Leiden University – Faculty of Governance and Global Affairs

Institute of Security and Global Affairs

Master programme: Crisis and Security Management

Master thesis

It's very nice… but do we really need it?

Outlining the use of open-source information by the The Hague Regional Intelligence Service within set security principles applied to the case of online right-wing extremism in the Hague.

Maaike Grootjans – s1697722

February 20th, 2021

Wordcount (excl. bibliography): 17.908

Supervisor: Dr. E. De Busser

Second reader: Dr. F. Cristiano

ACKNOWLEDGEMENTS

When starting my master's degree in Crisis and Security Management, my interest in the field of security was broad to the extent that the topic of my thesis shifted considerably. One topic that I always found myself going back to was intelligence. The mysterious character and growing importance of it attracted me to the topic and I was keen on exploring it beyond the framework of my curriculum. This exploration started with my function as student ambassador for the Regional Intelligence Service in The Hague. Not only did this give me insight in the field of intelligence, it also gave me the opportunity to dedicate my thesis to a topic within intelligence for which I am thankful.

I, therefore, would like to proudly present my thesis about open-source intelligence and its use within the Regional Intelligence Service of The Hague specified to the case of right-wing extremism and digital meeting places.

I would like to thank my thesis supervisor dr. Els de Busser for her guidance during this thesis process. Our conversations not only provided me with useful feedback and insights but also motivated me to continue my research. Secondly, I would like to offer my gratitude to my supervisor from the police, Tim, who handed me this topical subject and gave me his trust and freedom to research it the way I saw fit. Also, I would like to thank him for providing useful contacts, fun conversations and the opportunity to present my outcomes on a national level. The idea that my research will be practically useful drove me to engage in my most extensive research yet. Furthermore, I would like to thank everybody from the police who have helped me in my study.

All though distractions were limited, writing a thesis amidst a lockdown is not easy. On a personal level, I would like to thank my boyfriend for listening to my endless ideas and frustrations and advising and motivating me. Moreover, I would like to thank my housemates who had to put up with a closed door the majority of the time. Finally, I would like to thank my family for their continuous support in everything I do.

I hope you read this thesis with pleasure.

Maaike Grootjans,
Den Haag, February 2021

ABSTRACT

Increasingly, law enforcement focuses on the prevention of crime. In this approach, the role of information is important. Especially combined with the technological advancements of Internet and social media make that using publicly accessible information that is inevitable. Whether this implies that such "open-source information" is freely accessible to law enforcement officers tasked with intelligence-led policing and creating intelligence remains to be the question. By means of a literary analysis, document analysis, interviews with practitioners and a single case study this research aimed to find out how intelligence officers can make use of this vast and valuable amount of information whilst adhering to security principles of surveillance and entrapment. This study found that there is no judicial framework built around creating intelligence as is the case with ongoing criminal investigations and surveillance is only partially possible. Article 3 of the Police Directive functions as the basis of officer's functioning and any privacy breach that is more than necessary needs to be carefully considered under principles of proportionality and necessity. The assessment of these is thus vital, especially when applied to issues of national security – e.g. right-wing extremism – where these two principles have the opportunity of clashing. The study also found that a clear distinction between tasks of the public prosecutor and the municipality is of importance in order for intelligence officers to engage in effective intelligence-led policing. Finally, the attitude towards information as merely "nice-to-have" within intelligence-led policing needs to shift towards "need-to-have" to properly assess necessity and proportionality.

LIST OF ABBREVIATIONS

AIVD	General Intelligence and Security Service	*Algemene Inlichtingen- en Veiligheidsdienst*
BOB	Special Investigative Powers	*Bijzondere opsporingsbevoegdheden*
CFR	The Charter of Fundamental Rights to the European Union	
CIA	Criminal intelligence analysis	
DRIO	Regional Intelligence Service	*Dienst Regionale Informatie Organisatie*
ECHR	European Convention on Human Rights	
FBIS	Foreign Broadcasting Information Service	
FCA	Formal concept analysis	
GDPR	General Data Protection Regulation	
GEOSINT	Geospatial intelligence	
HUMINT	Human intelligence	
IGP	Informatiegestuurd politiewerk	
ILP	Intelligence-led policing	
IMINT	Imagery intelligence	
MASINT	Measure and Signature intelligence	
NIM	National Intelligence Model	
OM	Public prosecutor	*Openbaar Ministerie*
OO&V	Public Order and Safety	*Openbare Orde en Veiligheid*
OSINF	Open-source information	
OSINT	Open-source intelligence	
PolW	Police Directive	*Politiewet*
SIGMINT	Signals intelligence	
SMM	Social media monitoring	
SNA	Social network analysis	
Sr	Criminal law	*Wetboek van Strafrecht*
Sv	Criminal procedures	*Wetboek van Strafvordering*
UK	United Kingdom	
US	United States	
Wpg	Police Data Directive	*Wet Politiegegevens*

LIST OF FIGURES

FIGURE 1: STEPS IN INTELLIGENCE AND POLICE INVESTIGATION TO BE ALTERED BY SOCIAL MEDIA (AS TRANSLATED FROM SMILDA & DE VRIES, 2017, P. 196)..... 15

FIGURE 2: THE FOUR CATEGORIES OF OPEN SOURCE INFORMATION AND INTELLIGENCE AS DESCRIBED BY GIBSON (2017, P. 70)..... 19

FIGURE 3: GEOGRAPHICAL DEPICTION OF POLICE UNIT THE HAGUE 23

TABLE 1: RESPONDENTS 24

FIGURE 4: STEPS IN ASSESSING NECESSITY. SOURCE: EUROPEAN DATA PROTECTION SUPERVISOR (2017, P. 9) 41

FIGURE 5: STEPS IN ASSESSING PROPORTIONALITY. SOURCE: EUROPEAN DATA PROTECTION SUPERVISOR (2019, P. 14) 42

FIGURE 6: NECESSITY AND PROPORTIONALITY TOOLKIT 43

TABLE OF CONTENTS

INTRODUCTION **8**

I. RESEARCH PROBLEM 8
II. RESEARCH OBJECTIVE 9
III. RESEARCH QUESTIONS 10
IV. RELEVANCE 10
V. READING GUIDE 11

THEORETICAL FRAMEWORK **12**

I. INTELLIGENCE 12
II. OSINT 12
III. SOCMINT 13
IV. POLICING IN A PRE-CRIME SOCIETY 16
V. CRIME INTELLIGENCE ANALYSIS AND THE INTELLIGENCE PROCESS 18
VI. POLICING IN THE NETHERLANDS 20

METHODOLOGY **22**

I. RESEARCH DESIGN 22
II. DATA COLLECTION 23
III. CONCEPTUALISATION AND OPERATIONALISATION 24
IV. ADDITIONAL CLARIFICATIONS 28
V. LIMITATIONS 28

JUDICIAL FRAMEWORK **30**

I. THE POLICE DIRECTIVE 30
II. THE EUROPEAN CONVENTION ON HUMAN RIGHTS 31
III. THE CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION 31
IV. THE GENERAL DATA PROTECTION REGULATION 31
V. THE POLICE DATA DIRECTIVE 32
VI. SPECIAL INVESTIGATIVE POWERS 33
VII. CONCLUSION 36

THE CASE: RIGHT-WING EXTREMISM **37**

I. RIGHT-WING EXTREMISM 37
II. GATHERING INFORMATION IN PRACTICE 40
III. SOCIAL MEDIA ANALYSIS 44

CONCLUSION **46**

I. CONCLUSION 46

II. DISCUSSION 47

BIBLIOGRAPHY 51

INTRODUCTION

From the early developments of nation states, the police have occupied a professional function in civilian security through crime control (Garland, 1996, p. 448; Perlinger, Hasisi & Pedahzur, 2009, p. 1280). The dynamics of this responsibility, however, have changed significantly over the years. Post-9/11, terrorist attacks worldwide showed the necessity for information, both domestically as well as internationally (Lefebvre, 2003, p. 527). As the field of security changed, actors providing security were also challenged to change their modus operandi. Policing has expanded from community and problem oriented methods towards a more intelligence-led approach (Carter & Carter, 2009, p. 310). Translated, this implies a shift from "reactive" policing to a more "proactive" style of crime prevention (Burcher & Whelan, 2019, p. 139). Such methods seek to place information at the forefront of decisions concerning crime control (Burcher & Whelan, 2019, p. 140).

In this new approach to crime control, an important role is laid down for information. With the evolution of the Internet, large amounts of information have become accessible to the public and thus to police authorities. In addition, the development of social media platforms increased the amount of personal information that roams around the Internet (Eijkman & Weggemans, 2013, p. 285). More increasingly, private lives and thoughts move out of their shadows through the use of mobile phones and social platforms. While this puts our privacy at risk, the use of social media and other publicly accessible platforms in suspects' everyday life creates new opportunities for the police and its several processes to reduce crime (Rønn & Søe, 2019, p. 367). Driven by these technological advancements is the use of open source information which facilitates "the gathering of information through publicly available sources that are unclassified" with open-source intelligence (OSINT) as its deliverable (Eijkman & Weggemans, 2013, p. 285). Over the course of the years, OSINT developed itself as a method in which the information gatherer has the ability "to locate relevant and freely accessible information and mould it into a sense-making whole in a completely transparent fashion that treats information as a resource rather than a commodity" (Glassman & Kang, 2012, p. 675). As a result, the police is able to execute a more proactive style of policing which has proven to be necessary.

I. Research problem

Not only have the Internet and social media platforms become a source of information, they also contributed to the creation of moving offline conversations to an online environment. Social media platforms, for example, are important as an infrastructure to communicate, activate, engage and mobilise (Akram & Albalawi, 2016). As the current generation profiles itself as "masters of the Internet" opportunities and illnesses of the online world go hand in hand (Bishop, 2014, p. 1). People can somewhat anonymously meet each other, activate each other, mobilise groups or even recruit each other for criminal or terrorist offenses (Bishop, 2014; Weimann, 2016).

Traditional – oftentimes classified – information does then not fall within the scope of the current crime environment as certain police processes are not sufficiently tasked to make use of online information (Europol, 2020; Pool & Custers, 2017, p. 124). As mentioned, OSINT creates new opportunities for police processes but does this enlargement of publicly accessible information automatically imply its free usage by the Dutch police? Even though it concerns openly accessible sources or open profiles on Facebook, rules still apply. Those rules are, however, ambiguous and limited (Koops, 2012, p. 31). Moreover, the specific context in which the police operates is important: Does it imply surveillance or simple "browsing" or does it entail an investigation – either systematically or not. Simply formulated: what are the legitimate grounds for the use of open sources in intelligence-led policing? Within the investigation branch of police processes, a large amount of jurisdiction and legislation lays down the framework in which the police can make use of investigative powers to gather information both online and offline. Street surveillance by the police is, for example, largely accepted (Pool & Custers, 2017, p. 124). Internet data of individuals, however, is protected by a variety of jurisdictions and legislations such as the European Data Protection Directive and several Dutch legislations concerning (special) investigative powers (Custers, van der Hof & Schermer, 2014, p. 268).

Within the process of intelligence and information gathering at the forefront of an investigation, jurisdiction and legislation is rather limited. This causes difficulties for analysts in their intelligence-led approach to crime control. A second issue stems from these difficulties and concerns the grey area between the notions of surveillance and entrapment by the police. Social media has become a primary infrastructure for mobilisation, activism and radicalisation (Calatayud & Vázquez, 2018, p. 22; Pelzer, 2018). More tools and social media monitoring (SMM) devices are being developed for policing institutions with the aim to execute their task as surveillant (Trottier, 2017). As social space opens up, police authorities are oftentimes met with either an illegitimate use of the principle of surveillance or the notion of entrapment in which "issues that do not find their expression in commonly accepted protocols and means of evidence are given a voice as a result of defiant, emotional and provisional use of technology" (Grommé, 2016, p. 1008). Not only does this result in resistance towards SMM, it also tarnishes the line between surveillance and entrapment. Both the judicial and security related issue decrease effective intelligence-led policing.

II. Research objective

The central goal of this research is to decrease the existing ambiguity surrounding the use of open-source information (OSINF) for practitioners. Principles of surveillance and entrapment are not unknown to police authorities but can easily fade when unclarity exists about them (Trottier, 2017). This thesis aims at exploring the embeddedness of open-source information within the Regional Intelligence Service (Dutch: Dienst Regionale Informatie Organisatie, henceforth: DRIO) of Police Unit The Hague within security principles of surveillance and entrapment. As mentioned, the majority of this ambiguity stems from the lack of a clear legitimate basis. It is therefore imperative to touch upon the role of OSINF

within the current legislation about surveillance. This thesis will, however, not limit itself to the judicial question about this topic but will built from it by finding a balance between the use of OSINF and surveillance in the field of security provision by the police. This will, ultimately, result in an understanding of the boundary between these two principles and how practitioners can embed open-source intelligence within these principles to enhance crime control.

III. Research questions

To address the above-mentioned problem, the following research question will be answered:

To what extent does the Regional Intelligence Department of the Police Unit The Hague have the ability to employ open-source information and intelligence as a means in their intelligence-led policing towards digital meeting places of right-wing extremism whilst adhering to the boundaries of surveillance and entrapment?

To properly answer this question, the following sub-questions will be asked:

i. What is the role of social media in OSINT?
ii. How is the use of OSINF in intelligence-led policing embedded in relevant jurisdiction and legislation?
iii. How is OSINF currently employed by the DRIO of Police Unit The Hague?
iv. What do the principles of surveillance and entrapment imply within policing?
v. What are the boundaries of surveillance and entrapment in policing tasks within the DRIO?
vi. Case study: How can OSINF be applied within the case of digital meeting places within right-wing extremism?

IV. Relevance

A variety of practitioners from the DRIO have expressed the necessity for a research of this nature. While professionals recognise the increasing value for OSINT in their work, a struggle prevails concerning the practical knowledge about this phenomenon. As the notions of surveillance and entrapment can easily blend or be used disproportionately, practitioners benefit from a research which explains these two principles and the justification of these. The application of this research to the case of digital meeting places within right-wing extremism adds to this relevance as it deepens the understanding.

From an academic perspective, this research can serve as a starting point from which future research on this topic can be build. While a vast amount of literature exists on the judicial framework concerning police (online) investigative powers, little research exists about legislation within the information gathering and intelligence process of the police. Moreover, the grey area concerning the notions of surveillance and entrapment is rarely mentioned. Being that the use of the latter is built upon these formerly mentioned legislations, it is important to explore both phenomena separately but also to

explore their connection. Seeking this connection is not only important for professionals in the working field, but will also provide a more in-depth understanding of these topics in both the academic fields of law and security studies. Moreover, the body of knowledge within the field of intelligence is expanded by this research as it focuses on OSINT rather than traditional forms of intelligence and also takes into account the role of social media in intelligence, which is currently a topical discussion within the academic field of intelligence.

V. Reading guide

Building from this introductory chapter, this research will continue with a theoretical framework. This will consist of the necessary background information derived from academic literature. It is aimed at providing the context for the continuance of this research as well as building the current position of this research project in the existing body of knowledge. Chapter 3 will illustrate the methodology used in order the answer the central research question and sub-questions. It will go in depth about the used research methods, data collection and scope while also providing necessary conceptualisations, operationalisations and reliability and validity of data. Chapter 4 will continue with the judicial framework and the principles of surveillance and entrapment. Chapter 5 will finalise the analyse by applying and summarizing the previously built chapters onto the case of right-wing extremism and their use of social media. It will introduce right-wing extremism, shortly engage in social media analyse and explore the possibilities for intelligence officers to engage within the established judicial framework. This thesis will finish with a conclusion, discussion and a list of referenced literature. Finally, an appendix is added which includes the interview reports. This will be an additional document which can only be requested to the writer of this thesis.

THEORETICAL FRAMEWORK

I. Intelligence

Post-9/11, the continuance of catastrophic risks have significantly increased pressure on governments and security actors to think and act pre-emptively (Zedner, 2007, p. 264). According to Brodeur (2007), such issues are paired with "high policing" which implies the collection of data and processing of intelligence which goes beyond the scope of solving a single crime. Here, the notion of "intelligence" rapidly developed amongst governments and security actors (Lefebvre, 2003, p. 527). While intelligence may seem like it only developed in the last two decades, it has always been an important notion in security. The art of winning a battle or a war partly relied upon information sources which were gathered in secrecy by generals (Kahn, 2001, p. 80). This occurred rather sporadically but, as we skip towards the end of the Cold War, intelligence shifted into a well-established organisation within security actors that developed due to globalisation and technology (Kahn, 2001, p. 80; Pedersen & Jansen, 2019, p. 882).

"Intelligence" is different from mere information to the extent that intelligence is the product of interpreting collected information in order to give it its meaning (Reuser, 2013, p. 2; United Nations, 2011, p. 9). The collection of this information is generally done through five methods: Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Geospatial Intelligence (GEOSINT) which also includes imagery intelligence (IMINT), Measurement and Signature Intelligence (MASINT) and OSINT (Colleen, 2007; Lowenthal & Clark, 2016, p. 48; Miller, 2018). Through these disciplines, information will be collected, interpreted and analysed from which actions towards crime control follow. This is organized around the "intelligence process" which ultimately forms the bases of intelligence-led policing (Innes, Fielding & Cope, 2005, p. 43).

II. OSINT

As mentioned above, OSINT is a discipline to gather intelligence (Staniforth, 2016). As Williams and Blum (2018, p. 1) explain, OSINT has the ability to replace and/or complement access to information that was once gained in a more dangerous manner.

Williams and Blum (2018, p. 2) explain that one can differentiate between a first generation OSINT and second generation OSINT in which the development of the Internet on the one hand and the growth of its dynamic and communicative characteristics on the other hand play a large role. The systematic gathering of information through open sources dates back to beginning of the Second World War. In the United States (US) the Foreign Broadcast Information Service (FBIS) emerged with the intention to translate foreign broadcasts for the benefit of government agencies during war times (Roop, 2009, p. 2). Similar services were launched in European countries such as the United Kingdom (UK) where the British Broadcasting Company (BBC) executed similar tasks (Roop, 2009, p. 3). Williams and Blum (2018, p. 4) rank this under first generation OSINT of which the primary function held the

collection of material. Second generation OSINT largely evolved because of Web 2.0 and social media (Williams & Blum, 2018, p. 40). The initial stages of the Internet were predominantly passive, as it allowed for a bulk of information with no participatory features for users. Web 2.0 and social media shifted the Internet to a dynamic atmosphere with user-generated content (Williams & Blum, 2018, p. 39). This makes it possible for analysts to get access to real-time information about ongoing events (Williams & Blum, 2018, p. 40).

Generally, intelligence professionals agree that open source information is useful and should, similar to data derived from classified sources, be collected and analysed (Best & Cumming, 2007, p. 3). Reuser (2013) continues by describing several significant features of OSINT to intelligence professionals:

- *Huge:* There is a lot of data available and more increasingly, the majority of information comes from open sources;
- *Safe:* The collection of information is less dangerous than traditional collection methods like espionage;
- *Reliable:* Information from open source mostly include names, sources, references, dates, etc. which make the information easily checkable for reliability and validity;
- *Easy to share:* There are little security restrictions to open source information which makes it easy to share;
- *Cheap:* The methodology, tools and databases are cheap or free.
- *Everywhere:* OSINT covers the world;
- *Fast, real-time and mobile:* Given that information is produced by the masses at any time, it is quickly available during or after an incident. This also makes it real-time.

These advantageous features should, however, be approached with caution as there are obvious downsides to OSINT. Pedersen and Jansen (2019, p. 891) showed that intelligence analysts assign significantly higher credibility to classified intelligence than to OSINT even when the two reports put forward were identical. With the growing open source information accessibilities, also came the rapid evolution of misinformation and fake news which has evident implications for intelligence analysts who rely on OSINT (Olaru & Stefan, 2018, p. 393). This makes OSINT less trustworthy as Reuser (2013) presents. It is therefore imperative that a thorough analysis needs to be applied in order to generate trustworthy OSINT.

III. SOCMINT

As briefly touched upon, the development of Web 2.0 brought forward a way for the Internet to be used two-sided instead of one-sided. More specifically, Web 2.0 effectively takes advantage of "network effects" which is the idea that some things are more valuable when more people participate (Blank & Reisdorf, 2012, p. 538; Trottier, 2017, p. 457). Alongside, Web 2.0 makes use of platforms which create

simple, and reliable environments for users to express themselves (Blank & Reisdorf, 2012, p. 539). This expression is translated to "user-generated content" which is provided by users, for users. It typically consists of 1) public information that is publicly available on the Internet, 2) information that incorporates a certain amount of creative effort and 3) information that is created outside of professional routines or practices (Antonius & Rich, 2013, p. 43). In turn, social media is considered the application in which Web 2.0 is built and user-generated content is published. Antonius and Rich (2013, p. 44) provide a helpful summary to understand the relationship between Web 2.0, user-generated content and social media:

"… Web 2.0 provides the technological infrastructure for user-generated content, which in turn represents ongoing knowledge creation, sharing and consumption, giving rise to what is termed social media."

Kietzmann, Hermkens, McCarthy and Silvestre (2011b) explore the seven functional blocks of social media:

- *Identity:* The extent to which users reveal their identities in a social media setting;
- *Conversations:* The extent to which users communicate with other users in a social media setting;
- *Sharing:* The extent to which users exchange, distribute and receive content;
- *Presence:* The extent to which users can know if other users are accessible;
- *Relationships:* The extent to which users can be related to other users;
- *Reputation:* The extent to which users can identify the standing of others, including themselves, in a social media setting;
- *Groups:* The extent to which users can form communities and sub-communities.

As social media are increasingly becoming essential elements in our daily lives, one can assume that the information provided through these seven building blocks can be of high value to organisations like the police (Rønn & Søe, 2019, p. 367). Especially with the advantage of being accessible for an extended period of time (Moe & Schweidel, 2014, p. 3).

Both within academics and practitioners, discussion exists about the inclusion or exclusion of social media intelligence (SOCMINT) in OSINT. As presented earlier, OSINT is gathered and analysed using publicly available information such as witnessing demonstrations, information websites, literature, media outlets, and so on. SOCMINT can therefore be considered as a subset of OSINT. Contrarily, social media includes information to the field of intelligence that has been generated by the user in conversation-like formats which is different from typical OSINT formats and can therefore be recognised as a different intelligence method (Antonius & Rich, 2013, p. 45). The creation of SOCMINT has various beneficial usages similar to the use of OSINT. Firstly, it allows for the understanding of a specific phenomenon such as radicalisation (Omand, Bartlett & Miller, 2012, p. 805). From a more

operational point of perspective, social media gives near real-time situational awareness, for example prior to and during an event (Omand, Bartlett & Miller, 2012, p. 805-806). Moreover, one can gain insight into groups to better understand activities and get familiar with behaviour of certain groups that are already of interest to the police (Omand, Bartlett & Miller, 2012, p. 806; Trottier, 2017, p. 458). Finally, it also allows for the "identification of criminal intent or criminal elements in the course of an enquiry both for the prevention and prosecution of crime" (Omand, Bartlett & Miller, 2012, p. 806; Trottier, 2017, p. 458). As can be seen, the majority of the advantages can be related back to the foundational building blocks of social media presented by Kietzmann, Hermkens, McCarthy and Silvestre (2011b). Smilda and de Vries (2017, p. 196) express that elements from the Dutch traditional model of profiling crime scenes, victims and perpetrators will be altered by social media which is displayed in the figure below.

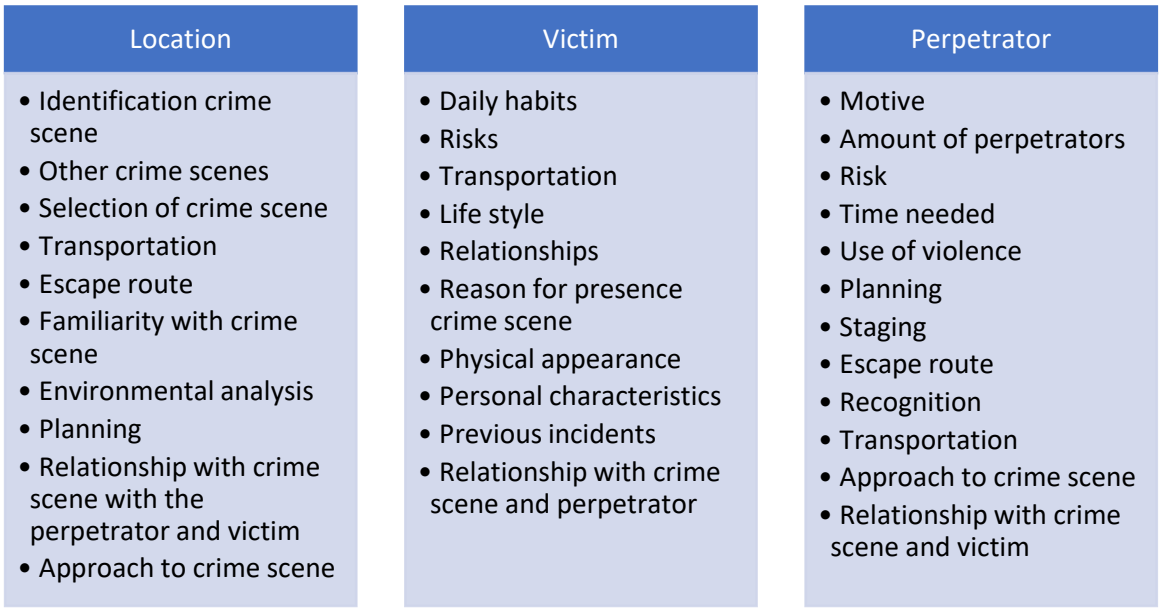

Figure 1: Steps in intelligence and police investigation to be altered by social media (as translated from Smilda & de Vries, 2017, p. 196)

Omand, Bartlett and Miller (2012, p. 807) do recognise challenges of SOCMINT which are based in necessity and legitimacy. The principle of necessity explains that SOCMINT must work for it to be collected. Success of SOCMINT then relates to the effects that it has in decision-making, rather than the secrets that are being discovered (Omand, Bartlett & Miller, 2012, p. 807). Different intelligence methods have different thresholds of how it moves its way through the intelligence cycle in order for it to be considered successful (Omand, Bartlett & Miller, 2012, p. 807). For OSINT, for example, this is most often done through the triangulation of reliable sources as Gibson (2017) described. In general, SOCMINT tries to understand online human behaviour and the typical academic sciences – social, political, anthropology, psychology, etc. – have not kept up with the large pace in which this human behaviour ought to be understood through big data sets that are generated by intelligence specialists

(Omand, Bartlett & Miller, 2012, p. 816). In order for SOCMINT to be methodologically robust for intelligence, it must rely on social media sciences which combines enough computational, technological and human disciplines to engage in sense-making from a data-led approach as well as a human behaviour-approach (Omand, Bartlett & Miller, 2012, p. 816). Thus, within the principle of necessity, validation of SOCMINT is the most challenging.

A second condition of SOCMINT is that it must be legitimate. Omand, Bartlett and Miller (2012, p. 816) explain that all intelligence rests on a balance between the maintenance of national security including public order and public safety; citizen's right to the rule of law, liberty and privacy, and the overall economic and social wellbeing of the nation and its citizens. Thus, in order to use SOCMINT the risks to the three public goods mentioned above must be recognised. This also includes the public concern of privacy. What "privacy" means continuously alters as society changes, especially with the development of social media. The privacy of one's identifiable information, for example, is protected through "informed consent" on social media platforms where the users gives its consent to gain access to personal information (Rønn & Søe, 2019, p. 365). Participatory surveillance is another key concept which explains that by participating on social media, people enable surveillance over themselves and others (Rønn & Søe, 2019, p. 365). Both notions make it difficult to restrict access to personal information as social media platforms are often designed to spark the curiosity of users to engage in these principles. In order for SOCMINT to be considered legitimate, states and security actors have to keep up with the fast pace of changing attitudes towards the three public goods mentioned above, of which privacy is the most pressing. It makes the balance between recognising risks on the one hand and providing mitigating or preventive steps on the other hand more complex.

IV. Policing in a pre-crime society

The post-crime society which focuses on crimes, offenders, investigations, trails and punishments is shifting more towards a pre-crime society in which governments and security actors anticipate and focus on surveillance and prevention (Zedner, 2007, p. 262). Simultaneously with the shift towards a pre-crime society came technological advancements such as computers and the Internet which are considered catalysts for this shift (Pedersen & Jansen, 2019, p. 882). Given these developments, adjusted policing methods were necessary of which the most dominant were problem oriented policing and community policing (Reisig, 2010).

Problem-oriented policing was initiated by Goldstein (1979) who laid down the structure of this method. It searches for the breeding ground of crime instead of focusing on individual crimes and perpetrators (Meershoek & Kop, 2017, p. 42). He argues that problems need to be defined with greater specificity instead of through broad categories given that each type of incident poses a different problem for the police (Goldstein, 1979, p. 245). Secondly, it is of importance that the problem is properly researched and explored to understand the nature of it in order to design an effective police response

(Goldstein, 1979, p. 248). Finally, alternatives must be explored that might be an improvement of the current process (Goldstein, 1979, p. 250). Given that the problem has been adequately researched in the first steps, this should pose no trouble. Goldstein (1979, p. 256) does argue that these three steps should be complemented by a number of intervening steps which, amongst others, include the involvement of the community. This is the core objective of community policing. It is characterised by the value police officers give to the active contribution of a community in crime fighting and decision-making (Weisburd, Shalev & Amir, 2002, p. 86). Community police offers aim at creating a trustworthy position within neighbourhoods. The importance thus lies in police-community partnerships which can increase this trust (Reisig, 2010, p. 5). Acting as street-level bureaucrats, community police officers can be aided in their work by partnerships with the community built on trust, enhancing their information position on crime topics (Reisig, 2010). This is similar to the steps mentioned within problem-oriented policing, as community police officers investigate and develop an understanding of local problems for which community-specific solutions are offered (Reisig, 2010, p. 6).

Information plays a valuable role in both policing methods as it increases the position police officers have in society and towards crime. Additionally, their knowledge and understanding of crime is also enhanced. As mentioned earlier, raw information becomes an even more valuable asset for police officers once it has been transformed into intelligence through analysis (Reuser, 2013, p. 2). More increasingly, the police started to adopt an intelligence-led policing (ILP) model which advocates a more proactive style of crime prevention originating from the intelligence position on crime (Burcher & Whelan, 2019, p. 139). Intelligence-led policing developed alongside other intelligence-oriented models such as the National Intelligence Model (NIM) which originated in the UK (Fyfe, Gundhus & Rønn, 2018, p. 7). The NIM was a result of a movement by the British government which began implementing "business plan" philosophies for government services (Carter & Carter, 2009, p. 2). Essentially, NIM was a business process model designed to enhance crime control by embedding ILP. As Ratcliffe, a founding figure in ILP, points out:

> *"Instead of tackling crime one laborious investigation at a time, never truly having an impact on the more expansive criminal opportunity structure, the capacity to step back and place threats and risks into a holistic perspective that assesses the social harm of criminality may allow policing to prevent crime across a wide area rather than solve a single event that has already occurred."*
>
> (Fyfe, Gundhus & Rønn, 2018, p. 2)

The core philosophy of ILP is thus to include intelligence in the operation of law enforcement in order to deal more effectively with emerging threats and serious crimes (Carter & Carter, 2009, p. 9). It collects raw information within defined threat parameters that can be used for analysis (Carter & Carter, 2009, p. 11). The model does not provide concrete analytical tools into collecting information and transforming it into relevant intelligence but can rather be viewed as a business model explaining how policing should

be conducted (Fyfe, Gundhus & Rønn, 2018, p. 4). The basic principle of ILP is delivering "actionable intelligence" in order to develop interventions to threats (Carter & Carter, 2009, p. 12).

At first glance, ILP and problem-oriented policing seem to converge. Both models aim at building a stronger information position towards crime and more evidence-based policing (Tilley, 2008, p. 385). ILP is, however, considered a business model rather than a policing strategy as was intended by the British government (Carter & Carter, 2009, p. 2). It focuses more on decision-making and law enforcement than problem-oriented policing which is interested in all alternative approaches to crime control (Goldstein, 1979, p. 250). There are also differences in data collection and analysis. ILP employs analysts to look at serious offenders and their networks, while problem-oriented policing does not necessarily require analysts but emphasizes the role of community partnerships which may not always result in strictly police related problems (Tilley, 2008, p. 385).

V. Crime intelligence analysis and the intelligence process

Analysis is the key feature into ILP as it translates raw information to operational valuable intelligence (Cope, 2004, p. 201). While analysis is not the focal point of this thesis, this section will provide brief background information into the two most dominant analysis methods.

Criminal intelligence analysis (CIA) is a dominant philosophy explaining how the investigation of crime and criminals can be approached through information that has been collected (United Nations, 2011, p. 7). Essentially, CIA is a combination of different exploratory, statistical and visualization methods to help discover patterns in the large amounts of information that law enforcement gathers (Ribaux, 2003, p. 54). Here, the revelation of "hot spots" which are either geographical or temporal are important. By depicting intelligence about similarities in incidents either through their similar location, time, modus operandi or victims, CIA allows analysts to indicate the existence of a problem (Ribaux, 2003, p. 54). Criminal intelligence analysis visualizes the criminal environment from which an interpretation and forecasting of crime and crime trends follows by analysts (United Nations, 2011, p. 7). Ratcliffe continues by explaining the 3-i model: *interpret, influence and impact* (Fyfe, Gundhus & Rønn, 2018, p. 3). Here, the crime analyst interprets the criminal environment from which it generates a position to influence decision-makers (Fyfe, Gundhus & Rønn, 2018, p. 3). Decision-makers must then allocate their resources effectively in order to impact the criminal environment (Fyfe, Gundhus & Rønn, 2018, p. 3). As became clear earlier, intelligence-led policing places a larger influence on decision-making which can also be seen in its analysis. Innes, Fielding and Cope (2005) contrarily argue that CIA delivers intelligence products which are disproportionately stated as being 'scientifically objective'. It is then wrongfully implied of being representative to the accurate crime problems, while the product itself is left to interpretation by decision-makers (Innes, Fielding & Cope, 2005). According to Innes, Fielding and Cope (2005, p. 54) products of CIA should be treated as an artefact of data and methods rather than an accurate representation of crime problems.

A second broadly recognised concept of intelligence analysis is the intelligence process, or cycle, which is believed to be the foundation of intelligence analysis (United Nations, 2011, p. 11). Similar to CIA, the intelligence cycle converts undefined information into intelligence which is made useful for practitioners (Wozniak, 2013, p. 675). While scholars disagree about whether the cycle constitutes four, five or six stages, the intelligence process at least consists of: collection, processing, analysis and dissemination (Colleen, 2007, p. 47; United Nations, 2011, p. 10; Wozniak, 2013, p. 675). Additional steps – which are either incorporated into the four mentioned above or posed as separate steps – include direction and feedback (Marzell, 2016). Summarised, the cycle starts with needs from a client from which information is collected. From here, the information is evaluated which is an assessment about the reliability and quality of the source. After this evaluation, the data is organised into a format from which it will be analysed. Finally, the analysis is presented towards the client where it is re-evaluated and provided with necessary feedback (Colleen, 2007; United Nations, 2011). As expected, the analysis within the intelligence process plays a critical role as it is a careful examination of the information. The first phase is data integration in which data from different sources is combined. A variety of techniques display this information, from link charting to financial profiling (United Nations, 2011, p. 14). These merely function as tools to give meaning to the information. Afterwards, the information is interpreted which also requires a certain amount of logical reasoning as the analysts move beyond the facts (United Nations, 2011, p. 14). Critics of this approach, however, claim that the intelligence process is more fluid than the stages described above (Fyfe, Gundhus & Rønn, 2018, p. 7).

As mentioned earlier, OSINF needs to be thoroughly analysed in order to generate trustworthy OSINT. While the majority of the intelligence institutions follow the steps of the intelligence cycle, Gibson (2017) takes a different approach: *Open Source Data* will be processed into *Validated Open Source Intelligence* through *Open Source Information* and *Open Source Intelligence*. Translated: raw data will be processed into open source information which will be compiled with other information into OSINT. From this, the intelligence will be validated into actionable and trustworthy intelligence (Gibson, 2017).

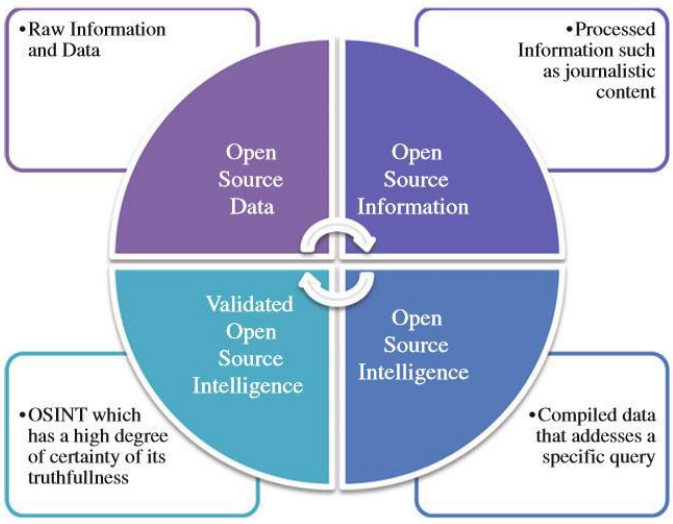

Figure 2: The four categories of open source information and intelligence as described by Gibson (2017, p. 70)

VI. Policing in the Netherlands

Similar to policing practices worldwide, the Dutch police took a primarily reactive approach towards crime (Meershoek & Kop, 2017). Through the decades, various societal and technological changes have shifted this reactive approach towards the more proactive approach that the police currently takes (Meershoek & Kop, 2017, p. 39). Catalysts in this shift were the development of the computer and the Internet on the one hand and the increased and strengthened criminality on the other hand (Meershoek & Kop, 2017, p. 40; Pedersen & Jansen, 2019, p. 882). Gathering information has always been a core task of the Dutch police and these developments brought forwards not only its necessity but also its possibility.

The earlier mentioned problem-oriented and community policing methods were also initiated in the Dutch police organisation. Community policing was initiated in the 1980s with the development of district teams. The goal was, following the core philosophy, to establish a position for the community officer within the neighbourhood and enhance its information position on local crime through trustworthy partnerships (Meershoek & Kop, 2017, p. 42). Community policing in the Netherlands developed as a result from the initiation of problem-oriented policing. As the concept moved across the world, the Dutch police embedded this approach to crime control in its daily modus operandi in which district teams and hence community policing would play an important role (Meershoek & Kop, 2017, p. 42)

ILP in the Netherlands (Dutch: Informatiegestuurd politiewerk, IGP) unfolded from these methods and objectives in the 1990s through collaboration with the Kent Police (Kop & Klerks, 2009, p. 15). It was primarily positioned within the investigative processes of the police, in which intelligence would aid in designing specifically targeted approaches and solutions to frequent crime (Meershoek & Kop, 2017, p. 43). The police, however, wanted to broaden the scope of this approach to different police processes (Meershoek & Kop, 2017, p. 43). Similar to the British police, ILP was regarded as a business model meant to steer the process-based management from the police (Kop & Klerks, 2009, p. 16). ILP would increase the quality of the Dutch police work and also establish effective guidance of managers in information gathering (Kop & Klerks, 2009, p. 16). The intention of ILP in general, was for the Dutch police to shift from a reactive law enforcement authority towards a knowledge-based organisation designed to more effectively execute operational tasks (Kop & Klerks, 2009, p. 16). Additionally, the Dutch police forces followed the British example of formulating a National Intelligence Model which formulates how police should be led by information and how the gathering and analysis of information should be managed (Meershoek & Kop, 2017, p. 44). Alongside, the programme Intelligence was initiated to enhance the collaboration between regional and national information organisations of the police (Kop & Klerks, 2009, p. 18). This, for example, organised information into three levels: local, regional and national (Kop & Klerks, 2009, p. 20). Moving forward, ILP and NIM are embedded within the Dutch police through on the one hand the organisation of information gathering and analysis on a

local, regional and national level and the cohesion between these levels, and on the other hand through the current modus operandi of the police which is to enhance its position within the pre-crime society.

METHODOLOGY

I. Research design

The purpose of this research is mainly exploratory as both little academic and practical contributions exist within this field. The study aims at exploring the relationship between OSINT and surveillance and entrapment through describing current concepts, mechanisms and frameworks from a practitioner's point of perspective. Subsequently, this research will explore relationship between these within the model of intelligence-led policing by the Dutch police.

The use of OSINT within principles of surveillance and entrapment is complex and has not been extensively researched before. The main research design for this study includes a document analysis in combination with interviews as qualitative research methods. Given that a variety of documents are a staple in this study, a document analysis is best suitable as it includes this variety of documents and offers a systematic procedure for reviewing and evaluating these documents (Bowen, 2009, p. 27). The types of documents used for this research will be elaborated later in this chapter.

It is common for a document analysis to be accompanied by another qualitative research methods as a means of triangulation, which decreases chances of bias and insufficient information (Bowen, 2009, p. 28-31). Here, the researcher opted for the inclusion of interviews with practitioners from the police. Interviews complement and deepen other documentation with contextualised interpretations from practitioners which is necessary for both the explorative nature of this study as well as the limited body of knowledge of this subject (Gill, Stewart, Treasure & Chadwick, 2008, p. 292; Yin, 2003). Especially when performing a case study, interviews are the most important source of information given the subjective information that is received. Interviews are not a primary source of data collection in this research but will function as a completion to the academic literature and other documents used. The interviews are semi-structured, which is an approach to interviews in which there are pre-determined questions but there is also the flexibility to diverge in order to explain something in more detail (Gill, Stewart, Treasure & Chadwick, 2008, p. 291). Moreover, this structure also allows for the discovery or elaboration of a subject that is important to the respondents but was initially overlooked (Gill, Stewart, Treasure & Chadwick, 2008, p. 291).

Finally, the balance of these modus operandi are analysed and applied to the case of digital meeting places within right-wing extremism. The researcher has opted for a case study as it is a suitable approach towards the exploration of new processes of which little is understood (Meyer, 2001, p. 330). The aim of the researcher to use a single case study design is primarily to provide a precise and in-depth exploration of a phenomenon which has not been studied before. In this situation, a single case study is more advantageous than exploring multiple cases, for these mainly have a comparative purpose (Lijphart, 1971, p. 333; Meyer, 2001). Moreover, an advantage of a single case study is the possibility to extensively study a phenomenon with limited resources or time which is favourable for this study

(Lijphart, 1971, p. 691). In conversations with intelligence officers from the DRIO, the chosen case of digital meeting places amongst right-wing extremists proved to be distinctive towards the research problem considered in this study. Firstly, the case shows a value for OSINF as the potential for digital meeting places are found within publicly accessible social media platforms (Kietzmann, Hermkens, McCarthy & Silvestre, 2011a; Smahel, 2008). Additionally, researching where right-wing extremists mobilize online requires the use of mechanisms which function within the principles of surveillance and entrapment, both underexplored concepts when combined with OSINT. While this case is best suitable for this study, it is ideal that the results of this study can be applied towards every security topic within the DRIO.

I.I. Scope

The central research question of this study illustrates the scope which will be clarified here.

Firstly, this study will focus on the intelligence department of the Police Unit The Hague which will henceforth be referred to as the DRIO. The DRIO is responsible for information gathering throughout the region of The Hague which encompasses a large amount of Dutch municipalities. Figure 1 illustrates the region of the DRIO. The researcher may refer in this thesis to "police", "law enforcement", "intelligence officers", and so forth, which are all directed towards the Police Unit The Hague and the DRIO..

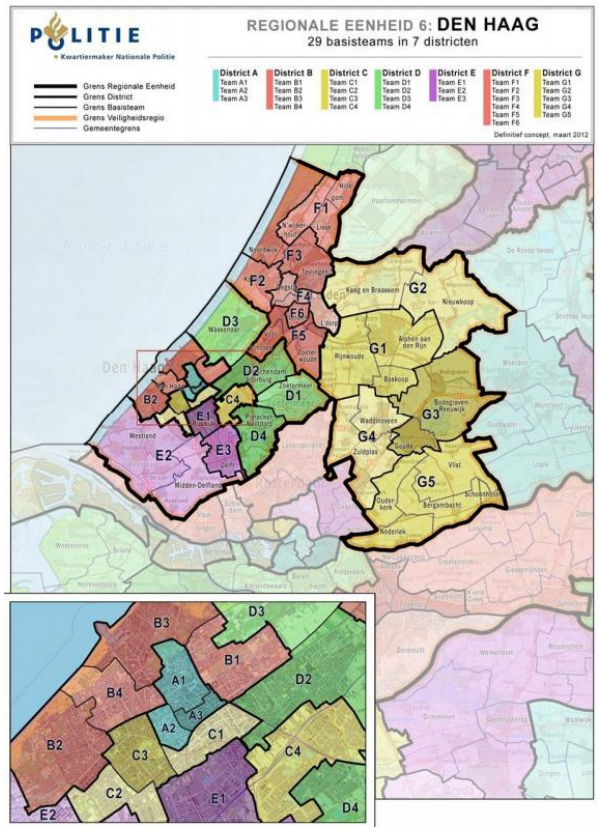

Figure 3: Geographical depiction of Police Unit The Hague

II. Data collection

As mentioned, a document analysis allows a variety of documents to be analysed (Bowen, 2009, p. 27). The documents used in this study include at least academic literature, jurisdiction and legislation, hearing outcomes, governmental documentation, media reports, and police policy documents. Using different types of documents has the advantage of gaining a better understanding of the phenomenon from different perspectives which decreases bias. Only openly accessible sources are used to minimise data accessibility limitations. Additionally, this is also the most feasible within the time frame of this study. Furthermore, the position of the researcher within the police is beneficial in finding relevant documentation, but could also increase bias which will be elaborated upon in the section **V. Limitations.**

Continuing, the position of the researcher within the DRIO allows for quick and feasible sampling of interview respondents. The researcher aimed at speaking to practitioners within the field of

OSINT, privacy, legislation and public prosecutors. This combination of respondents will provide the most complete picture of the incorporation of OSINT within the DRIO as well as the judicial framework built around it. Through snowball-sampling and convenience-sampling, the researcher was able to get into contact with the relevant practitioners for this research. As the interviews have a complementary task, the researcher aims to interview one respondent from each field mentioned earlier. The researcher did take into account the possibility for more relevant respondents which are not mentioned in the pre-selected sample. Concluding, the following interviews were conducted:

Respondent code	Function
R1	Intelligence officer DRIO
R2	Intelligence officer DRIO
R3	Lawyer and former intelligence officer DRIO, also experience with criminal investigations and currently writing a PhD in a similar topic.
R4	Public prosecutor
R5	Expert on right-wing extremism

Table 1: Respondents

III. Conceptualisation and operationalisation

III.I. Open sources

The name "open sources" already suggests that the sources used for information gathering are open and are not discovered, recruited, intercepted or sensed technologically as is the case with other covert intelligence collection methods (Miller, 2018, p. 705). In literature, the term "open source" is followed by a summary of every source that has the possibility of being publicly and freely accessible, for example mass media; public data; grey literature; and observation and reporting (Miller, 2018, p. 706). In policing literature, open sources are defined as sources which can be accessed without intervention of a third party (Stol & Strikwerda, 2018, p. 17). As Sampson (2017, p. 56) explains, information collection does not include clandestine methods of collection.

The coherence of "open sources" with the phrase "publicly accessible" in the majority of the definitions is troublesome to some extent. It could, for example, imply that sources for which registration is needed before they become publicly accessible would not fall within the scope of open sources (Koops, 2012, p. 33). In this case, open sources can either be "open" or "closed". The latter implying that registration is needed before a source is publicly accessible and the first implying that a source is publicly available without registration. On the other hand, the term "publicly accessible" could also imply that law enforcement officials may have access to any data that is available to the public, even after registration. This interpretation is, for example, suggested by the Convention of Cybercrime (ETS

185), article 32.[1] A Guidance Note to this convention elaborates on this terminology by adding that "it is commonly understood that law enforcement officials may access any data that the public may access, and for this purpose subscribe to or register for services available to the public," thus implying that publicly available open sources include those where registration or payment is necessary.[2] This would also include the option for law enforcement authorities to register themselves which could lead to cases of entrapment. This will be discussed later in this thesis.

Given that the context of this study falls entirely within the Dutch police, it is important to use the concept of "open sources" as it is enforced in the Dutch police. Within the investigative branch of Dutch police departments, there is a compliance with the definition and operationalisation illustrated in the Convention of Cybercrime: open sources include all sources which are publicly accessible, whether or not it includes registration or payment (Lassche, 2019, p. 47). There are discussions amongst intelligence officers to what extent they comply with this operationalisation or limit themselves to the more "closed" version of open sources. For the purpose of this study, it is assumed however that the DRIO also complies with the Convention of Cybercrime and treats any publicly accessible source as an open source.

III.II. OSINT

As illustrated in the **Theoretical framework**, information and intelligence are easily confused but are not the same. Intelligence is the actionable deliverable after raw information is analysed. In the case of OSINT, it is intelligence that is produced from publicly available information (Miller, 2018, p. 706). The emphasis of OSINT does not lie within the availability and gathering of information but in the transformation of it towards an actionable form (Glassman & Kang, 2012, p. 675). Moreover, Glassman and Kang (2012, p. 680) explain that OSINT is always transparent and treated more as a community resource than an individual commodity. They, for example, pose that OSINT should always be a well-referenced and transparent report for the end user meaning that references are publicly accessible (Glassman & Kang, 2012, p. 675). Additionally, the end user should be able to locate information to immediate problems but also understand how information can be used in other target nodes (Glassman & Kang, 2012, p. 675). Another definition is proposed by the Office of the Director of National Intelligence (as described in Williams & Blum, 2018, p. 1) who explains OSINT as "intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement." This definition is more suitable to this research and will, therefore, be used.

[1] Cybercrime Convention Committee (T-CY). Budapest, November 23rd, 2001. *Convention on Cybercrime (ETS No. 185).* Retrieved on November 12th, 2020 from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[2] Cybercrime Convention Committee (T-CY). December 2014. *Guidance Notes: Transborder Access (Article 32).* Retrieved on November 12th, 2020 from: https://www.coe.int/en/web/cybercrime/guidance-notes

III.III. Surveillance

In the early developments of the nation states, law enforcement authorities were not occupied with the investigation of crime but solely responded to breaches of peace (Rosenthal, 2017, p. 310). The notion of surveillance within a policing context is therefore fairly new as police officers became more occupied with investigations at the forefront. Contrary to the earlier days of police authorities, surveillance is a preferred response and well-embedded police task for dealing with a variety of problems (Haggerty, 2012, p. 235). Hence, the expanding use of surveillance techniques by public and private actors make that the pre-crime society Zedner (2007) explains is more increasingly being looked at as a "surveillance society" (Marx, 2015, p. 733).

Trottier (2017, p. 460) defines surveillance as the "close and sustained scrutiny of individuals through the collection and analysis of information, with the intention of heightened knowledge and manipulation of that population." Wang and Tucker (2017, p. 145) give a similar definition proposed by Lyon (2007, as described in Wang & Tucker, 2017, p.145) in which he describes surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or detection." These definitions suggests two things. Firstly, surveillance comprises a critical examination or observation of a target and thus, to some extent a breach of privacy. This automatically places surveillance within foundational documents such as constitutions, conventions, charters, etc. (Gray & Henderson, 2017, p. 1). Article 8 of the European Convention on Human Rights (ECHR), for example, stresses the right to a private and family life.[3] The extent to which surveillance is then allowed whilst respecting these rights, depends on the second notion of surveillance: it must have an intention. Generally, surveillance is intended to ensure safety, security and stability (Gray & Henderson, 2017). Lyon (2007, as described in Wang & Tucker, 2017, p.145) addresses three purposes of surveillance: keeping control, social sorting and mutual monitoring. The first of these purposes is attributed towards authorities like the government and the police (Wang & Tucker, 2017, p. 145).

A definition of "surveillance" from a practitioner's point of view is limited since they regard surveillance as a method of policing rather than a principle in the field of security. According to the Dutch police law, surveillance is allowed on the grounds of Article 3 of the Police Directive (PolW) which explains the core task of Dutch police: maintaining order (Oerlemans & Koops, 2012, p. 35).[4] This is coherent to first purpose of the three stated by Lyon (2007, as described in Wang & Tucker, 2017, p.145) and will be dominant in this study. It falls outside the scope of this study to go into depth about the different surveillance techniques of the Dutch police as the concept of "surveillance" is not regarded as a policing method but rather as a policing construct.

[3] Article 8. ECHR 2010. (2010, June 1st). Retrieved on November 13th, 2020 from: https://www.echr.coe.int/documents/convention_eng.pdf
[4] Article 3. Politiewet 2012. (2012, July 12th). Retrieved on November 14th, from: https://wetten.overheid.nl/BWBR0031788/2013-05-01

III.IV. Entrapment

In literature, the term provocation is oftentimes linked to the excessive use of force by police officers (Noppe, 2018, p. 605). This study will, however, make use of the term entrapment which is more suitable for this thesis. Moreover, the focus will be on online entrapment by intelligence officers.

Grommé (2016, p. 1008) expresses that entrapment raises evidence that does not have its basis in accepted protocols and are a result of defiant usage of technology. Boudana and Segev (2017, p. 329) define entrapment as "an action or speech that may be intentional and may stimulate a reaction." Both definitions illustrate that entrapment is a means that steers behaviour intentionally. The Dutch Cybercrime law, adopted in 2018, *(*Dutch: Wet computercriminaliteit III*)* makes it for example possible for the police to install hack and spyware on computers (Custers, 2018, p. 100). Although this can only be done under certain circumstances, it does create possibilities for entrapment by the police (Custers, 2018, p. 112). Article 47 of the Dutch criminal law (Dutch: Strafrecht, henceforth: Sr), mentions that individuals engaging in entrapment is punishable.[5] This means that engaging in entrapment must comply with the following conditions: 1) there is a clear intention of the emitter to engage in entrapment, 2) clear encouragement to entrapment towards the receiver, 3) the use of one of multiple means of entrapment – e.g. gifts or promises, 4) the provoked offense is monitored, 5) the provoked offense is punishable. Here, both the emitter and the receiver are punishable. Therefore, article 5.3.1. of the Dutch criminal procedures (Dutch: Strafvordering, henceforth: Sv), explains that entrapment can be requested by the public prosecutor towards the Minister of Justice and Security if the public prosecutor deems this necessary.[6] What is important here, is that such means is available to the investigative branch of the police.

Following these regulations, an issue is raised referring back to the open sources that police have access to: could creating a profile on social media platforms initiate provocative purposes by the police? If we take this into account, entrapment by the police would then include the disproportionate and illegitimate use of authorizations. This clashes with the definition of Grommé (2016) which suggests that entrapment exists outside accepted protocols. For this study, the focus will be on the disproportionate and illegitimate use of police competences but will not exclude the operationalisation by Grommé (2016). The researcher has opted for this as the use of OSINF is not well established within a defined judicial framework or within the notions of surveillance and entrapment, which makes the existence of entrapment outside of accepted protocols possible.

Lastly, the importance of "intentionality" within the definition of entrapment is evident. Boudana and Segev (2017, p. 332) explain how intention can be perceived differently towards the

[5] Article 47, Sr 2020. (2020, July 25th). Retrieved on February 1st, 2021 from: https://wetten.overheid.nl/BWBR0001854/2020-07-25#BoekEerste
[6] Article 5.3.1., Sv 2021. (2021, January 1st). Retrieved on February 1st, 2021 from: https://wetten.overheid.nl/BWBR0001903/2021-01-01

emitting and receiving party of an action. The receiver could, for example, interpret an action as being intended to force a certain reaction which might not have been the purpose of the emitter. Within this study, entrapment will be viewed as being intentional by the emitter which is the police in this case.

IV. Additional clarifications

IV.I. ILP or IGP?

The **Theoretical framework** referred to intelligence-led policing from an international perspective as well as from a Dutch perspective. With the adoption of intelligence-led policing in the Netherlands, a discussion about the correct framing of the method initiated (Kop & Klerks, 2009, p. 8). The Dutch term reads "informatiegestuurd politiewerk" which in essence is a direct translation from the English term. In practice, there are differences between the two methods which are visible in the dominant role of the regional police units in the Netherlands (Kop & Klerks, 2009). In this thesis, the Dutch model of intelligence-led policing will be managed. Given, however, that the primary language of this study is English, the researcher has chosen to refer to the English term of intelligence-led policing.

V. Limitations

V.I. Reliability

Reliability refers to the extent to which a study can be reproduced, thus being consistent over time (Noble & Smith, 2015). Given that this study encompasses the process through which the researcher went to answer the research question, it is possible to reproduce the study in a similar matter. The difficulty lies within the sampling method of the interview respondents, as these were sampled through the personal circle of the researcher. Additionally, reliability is increased when bias is limited (Golafshani, 2003, p. 601). In this research, bias has a possibility of occurring as most of the data will be collected from one organisation: the DRIO. While the researcher aims to analyse documents and interview respondents from different perspectives, the majority of the data originates from the police. As documents are retrieved through the DRIO, it could be that these were subjectively selected by police and intelligence officers in order to steer the study in a preferred direction. The researcher aims, however, to complement this data with data that has been retrieved outside the police organisation to increase reliability.

V.II. Validity

The validity of a research refers to the precision in which the findings accurately reflect the data (Noble & Smith, 2015). The use of triangulation within this study increases construct validity (Meyer, 2001, p. 346). Triangulation implies that multiple methods or data sources are used (Golafshani, 2003, p. 603). The validity of evidence is then enlarged because it cannot be referenced back to a single source. This study responds to this requirement by using multiple sources, multiple analysis methods and multiple perspective from interview respondents. This primarily increases the construct validity of this study

which refers to correct correspondence between the theoretical paradigm and the observation (Meyer, 2001, p. 345).

The scope of this research is limited in several ways which could decrease external validity – the generalisability of the study (Calder, Phillips & Tybout, 1982, p. 240). Firstly, the case is limited to The Hague in which the criminal environment is different than in other Dutch regions. There is thus no assurance that findings that result from the case study are representative to the general Dutch criminal environment or other specific Dutch regions. From a larger geographical perspective, there is no assurance that these findings are of meaning to a broader European or global context. The same limitation counts concerning the focus on the intelligence department from the police. The use of OSINF and OSINT does not limit itself to police authorities but is also of value to other national security agencies or private organisations in problem-solving (Glassman & Kang, 2012, p. 673). The generalisability of this study is therefore small as these organisations all differ in scope, strategy, structure and modus operandi. Additionally, the judicial framework in which all the actors work are different.

On the other hand, this study aims at building a framework for the use of OSINT within surveillance and entrapment which can be used for any type of incident or problem for the DRIO The Hague or other intelligence departments from the Dutch police. Generalisability is then of little relevance when the intention is particular to a phenomenon or case (Meyer, 2001, p. 347). Based on the same interest and methods, other researcher or security agencies are able to reproduce this study for their country, case or organisation.

JUDICIAL FRAMEWORK

There are two sides to policing which are laid down in the Police Directive. Firstly, there is the investigative branch which is involved with criminal investigations. This approach to policing is under close scrutiny of a variety of laws and is accountable to the public prosecutor (Dutch: Openbaar Ministerie, henceforth: OM).[7] Secondly, there is the information-gathering branch of policing which is involved with the general information-gathering without there having been a criminal offence. This branch, also referred to as Public Order and Safety (Dutch: Openbare Orde en Veiligheid, henceforth: OO&V), is under scrutiny of the mayor (Nederlands Genootschap van Burgemeesters, 2017, p. 79).[8] This is an important distinction to make as each branch has a separate judicial framework built around it which heavily affects the competences of the police. These three actors – the public prosecutor, the mayor and the police – are bound by Article 13 of the PolW to meet periodically about the task performance of the police, local priorities with respect to crime control and police deployment with respect to maintaining public order and safety (Nederlands Genootschap van Burgemeesters, 2017, p. 79-80).

This chapter will go into depth about the police its function within OO&V and the judicial framework built around it. A variety of laws and regulations are important here amongst which are the General Data Protection Regulation (GDPR), the ECHR, the PolW and the Police Data Directive (Dutch: Wet Politiegegevens, henceforth: Wpg).

I. The Police Directive

The PolW describes the organisation of the Dutch police as well as their core task.[9] The latter is most important for this study, as it lays down the foundations of police tasks in both the investigative branch as well as the intelligence branch. Article 3 PolW describes the essential policing task as followed:

> *"The police have the task, in subordination to the competent authority and in accordance with the applicable legal rules, to ensure the effective enforcement of the legal order and to provide assistance to those who need it."*[10]

When asking about the judicial framework during the interviews, all respondents explained that the justification of their work must be traceable to Article 3 PolW. If this is not possible, for example because intelligence officers engage in a privacy breach that is more than necessary, other regulations need to be uphold.

[7] Article 11, Politiewet 2012. (2012, July 12th). Retrieved on January 19th, 2021 from: https://wetten.overheid.nl/BWBR0031788/2021-01-01#Hoofdstuk2
[8] Article 12, Politiewet 2012. (2012, July 12th). Retrieved on January 19th, 2021 from: https://wetten.overheid.nl/BWBR0031788/2021-01-01#Hoofdstuk2
[9] Politie. (n.d.). Politiewet. Retrieved on January 19th, 2021 from: https://www.politie.nl/over-de-politie/politiewet.html
[10] Article 3, Politiewet 2012. (2012, July 12th). Retrieved on January 19th, 2021 from: https://wetten.overheid.nl/BWBR0031788/2021-01-01#Hoofdstuk2

II. The European Convention on Human Rights

When such breaches tend to become more excessive, additional competence is needed. Article 8, paragraph 2 of the ECHR describes this necessity of public authority interference. It namely explains that a breach of privacy is allowed when "in accordance with the law and … necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[11]

III. The Charter of Fundamental Rights of the European Union

Similar to the ECHR, the Charter of Fundamental Rights of the European Union (CFR) describes the right to the protection of personal data in Article 8.[12] This right may be limited however as long as they comply with Article 52(1) which explains that limitations:[13]

- Must be provided for by law;
- Respect the essence of the rights and freedoms of the Charter;
- Are subject to the principle of proportionality;
- May only be made when they are necessary;
- May only be made when they genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

This article thus lays down two important principles that ought to be met when, in this instance, the privacy of individuals is breached: necessity and proportionality.

IV. The General Data Protection Regulation

The dominant regulation which concerns the protection of personal data is the GDPR which has been implemented on a European level and entered into force in 2016.[14] It differentiates between personal data and special categories of personal data, which is a distinction that police employees also must take into account. Personal data as a whole is defined in the GDPR as "… any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[15] The special

[11] Article 8(2), ECHR 2010. (2010, June 1st). Retrieved on January 19th, 2021 from: https://www.echr.coe.int/documents/convention_eng.pdf
[12] Article 8, the Charter 2012. (2012, October 26th). Retrieved on February 3rd, 2021 from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN
[13] Article 52(1), the Charter 2012. (2012, October 26th). Retrieved on February 3rd, 2021 from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN
[14] European Commission. (n.d.). Gegevensbescherming in de EU. Retrieved on February 3rd, 2021 from: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_nl
[15] Article 4(1), GDPR 2016. (2016, April 27th). Retrieved on January 19th, 2021 from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=NL

categories of personal data concern the latter part of the definition and include data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health and data concerning a natural person's sex life or sexual orientation.[16] While Article 9(1) of the GDPR states the prohibition of processing such data, exceptions are mentioned which the police can invoke such as protecting substantial public interests (Article 9.(2g), GDPR, 2016).

According to R3, the police must adhere to the GDPR to the extent that personal data must be gathered under the right circumstances. These mostly comprise a clear necessity and goal for the information that is wished to be collected which is especially important for the collection of above mentioned special categories of personal data. R3 mentions the following example:

"The goal and reason for your research must be coherent to the type of information that you wish to gather. If you are researching an Nuclear Security Summit, which was held in the Hague a few years ago, it is relevant to research political opinions and backgrounds of people who might create a risk. If you, however, researching football hooligans, information about political opinions and backgrounds is irrelevant and should not be gathered."

Additionally, the police also gathers information irrelevant to public order and investigations, for example when granting permits.[17] Such information should also be gathered and processed according to the GDPR.

V. The Police Data Directive

Personal data become police records after they have been collected in accordance to the GDPR. The Wpg lays down how police records should be protected and processed. It does so by, for example, explaining authorisations, the limitation period of records, the sharing with third parties such as the Royal Dutch Police.

Article 3, paragraph 1 and 2 of the Wpg explain that information may only be gathered and processed to the extent that this is necessary, serving the goal and non-excessive.[18] It is thus the responsibility of the employee to assess these principles given that the relevancy of information is not instantly clear. Article 5 Wpg specifically explains that the processing of special categories of personal data is only allowed when this is inevitable to the cause and necessity of the police.[19] Moreover, Article 10(2) and 10(4) Wpg also differentiate between suspects of a criminal offence and reasonable

[16] Article 9(1), GDPR 2016. (2016, April 27th). Retrieved on January 19th, 2021 from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=NL
[17] Autoriteit Persoonsgegevens. (n.d.). Politie. Retrieved on January 26th, 2021 from: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/politie-justitie/politie
[18] Article 3, Wpg 2020. (2020, January 1st). Retrieved on January 26th, 2021 from: https://wetten.overheid.nl/BWBR0022463/2020-01-01
[19] Article 5, Wpg 2020. (2020, January 1st). Retrieved on January 21st, 2021 from: https://wetten.overheid.nl/BWBR0022463/2020-01-01

presumption of individuals in accordance to Article 10(1a) and 10(1c) Wpg.[20] These latter two sections explain respectively the planning and executing of a felony and actions which could cause serious danger to the public order based on their nature, frequency or the organisation. According to the Wpg, processing information on individuals where a criminal offence is absent is allowed. This is, similar to regulations mentioned earlier, dependent on the necessity, proportionality and purpose of the data (Nederlands Genootschap van Burgemeesters, 2017, p. 95).

Article 16 Wpg sheds light on the distribution of police records to authorities.[21] Given that the mayor is responsible for public order, the mayor is allowed to receive police records on the basis of firstly the extent to which they have the authority over the police and secondly in the context of maintaining public order.[22] It is therefore imperative that the mayor and the territorial chief of police carefully lay down the extent of information-sharing (Nederlands Genootschap van Burgemeesters, 2017, p. 96).

VI. Special investigative powers

As mentioned, the investigative branch of policing differs from the information-gathering branch in a variety of ways. Other than the focus being on a criminal offence, the investigative branch has to comply to a different set of regulations amongst which is Sv. This defines how a criminal offence is prosecuted. According to R4, the enforcement of the Sv within the information-gathering branch of policing is not possible because no criminal offence has taken place. Intelligence analysts act upon reasonable presumption which does not fall within the scope of the Sv.

Specifically for the police, the first chapter of the Sv is of importance as it lays down the Special Investigative Powers (Dutch: Bijzondere opsporingsbevoegdheden, henceforth: BOB) which can be used in criminal offences as it specifies special investigative powers such as surveillance, wiretapping conversations, etcetera.[23] While this study will not go into detail about each, one special investigative power is worth describing further.

[20] Wpg 2020. (2020, January 1st). Retrieved on January 21st, 2021 from: https://wetten.overheid.nl/BWBR0022463/2020-01-01
[21] Article 16, Wpg 2020. (2020, January 1st). Retrieved on January 21st, 2021 from: https://wetten.overheid.nl/BWBR0022463/2020-01-01
[22] Article 16.1b, Wpg 2020. (2020, January 1st). Retrieved on January 21st, 2021 from: https://wetten.overheid.nl/BWBR0022463/2020-01-01
[23] Eerste Boek, Algemeene bepalingen, Sv 2021. (2021, January 1st). Retrieved on January 21st, 2021 from: https://wetten.overheid.nl/BWBR0001903/2021-01-01#BoekEerste

VI.I. Systematic observation

Systematic observation is a special investigative power in which an investigating officer is allowed to engage in a longer period of surveillance. It can only be granted by the public prosecutor when it is in the interest of a criminal investigation.[24]

As mentioned earlier, the BOB is meant for criminal investigations after an offence has taken place and therefore excludes the information-gathering branch of the police. Simply put; systematic observation is not possible within the DRIO.[25] It is therefore questionable to what extent intelligence officers can engage in surveillance when they can only act on reasonable presumption. Koops (2012, p. 37) argues that systematic observation with respect to maintaining public order is not allowed as there is no legal justification for it. Stol (2010, as described in Koops, 2012, p. 37) continues by addressing that internet surveillance should only be used in the context of an investigation as it makes police officers too attached to the internet.

In practice as well, questions are being asked about the extent of observation that is allowed for intelligence officers. R1 and R2 explain that this depends on the degree of the privacy breach, the following example is given:

"You must have a reason or presumption to engage in open-source information gathering. When this presumption lies within the field of extremism for example, it is allowed to search "neo-Nazis" and their groups multiple times. If we, however, wish to dive deeper into these groups we arrive at an individual and personal level and we need permission to continue our research. If we would continue without this permission and engage in a degree of privacy breaching which is more than necessary, the information found cannot be used continuing investigations or even in court."

R3, contrarily, explains that even a one-time search as is mentioned in the example is not a given. This also depends on the type of information you wish to gather, similar to the example of researching a summit or football hooligans. A breach of privacy is thus not solely dependent on the amount of observations an intelligence officer does but also depends on the type of information, how you store it, why it is being gathered, etcetera.[26] As Franken (2017, p. 78) explains, it is not allowed to store data "in case it might come in handy." Such criteria are weighed against the source (with or without door policy) and processed in a decision tree. Unfortunately, this is not publicly accessible.

Multiple respondents explain that granting said permission and continuing research is not similar to the systematic observation as systematic observation is broader and intelligence officers need permission with each new step they take. The only exception that exists to this is laid down in Article

[24] Article 126g, Sv 2021. (2021, January 1st). Retrieved on January 21st, 2020 from: https://wetten.overheid.nl/BWBR0001903/2021-01-01#BoekEerste
[25] Interview R1, R2, R3 and R4.
[26] Interview R3.

126gg Sv which explains the possibilities of an exploratory research.[27] R3 explains that this exception is only justifiable when indications that within a "collection of persons" serious offences are plotted or executed. R3 further explains that this article shifts the border from information-gathering and investigation to an earlier stage as this research is being executed under the authority of the public prosecutor instead of the mayor. It is, however, difficult to be granted this exploratory research. R1 gives the example of a demonstration:

"When we get permission of the public prosecutor to engage in a broader exploratory research, our possibilities extent. Anything that is related to the event, for example a demonstration, can be researched. In such cases, I could engage in research for weeks without asking for permission in between because it is related to the exploratory research."

The role of the public prosecutor here is remarkable. As discussed earlier, the role of the public prosecutor is most dominant in criminal investigations. Information-gathering with respect to maintaining public order falls under the authority of the mayor. Each respondent, however, clearly indicated that intelligence officers regularly discuss with a public prosecutor about the extent to which they are allowed to engage in surveillance. In an interview with a public prosecutor (R4) it emerged that the role of the OM is up for discussion and the following dilemma arises:

"There are multiple demonstrations in the Hague and I am oftentimes called to grant permission to engage in surveillance at the forefront. I sometimes wonder if I need to make these decisions or whether it should be the municipality or the mayor. On the other hand, this would imply that the mayor is responsible for granting permissions about online surveillance which is essentially a task of the OM."

VI.II. Entrapment

As explained in the chapter **Methodology**, entrapment occurs when evidence is gathered outside of accepted protocols (Grommé, 2016, p. 1008). To what extent is entrapment possible for intelligence officers after having witnessed a lack of judicial grounds for their work?

R3 makes a distinction between deception and entrapment. R3 explains that a large spectrum of opinions exist about this matter. One of those opinions explains that someone engages in deception from the moment they are not visible as a police officer. If this definition were to be followed, anything an individual says that would not have been said with the knowledge that the other person is a police officer is misleading and should not be allowed. There are also more nuanced opinions. R3 mentions that deception is vague given that police officers rarely operate under their own name as this is practically

[27] Article 126g, Sv 2021. (2021, January 1st). Retrieved on January 25th, 2020 from: https://wetten.overheid.nl/BWBR0001903/2021-01-01#BoekEerste

not feasible. Entrapment, R3 explains, is different as it means purposefully steering behaviour by police officers.

When asked to what extent entrapment is possible in information-gathering, R1 and R2 both responded that this is not feasible as they engage in passive research. The following example is given:

"It is not allowed to say or 'like' anything. If research is being conducted on a certain platform and the operator of the platform demands everybody to post "LEFT" to show support for the platform and their opinion, it is not allowed to participate to keep the cover. It is then not possible anymore to further conduct the research."

VII. Conclusion

This chapter has shown that no judicial framework exist around the possibilities for intelligence officers to conduct thorough research in open sources, like social media platforms. Article 3 PolW lies at the heart of intelligence officer's functioning and anything that deviates from this should be coordinated with the public prosecutor. The role of the public prosecutor is, however, a point of discussion as such coordination should in theory be done with the mayor.

In assessing the extent to which surveillance is thus allowed, the principles of proportionality, subsidiarity and effectiveness in relation to the goal. These combined, R3 says, allow for an estimation of necessity which is another important principle to take into account. Firstly, it is important for intelligence officers to have the capability of assessing these principles within Article 3 PolW as their main functioning is based on this. Only when an officer's operating exceeds Article 3 PolW, should the public prosecutor be able to assess these principles. A similar approach is taken towards assessing legitimacy. This is most difficult in this context as there is, except Article 3 PolW, no legal framework built around information-gathering.

THE CASE: RIGHT-WING EXTREMISM

So far, this study has provided for an elaborate theoretical framework explaining the current position of intelligence within the Dutch police, different intelligence disciplines and dominant intelligence analysis methods. Additionally, the previous chapter has shown how surveillance and entrapment are embedded in a judicial framework surrounding the policing branch of information gathering. It has shown that there is a lack of legislation and regulations with respect to said policing branch which makes conducting research on a certain topic rather vague. The unclarity that exists around this phenomenon did, thus far, show that entrapment is not possible within information gathering as intelligence officers engage in passive research.

This chapter aims to bring practice to theory by applying information from the previous chapters to the case of right-wing extremism. It will do so by first introducing right-wing extremism before engaging in the further application.

I. Right-wing extremism

Since the 1980s, European countries have seen a revival of the extreme or radical right ideology and parties and is therefore placed within the "third wave" of terrorism (Bakker, 2015, p. 53; Carter, 2018, p. 157; Merkl & Weinberg, 2003, p. 3). Right-wing extremism can be considered as an umbrella for a variety of beliefs and ideologies such as anti-government, white supremacist movements, nationalism or xenophobia (Kurzman, Kamal & Yazdiha, 2017, p. 1; Merkl & Weinberg, 2003, p. 5). Essentially, the right believe that existing inequalities are natural and cannot and should not be eradicated (Carter, 2018, p. 161).

Given that the concept of "right-wing extremism" exists within the "right" span of politics, it is a difficult concept to define. Additionally, it is a highly contested concept as it entails a variety of actors and beliefs whilst ranging from political parties to militant or terrorist groups (Ravndal, 2018, p. 847). According to Carter (2018, p. 174) it at least includes a sense of anti-democracy, authoritarianism and holistic nationalism. Moreover, Merkl and Weinberg (2003, p. 4) explain that right-wing supporters favour regimes that are identifiable with those of Mussolini, Hitler or Franco.

In the first half of the twentieth century hostilities generated by immigration played a minor role in the development of national socialism (Merkl, 2003, p. 25). Today, however, the current rise of right-wing extremism can to a large extent be explained through the ongoing migration crisis which fuels fear, uncertainty and polarisation amongst European countries (Merkl, 2003, p. 25; NCTV, 2018, p. 9; Ravndal, 2018, p. 862).

The terrorist threat of right-wing extremism is not as evident in public and politics than its jihadist variant. Europol, for example, estimated the threat of right-wing extremism to be low for several years based on data obtained through a variety of national police systems (NCTV, 2018, p. 13). Koehler

(2016) contrarily expresses that there has been a significant increase in right-wing extremism and terrorism in Western-Europe. Moreover, the 2020 Munich Security Report ranked right-wing extremism as a top global security threat.[28] Since 9/11, more people in the United States have been killed through right-wing extremism than jihadist extremism.[29] Moreover, the Centre for Strategic and International Studies reported that far-right groups are not only considered "the most persistent and lethal threat in the US" but also committed the majority of the terrorist attacks in 2020.[30] Bouhana, Corner, Gill and Schuurman (2018, p. 150) express that the threat of right-wing extremism largely exists in the amount of lone-actor terrorism. The 2020 Munich Security Report also warns for other signals that may add to the threat of right-wing extremism. They, for example, increasingly connect online through both mainstream platforms such as Facebook as well as fringe platforms like Discord and 8chan.[31]

Van Dongen (2020) is opinionated that right-wing extremism cannot be considered the "next wave of terrorism" as they lack organisational capacities to sustain such a wave. He argues, for example, that it is not possible to speak of "one" movement, as it encompasses many different beliefs and actors as suggested earlier (Van Dongen, 2020, p. 103). Moreover, right-wing extremists lack a space where they can mobilise and train. So far, right-wing extremism has been the work of isolated groups, cells or lone actors (Bouhana, Corner, Gill & Schuurman, 2018, p. 151; Van Dongen, 2020, p. 104). The Dutch General Intelligence and Security Service (Dutch: Algemene Inlichtingen- en Veiligheidsdienst, henceforth: AIVD), however, explains that groups are increasingly becoming less important within right-wing extremism and that this fluidity makes them unpredictable and dangerous (AIVD, 2018, p. 12). A second reason mentioned is the preferred tactics executed by right-wing extremists. These typically tend to be non-violent and more oriented towards influence through political parties (Van Dongen, 2020, p. 109). They, thus, use political parties to their advantage by adding to the political mainstream and influencing the agenda. Unfortunately, violent tactics are executed. Examples of these were the shootings of Anders Breivik (Norway, 2011) and Brenton Tarrant (Christchurch, 2019). As Bouhana, Corner, Gill and Schuurman (2018) explain, these are examples of lone actor terrorists who do execute their attacks to convey a message. Responsibility of any overarching group is never claimed however (Koehler, 2016, p. 98; Van Dongen, 2020, p. 112). Koehler (2016, p. 98) mentions that this

[28] Munich Security Conference. (2020). Munich Security Report 2020. Retrieved on December 15th, 2020 from: https://securityconference.org/assets/user_upload/MunichSecurityReport2020.pdf
[29] *Ibid.*
[30] Gross, J. (2020, October 24th). Far-Right Groups Are Behind Most U.S. Terrorist Attacks, Report Finds. *The New York Times.* Retrieved on December 15th, 2020 from: https://www.nytimes.com/2020/10/24/us/domestic-terrorist-groups.html
[31] Video: Nieuwsuur. (2019, May 17th). Hoe wordt rechts-extremisme verspreid? En wat kunnen we eraan doen? Retrieved on December 15th, 2020 from: https://www.youtube.com/watch?v=jIg1Yt7UpXA&feature=youtu.be
Munich Security Conference. (2020). Munich Security Report 2020. Retrieved on December 15th, 2020 from: https://securityconference.org/assets/user_upload/MunichSecurityReport2020.pdf

indicates that right-wing terrorists perceive their message and action as self-explanatory which could inherently raise the danger of the intent and nature of attacks.

I.I. Right-wing terrorist threat in the Netherlands

In the Netherlands, the Dutch Peoples-Union (Dutch: Nederlandse Volks-Unie) was the first political party which expressed its hatred against migrants whilst maintaining an anti-Jew attitude and neo-Nazist ideas (NCTV, 2018, p. 10). Alongside, several extreme-right parties and groups developed similar ideas. None of these, however, gained any influence in Dutch politics (NCTV, 2018, p. 10). Racist violence has always been presence in the Netherlands but were to a lesser extent categorised as right-wing extremism. Moreover, the Dutch government and law enforcement never closely monitored such groups up until 1996 and attacks and incidents that did occur could never directly be linked to right-wing extremist groups (NCTV, 2018, p. 11). In the first half of the twenty-first century, violence related to right-wing extremism decreased (NCTV, 2018, p. 11). Right-wing extremism was less evident within security and intelligence organisations because it was dominated by jihadist and Islamist terrorism (NCTV, 2018, p. 5). Earlier mentioned attacks by lone actors did however call for a more thorough analysis of right-wing extremism. In the Netherlands, incidents where right-extremism is at the basis have increased with the limitation that identification of perpetrators within this context was complex as the right-wing intent never became evident (NCTV, 2018, p. 15).

The AIVD showed that right-wing extremism goes along with the topical societal and political debate. Incidents decreased when the debate on immigration decreased but increased when the debate of the Dutch "Zwarte Piet" started (AIVD, 2018, p. 19). Continuing, the AIVD beliefs that right-wing extremism in the Netherlands will grow with the societal debate and the ongoing polarisation that might result from it. A similar situation is mentioned by R5, an expert on right-wing extremism:

"Currently, we are witnessing that people find themselves in their anti-government sentiment. COVID-19 and the precautions towards it is the common denominator in this case as there is a large group that is against this. On the other hand, the presence of right-wing extremism is limited. There was, for example, no connection with right-wing extremists or groups during the riots that followed the curfew in the Netherlands. Similarly, demonstrations that got out of hand were a result of hooligans and not of people affiliated with right-wing extremism."

Internationally, right-wing extremism occurs more visibly as became evident in Norway (2011) and Christchurch (2019). More recently, the attack on the US Capitol raised questions about

domestic terrorism, white supremacists and right-wing nativists.[32] When asked about the influence of such events on the Netherlands, R5 explained the following:

"The influence of the storming of the US Capitol initiated some commotion amongst Dutch groups but on a very small scale. Individuals do express themselves online and call for action, but this does not occur in practice. In the States, for example, the Proud Boys had a large role in the attack on the Capitol. In the Netherlands, we occasionally see a Proud Boys-flag during a demonstration but that's it. Dutch groups are thus not very affected by international events."

I.II. Right-wing extremism and social media

As mentioned earlier in this chapter, right-wing extremist more increasingly meet and mobilize through online platforms. The Christchurch-attacks in 2019 proved to be the most evident of this as the attacker livestreamed his attack (AIVD, 2020, p. 17). This also initiated copycat behaviour which was stimulated through social media (AIVD, 2020, p. 17). Social media is used to invite individuals to closed networks with more extreme content which can initiate radicalisation (AIVD, 2018, p. 11; 2020, p. 17). Social media platforms such as Vkontakte, WhatsApp, Telegram, Discord and 8chan are especially popular amongst sympathizers of right-wing extremism (AIVD, 2018, p. 11).[33] This is also recognised by R5.

"Right-wing extremism in the Netherlands predominantly occurs online. Online, people say a lot of big things but this is not in accordance with physical activities that you see and would expect. Terrorist attacks never occur in the Netherlands with a right-wing extremist intent. What we do see is a certain amount of activism, during demonstrations in the Hague for example. The capacity to organise right-wing extremism is therefore limited in the Netherlands."

II. Gathering information in practice

The main question to be asked by intelligence officers is to what extent information is *nice* to have or is strictly *necessary*. The latter chapter concluded that there is a lack of judicial regulation concerning information-gathering for police employees which leaves this question unanswered. It became evident that principles such as proportionality and necessity are most important to clarify as these define the scope in which officers can function.

Is information about individuals associated with right-wing extremism nice to have or is it necessary to have? Conform the definition of the European Union Agency for Fundamental Rights and Council of Europe (2018, p. 40) and Article 8(2) of the ECHR, it is necessary to have as it serves the pressing and serious social issue of national security and the fight against terrorism. The ECHR defines

[32] Gaouette, N. (2021, January 16th). Terrifying scope of Capital attack becoming clearer as Washington locks down for Biden's inauguration. *CNN*. Retrieved on February 6th, 2021 from: https://edition.cnn.com/2021/01/16/politics/insurrection-investigation-washington-lockdown/index.html

[33] Video: Nieuwsuur. (2019, May 17th). Hoe wordt rechts-extremisme verspreid? En wat kunnen we eraan doen? Retrieved on December 15th, 2020 from: https://www.youtube.com/watch?v=jIg1Yt7UpXA&feature=youtu.be

"necessity" as "… the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued" (European Union Agency for Fundamental Rights & Council of Europe, 2018, p. 42). The definition already touches upon the second principle, proportionality. Proportionality is explained as "acts … be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives" (European Data Protection Supervisor, 2017, p. 5). Proportionality is thus fact-based and case-dependent and encompasses necessity. This implies that allthough storing information about an association with right-wing extremism might be necessary to national security, the measure to gather information online might not be proportional as a mere association remains vague, general and unsupported by facts as there has not been an actual conviction. The "pressing social need", read: necessity, is therefore undermined as well and information then becomes merely "nice to have".

Principles such as necessity and proportionality are easily intertwined but should, according to the European Data Protection Supervisor (2017, p. 5) be strictly separated. Necessity is a pre-condition to proportionality and in general, it is common to first assess the necessity of a measure before its proportionality is assessed (European Data Protection Supervisor, 2017, p. 6; 2019, p. 10). Moreover, the European Data Protection Supervisor (2017) presents the following steps in assessing necessity:

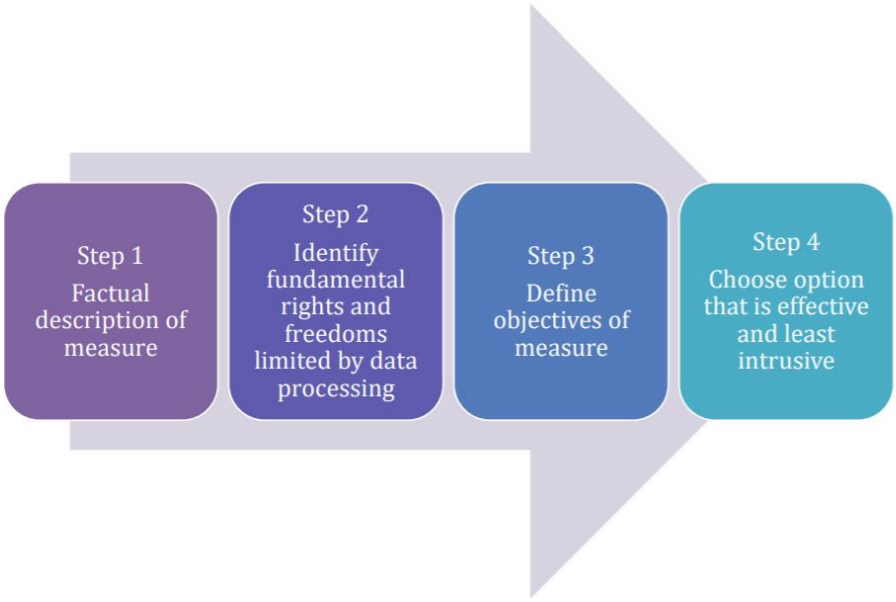

Figure 4: Steps in assessing necessity. Source: European Data Protection Supervisor (2017, p. 9)

In summary, it explains how the measure should be described in detail before starting the assessment of necessity. Secondly, the laws that limit the measure should be identified, e.g. rights concerning privacy, before defining the objectives of the measure against which the necessity is assessed. Finally, the option should be chosen that is most effective with the least intrustion (European Data Protection Supervisor, 2017, p. 9). That information should be gathered about right-wing

extremism is generally not up for debate as it is important to protect national security and maintain public order. It is, however, still important that a proper review is conducted as it not only illuminates on the importance of the issue itself but also serves as a prerequisite for assessing proportionality that may even be more important in this case.

A similar approach is taken to, subsequentely, test proportionality. Generally, a test of proportionality can only be executed if the principle of necessity is met. According to the European Data Protection Supervisor (2019, p. 10), a proportionality assessment involves defining what safeguards should accompany the measure in order to reduce the risk of excessive intrustion. It is formulated as followed:

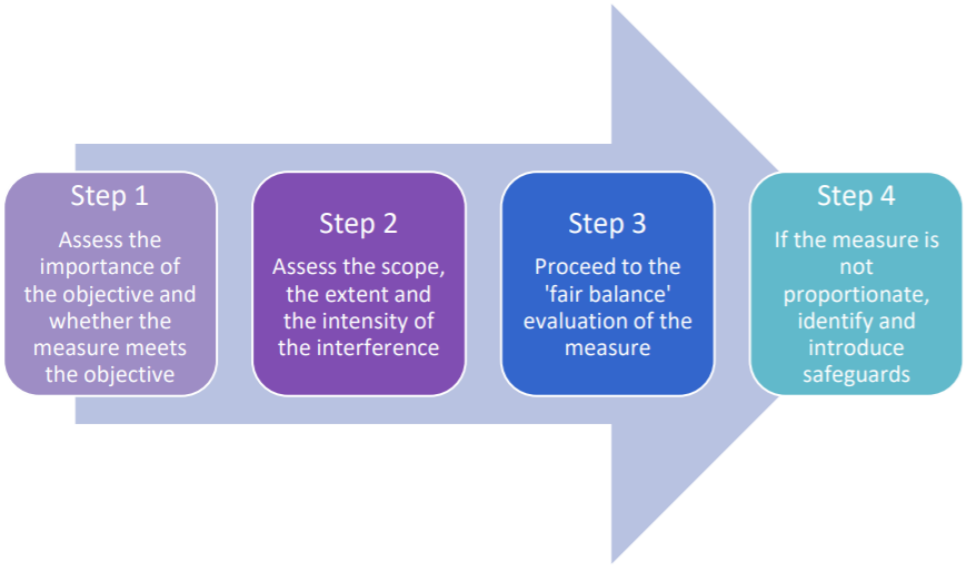

Figure 5: Steps in assessing proportionality. Source: European Data Protection Supervisor (2019, p. 14)

The primary step assesses the importance of the measure that has been identified under Step 3 of the Necessity Toolkit and to what extent the proposed measure meets the objective and addresses the identified issue. Secondly, the scope, extent and intensity of the measure – which has been defined under Step 2 of the Necessity Toolkit – is identified regarding the impact it has on rights to privacy and personal data protection. Step 3 proceeds to the "fair balance" evaluation of the measure. Such a fair balance could consist of a tradeoff between benefits/costs or advantages/disadvantages. Finally, a go/no go is decided and safeguards are introduced if necessary (European Data Protection Supervisor, 2019, p. 13-14).

Measures intented to gathering information about right-wing extremism in an online environment can quickly lead to privacy breaches as it concerns personal data about a subject. Assessing the proportionality of the measure is thus an important step for justification. If this is not met, the information cannot serve as evidence in a future criminal investigation.[34] An important step is defining

[34] Interview R5

the specific information that is needed in the case of right-wing extremism as this alters proportionality continuously. This also goes for the social media channels that need to be monitored.

Combining the two toolkits will look as followed:

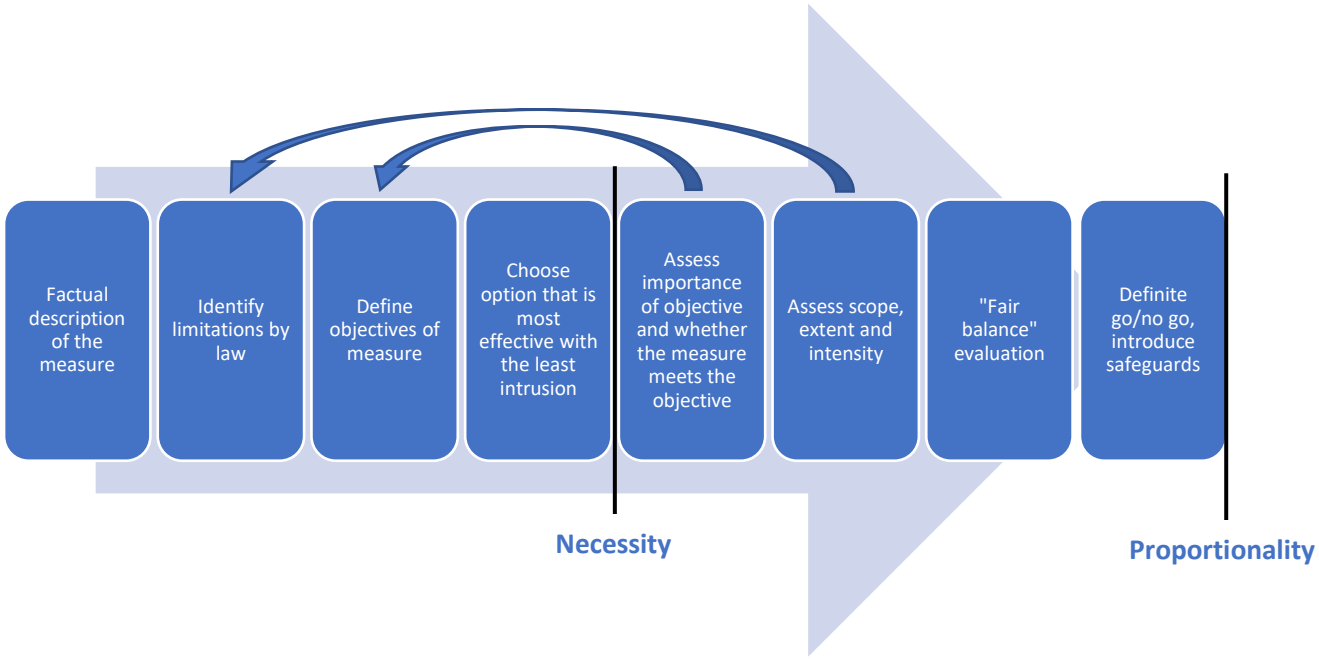

Figure 6: Necessity and Proportionality Toolkit

As learned from R3, the police already works with a toolkit and certain criteria to assess the privacy breach and, hence, the necessity and proportionality of a means. Combining the existing framework with the steps mentioned above could however result in the most extensive toolkit possible as it takes into account legislation mentioned in the previous chapter. Moreover, it allows for a clear distinction between information that is "nice-to-have" and "need-to-have" given that the assessment could work for both. Assessing necessity and proportionality in the case of information that is "nice-to-have" allows for properly defining the issue, the measure, the objective and also formulates safeguards to uphold these. Information that is merely "nice-to-have" than becomes valuable to the extent that is might be necessary to have. Applying this assessment similarly to information that is necessary to have also allows for the most justifiable tools and safeguards.

The role of these safeguards can thus be very important as they improve proportionality and, thus, need to be considered carefully. An example is adding a systematical aspect to surveillance, as is similar in the investigation branch of policing, would safeguard the proportionality of a measure in the case of right-wing extremism. A systematic approach to surveilling right-wing extremism could then imply a limitation to specific social media channels, groups, individuals or activities. One could then carefully suggest that systematic observation as is common in criminal investigations, could also exist in the information-branch as it upholds necessity and proportionality.

Another additional step that could be taken occurs at the forefront concerns the description of the social issue for which the measure is meant which needs to be defined clearly and detailed. Understanding the issue that needs to be tackled offers more insight into the necessity and proportionality of the measure before the assessment has commenced and, again, allows for a clear distinction between "nice-to-have" and "need-to-have".

III. Social media analysis

As mentioned in the **Theoretical framework** and by multiple academics, the analysis of social media information and its validation remains challenging due to a lack of technological tools and its combination in human behaviour sciences. This study does not have the capacity to engage in social media analysis but this chapter does present the most dominant methods as described in academic literature, these could be used in practice by intelligence officers.

Andrews, Brewster and Day (2016) introduce "formal concept analysis" (FCA) in the case study of weak signals of organised crime on social media. The authors have provided an extensive taxonomy of organised crime and its concepts. They argue that one single message containing such a weak signal does not necessarily imply its meaningfulness to police authorities. Similar multiple messages can be meaningful (Andrews, Brewster & Day, 2016, p. 144). The corroboration of these messages containing weak signals can be automated by FCA which clusters these messages, with one attribute being the location of the message and the other being the crime or an element of it (Andrews, Brewster & Day, 2016, p. 144). Prior to this, one must engage in social media scanning which consists of crawling, categorisation, filtering and fact extraction which ultimately results in structured data output (Andrews, Brewster & Day, 2016, p. 144). The final output is a formal concept tree in which it becomes clear how many messages (Tweets for example) originate from a single location (city) and contain weak signals of a crime (human trafficking) (Andrews, Brewster & Day, 2016, p. 145). A possible next step within FCA is a "drill-down" in which analysts will further disseminate messages into earlier established concepts relating to the crime or the location (Andrews, Brewster & Day, 2016, p. 146).

Antonius and Rich (2013) differentiate between a preliminary analysis and a targeted analysis where facets of social network analysis (SNA) are also employed. A preliminary analysis refers to outlining the scope of the social media content, e.g. how many accounts are active, how many followers do groups have, a timeline of posts, types of posts, etc. (Antonius & Rich, 2013, p. 48). A targeted approach uses specialised analytical tools to generate a deeper insight into the sampled population (Antonius & Rich, 2013, p. 49). Social network analysis tools, for example, can group accounts together and visualise their connection. Geospatial tools can, for example, reveal important geographical information. SNA can be used to characterise criminal organisations, the operation of illicit markets and links and relationships between individuals or groups of interest to the police (Bright, Hughes & Chalmers, 2011). SNA includes data collection from a variety of sources, including open sources. Krebs

(2002) used media reports to calculate degree, betweenness and closeness centrality to create a network map of the terrorist group involved and organising the 9/11-attacks.

Another approach to social media analysis is sentiment analysis which shifts away from the statistical analysis of texts and focuses on sentiments and opinions on a specific topic (Lyu & Kim, 2016, p. 942). Essentially, a sentiment dictionary is created which maps words to sentiment (Lyu & Kim, 2016, p. 942). In order to account for multiple sentiments, given that everyone's emotion to a topic is different, two approaches are presented. Firstly, scores are assigned to represent the sentiments of words from different facets such as gender, age, race, culture, levels of education, etc. The average of these scores is determined to construct norms (Lyu & Kim, 2016, p. 942). A second approach expands the sematic relation of words by assigning "seed words" from which the dictionary is expanded with other words that have a relation with these seed words (Lyu & Kim, 2016, p. 942). An important step of sentiment analysis is the sentiment weight which is expressed by "pointwise mutual information". This calculates the association between two random variables, e.g. a word and a seed word (Lyu & Kim, 2016, p. 942). What is challenging about this analysis is that it is time-consuming and that it is impossible to expand from words which are not in the sentiment dictionary. Moreover, the seed words have a major impact on the determination of the sentiment and must be chosen carefully (Lyu & Kim, 2016, p. 943).

CONCLUSION

This chapter outlines the most important results of the analysis. This is followed by a discussion where the results are interpreted and related to the existing body of knowledge. Finally, limitations of this study as well as possible avenues for future research are addressed here as well.

I. Conclusion

The aim of this thesis was to lay down the current unclarity that exists around using OSINF and OSINT for intelligence officers in intelligence-led policing. The case of right-wing extremism and their use of social media was used to make this more apprehendable. In doing so, this study took both a descriptive and explorative approach. On the one hand, it described the current judicial framework concerning data gathering and relevant privacy legislation by doing a document analysis. On the other hand, this study explored the use of OSINT in practice by conducting interviews and explored the potential of using information by means of existing toolkits of assessing principles such as proportionality and necessity.

It is now possible to answer the main research question: *To what extent does the Regional Intelligence Department of the Police Unit The Hague have the ability to employ open-source information as a means in their intelligence-led policing towards digital meeting places of right-wing extremism whilst adhering to the boundaries of surveillance and entrapment?* The answer to this question is as clear as it is vague. Generally, the boundaries for using open-source information is clear in that these are non-existent. Contrary to the judicial body built around criminal investigations, the information-gathering branch of policing does not have access to such a judicial framework that lays down special investigative powers. The basis of their operation is built upon Article 3 PolW that explains the general policing tasks and can be interpreted in the broadest way possible.

At first instance, this is a clear answer to the proposed research question but embeds more vagueness than it does clarity. Given that there is no judicial framework similar to criminal investigations using open-source information, it becomes unclear how intelligence officer ought to function. Surveillance, for example, is only vaguely allowed if there is a certain presumption and permission from the public prosecutor. An appeal is made on the discretionary powers that police officers have regarding asking for this permission or acting on an officer's own presumption as no guideline specifically mentions when one or the other should be performed. Entrapment, on the other hand, cannot occur in intelligence-led policing as research is bound to be passive rather than that officers actively engage in platforms with individuals.

The general answer, and what is also witnessed in practice, is that anything is allowed as long as it complies with essential articles of the Police Directive and various European legislations. An excessive breach of privacy is, for example, only allowed when proportional and necessary. Under these circumstances, information-gathering is allowed. Given that proportionality and necessity are amongst the most difficult concepts to define, what can and cannot be done remains to be unclear. What makes

it all the more complex is the ambiguity that exists around the concept of "open-source information". Interviews showed that different approaches exist towards this concept and assessing necessity and proportionality is therefore difficult as it lacks the foundation of a clear starting concept.

The twofold answer to the central research question also shows that cases like right-wing extremism cannot be as easily researched as initially thought. Distinguishing between "nice-to-have" and "need-to-have" depends on how necessity and proportionality are assessed and **The case: right-wing extremism** concluded that these two concepts could clash when judging this from a security point-of-view: while information about such a case might be necessary to guarantee national security, it may not be proportional due to the vagueness that exists in this topic as well. Therefore, a proper assessment of proportionality and necessity is even more vital when analysing from a security-perspective.

II. Discussion

This study is a first attempt in exploring the use of open-source information before a suspicion or an investigation. It was built around a theoretical framework which focused mainly on the role of information and intelligence in security and on the dominant policing method: intelligence-led policing. As seen in the **Theoretical framework**, the role of information is important in preventing serious crime and to uphold national security. One could thus argue that intelligence-led policing is built around information that is nice-to-have and just-in-case. As found later in the study, it is precisely this attitude towards information that makes it difficult to actually engage in intelligence-led policing as it undermines principles of necessity and proportionality. This can partially be explained by the approach towards ILP as a whole which is more business-like rather than an operational policing method as is the case with problem-oriented policing and community policing. Assessing necessity and proportionality according to the tests of the European Data Protection Supervisor (2017, 2019) has the possibility to decrease this limitation and let intelligence-led policing function to its true potential of providing for a safe society. It could, however, also be argued that the difficulty does not necessarily lies with the assessment of legal principles and the interpretation of laws but with the phenomena of intelligence-led policing and how it is embedded in a policing organisation. As mentioned, the role of information is important but ought to be distinguished between information that is nice-to-have and necessary-to-have. If such a distinction is made, ILP as a policing method could be implemented and exercised in a way that decreases the broad interpretability of the method. Additionally, the current conceptual discussion of "open-source information" and SOCMINT remain a challenge as it increases further unclarity about what is and what is not allowed.

The conclusion showed that the answer to the central research question mainly exists in a legal, security and conceptual scope. Legal because a judicial framework lacks which further increases difficulties for intelligence officers. Security because the objective of this questions exists in national security and public order. Conceptual because it involves legal principles such as necessity,

proportionality, intelligence-led policing and open-source information. This study, however, also exists in an administrative and political context in which the "driehoek" – consisting of the municipality, the police and the public prosecutor – plays a large role. Interpreting this question from this perspective, the answer would differ from what this study originally found namely that the relationships between these vital actors limit intelligence officers to use open-source information. Currently, the public prosecutor has a large role in assessing necessity and proportionality while this should, officially, be a task of the mayor. The assessment of necessity and proportionality is thus differently approached than it should be which could have implications for the work of intelligence officers and intelligence-led policing as a whole. Questions could be asked about the desirability of this.

II.I. Recommendations

The recommendations derived from this study are twofold. Firstly, recommendations are made towards the academic world. Secondly, this study provides practical recommendations which are in the interest of the DRIO.

From an academic perspective, this is the first research presented on this topic. The role of the municipality and the mayor remain underexposed and serve as an interesting starting-point for future research. Researching the relationship between the municipality, the police and the public prosecutor within maintaining public order could deepen this study from a political and administrative perspective which is also necessary for the proper functioning of intelligence officers and public prosecutors. Another interesting follow-up research concerns the application of this to a different case. The case of right-extremism proved to be challenging because the topic itself is approached very differently in comparison to other security topics. The application to cases that do not require a different approach could make this topic more comprehensible. Such a case is also less prone to classified information as is oftentimes the case with terrorism.

On a practical level, it is most important that the police organisation finalise discussions before assessing the practicality of this study. One example is the definition of open-source information. The interviews concluded that there are various definitions of this concept that confuse the operationality of it. SOCMINT, for example, is a concept that is yet to be fully implemented by the DRIO and distinguishing OSINT from SOCMINT could be important to properly design interferences and analyses. From a legal perspective, open sources from online environments and offline environments occur in different legislative documents which make a proper distinction important as well. Consequently, the **Theoretical framework** explained that the intelligence cycle is most common as an analysis method. However, analysing social media content is of another calibre as it concerns large amounts of information which are often free interpretable. Assessing social media analysis methods as mentioned in the case analysis could improve SOCMINT and could possibly improve assessments of objectives, measures, proportionality and necessity. Similarly, the principles of intelligence-led policing

also need further clarification as the nice-to-have attitude towards information poses challenges towards intelligence officers. A revision of ILP and how it should be implemented to engage in functional information gathering is thus necessary. Finalising such discussions is an important first step in resolving unclarity about the use of open-source intelligence in intelligence-led policing. Another recommendation concerns starting conversations with the municipality and the mayor as these seem to be non-existent at the moment. Considering that the mayor is responsible for public order, these conversations are important for effective law enforcement. Finally, the researcher encourages police officers to apply this study with classified documents that are of interest to this topic, the *Limitations* will elaborate on these. Given the current position of the researcher within the DRIO, it is the intent to continue with this research with said documents. This way, the approach and outcome of this study can be made more applicable in the daily functioning of the DRIO and enhance information-gathering and creating intelligence in the pre-crime society.

II.II. Limitations

While the data and conclusions presented in this thesis have been derived from academic literature, document analysis and an interview, the reliability of it is impacted by a variety of issues. These will be addressed hereafter for the reader to correctly assess the conclusions and results that have been drawn from this study.

The **Methodology** outlined the use of publicly accessible information to answer this research question. To the largest extent, it was possible to answer the research question properly with information derived from publicly accessible information. There are, however, two instances in which the use of classified information could have further elaborated on the issue of this study and deepened the conclusion. Firstly, R3 mentioned the existence of a matrix which has been drafted by police officers and public prosecutors. This matrix outlines the possibilities for information-gathering by intelligence officers by defining certain criteria amongst which are proportionality, subsidiarity and necessity. Access to this matrix could have provided better insight into the functioning of ILP within the DRIO, their assessment of necessity and proportionality, other criteria upon which a measure is designed and decided upon and the differences they make in different online platforms and sources. The existence of this matrix has been taken into account when conducting this research. Another example is the counter-terrorism approach of the Dutch police which is not publicly accessible. This is, as was mentioned by R5, a very different approach to information-gathering compared to other security topics within the DRIO. The case, therefore, remained to have a more academical approach than a practical approach. Especially in combination with the above-mentioned matrix, this could have been used in the case study and would have provided a deepened insight into ILP, the legal framework and proportionality and necessity assessments.

A second limitation concerns the interviews. The researcher was able to conduct interviews with relevant and professional experts on the field of this topic. Given that the municipality and the mayor also have a role in this issue, an interview with a relevant stakeholder from this branch would have offered a nice completion to the other respondents. Efforts that were made remained unanswered unfortunately, therefore limiting the relevant information on this topic.

All in all, the limitations do not severely impact the outcome of this research to the extent where its conclusion. Contrarily, as mentioned in *Recommendations,* they offer opportunities for both academics and practitioners to engage in future research on this topic or improve the practicality of this one in order to engage in the most effective and legitimate crime control.

BIBLIOGRAPHY

AIVD. (2018). *Rechts-extremisme in Nederland: Een fenomeen in beweging.* Algemene Inlichtingen- en Veiligheidsdienst. Den Haag. Retrieved on from:

AIVD. (2020). *AIVD jaarverslag 2019.* Algemene Inlichtingen- en Veiligheidsdienst. Den Haag. Retrieved on from: https://www.aivd.nl/documenten/jaarverslagen/2020/04/29/jaarverslag-2019

Akram, M. S. & Albalawi, W. (2016). Youth's Social Media Adoption: Theoretical Model and Empirical Evidence. *International Journal of Business and Management, 11*(2), 22-30.

Andrews, S., Brewster, B. & Day, T. (2016). *Organised Crime and Social Media: Detecting and Corroborating Weak Signals of Human Trafficking Online.* ICCS. Annecy, France. Retrieved on from:

Antonius, N. & Rich, L. (2013). Discovering collection and analysis techniques for social media to improve public safety. *The International Technology Management Review, 3*(1), 42.

Autoriteit Persoonsgegevens. (n.d.). *Politie. Autoriteit Persoonsgegevens.* Retrieved on from https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/politie-justitie/politie

Bakker, E. (2015). *Terrorism and Counterterrorism Studies: Comparing Theory and Practice*. Leiden, The Netherlands: Leiden University Press.

Best, R. A. & Cumming, A. (2007). *Open Source Intelligence (OSINT): Issues for Congress.* Congressional Research Service. Retrieved on from:

Bishop, J. (2014). Digital Teens and the 'Antisocial Network': Prevalence of Troublesome Online Youth Groups and Internet trolling in Great Britain. *International Journal of E-Politics, 5*(3), 1-15.

Blank, G. & Reisdorf, B. C. (2012). THE PARTICIPATORY WEB: A user perspective on Web 2.0. *Information, communication & society, 15*(4), 537-554.

Boudana, S. & Segev, E. (2017). Theorizing Provocation Narratives as Communication Strategies. *Communication theory, 27*(4), 329-346.

Bouhana, N., Corner, E., Gill, P. & Schuurman, B. W. (2018). Background and preparatory behaviours of right-wing extremist lone actors: a comparative study. *https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2018/issue-6/a10-bouhana-et-al.pdf*.

Bowen, G. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal, 9*, 27-40.

Bright, D. A., Hughes, C. E. & Chalmers, J. (2011). Illuminating dark networks: a social network analysis of an Australian drug trafficking syndicate. *Crime, law, and social change, 57*(2), 151-176.

Brodeur, J.-P. (2007). High and Low Policing in Post-9/11 Times. *Policing: A Journal of Policy and Practice, 1*(1), 25-37. Retrieved from https://doi.org/10.1093/police/pam002

Burcher, M. & Whelan, C. (2019). Intelligence-Led Policing in Practice: Reflections From Intelligence Analysts. *Police quarterly*, *22*(2), 139-160.

Calatayud, M. M. & Vázquez, A. S. (2018). Mobilisation and surveillance on social media. In L. Melgaço & J. Monaghan (Eds.), *Protests in the information age: Social movements, digital practices and surveillance*. London: Routledge.

Calder, B. J., Phillips, L. W. & Tybout, A. M. (1982). The concept of external validity. *Journal of consumer research*, *9*(3), 240-244.

Carter, D. L. & Carter, J. G. (2009). Intelligence-Led Policing:Conceptual and Functional Considerations for Public Policy. *Criminal Justice Policy Review*, *20*(3), 310-325. Retrieved from https://journals.sagepub.com/doi/abs/10.1177/0887403408327381

Carter, E. (2018). Right-wing extremism/radicalism: reconstructing the concept. *Journal of Political Ideologies*, *23*(2), 157-182. Retrieved from https://doi.org/10.1080/13569317.2018.1451227

Colleen, M. (2007). *Data Mining and Predictive Analysis : Intelligence Gathering and Crime Analysis*. Amsterdam: Butterworth-Heinemann.

Cope, N. (2004). 'INTELLIGENCE LED POLICING OR POLICING LED INTELLIGENCE?': Integrating Volume Crime Analysis into Policing. *British Journal of Criminology*, *44*(2), 188-203.

Custers, B. (2018). Nieuwe online opsporingsbevoegdheden en het recht op privacy. *Justitiële Verkenningen*, *5*, 100-117.

Custers, B. H. M., van der Hof, S. & Schermer, B. (2014). Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies: Privacy Expectations of Social Media Users. *Policy and internet*, *6*(3), 268-295.

Convention on Cybercrime (ETS 185), 185 C.F.R. (2001). Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561

Guidance Notes: Transborder Access (Article 32), (2014). Retrieved from https://www.coe.int/en/web/cybercrime/guidance-notes

Eijkman, Q. A. M. & Weggemans, D. (2013). Open Source Intelligence and Privacy Dilemmas: Is it Time to Reassess State Accountability? *Security and Human Rights*, *23*(4), 285-296.

European Commission. (n.d.). *Gegevensbescherming in de EU*. Retrieved on from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_nl

European Convention on Human Rights, (2010). Retrieved from https://www.echr.coe.int/documents/convention_eng.pdf

European Data Protection Supervisor. (2017). *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*. European Data Protection Supervisor. Retrieved on from: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf

European Data Protection Supervisor. (2019). *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data.* European Data Protection Supervisor. Retrieved on from: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

General Data Protection Regulation, (2016). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=NL

Charter of Fundamental Rights of the European Union, (2012). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN

European Union Agency for Fundamental Rights & Council of Europe. (2018). *Handbook on European data protection law.* European Union Agency for Fundamental Rights

Council of Europe. Luxembourg. Retrieved on from:

Europol. (2020). *Internet Organised Crime Threat Assessment (IOCTA) 2020*. Retrieved from https://www.europol.europa.eu/iocta-report

Franken, S. (2017). De Wpg. In M. Den Hengst, T. ten Brink, & J. ter Mors (Eds.), *Informatiegestuurd politiewerk in de praktijk* (pp. 65-86). Deventer: Vakmedianet.

Fyfe, N. R., Gundhus, H. O. I. & Rønn, K. V. (2018). *Moral Issues in Intelligence-led Policing*. Abingdon, England: Routledge.

Gaouette, N. (2021). *Terrifying scope of Capitol attack becoming clearer as Washington locks down for Biden's inauguration*. *CNN*. Retrieved on from https://edition.cnn.com/2021/01/16/politics/insurrection-investigation-washington-lockdown/index.html

Garland, D. (1996). The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society. *The British Journal of Criminology, 36*(4), 445-471.

Gibson, H. (2017). Acquisition and Preparation of Data for OSINT Investigations. In B. Akhgar, P. Bayerl, & F. Sampson (Eds.), *Open Source Intelligence Investigations: From Strategy to Implementation*: Springer.

Gill, P., Stewart, K., Treasure, E. & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *Br Dent J, 204*(6), 291-295.

Glassman, M. & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior, 28*(2), 673-682. Retrieved from http://www.sciencedirect.com/science/article/pii/S0747563211002585

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report, 8*(4), 597-607.

Goldstein, H. (1979). Improving Policing: A Problem-Oriented Approach. *Crime and delinquency, 25*(2), 236-258.

Gray, D. & Henderson, S. E. (2017). Introduction. In D. Gray & S. E. Henderson (Eds.), *The Cambridge Handbook of Surveillance Law* (pp. xvi-4). Cambridge: Cambridge University Press.

Grommé, F. (2016). Provocation: Technology, resistance and surveillance in public space. *Environment and planning. D, Society & space, 34*(6), 1007-1024.

Gross, J. (2020, January 20th, 2021). *Far-Right Groups Are Behind Most U.S. Terrorist Attacks, Report Finds. The New York Times.* Retrieved on from https://www.nytimes.com/2020/10/24/us/domestic-terrorist-groups.html

Haggerty, K. D. (2012). Surveillance, crime and the police. *Routledge handbook of surveillance studies*, 236-243.

Innes, M., Fielding, N. & Cope, N. (2005). 'The Appliance of Science?': The Theory and Practice of Crime Intelligence Analysis1. *The British Journal of Criminology, 45*(1), 39-57. Retrieved from https://doi.org/10.1093/bjc/azh053

Kahn, D. (2001). An historical theory of intelligence. *Intelligence and National Security, 16*(3), 79-92.

Kietzmann, J., Hermkens, K., McCarthy, I. & Silvestre, B. (2011a). Social Media? Get Serious! Understanding the Functional Building Blocks of Social Media. *Business Horizons, 54*, 241-251.

Kietzmann, J. H., Hermkens, K., McCarthy, I. P. & Silvestre, B. S. (2011b). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons, 54*(3), 241-251. Retrieved from http://www.sciencedirect.com/science/article/pii/S0007681311000061

Koehler, D. (2016). Right-wing extremism and terrorism in Europe, current developments and issues for the future. *Prism, 6*(2).

Koops, E. J. (2012). Politieonderzoek in open bronnen op het internet. Strafvordelijke aspecten. *Tijdschrift voor Veiligheid, 11*(2), 30-46.

Kop, N. & Klerks, P. (2009). *Doctrine intelligencegestuurd politiewerk.* Politieacademie: Lectoraat Recherchekunde Apeldoorn. Retrieved on from: https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/72506.pdf

Krebs, V. (2002). Mapping Networks of Terrorist Cells. *24*.

Kurzman, C., Kamal, A. & Yazdiha, H. (2017). Ideology and Threat Assessment: Law Enforcement Evaluation of Muslim and Right-Wing Extremism. *Socius: Sociological Research for a Dynamic World, 3*.

Lassche, H. (2019). *Digitalisering en de opsporingspraktijk.* Politieacademie. Apeldoorn. Retrieved on from: https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/90036.PDF

Lefebvre, S. (2003). The Difficulties and Dilemmas of International Intelligence Cooperation. *International Journal of Intelligence and CounterIntelligence, 16*(4), 527-542.

Lijphart, A. (1971). Comparative Politics and the Comparative Method. *Am Polit Sci Rev, 65*(3), 682-693.

Lowenthal, M. M. & Clark, R. M. (2016). *The Five Disciplines of Intelligence Collection*. Los Angeles: Sage.

Lyu, K. & Kim, H. (2016). Sentiment Analysis Using Word Polarity of Social Media. *Wireless personal communications, 89*(3), 941-958.

Marx, G. T. (2015). Surveillance Studies. *International Encyclopedia of the Social & Behavioral Sciences, 23*(2), 733-741.

Marzell, L. (2016). OSINT as Part of the Strategic National Security Landscape. In B. Akhgar, P. Bayerl, & F. Sampson (Eds.), *Open Source Intelligence Investigation. Advanced Sciences and Technologies for Security Applications*: Springer.

Meershoek, G. & Kop, N. (2017). Kennis voor politiewerk: een blik uit het recente verleden. In M. den Hengst, T. ten Brink, & J. ter Mors (Eds.), *Informatiegestuurd politiewerk in de praktijk*. Deventer: Vakmedianet.

Merkl, P. (2003). Stronger than Ever. In P. Merkl & L. Weinberg (Eds.), *Right-Wing Extremism in the Twenty-First Century* (pp. 21-44). London: Routledge.

Merkl, P. & Weinberg, L. (2003). *Right-wing Extremism in the Twenty-first Century* (Vol. 2nd rev. ed). London: Routledge.

Meyer, C. B. (2001). A Case in Case Study Methodology. *Field Methods, 13*(4), 329-352.

Miller, B. H. (2018). Open Source Intelligence (OSINT): An Oxymoron? *International Journal of Intelligence and CounterIntelligence, 31*(4), 702-719. Retrieved from https://www-tandfonline-com.ezproxy.leidenuniv.nl:2443/doi/pdf/10.1080/08850607.2018.1492826?needAccess=true

Politiewet 2012, (2012). Retrieved from https://wetten.overheid.nl/BWBR0031788/2013-05-01

Wet politiegegevens, (2020a). Retrieved from https://wetten.overheid.nl/BWBR0022463/2020-01-01

Wetboek van Strafrecht, (2020b). Retrieved from https://wetten.overheid.nl/BWBR0001854/2020-07-25#BoekEerste

Wetboek van Strafvordering, (2021). Retrieved from https://wetten.overheid.nl/BWBR0001903/2021-01-01

Moe, W. W. & Schweidel, D. A. (2014). The Beginnings of Social Media Intelligence. In D. A. Schweidel & W. W. Moe (Eds.), *Social Media Intelligence* (pp. 3-17). Cambridge: Cambridge University Press.

Munich Security Conference. (2020). *Munich Security Report 2020.* Munich. Retrieved on from: https://securityconference.org/assets/user_upload/MunichSecurityReport2020.pdf

NCTV. (2018). *De golfbewegingen van rechts-extremistisch geweld in West-Europa: Aard, ernst en omvang van de rechts-extremistische geweldsdreiging in West-Europa, inclusief Nederland.* Nationaal Coördinator Terrorismebestrijding en Veiligheid. Den Haag. Retrieved on from:

Nederlands Genootschap van Burgemeesters. (2017). *Zakboek: Openbare orde en veiligheid.* Nederlands Genootschap van Burgemeesters. Retrieved on from:

https://www.burgemeesters.nl/sites/www.burgemeesters.nl/files/File/Zakboek%20orde%20en%20veiligheid%202017.pdf

Nieuwsuur (Producer). (2019). Hoe wordt rechts-extremisme verspreid? En wat kunnen we eraan doen?

Noble, H. & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evid Based Nurs, 18*(2), 34-35.

Noppe, J. (2018). Are all police officers equally triggered? A test of the interaction between moral support for the use of force and exposure to provocation. *Policing and Society, 28*(5), 605-618. Retrieved from https://doi.org/10.1080/10439463.2016.1199024

Oerlemans, J. J. & Koops, B. J. (2012). Surveilleren en opsporen in een internetomgeving. *Justitiële Verkenningen, 38*(5), 35-49.

Olaru, G. & Stefan, T. (2018). *Fake News - A Challenge for OSINT*. Paper presented at the International Conference: Redefining Community in Intercultural Context, Bucharest.

Omand, D., Bartlett, J. & Miller, C. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security, 27*(6), 801-823.

Pedersen, T. & Jansen, P. T. (2019). Seduced by secrecy - perplexed by complexity: effects of secret vs open-source on intelligence credibility and analytical confidence. *Intelligence and National Security, 34*(6), 881-898. Retrieved from https://www-tandfonline-com.ezproxy.leidenuniv.nl:2443/doi/pdf/10.1080/02684527.2019.1628453?needAccess=true

Pelzer, R. (2018). Policing of Terrorism Using Data from Social Media. *European Journal for Security Research, 3*(2), 163-179. Retrieved from https://doi.org/10.1007/s41125-018-0029-9

Perlinger, A., Hasisi, B. & Pedahzur, A. (2009). Policing Terrorism in Israel. *Criminal Justice and Behaviour, 36*(12), 1279-1304.

Politie. (n.d.). *Politiewet*. Retrieved on January 19th, 2021 from https://www.politie.nl/over-de-politie/politiewet.html

Politiewet 2020, (2012, July 12th). Retrieved from https://wetten.overheid.nl/BWBR0031788/2013-05-01

Pool, R. L. D. & Custers, B. H. M. (2017). The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime. *European Journal of Crime, Criminal Law and Criminal Justice, 25*(2), 123. Retrieved from https://brill.com/view/journals/eccl/25/2/article-p123_3.xml

Ravndal, J. A. (2018). Explaining right-wing terrorism and violence in Western Europe: Grievances, opportunities and polarisation. *European journal of political research, 57*(4), 845-866.

Reisig, M. D. (2010). Community and Problem-Oriented Policing. *Crime and justice (Chicago, Ill.), 39*(1), 1-53.

Reuser, A. H. P. (2013). OSINT and Intelligence: On the significance of OSINT for the overall intelligence effort. *Reuser's Information Services, 3*, 8.

Ribaux, O. (2003). Forensic intelligence and crime analysis. *Law, probability and risk, 2*(1), 47-60.

Rønn, K. V. & Søe, S. O. (2019). Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security, 34*(3), 362-378.

Roop, J. E. (2009). *Foreign Broadcast Information Service: History Part 1: 1941-1947*: CIA Historical Declassification Division.

Rosenthal, L. (2017). The Case for Surveillance. In D. Gray & S. E. Henderson (Eds.), *The Cambridge Handbook of Surveillance Law* (pp. 308-329). Cambridge: Cambridge University Press.

Sampson, F. (2017). Intelligent evidence: Using open source intelligence (OSINT) in criminal proceedings. *Police journal (Chichester), 90*(1), 55-69.

Smahel, D. (2008). Attending online communities: Culture of youth? *Institute for Research on Children, Youth and Family, Faculty of Social Studies, Masaryk University, Czech Republic*.

Smilda, F. & de Vries, A. (2017). Social media. In M. den Hengst, T. ten Brink, & J. ter Mors (Eds.), *Informatiegestuurd politiewerk in de praktijk* (pp. 193-207). Deventer: Vakmedianet.

Staniforth, A. (2016). Police Use of Open Source Intelligence: The Longer Arm of Law. In (pp. 21-31).

Stol, W. & Strikwerda, L. (2018). Online vergaren van informatie voor opsporingsonderzoek. *Tijdschrift voor Veiligheid, 17*(1-2), 8-22.

Tilley, N. (2008). Modern approaches to policing: community, problem-oriented and intelligence-led. *Handbook of policing, 2*.

Trottier, D. (2017). 'Fear of contact': Police surveillance through social networks. *European Journal of Cultural and Political Sociology, 4*(4), 457-477.

United Nations. (2011). *Criminal Intelligence: Manual for Analysts.* United Nations Office on Drugs and Crime. Vienna. Retrieved on from:

Van Dongen, T. (2020). Normalisation, Party Politics and Vigilantism: Why the Next Terrorist Threat will not be Right-Wing Extremist". *The International Centre for Counter-Terrorism - The Hague (ICCT) Evolutions in Counter-Terrorism, 2*, 101-120.

Wang, V. & Tucker, J. V. (2017). Surveillance and identity: conceptual framework and formal models. *Journal of Cybersecurity, 3*(3), 145-158.

Weimann, G. (2016). The Emerging Role of Social Media in the Recruitment of Foreign Fighters. In A. Guttry, F. Capone, & C. Paulussen (Eds.), *Foreign Fighters under International Law and Beyond*. The Hague: T.M.C. Asser Press.

Weisburd, D. L., Shalev, O. & Amir, M. (2002). Community Policing in Israel: Resistance and Change. *Policing: An International Journal of Police Strategies and Management, 25*(1), 80-109.

Williams, H. J. & Blum, I. (2018). *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise.* RAND Corporation. Santa Monica. Retrieved on from:

Wozniak, K. F. (2013). Intelligence cycle. In J. M. Houston & G. K. Piehler (Eds.), *Encyclopedia of Military Science* (pp. 675-676). Los Angeles: Sage Publications, Inc.

Yin, R. K. (2003). *Case Study Research: Design and Methods* (Third Edition ed.): SAGE.

Zedner, L. (2007). Pre-crime and post-criminology? *Theoretical Criminology*, *11*(2), 261-281. Retrieved from https://journals.sagepub.com/doi/abs/10.1177/1362480607075851