiltrate online sites in the pursuit of data acquisition. They would appear to contradict any overt possibilities of OSINT as well as massively stretching definitions of what is deemed 'publicly available'. As such, levels 4-5 of OSINT usually require the highest levels of surveillance authority in place (National Police Chiefs Council, 2015; Home Office, 2014). These levels are generically accepted to be:

1. Overt OSINT Investigations/Research
2. Core OSINT Investigation/Research
3. Covert Advanced OSINT Investigation/Research
4. Covert Internet and Networks Investigations
5. Undercover Online/Covert Internet Investigator

Level 5 OSINT deployment is of particular interest, because it appears to blur the line between OSINT and covert surveillance and interception the most. It is defined as;

> *"Online covert activity 4.32 The use of the internet may be required to gather information prior to and/or during a CHIS operation... the CHIS may need to communicate online, for example this may involve contacting individuals using social media websites. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this code." (National Police Chiefs Council, 2015; Home Office, 2014).*

The above three contradictions show that many existing definitions of OSINT are somewhat ambiguous when considering the technical practicalities of both contemporary law enforcement and military approaches. It may be of interest to explore whether these definitions are kept deliberately vague to allow the optimal access to investigative equipment, tactics and data sources.

3. INTEGRATION OF OSINT AS AN INTELLIGENCE DISCIPLINE

Despite the military being one of the key proponents of the use of OSINT, both from the US and also NATO (who produced the de facto OSINT handbook in 2001) the extent to which open source information is used in military operations is underreported with, perhaps unsurprisingly, few examples in the public domain. Nevertheless, there are continued efforts to push forward the use of OSINT in combination with data mining techniques as well as text analytics and artificial intelligence as a solution to enhance the capabilities of intelligence analysts. Such analyses are now feasible and, in fact, demanded due to the growing availability of real-time and predictive analytics which can utilise information from the past and present and use it to predict what may happen in the future (McCue, 2014).

Although OSINT has merits of its own as a single intelligence source, particularly in the military domain it can also be used to validate information garnered from closed intelligence sources and as such may enable the protection of a closed source though obtaining the same information from an open one. OSINT can also be utilised as part of an 'all-source analysis' bringing further credibility to the intelligence as it has been verified through multiple sources (Haigler, 2012).

In the near future, it is expected that the use of OSINT within the military will only increase simply due to the amount of information being made available online, the ease with which it can be accessed, the relatively low-cost of obtaining it compared with other intelligence sources as well as counteracting the feeling of not being left behind (i.e., everyone else is doing it) (Homeland Security Research, 2017)

Due to the UK police's reliance on OSINT to help provide evidence as well as enhance and parallel evidence from other sources, it may be argued as to having a greater structure and focus than in the military, partially due to the greater reliance on capturing evidence and the requirement for such evidence to stand up reliably in court when called upon.

In many cases, obtaining open source intelligence may be considered a form of directed surveillance, when conducted at level two and above in the aforementioned levels of open source research. In order to carry out such an investigation the police and the specific case in question is authorised via a directed surveillance authority (DSA). Such a permission may be given by "... an authorising officer where he or she believes that the authorisation is necessary in the circumstances of the particular case on the grounds that it is: (a) in the interests of national security; (b) for the purpose of preventing or detecting crime or of preventing disorder; (c) in the interests of the economic well-being of the UK; (d) in the interests of public safety; (e) for the purpose of protecting public health" (Home Office, 2014)

Such legislation may appear to further muddy the definitions of OSINT, as levels 2+ of OSINT investigative deployment appear to require 'covert surveillance authorities' to be in place and set the conditions and limitations of the operation (with the exception of imminent threats to life or serious bodily harm). This may appear to the wider public as somewhat ambiguous for the collection of open or publicly available data, but is specifically to protect privacy via the *means of collection*. To ensure that data and evidence is captured in the correct open source manner, the JAPAN principles are still deemed by law enforcement as a suitable approach for OSINT analysts and officers (Kent Police, 1998). JAPAN is an acronym for **J**ustified, **A**uthorised, **P**roportionate, **A**uditable, **N**ecessary; and such an approach ensures that the values of the 1998 Human Rights Act are preserved (UK Government, 1998), most noticeably (Article 8) privacy, and to ensure everyone is treated with fairness and respect.

Military OSINT operations and intelligence have the benefit of being able to work from the UK remotely, assisting in operations across the globe. However this still means they are bound by RIPA (Regulation of Investigatory Powers Act) (UK Government, 2000) the same as UK police forces. There is not necessarily a requirement for the MoD to apply RIPA when conducting intelligence operations overseas; however, it is MoD policy to apply RIPA to any intelligence operation regardless of the country the intelligence is being gathered in citing the fact that "... [RIPA] provides a well-established regulatory framework for such operations and reduces the chances of improper conduct and abuse" (British Army, 2009). Nonetheless, from an outsider's perspective it is impossible to be certain how rigorously this mandate is being applied.

Particularly in the world of OSINT the application of RIPA can be problematic given that online investigations and specifically those on social media, which are becoming ever more common, are not sufficiently covered by RIPA (Bartlett et al., 2013) as it was written prior to the massive SM explosion from 2007 onwards (Digital Trends, 2016). Thus the sooner that all legislation can catch up with the growth of technology the more protection there will be for those who are utilising OSINT and those who are being investigated.

4. RELIABILITY OF OSINT

Open source information, in the UK the policing 5x5x5 grading system, tends to never be considered better than E41 Intelligence. E41 stands for an untested source, of which the reliability cannot be judged but it can be disseminated within the UK Police Service and to other law enforcement agencies as specified (College of Policing, n.d.).

Open source intelligence, is usually defined as being: "Open sources of information are widely available but may not be accurate, reliable or valid. The main uses of open-source information are to:

- Develop an understanding of the locations relevant to a piece of analysis
- Identify the potential impact of social and demographic changes
- Identify external factors that may impact on crime, disorder and community concerns
- Support and develop investigations by indicating lines of enquiry or corroborating other information
- Support the development of subject profiles and problem profiles.

There are several factors to take into account when using open-source information:

- Access may require the user to register or pay a fee (eg, online news media, the electoral roll)
- The use of open-source information should be audited
- The effect of local security policies on access to open-source information (eg, some sites are not available to local users)
- It is not subject to the same quality standards as closed sources
- It should be corroborated by supporting information

When accessing open-source information online, a footprint identifying the police address is left on the website. A non-attributable IT identity is sometimes required to avoid law enforcement being identified as the originator of the enquiry. An accredited covert internet investigator should be asked to advise in these instances." (College of Policing, 2013)

This is the same for both military and police classifications, whilst OSINT is seen as valuable, it is best through 'paralleling' or 'clustering' techniques. Paralleling is the process of using alternative research/investigative resources (such as OSINT) to find exact or associated information that has come from a closed source (Donohue, 2015). This is particularly useful for preserving the integrity and security of hidden and embedded assets, additionally this approach can be used to find and document a chain of evidence from intelligence leads.

Clustering, is a technique that utilises a collection of strong and, or, weak 'signals' to predict the bigger picture (Lesca and Lesca, 2011). For example, when trying to guess the end product of a recipe; the more individual ingredients that are learned, the greater the probability of understanding the specific type of cake. OSINT can be particularly useful for feeding in big data crawling results to help further validate or expand stronger human led analysis.

Paralleling is not the only use of OSINT though, and while many were still sceptical of open source information, the 9/11 attacks brought OSINT back to the fore in the military domain, as intelligence managers realised that such information could not be easily discounted (Hulnick, 2010). Post these attacks, researchers were even able to put together a network from open sources of the links between many of the hijackers and associates, thus leading to a better understanding of how the hijackers communicated and were able to remain undetected for long enough to carry out such an atrocity (Krebs, 2002). Thus despite the claims over its unreliability OSINT has proven itself to be useful not only for validating other intelligence, but also as an intelligence source in its own right. The onus is on the investigating analyst to have the training, knowledge and expertise to accurately assess the OSINT source individually and make a reasonable assumption about the reliability of the source on its own merits independent of whether it was obtained openly or not.

5. DIFFICULTIES AND DISPARITIES DEFINING OSINT IN MODERN SECURITY

As previously discussed there is not an accepted definition of open source intelligence be it for law enforcement, the military or elsewhere and even within existing definitions the scope of the material and the means that can be used to obtain it are not standardised and varies across different practices. This causes issues to new people entering the field as there is no standard reference or accepted form of OSINT. Even established books, such as Michael Bazzell's Open Source Intelligence Techniques (2016) include social engineering techniques that may not be considered acceptable for LEAs or military usage.

Law enforcement and the military may also collect OSINT for different reasons and we are at pains to point out the difference between OSINT for digital evidence capture and OSINT for intelligence capture.

As of June 2017, the UK military do not use the equivalents of CHIS or OSINT levels 4-5 in operations deemed open source intelligence or research gathering. Some exceptions to this may be 77th Brigade (British Army, 2017) who are known to use Facebook, Twitter and other social media to engage in non-lethal warfare (MacAskill, 2015). However, as a force wide security policy the majority of military OSINT does not involve any form of impersonation/engagement or CHIS approaches.

In gathering SM data, two primary types of profiles may be deployed; 'grey man' and 'embedded' accounts. (Nottinghamshire Police Open Source Intelligence Investigator, 2016, personal communication, August 2016). Grey man accounts are necessary to pass through the basic 'log in' requirements of SM sites such as Facebook, VK and Telegram, allowing the account access to a greater degree of content, than if the investigator wasn't registered with the site. These grey man accounts do not 'befriend, follow, or engage' in any form of communication with other profiles, their benefit is to simply pass through SM site login barriers to obtain open source content within. This approach is commonly used by the MoD and other non-policing governmental actors as they are considered to be deployed at OSINT levels 1-2. Beyond this, 'embedded

accounts' may be used (usually within law enforcement with regards to a specific tasking and a DSA). Such accounts are deliberately presented and maintained as genuine users, with friend lists, active statuses, profile interests, etc. These are designed to enable the profile to 'infiltrate private groups inside SM provider sites, or to gain access to suspect profiles with a greater degree of security. The specifics of how and to what extend such profiles are populated and integrated into social media networks is dependent on the localised force policy in the police.

In using OSINT for investigations both the military and the police have to tread a fine line around perception and how this impacts on the privacy of those who are under investigation. Furthermore, there is a blurring of lines between HUMINT and OSINT (particularly when dealing with crowdsourcing intelligence) (Mak et al., 2017). This concern would also be present when police or military extrapolate investigations and operations to third parties or outside experts.

There are also wider growing concerns around the expectations of privacy online ranging from the mantra that online privacy is dead and that those who are worried about exposing their personal details should just 'get over it' to legitimate concerns (Edwards and Urquhart, 2016). As the GDPR (General Data Protection Regulation) comes into force this also raises concerns around the access and storage of personal data; although, there are exceptions around law enforcement. Further confusing the issue are the complications that will arise as the UK looks to leave the EU and implements its own legislation away from existing EU law (O'Sullivan, 2017).

6. DIFFERENCES BETWEEN UK LAW ENFORCEMENT AND MOD USE OF OSINT:

6.1 Priorities for counterintelligence and OSINT leakage are different between the military and police

In UK law enforcement, ACPO (Association of Chief Police Officers), now formally known as the NPCC (National Police Chiefs Council), laid a foundation for online and social media privacy standards for police staff in their 2013 document: Guidelines on the Safe Use of the Internet and Social Media by MDP Officers (Ministry of Defence Police, 2013), officers are encouraged to use the internet for social media purposes, but insist that because *information on SM may be made public* they ought to behave as they would *on duty* given that "Information placed on the Internet or social media could potentially end up in the worldwide public domain and be seen or used by someone it was not intended for, even if it was intended to be 'private' or is on a closed profile or group. It is likely that any information placed on the Internet or social media will be considered to be a public disclosure." In this document, it is worth noting that Section 6 relates to: Safeguarding Personal and Sensitive Data which reiterates the requirement for police not being able to leak or disclose others' personal and private data, whilst Section 7 relates directly to preserving the integrity of the police force reputation.

Section 8**,** of the same document, is entitled: 'Keeping your private life private'. Due to the potential for criminals and malicious actors to use the internet, particularly social media to identify personal information about police officers. They may be capable of obtaining; 'embarrassing, discrediting, harassing, corrupting or blackmailing them or their families'. Therefore the guidance to "Ensure privacy settings for social media are set to the highest level, not to register on social media using pnn.police.uk e-mail addresses, to be careful when accepting 'friends' to access their social media, not to be associated with inappropriate material on 'friends' social media, not to be associated with social media of criminals and not to be associated with the social media of persons involved in serious organised crime." are issued to all officers governing their use of social media overall, (Derbyshire Police, 2012).

Furthermore, officer are encouraged not to post online specific details such as employer, job post, hobbies and locations frequented, images in uniform, mobile numbers and email addresses, vehicle and home addresses, family member details, etc. Additionally; "It is also recommended that police officers who may wish to pursue duties in covert policing carefully consider whether the publication of personal images and information on social media may restrict their future career opportunities in such areas on the grounds of personal safety, public safety and operational security."

The MoD has published similar standards in the; 'Online Engagement Standards' document of 2009 (Ministry of Defence, 2009). This document covers the same areas as UK law enforcement, however arguably with greater detail and is stricter with organisational and operational data security. Military personnel are encouraged to never speak as if they are doing so on behalf of their organisation without oversight from a senior commanding officer. Additionally, they should avoid publishing material that:

- Relates to operations or deployments
- Offers opinions on wider Defence and Armed Forces activity, or on third parties without their permission
- Attempt to speak, or could be interpreted as speaking, on behalf of your Service or the MoD
- Relates to controversial, sensitive or political matters

Additionally, it is advised that; "Such online presences provide an opportunity for Service and MoD civilian personnel to explain their work. But they also carry risks to individuals, to their Service and to Defence. Service and MoD civilian personnel are already using online presences and Defence information is entering the public domain unofficially. Guidelines are therefore required." This shows that there is a greater emphasis on security due to the increased security risks to individual personnel, the wider organisation, as well as in the data itself - which may be used by belligerent nations with a far greater skillset than the average 'criminal organisation'. Such personal data may give away operational and tactical intelligence such as vehicles and munitions, coordinates, time and date, movements, number of associates, ranks and specialisations.

Such data has recently been observed being publicised by journalists and military analysts relating to alleged Russian involvement in the Crimea. Indeed, the Russian soldier; Alexander Sotkin, nicknamed 'Sergeant Selfie', was ridiculed and criticised for seemingly leaking his geolocation and interior of his armoured signals vehicle publicly on Instagram (Gallagher, 2014). Although there is some debate as to the whether the geolocation (which appears to show activity across the border in Ukraine) is accurate, but nonetheless the incident caused a degree of international controversy, additionally with the individual in question being allegedly stripped of his rank as sergeant. Further social media embarrassments have been reported against U.S military families who received fake orders to leave South Korea. US Army counterintelligence are investigating the incidents of late September 2017 in which fake social media and mobile alerts were sent out; "warning American military families and Defense Department personnel of orders to evacuate the volatile peninsula" (Lamothe, 2017).

In the UK, armed forces are able to operate closed social media groups, such as restricted, private Facebook groups to inform family members about a group's well-being when oversees on campaigns with little internet connectivity, or, with a high level of secrecy involved (Royal Navy, 2017). It is likely such SM groups are the target of belligerent states for espionage and sabotage such as in the case of Alexander Sotkin's data leakage and the South Korean military family's hoax. Such incidents are taken very seriously from a military point of view as they may hint towards serious counterintelligence vulnerabilities, allowing for manipulation, espionage and disinformation campaigns to work effectively against operations, personnel and even target family members.

6.2 Usage of the Dark Web

As of early 2017, open source investigation sectors of the military did not officially classify the Dark Web as an 'open source' resource (Pattar, 2017), this decision is currently paralleled elsewhere the HMRC who also usually operate at open source levels 1-2 and do not access dark web URLs. Whilst this is in part due to security and infrastructure constraints, it has been recognised to be somewhat problematic and will

likely change in the foreseeable future. In particular OSINT investigators within the military may recognise the wealth of potential to investigate Dark Markets for associations towards funding terrorist groups and other foreign threats (Weiman, 2016).

It may be argued that the priorities of open source access to the dark web are different between the UK military and law enforcement agencies. In addition to terrorist, enemy state and other foreign concerns, UK police operations focus on leading priorities such as; child sexual exploitation (CSE), drug trafficking, online fraud and scamming communities, money laundering and various other organised criminal network forums and dark marketplaces (Buxton and Bingham, 2015; Home Office, 2017). Particularly, the strong focus on fighting CSE has encouraged an essential need for police officers and analysts to operate on the dark web as clarified by the HMIC (Her Majesty's Inspectorate of Constabulary) in 2017: "*The dark net provides abusers with a means of distributing indecent images of children around the globe to those who share their interest. It has provided an opportunity for such offending to be undertaken more widely. It has made the job of the police service and other agencies responsible for safeguarding children more difficult.*" The perceived anonymity, capacity to mask IP addresses and geolocation, as well as the difficulty of searching and penetrating dark net 'friend circles' has made it essential for law enforcement to pursue suspects and offenders on Tor and similar dark web browsers.

Further surrounding the topic of OSINT and CSE; a particular area of growing controversy and debate in the UK is for law enforcement dealing with such E41/Hearsay intelligence from the rise in popularity of 'paedophile hunter' vigilante groups such as; Guardians of the North (2017), The Hunted One (2017) and Dark Justice (2017). Such groups often impersonate underage children upon social media sites, but also utilise mobile messaging and dating applications such as Kik, Badoo, Snapchat, and WhatsApp.. The majority of paedophile hunter 'stings' utilise the described OSINT investigation levels 4 and 5. Indeed, the actions of paedophile hunter groups amount to OSINT SM account takeovers as well as online CHIS, these are carried out without a DSA or legal authorisation and provided to law enforcement. Whilst the police may make use of such intelligence and use paralleling techniques to capture their own evidence, this approach has come under significant criticism, both

internally within the force as well as externally for encouraging 'vigilantism' and dangerous practices with little or no concern for suspects to be mistaken, entrapped and publicised from amateur and possibly fallible investigative techniques (Perraudin, 2017).

Such concerns are not observably present in the media concerning military intelligence measures, nor are they likely to be treated with as much concern as law enforcement does. This is primarily due to the military's 'foreign facing' scope, (with the exception of national security threats such as terrorism), it is likely that such E41 intelligence obtained from a similar process about military interests would be treated as valuable, or at least worth researching or investigating further. Indeed, there exist many amateur OSINT online publications of interest to the MoD, some examples being bloggers that record and report on the movements of battleships near their coastal homes, journalists who carry out OSINT research into topics such as the aforementioned Russian military movements, but also into the analysis of publications and propaganda material of terrorist groups (e.g., Bellingcat, 2017).

The comparative reduction of the UK judicial systems involvement in the military collecting of intelligence for operational and tactical usage allows them a greater degree of freedom than having to pursue a chain of evidence for suspect conviction. Furthermore, this may in turn reduce the manual workload required by investigating and authorising officers and analysts.

6.3 Utilisation of External Advisors and Support

UK law enforcement often draws upon OSINT services through advice and direction from the Home Office's Centre of Applied Science and Technology (CAST). Products such as Cosain, Repknight and Echosec are listed through Home Office vetting and recommendations on an online 'portal' (CAST, 2017). Of these products, the majority are commercially engineered by the private sector as external developers, some of which are available for additional public and private workplaces. It has also been shown that law enforcement may get locked into certain products (e.g., Palantir) and there are concerns about background

information sharing that are barely acceptable at a law enforcement level but could be disastrous for a military operation, thus the tools utilised by the military must be carefully scrutinised before deployment (Harris, 2017).

While the military do make use of off-the-shelf tools they also utilise work with organisations to develop OSINT tools customised bespokely for military usage and are usually locked into being only available for them. The military ensures the signing of strict NDAs as well as secrecy agreements, the individuals developing products go through alpha and beta stages on site at military bases. Individuals working on them externally are usually required to have DV vetting (Ministry of Defence, 2017).

7. BENEFITS OF SHARING BEST PRACTICES BETWEEN DEFENCE AND LAW ENFORCEMENT

With regards to OSINT, law enforcement and the military often operate in the same space, utilising many of the same tools and techniques and thus may benefit from the experience of sharing best practices

7.1 Increased interoperability

With the future merger of the Home Office and MoD (DSTL) (Home Office, 2017b) it is likely in the future that the two organisations will increase their areas of overlap and collaboration on joint operations and intelligence sharing exercises. Therefore it would be beneficial to increase the resilience and capacity of both parties if feasible. Increasing interoperability of OSINT investigations and research towards a compatible system would allow for greater collaboration on overlapping areas. For example, considering concerns such as domestic terrorist threats, increased interoperability could in the case of OSINT, lead to increased police capability to parallel military intelligence, but more importantly, enhanced military procedures to investigate and research threats in a manner compatible with policing 'chain of evidence concerns'.

7.2 Enhanced rigour and chain of custody

It may be beneficial for military operations to begin a best practice of treating intelligence sources in a similar manner as the police do for evidence gathered on OSINT investigations. This includes protection of data (hashing), integrity of data in case it is needed as evidence or even to be posted publicly in case of criticism. Increasingly we are seeing media channels belonging to opposing nations utilising news reports in a negative propaganda fashion. Examples such as 'Russia Today' attempts to demoralise and criticise the UK and US through social, political and military reports (O'Sullivan, 2014; Johnson, 2016). Therefore, as all aspects of military and law enforcement are fair game for open criticism, it may be beneficial for military OSINT investigations and research

to embrace the evidence capture and auditing standards of the police force, perhaps embracing the JAPAN principles, this would provide fair justification of a reasonable and proportionate use of OSINT that would minimise the damage of triggering privacy and other human rights criticisms. Furthermore, by considering policing standards, there may be subsequent improvements in reviewing and managing open source analysts and researchers, particularly as good or bad intelligence leads could be traced back along the chain of evidence audit.

7.3 Improving security, personal and organisational counterintelligence standards

The contemporary digital age results in increasingly complex and strenuous taskings for counterintelligence military and security services. Whilst this is naturally a greater concern of the MoD, it may represent a best practice that the law enforcement may consider a horizon challenge to embrace today (Lord, 2015). Indeed, the high standards of confidentiality and security regarding counter intelligence and data leakage from the military perspective certainly aren't neglected or ignored by police guidance and best practices. However, there are notable differences with the inclusion of the media, particularly for documentaries and entertainment television, which seek to detail and even challenge state surveillance technologies (Channel 4, 2016). Such documentaries can be argued to enhance the police-public relationship through awareness and education in the interest of fostering greater communication and collaboration. This is perhaps a convenience the military does not need considering OSINT, as the UK public are rarely the subject of its investigations and operations. Therefore, this may allow a greater degree of secrecy for military analysts 'training, techniques and tactics' for locating and exploiting OSINT. It may be of value for the preservation of both military and policing open source practices to discuss, limit or reduce the number of law enforcement documentaries if they are deemed to be compromising valuable; tools, exploits and tactics.

As mentioned earlier in the MoD OSINT definition, there is a great emphasis on utilising trained analysts to optimise the usefulness and benefits of OSINT; "to ensure the intelligence produced is unbiased and

free of prejudice" (Ministry of Defence, 2011). Furthermore, the military place a great emphasis on developing OSINT tools and technologies in-house, this ensures that they have an immediate input to the development of open source products through Alpha and Beta development stages, as well as close contact to product contractors for quick and efficient training and software updates and patches.

7.4 Development of OSINT standardisation

Currently, different UK police forces apply different rules and best practices for the collection of data prior to achieving a DSA under RIPA (West Yorkshire Police Analyst 2017, personal communication 12 May). Some allow for a 'once over' single check of a profile, whereas others allow for up to, but no more than 3 looks at a unique profile (Sorinteq, 2017). Additionally, depending on the senior investigating officer (SIO) different approaches may be taken to acquire, or to work around a DSA (such as utilising a NOD, non-operational directive or getting a retrospective DSA). Whilst both the military and the College of Policing provide their own internal OSINT training packages, there are also a vast number of third party providers of OSINT training who are able to train both military and law enforcement in advanced open source analysis.

Much of the individual police officer and military analyst actions on an investigation or OSINT research job are dependent on the SIO (or Commanding Officer) leading the case, as well as upon the conditions specified in the Directed Surveillance Authority. As a result of this, OSINT investigative techniques, tools used, and working methodologies may be shared between different groups. It may be beneficial in the future to establish a wider set of standards and best practices that not only different military or individual police forces could use, but may also be used between military and law enforcement interchangeably.

CONCLUSION

In conclusion, UK police and military open source investigations from within the UK have a great deal of similarities; this is particularly due to them both being under the governance of RIPA (2000). However, there are several observable differences between the two organisations.

The first observable difference is in the handling of a chain of evidence between the two bodies. UK police forces often have to prioritise and integrate a chain of custody for any intelligence that may lead to prosecution or to be shown in a court of law. Therefore, the police tend to have a more structured and detailed approach to evidence gathering, for example following the JAPAN approach, that ensures intelligence is either processed or paralleled into a secure, auditable and useful format. As noted, the military may benefit somewhat from a similar system that could protect data integrity from public criticisms, as well as leading to greater management of researcher and analyst efficacy. Additionally, the military hold a greater capacity to act on E41 intelligence provided to them from external and untested sources, they face a lesser degree of public insight and subsequently potential criticism.

Secondly, there are noticeable differences between the use of third party software and developers. The UK MoD prioritise the use of bespoke software tools and in-house training solutions, often requiring DV security vetting for contractors to work on site and in association with them. Alternatively, law enforcement have traditionally used a variety of commercial and private sector solutions, some of which are specifically designed for police OSINT, however these are not developed with the same degree of bespoke and internal design.

Thirdly, there are differences with organisational approaches towards the dark web. As stated, currently the MoD have a far more cautious approach to operating on the dark web. As detailed, UK law enforcement have faced both pressure and necessity to operate in this domain, particularly due to police specific concerns such as online child sexual exploitation. It is likely however in the near future that the military will include the dark web as part of their open source domain. Therefore, it may be beneficial for the MoD to discuss merging best practices and standards that have been nurtured by contemporary policing approaches.

Additionally, there are slight observable differences between the military and policing structures in regards to counterintelligence. The MoD provide slightly stricter guidelines, particularly revolving around operational security, as such they also offer closed SM groups to provide direct information to families of serving members when they are restricted or not able to use SM personally. Furthermore, the military faces greater challenges of preserving intelligence from belligerent states as well as protecting its personnel and families from a higher severity of threat. As stated earlier, such concerns include disinformation campaigns which have been used internationally to disrupt and displace personnel and families.

Overall there are clearly more overlaps and similarities than differences. The observable differences are defined by either the relationship to judiciary and prosecution services, or through the severity of the risk and security level they operate at.

This document serves as a brief overview of observable differences between UK military and policing OSINT practices. A more in depth and detailed review would be ideal for formulating how, or why, these differences have occurred. In particular, envisioned next steps for future research may include; firstly identifying the extent of operational and tactical differences between the two organisations, and secondly; building a roadmap for mapping potential compatible best practices that may lead to greater interoperability (particularly when considering counter terrorism), organisational efficiency (primarily for military auditing and evidence capture), increased capability (such as military dark web best practices), and greater SM counterintelligence awareness (primarily for policing security).

Contacts:

Douglas Wells
CENTRIC
Sheffield Hallam University, UK
E-mail: d.wells@shu.ac.uk

Helen Gibson
CENTRIC
Sheffield Hallam University, UK
E-mail: h.gibson@shu.ac.uk

REFERENCES AND SOURCES

Bartlett, J., Miller, C., Crump, J., and Middleton, L., (2013). Policing in an Information Age. CASM Policy Paper. DEMOS. https://www.demos.co.uk/files/DEMOS_Policing_in_an_Information_Age_v1.pdf?1364295365

Bazzell, M. (2016) Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. 5th Edition. CreateSpace Independent Publishing Platform

Bellingcat (2017) https://www.bellingcat.com/

British Army (2009) British Army Field Manual. Volume 1 Part 10: Countering Insurgency. London: Ministry of Defence.

British Army (2017) 77th Brigade. http://www.army.mod.uk/structure/42952.aspx

Buxton, J., Bingham, T., (2015). The Rise and Challenge of Dark Net Drug Markets. *Global Drug Policy Observatory*. Swansea University. https://www.swansea.ac.uk/media/The%20Rise%20and%20Challenge%20of%20Dark%20Net%20Drug%20Markets.pdf

CAST (2017). Centre for Applied Science and Technology. Home Office Security, Science and Innovation. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/619286/introduction-to-cast-jun2017.pdf

Channel 4 (2016). Hunted: How the fugitives were hunted. http://www.channel4.com/info/press/press-packs/hunted-how-the-fugitives-were-hunted

CIA (2010) INTelligence: Open Source Intelligence. *Central Intelligence Agency* https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html [Accessed 1 October 2017]

Cleveland Police (2014). Social Media and Electronic Communication Guidance. (pp.6-7.) https://www.whatdotheyknow.com/request/409672/response/1002847/attach/2/Guidance%20document.PDF.pdf [Accessed 1 October 2017]

College of Policing (n.d.) Authorised Professional Practice. How to complete a 5x5x5 form http://library.college.police.uk/docs/APPref/how-to-complete-5x5x5-form.pdf

College of Policing. (2013). Intelligence Management: Intelligence Collection, Development and Dissemination. https://www.app.college.police.uk/app-content/intelligence-management/intelligence-cycle/?s=intelligence#top

COSAIN 9 (2017) Capita Business Services Limited

Dark Justice (2017) https://darkjustice.co.uk

Derbyshire Police (2012) Guidance on the safe use of the internet and social media by police officers and police staff.

http://www.derbyshire.police.uk/Documents/About-Us/Freedom-of-Information/Policies/SafeUseoftheInternetandSocialMediabyPoliceOfficersandPoliceStaffGuidance.pdf

Digital Trends (2016). The History of Social Networking. Digital Trends. https://www.digitaltrends.com/features/the-history-of-social-networking/

Donohue, L. (2015). The Dawn of Social Intelligence (SOCINT).Georgetown University Law Center. Vol. 63. http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2540&context=facpub

Echosec (2017) Echosec Systems. https://www.echosec.net/ [Accessed 1 October 2017]

Edwards, L., Urquhart, L. (2016) Privacy in public spaces: what expectations of privacy do we have in social media intelligence?. *International Journal of Law and Information Technology*, *24*(3), pp.279-310.

Haigler, K., 2012. Guide to Intelligence Support for Military Operations. *The Intelligencer Association of former Intelligence Officers*. 19(1). (pp. 51-55).

Gallagher, S., (2014). The Sad, Strange Saga of Russia's 'Sergeant Selfie'. Ars Technica. https://arstechnica.com/information-technology/2014/08/the-sad-strange-saga-of-russias-sergeant-selfie/

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* (pp. 9-23). Palgrave Macmillan UK.

Guardians of the North (2017) http://main.guardiansofthenorth.com/

Harris, M. (2017) How Peter Thiel's Secretive Data Company Pushed Into Policing. Wired. 8 September 2017. https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/

HMIC., (2015). Online and on the edge: Real risks in a virtual world: An inspection into how forces deal with the online sexual exploitation of children. HMIC. http://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/online-and-on-the-edge.pdf

Homeland Security Research. (2017). OSINT Market & Technologies - 2017-2022. http://homelandsecurityresearch.com/OSINT-market-technologies [Accessed 1 October 2017]

Home Office (2014) Covert Human Intelligence Sources; Codes of Practice. Pursuant to section 71(4) of the Regulation of Investigatory Powers Act 2000. TSO. p.33 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384976/Covert_Human_Intelligence_web.pdf [Accessed 1 October 2017]

UK Home Office. (2017). Home Secretary gives £20 million boost to tackle online grooming. Press Release. Gov.uk. https://www.gov.uk/government/news/home-secretary-gives-20-million-boost-to-tackle-online-grooming

UK Home Office. (2017). Integrating the Science and Technology Support for the UK's Defence and Security. Home Office, Ministry of Defence, and Defence Science and Technology Laboratory. https://www.gov.uk/government/news/integrating-the-science-and-technology-support-for-the-uks-defence-and-security

Hunted One, The (2017) https://www.youtube.com/channel/UCA86yT9Xh_w1pVa4BadXPZQ

Hulnick, A.S., 2010. The Dilemma of Open Sources Intelligence: Is OSINT Really Intelligence?. In The Oxford handbook of national security intelligence.

ISC - Intelligence and Security Committee of Parliament., (2015). Privacy and Security: A modern and transparent legal framework. http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf [Accessed 10th October 2017]

Johnson, A. H., (2016). Who's afraid of 'Russia Today'? The Nation. https://www.thenation.com/article/whos-afraid-of-russia-today/

Kent Police (1998) The JAPAN Test. https://www.kelsi.org.uk/__data/assets/pdf_file/0003/26706/Japan-Test.pdf [Accessed 1 October 2017]

Krebs, V., 2002. Uncloaking terrorist networks. First Monday, 7(4).

Kwoka, M, B., (2015). Leaking and Legitimacy. UC Davis Law Review. Vol. 48. https://lawreview.law.ucdavis.edu/issues/48/4/Articles/48-4_Kwoka.pdf [Accessed 19th October]

Lamothe, D., (2017). U.S families got fake orders to leave South Korea. Now counterintelligence is involved. Washington Post. https://www.washingtonpost.com/news/checkpoint/wp/2017/09/22/u-s-families-got-fake-orders-to-leave-south-korea-now-counterintelligence-is-involved/?utm_term=.4aee6602754e

Lesca, H., Lesca, N. (2011).Weak Signals for Strategic Intelligence: Anticipation Tool for Managers. Wiley. London, UK, ISTE. (p.32)

Lord, J. (2015) Undercover Under Threat: Cover Identity, Clandestine Activity, and Covert Action in the Digital Age, International Journal of Intelligence and CounterIntelligence, 28(4) pp. 666-69.

http://www.tandfonline.com/doi/full/10.1080/08850607.2015.1022464?src=recsys

MacAskill, E. (2015) British army creates team of Facebook warriors. 31 January 2015. https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade

Mak, K., Göllner, J., Prah, P., Meurers, C., Klerx, J. (2017) Cyber Documentation and Research Center "Horizon Scanning Center" for

Cyber Analysis and Monitoring. *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, pages 1-24.

McCue, C. (2015) Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis. Butterworth-Heinemann. (p.31)

Mercado, S.C. (2001) "FBIS Against the Axis, 1941-1945," Studies in Intelligence, Unclassified Edition 11 (pp. 33-43) https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/fall_winter_2001/article04.html [Accessed 1 October 2017]

Mercado. S. C. (2007). Sailing the Sea of OSINT in the Information Age. C*enter for the Study of Intelligence*. 48(3). https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html [Accessed 1 October 2017]

Ministry of Defence (2009) Online Engagement Guidelines. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27933/20090805UMODOnlineEngagementGuidelinesVersion10.pdf

Ministry of Defence (2011) Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations. *Ministry of Defence Development, Concepts and Doctrine Centre*. p. 12. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf [Accessed 1 October 2017]

Ministry of Defence Police (2013) Ministry of Defence Police; Guidelines on the Safe Use of the internet and Social Media by MDP Officers. January 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/329509/Guidelines-socialmedia-v1-jan13.pdf

Ministry of Defence. (2017). United Kingdom Security Vetting. https://www.gov.uk/guidance/security-vetting-and-clearance

National Police Chief Council (2015) NPCC Guidance on Open Source Investigation / Research. Kent and Essex Police https://www.suffolk.police.uk/sites/suffolk/files/003525-16_npcc_guidance_redacted.pdf [Accessed 1 October 2017]

NATO (2001) NATO Open Source Intelligence Handbook. http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf [Accessed 1 October 2017]

O'Sullivan, J., (2014). Russia Today is Putin's weapon of mass deception. Will it work in Britain? The Spectator. https://www.spectator.co.uk/2014/12/the-truth-about-russia-today-is-that-it-is-putins-mouthpiece/

O'Sullivan, K.T. (2017) The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU, by Hielke Hijmans. *International Journal of Law and Information Technology.*

Pattar, T., (2017). The Future of Open Source Intelligence (OSINT). DSEI Speaker Presentation. London. https://www.dsei.co.uk/dsei-strategic-conferences--seminar-programme/the-future-of-open-source-intelligence-osint#/

Perraudin, F., (2017). Paedophile hunters jeopardising police work, says senior officer. The Guardian https://www.theguardian.com/society/2017/apr/24/paedophile-hunters-jeopardising-police-work-child-protection

RepKnight (2017) RepKnight https://www.repknight.com/ [Accessed 1 October 2017]

Royal Navy (2017) Social Media. https://www.royalnavy.mod.uk/welfare/keeping-in-touch/social-media

Steele, R.D. (1995) The importance of open source intelligence to the military. *International Journal of Intelligence and Counter Intelligence*, 8(4), pp.457-470.

Sorinreq. (2017). Sorinteq Advanced Open Source Intelligence Training Course. Birmingham. January 2017. https://www.sorinteq.com/

UK Government. (1998). Human Rights Act 1998. https://www.legislation.gov.uk/ukpga/1998/42/contents [Accessed 1 October 2017]

UK Government (2000) Regulation of Investigatory Powers Act. https://www.legislation.gov.uk/ukpga/2000/23/contents [Accessed 2 October 2017]

Weiman, G., (2016). Terrorist Migration to the Dark Web. *Perspectives on Terrorism*. 10(3). http://www.terrorismanalysts.com/pt/index.php/pot/article/view/513