Report on State of the Art Review
Deliverable D1.1

Co-funded by the Horizon 2020 Framework Programme of the European Union
Please note that this report is a final draft and is awaiting final acceptance by the European Commission.


Authors:
P. van den Brink, C. Broekman, M. Rijken, S. Oggero, T. Verburgh & A. de Vries (TNO) J. Coaffee and K. Hadjimatheou (University of Warwick), R. Dekker (Utrecht University), S. Denef (Fraunhofer IAO), E. Fontanille & P. de la Torre (EFUS), E. Kermitisis, N. Moustakidis & D. Mytts (KEMEA) K. Tani (EOS)

The research leading to these results has received funding from the European Union’s Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700281.
## Contents

Contents ........................................................................................................................................... ii  
Executive Summary ............................................................................................................................ i  
1. Introduction ................................................................................................................................... 1  
   1.1 MEDI@4SEC ................................................................................................................................. 1  
   1.2 Work Package 1 .............................................................................................................................. 1  
   1.3 Deliverable D1.1 ............................................................................................................................ 2  
   1.4 Outline report ............................................................................................................................... 3  
2. Method ........................................................................................................................................... 4  
   2.1 Systematic Literature Review according to the PRISMA method .............................................. 4  
   2.2 Definition of the parameters of the review .................................................................................. 4  
   2.3 Collection and relevance assessment ......................................................................................... 5  
   2.4 Analysis and reporting of meta-synthesis ................................................................................... 6  
3. Overview of literature .................................................................................................................... 1  
   3.1 Trends in number of publications ............................................................................................... 1  
   3.2 Scientific disciplines .................................................................................................................. 1  
   3.3 Relevance to project themes ....................................................................................................... 2  
   3.4 Country setting .......................................................................................................................... 3  
   3.5 Types of social media ................................................................................................................ 3  
   3.6 Social media users ....................................................................................................................... 4  
   3.7 Reflection on the literature ........................................................................................................ 5  
4. The use of social media for law enforcement .............................................................................. 6  
   4.1 Goals to use social media ............................................................................................................ 6  
   4.2 Communication and engagement .............................................................................................. 7  
   4.3 Emergency services & Crisis Management ............................................................................... 9  
   4.4 Surveillance ............................................................................................................................... 10  
   4.5 Criminal investigation ............................................................................................................... 11  
   4.6 Community policing .................................................................................................................. 13  
   4.7 Intelligence .................................................................................................................................. 13  
   4.8 General Reflections .................................................................................................................... 14  
5. DIY policing .................................................................................................................................. 18  
   5.1 The use of social media in the domain of public security and policing ...................................... 18
5.2 The influence and impact of social media use in the domain of public security and policing .......................................................... 19
5.3 Inventory of strengths, weaknesses, opportunities and threats ................................................. 20
5.4 Reflection and conclusion ................................................................................................................. 22
6. Riots and mass gatherings ................................................................................................................. 23
6.1 The use of social media in the domain of public security and policing ........................................ 23
6.2 The influence and impact of social media use in the domain of public security and policing ...................................................................................................................... 25
6.3 Inventory of strengths, weaknesses, opportunities and threats ................................................. 26
6.4 Reflection and conclusion ................................................................................................................. 28
7. Everyday Security ............................................................................................................................. 30
7.1 The use of social media in the domain of public security and policing ........................................ 30
7.2 The influence and impact of social media use in the domain of public security and policing ...................................................................................................................... 33
7.3 Inventory of strengths, weaknesses, opportunities and threats ................................................. 35
7.4 Reflection and conclusion ................................................................................................................. 38
8. Dark web ........................................................................................................................................... 40
8.1 The use of social media in the domain of public security and policing ........................................ 40
8.2 The influence and impact of social media use in the domain of public security and policing ...................................................................................................................... 45
8.3 Inventory of strengths, weaknesses, opportunities and threats ................................................. 46
8.4 Reflection and conclusion ................................................................................................................. 49
9. Trolling ............................................................................................................................................... 51
9.1 The use of social media in the domain of public security and policing ........................................ 51
9.2 The influence and impact of social media use in the domain of public security and policing ...................................................................................................................... 53
9.3 Inventory of strengths, weaknesses, opportunities and threats ................................................. 54
9.4 Reflection and conclusion ................................................................................................................. 60
10. Innovative market solutions ............................................................................................................. 61
10.1 The influence and impact of social media market solutions use in the domain of public security and policing ................................................................................................................. 61
10.2 The use of social media market solutions in the domain of public security and policing ...................................................................................................................... 62
10.3 Inventory of strengths, weaknesses, opportunities and threats (for use of social media market solutions) ...................................................................................................................... 65
Executive Summary

The MEDI@4SEC project focuses upon understanding the opportunities, challenges and ethical considerations of enhancing social media use for public security: the good, the bad and the ugly. The good comprises using social media for problem solving, fighting crime, decreasing fear of crime and increasing the quality of life. The bad is the increase of digitised criminality and terrorism with new phenomena emerging through the use of social media. The ugly comprises the grey areas where trolling, cyberbullying, threats, or live video-sharing of tactical security operations are phenomena to deal with during incidents. Making use of the possibilities that social media offer, including smart ‘work-arounds’ is key, while respecting privacy, legislation, and ethics. This changing situation raises a series of challenges and possibilities for public security planners. The role of this report, as the first output of Work Package 1 (WP1), is to link the project activities and outcomes to the existing body of knowledge through a series of stocktaking and inventories on the influence of social media on public security planning and the potential threats and challenges this uptake brings about.

This report identifies the state-of-the-art of the use social media not only by police and other public security planners but also by criminals (as this group is very active in applying new possibilities). It includes an analysis of current academic research on social media and security, a dark web study and red-teaming expert opinion (viewing the problem from the criminal perspective) as well as existing EU funded research across a number of linked domains. The review is focused around the impact of social media upon a range of public security tasks - 1) communication and engagement, 2) emergency services and crisis management, 3) surveillance, 4) criminal investigations, 5) community policing and 6) intelligence - that identify the challenges and opportunities for the actors responsible for the security in the public domain.

The introduction of social media in the domain of public security has shown differences in the conditions required for success. Many police organizations adopting social media, consider the usage very fruitful for different purposes in both the operational police tasks, e.g. investigation, crowd control (Knibbs, 2013), organizational purposes and reputation (Jamieson, 2016) and recruitment (De Smet, 2012). The review highlights that entrepreneurship - employees trying new things within the organization - is crucial for the experimentation with social media as is the need for a coherent strategy for and training in the correct usage of social media, conducting organizational goals and sufficient ICT necessary for successful implementation of social media (Mauritz 2011). Furthermore, the more social media are used the more effect and the more response can be expected, which also helps to gain more interaction (De Smet, 2012). Social media usage, in this sense, is self-perpetuating, but must be undertaken with care. Here the tone of the messages is important. Messages sent from a central account should be more formal, messages sent from a personal police officer account should be more informal. However, this is a fine line (Foster, 2016). Importantly, engagement requires not only sending information, but also two-way communication.

The use of social media has both brought forward tremendous benefits as well as challenges. Being present on social media and using data from social media takes a lot of
time, which conflicts with cutting in police-budgets. A second challenge is the large amount of different types of social media which have different characteristics and lead to people being spread over different digital places. Furthermore, anonymity of social media brings up challenges of trust and privacy, because it is not clear who did what and to know if something is trustworthy or not.

In this report we illuminate these challenges and opportunities through a number of different themes that showcases the ways social media are used and have an increasingly prominent role in, or impact on, public security. The six themes we explore in depth are:


DIY policing questions the general division of responsibilities and legitimate power between citizens and law enforcement agencies. The key questions for many security planners are about where and how to cooperate with citizens, when to take control and how to avoid negative effects. We highlight how, on the one hand, we see citizens taking coordinated action in places where public security falls short or fails. This leads to the question: can DIY policing become a factor for public security organizations to use in targeting where their resources are best deployed and where citizens can aid their operations? On the other hand, it appears that some (especially Dutch) police forces have taken these concerted efforts in co-creating safety jointly with citizens. The many platforms and initiatives that were studied, underline the Dutch forerunner role in encouraging DIY activities. DIY policing does raise a range of delicate ethical questions. Empowered citizens have the means to fight injustice and produce desirable change, while at the same time, they can also create great harm when acting irresponsibly.

2. Riots and mass gatherings: the role of social media (data) during riots and mass gatherings and ensuring public security by monitoring, signalling and communicating with the public.

The rapid adoption of social media has enabled social movements and mass gatherings in two ways: 1) in organization and coordination of the event itself, and 2) by providing wider exposure that leads to increased participation. This report shows that policing of riots and mass gatherings is a critical issue for law enforcement agencies that poses key question. How to re-invent the current policing paradigm to incorporate new tools, organizational structures, staff, policies and technological infrastructure to support the use of social media in such situations? Here the focus should be on both, monitoring potential mass gatherings on social media as well as preparing for one and communicating with community. Moreover, in such instances it is vital to advance a communication strategy to ensure the uniform use of social media by authorities in a positive, friendly, instructive and helpful tone to promote citizen engagement, collaboration and trust. Such interactive communication can provide a substantial resource for situation awareness but should be done in an ethically aware way.
3. Everyday security: the everyday policing of public security, including cooperation with citizens via social media ‘community policing’ and social media/big data intelligence.

The recent massive increase in social media use has drastically transformed people’s communication and information habits, and provides authorities with new opportunities for intelligence sources and platforms to communicate. These new opportunities raise numerous questions, for instance, in what ways do the data and tools available through social media influence the work of intelligence services and LEA’s? How do local authorities use social media to facilitate and enhance their local crime prevention strategies? Or, how can community policing initiatives supported by social media contribute to the everyday management of security? One of the main challenges for law enforcement agencies using social media in policing is the adoption of formal policies and processes within agencies that enable a unified, consistent approach to modern technology usage. Incorporating specialized staff, budget dedicated to innovation and defining a clear legal framework and procedural protocols, become a priority for the agencies and policy planners in the public security domain.

4. The Dark web: organised (international) crime and their high-tech use of the dark web, the influence on public security, and the counter policing activities.

Historically, technology has revolutionized policing practices but it has also facilitated criminality with the Dark Web emerging as a key space for “high tech” (organized) cybercrimes. The analysis presented in this report raises a number of issues which should be taken into account in the discussion on policing against Dark Web: How to avoid limited applicability in a cybercrime community that is instead capable of quickly developing countermeasures with flexible and adaptable innovations policies? Furthermore, there should be no “size-fits-all” measures: strategies should differentiate between the types of crime, nor should there are “total-block” strategies: policies should seek balance between freedom of speech and crime facilitation. In the case of cryptomarket-related crimes, how to be able to tackle the ecosystem, instead of single targets, and focus on the demand first, instead of the vendors side only with strategies that focus on the “economical game”? Moreover, with violent extremism, how to set out strategies that focus on the producers, rather than on the consumers of extremist material? And also, how to empower the “good” and the “grey” users with spaces for open debate that allows extremisms to be blended and debated? Finally, what are the options of applying social media strategies from the Clear Web to the Dark Web, being aware of the differences between the two digital dimensions?

5. Trolling: all kinds of online bullying (cyberbullying), of which some activities are criminal offences and some or not.

Trolling broadly understood includes cyberbullying, cyberhate, cyberstalking, cyberharassment, revenge porn, sextortion, naming and shaming and flaming. The legal status of all the trolling-related acts just listed differs from jurisdiction to jurisdiction and from act to act. An impressive and varied array of preventive, counter-trolling, and criminal justice approaches to combatting trolling are currently employed by public security providers broadly understood. While the literature suggests that organic,
community-driven counter-trolling actions are cheaper, faster, more effective and more responsive to trolling than actions of public authorities, these cannot substitute the strong arm of the law in cases of serious harassment, stalking, and abuse of individuals online. There is some current literature examining the nexus between online and offline abuse, but this is scant and rudimentary. Further research in this area would be beneficial to public security providers and victims of trolling.

6. Innovative market solutions: new commercial products for including social media in police work. For example apps for smartphones, social media monitoring tools etc.

To digest, analyse, expand and share the valuable information on social media to the domain of public security and policing, constant innovations are required in order to meet these needs. An innovative market solutions focus on social media and applications used, aiming to increase the effectiveness of public authorities, with fast and accessible formats. From tweets to serious gaming, social media have pushed public security and policing to advance their investigative processes as well as their interaction with citizens. One key question that arises is what can be done to facilitate communication between the supply of and demand for new innovative social-media solutions? Furthermore, how can the training of public security planners in social media use be facilitated by new innovations? Overall, one of the most important question with new technology solutions is, how do we balance between security and rights in advancing new security? Solutions should advance, but the respect of personal data must advance as well. Data protection regulations have opened a new market dealing with the protection of data and their potential misuse. This raises questions like; what are the challenges with data been collected from third parties? And should there be pan-European requirements for the usage of that data? Ethical and societal considerations thus need to be at the forefront of new solutions; security cannot be above the law.

The questions, challenges and opportunities raised in this report provide insight for future research, and will be the focus of the upcoming policy and practice workshops in the MEDI@4SEC project.
1. Introduction

1.1 MEDI@4SEC

MEDI@4SEC focuses upon understanding the opportunities, challenges and ethical consideration of enhancing social media use for public security: the good, the bad and the ugly. The good comprises using social media for problem solving, fighting crime, decreasing fear of crime and increasing the quality of life. The bad is the increase of digitised criminality and terrorism with new phenomena emerging through the use of social media. The ugly comprises the grey areas where trolling, cyberbullying, threats, or live video sharing of tactical security operations are phenomena to deal with during incidents. Making use of the possibilities that social media offer, including smart ‘work-arounds’ is key, while respecting privacy, legislation, and ethics. This changing situation raises a series of challenges and possibilities for public security planners. MEDI@4SEC will explore this through a series of communication and dissemination activities that engage extensively with a range of end-users to better understand the usage of social media for security activities. MEDI@4SEC will seek a better understanding of how social media can, and how social media cannot be used for public security purposes and highlight ethical, legal and data-protection-related issues and implications. Activities centre around six relevant themes: DIY Policing; Everyday security; Riots and mass gatherings: The dark web; Trolling; and Innovative market solutions. MEDI@4SEC will feed into, support and influence changes in policy-making and policy implementation in public security that can be used by end-users to improve their decision making. By structuring our understanding of the impact of social media on public security approaches in a user-friendly way MEDI@4SEC will provide an evidence-base and roadmap for better policymaking including: best practice reports; a catalogue of social media technologies; recommendations for EU standards; future training options; and, ethical awareness raising.

1.2 Work Package 1

The role of Work Package 1 (WP1) is to link the project activities and outcomes to the existing body of knowledge through a series of stocktaking and inventories on the influence of social media on public security planning and the potential threats and challenges this uptake brings about.

In this project, social media are defined as “a group of internet based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content” (Kaplan & Haenlein 2010: 61). Social media that we predominantly focus on are the more widely used social media apps, notably Facebook, Twitter, WhatsApp, Youtube, and Instagram, but also (new) emerging social media that are widely adopted and that we come across. Online chat groups, fora and market places our not our key focus, but will be touched upon where relevant.
1.3 Deliverable D1.1

Deliverable D1.1 focuses on the current state of the art of social media use and impact in the domain of public security and policing, paying particular attention to the opportunities and challenges that these present. This task identifies the state of the art of the use social media not only by police and other public security planners but also by criminals (as this group is very active in applying new possibilities). This task will include:

1. Analysis of current academic research on social media and security including reactive and preventative elements. Analyses will include studies on using social media for predictive policing and early warning.
2. Dark web study and red-teaming expert opinions (viewing the problem from the criminal perspective) to create a long list of modus operandi by criminals using social media.
3. Review of existing EU funded research across a number of linked domains.

In order to identify the uses of social media and the impacts in the domain of public security and policing as defined above, the following questions will be addressed:

- What uses of social media in the domain of public security and policing have been reported?
- What impacts of the use of social media in the domain of public security and policing have been reported?
- What strengths, weaknesses, opportunities and threats are identified for different applications and stakeholders?

This state of the art review on the emerging role of new social media in enhancing public security, is focused around their impact upon a range of public security tasks - 1) communication and engagement, 2) emergency services and crisis management, 3) surveillance, 4) criminal investigations, 5) community policing and 6) intelligence – that identify the challenges and opportunities for the actors responsible for the security in the public domain. Subsequently we illuminate these challenges and opportunities through a number of different themes that showcases the ways social media are used and have an increasingly prominent role in, or impact on, public security. This in-depth focus will be the basis for six different workshops later on in the MEDI@4SEC EU project for hands-on knowledge and training for security planners. The six themes that have been explored in depth are:

2. Everyday security: About everyday policing of public security. Also including cooperation with citizens via social media ‘community policing’ and social media/big data intelligence (SOCMINT), social media intelligence.
3. Innovative market solutions: About new commercial products for including social media in police work. For example apps for smartphones, social media monitoring tools etc.
4. Trolling: About all kinds of online bullying (cyberbullying), of which some activities are criminal offences and some or not.

5. Riots and mass gatherings: the role of social media (data) during riots and mass gatherings and ensuring public security by monitoring, signalling and communicating with the public.

6. The Dark web: organised (international) crime and their high-tech use of the dark web, the influence on public security, and the counter policing activities.

1.4 Outline report

This report is divided into 11 chapters that assess the role of new social media for enhancing public security. Following the Introduction, the second chapter describes the methodologies underpinning this research. This will show how we undertook a systematic literature review using the PRISMA method and describe the search strings used to identify all the relevant academic publications alongside the academic literature review we also conducted a broad search of the grey literature as well as European project outputs. The EU partners of the consortium have all analysed parts of the literature, using the same consistent method in order allow us t conduct a meta-analysis of existing data sources.

The third chapter provides a top-level overview of our literature, giving some insights into the growth of research on social media in the domain of public security as well as the country setting, the different uses of, and researches on, social media, the different types of social media and the actors who employ them. This chapter concludes by reflecting upon the literature and identifying gaps and potentials for future research.

At a finer level of granularity, the fourth chapter unpacks the different security tasks - communication and engagement, emergency services and crisis management, surveillance, criminal investigations, community policing and, intelligence - and the current state of the art on using social media. By reflecting on the uptake and future of social media usage, identifying the impact and influence as well as the opportunities and challenges ahead this chapter illustrates the many themes where social media play a key role.

The following chapters (5-10) focus their analysis upon the six core themes. Finally in chapter eleven the overall opportunities and threats of using new social media for enhancing public security will be described and new areas of research identified.
2. Method

2.1 Systematic Literature Review according to the PRISMA method

The aim of Task 1.2 was to produce a thematic review of the outputs of completed and ongoing research projects, together with an analysis of relevant broader scholarship and knowledge. Our collection and analysis of relevant literature was steered by the overarching aims and research questions that underpin MEDI@4SEC. We applied the PRISMA method for systematic literature review. A systematic literature review can be defined as a ‘systematic, explicit, and reproducible method for identifying, evaluating, and synthesizing the existing body of completed and recorded work produced by researchers, scholars and practitioners’ (Fink, 2010: 3). The ‘Preferred Reporting Items for Systematic reviews and Meta-Analyses’ (PRISMA) statement is a method to ensure transparent and complete reporting of the systematic literature review (Moher et al., 2009; Liberati et al., 2009).

The PRISMA method can be translated into a three-step process of collection and analysis of literature. Step 1 entails defining the parameters of the review. Step 2 is the collection of publications and assessment of the relevance for our review. Step 3 deals with the analysis of the literature and reporting of the findings of the meta-synthesis. See appendix 1 for a flow chart visualizing these steps of the systematic literature review. While this suggests three consecutive stages, in reality this is an iterative process.

2.2 Definition of the parameters of the review

2.2.1 Types of publications

Task 1.2 concerns a systematic literature review of explicit knowledge (written publications) in the public domain. We took into account three types of literature. They were specified as follows:

1. Academic publications: Academic books and chapters, journal articles, PhD Theses and Conference papers. These publications are peer-reviewed and stored in academic databases.

2. Grey literature: Working papers, Reports from governments, NGOs, Advisory boards, Think Tanks or consultancy firms, popular books, trend studies, vision reports and BSc/MSc Theses. These publications are publicly available online or in hardcopy.

3. EU funded research reports: EU project deliverables, research reports, project Working papers, project summaries, project published outcomes beyond the lifespan of a project (not in academic journals). These publications were found in the EU Cordis database and on project websites.

2.2.2 Databases and search strategies

The PRISMA method is best suited for the collection of literature from delimited archives or databases which allow for Boolean search queries.1 This ensures transparency of the search strategy and allows the searches to be repeated in future studies. The PRISMA

---

1 Queries combining multiple search terms with AND, OR and NOT operators.
method proved better suited to the review of academic literature than other types of literature taken into account in this task. For the collection of grey literature and EU projects, we were more dependent on expert consultation and backward searches of references. The list below specified where and how we collected relevant publications:

1. **Academic publications**: Boolean queries in Scopus and Web of Science, the two largest bibliographic databases in the social sciences and humanities. Additionally, we asked all project partners to review the list of references.
2. **Grey literature**: Simplified Boolean queries in Google and Google scholar search engines while turning off personalized search filters.
3. **EU funded research reports**: EU project deliverables, research reports, project Working papers, project summaries, project published outcomes beyond the lifespan of a project (not in academic journals). These publications can be found in the EU Cordis database.

2.2.3 **Time frame**
We decided to take into account publications from 2010 to current (July 2016). We want the literature review to focus on the current state-of-the-art, as social media and their applications in policing and public security are changing rapidly. Pilot searches in databases did not yield many relevant publications from before 2010, indicating that this time frame is sufficient.

2.2.4 **Language**
We mainly focused our review on literature in English for both analytical and practical reasons. Our study focuses on the context of EU countries. English has become the primary language for academic publications and reports resulting from EU projects. Also many professional publications that have a broader relevance are nowadays published in English to reach a larger public. Furthermore, the language skills of the joint project partners allow us to effectively collect and analyse these publications. The database searches were based on English search strings and collecting English publications.

However, during the rounds of consultation of project partners and external experts, we also inquired about any relevant non-English publications. Where relevant we summarized these publications in English and took them into account in the analyses. The set of non-English publications in our sample is strongly biased toward the languages of the project partners (Dutch, Spanish, Greek, German).

2.3 **Collection and relevance assessment**

2.3.1 **Eligibility criteria**
We formulated a number of eligibility criteria to assess the relevance of each publication for the aims of our literature review (see appendix 3). These are closely related to the definition of the parameters of the review that we formulated in the first step of the process. Other criteria about the content of the publication were formulated as new rules during assessment of relevance.

2.3.2 **Number of publications at different stages of assessment**
After collection of literature from databases and consultation of all project partners we first removed duplicates. A second step was to judge eligibility of the publication for
review based on title and abstract. In a third and last step we assessed the eligibility of the record based on reading the full publication. The numbers of articles in various phases of this process are visualized in Appendix 4 and the final number of publications taken into account in the analysis for each type of literature is specified in Appendix 5.

2.4 Analysis and reporting of meta-synthesis

2.4.1 General coding
In a first round of analysis each publication was coded based on a codebook closely related to the research questions and the aims of this task (Table X: Analytic framework of codes). Slight variations of this codebook and coding categories were used for the different types of publications (Academic, grey, EU projects.). This first round of coding was done in an Excel spreadsheet as this software was available and known to all partners involved. Most fields could be freely filled in, for others (such as year of publication and type of publication) the coder could select the applicable category from a drop-down list. The analysis was a joint and integrated effort amongst a number of project partners. The various coders using the coding sheets regularly discussed their coding efforts in person, via Skype or via email.

2.4.2 Thematic meta-syntheses
For the thematic analysis of the publications, we divided the publications based on their relevance to each theme. Of themes that were very prevalent in the literature, only the (20-30) most relevant publications were included in this step of the review. The publications were re-reading and interpreted in relation to each other. The meta-synthesis was aimed at constructing a state-of-the-art of current knowledge on each of the workshop themes and identifying gaps in current knowledge.
3. Overview of literature

The general coding of the publications based on our analytic framework (Appendix 6) provides us with a good overview of studies of social media in the domain of public security. This chapter shortly presents some general developments in the current state-of-the-art: Trends in the number of publications, the disciplines they relate to, the country settings which were in focus, the types of social media and the stakeholders that were under scrutiny. We focus this overview on the academic publications only because these were collected most systematically.

3.1 Trends in number of publications

The years of publication give us an indication when social media in the domain of public security became a popular research topic. We collected publications from 2010 onward. The table and graph below show that the research topic grew in popularity during the past years to around 40 academic publications each year from 2013 onward.

Graph 3-1: Year of publications

Note: Publications were collected in July 2016.

3.2 Scientific disciplines

Academic articles on the topic of social media and public security have been published in a variety of scientific journals and presented at a variety of conferences relating to various scientific disciplines. This indicates that social media and public security is an interdisciplinary research topic. Based on publication and journal titles we made a typology of disciplines of domains that the publications (predominantly) relate to.

Table 3-1: Scientific disciplines

<table>
<thead>
<tr>
<th>Discipline</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminology/police studies</td>
<td>60</td>
</tr>
<tr>
<td>Information systems/ technology studies</td>
<td>43</td>
</tr>
<tr>
<td>Law / jurisprudence</td>
<td>26</td>
</tr>
<tr>
<td>Sociology / cultural studies</td>
<td>20</td>
</tr>
<tr>
<td>Public administration</td>
<td>18</td>
</tr>
<tr>
<td>Economics / business administration</td>
<td>6</td>
</tr>
<tr>
<td>Public Security</td>
<td>12</td>
</tr>
</tbody>
</table>
Table 3-1: Scientific disciplines indicates that most publications relate to the discipline of criminology/police studies and have been published in books, journals or conferences specific to this discipline. 12 studies were published in venues specifically relating to public security. Also a large number of studies focus on new (media) technologies and information systems and are published in related journals/sources. Besides these disciplines we encountered substantial numbers of relevant publications in law, public administration, sociology and business administration journals.

Most popular journals are ‘Policing and Society’ (7 publications), ‘Government Information Quarterly’ (5 publications and the ‘International Journal of Cyber Criminology’ (4 publications), ‘Computers in Human Behaviour’ (4 publications) and ‘Information and Communications Technology Law’ (4 publications).

3.3 Relevance to project themes

We assessed each publication’s relevance to the six project themes. The table below indicates that in academic publications everyday security has been the most prominent theme. Perhaps this is also due to the fact that his theme is relatively broad and can incorporate various security practices. The themes of Riots and Mass Gatherings, The Dark Web, and Trolling were equally represented in the literature. There has been less attention for DIY policing and Innovative Market Solutions.

Table 3-2: publication’s relevance

<table>
<thead>
<tr>
<th>Theme</th>
<th>Count of Relevance to six themes (primary theme)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIY policing</td>
<td>32</td>
</tr>
<tr>
<td>Everyday security</td>
<td>66</td>
</tr>
<tr>
<td>General (No specific theme)</td>
<td>73</td>
</tr>
<tr>
<td>Innovative market solutions</td>
<td>19</td>
</tr>
<tr>
<td>Other</td>
<td>49</td>
</tr>
<tr>
<td>Riots and mass gatherings</td>
<td>41</td>
</tr>
<tr>
<td>The dark web</td>
<td>73</td>
</tr>
<tr>
<td>Trolling</td>
<td>29</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>382</strong></td>
</tr>
</tbody>
</table>

24 publications did not relate to any specific theme but studied social media use for public security in general. Chapter four of this deliverable will further discuss these publications. 39 publications were characterized by another theme. Five main themes were central to these publications. Depending on the specific research topic, these articles were grouped and further analysed in one of the six project themes. The definitions of these six themes were elaborated and are defined at the beginning of each thematic chapter in this deliverable.
The studies focused on the uptake of social media for public security in a variety of countries. While in the first place provides an overview of where studies have taken place, it also gives a first indication in which countries, social media are used in the public security domain. The top three countries which have been studied most are the U.S., the U.K. and the Netherlands.

### Table 3-4: Country setting research

<table>
<thead>
<tr>
<th>Country setting research</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Afghanistan</td>
<td>1</td>
</tr>
<tr>
<td>Australia</td>
<td>3</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>1</td>
</tr>
<tr>
<td>Canada</td>
<td>6</td>
</tr>
<tr>
<td>China</td>
<td>5</td>
</tr>
<tr>
<td>Germany</td>
<td>1</td>
</tr>
<tr>
<td>Greece</td>
<td>1</td>
</tr>
<tr>
<td>India</td>
<td>1</td>
</tr>
<tr>
<td>Kenya</td>
<td>1</td>
</tr>
<tr>
<td>Malaysia</td>
<td>1</td>
</tr>
<tr>
<td>Nigeria</td>
<td>1</td>
</tr>
<tr>
<td>Pakistan</td>
<td>1</td>
</tr>
<tr>
<td>Russia</td>
<td>1</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>1</td>
</tr>
<tr>
<td>Singapore</td>
<td>1</td>
</tr>
<tr>
<td>South Africa</td>
<td>1</td>
</tr>
<tr>
<td>South Korea</td>
<td>1</td>
</tr>
<tr>
<td>Sweden</td>
<td>2</td>
</tr>
<tr>
<td>“EU countries”</td>
<td>3</td>
</tr>
<tr>
<td>“Latin American countries”</td>
<td>1</td>
</tr>
<tr>
<td>“North American countries”</td>
<td>1</td>
</tr>
<tr>
<td>Unclear/not applicable</td>
<td>107</td>
</tr>
</tbody>
</table>

### Table 3-5: Types of social media

<table>
<thead>
<tr>
<th>Types of social media</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Big data</td>
<td>3</td>
</tr>
<tr>
<td>Messenger services (Blackberry, MSN, Whatsapp)</td>
<td>2</td>
</tr>
</tbody>
</table>
3.6 Social media users

Publications on social media use for public security refer to various stakeholders using these social media. The table below provides an overview of the stakeholders that are named. Most frequently, academic publications study social media use by police (either individual policemen or police departments), citizens in general, government departments dealing with public security (besides the police) and LEA’s (probably referring to both police and other government departments).

Table 3-6: Stakeholders using social media

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citizens</td>
<td>15</td>
</tr>
<tr>
<td>Non-state actors dealing with security</td>
<td>3</td>
</tr>
<tr>
<td>Criminal investigators</td>
<td>3</td>
</tr>
<tr>
<td>Europol</td>
<td>1</td>
</tr>
<tr>
<td>Twitter influencers</td>
<td>3</td>
</tr>
<tr>
<td>LEAs</td>
<td>14</td>
</tr>
<tr>
<td>Local/municipal police</td>
<td>6</td>
</tr>
<tr>
<td>Government departments dealing with security</td>
<td>12</td>
</tr>
<tr>
<td>Police (departments)</td>
<td>41</td>
</tr>
<tr>
<td>Rioters</td>
<td>2</td>
</tr>
<tr>
<td>Police officers</td>
<td>4</td>
</tr>
<tr>
<td>Privacy advocates</td>
<td>1</td>
</tr>
<tr>
<td>Criminologists</td>
<td>1</td>
</tr>
<tr>
<td>Whistle blowers</td>
<td>1</td>
</tr>
<tr>
<td>Prosecutors</td>
<td>7</td>
</tr>
</tbody>
</table>
### 3.7 Reflection on the literature

Social media and public security is a research topic which is growing in popularity. It is unclear whether this trend has stabilized or still increasing. Studies have been published in a variety of journals from various scientific disciplines. Criminology/police studies and information systems/technology studies are the most prominent disciplinary fields. Trends in time and scientific disciplines of more specific research themes may vary.

Of the six research themes, DIY policing and innovative market solutions are underrepresented in academic publications. As these concern private initiatives and commercial projects, they are more difficult to find for academic researchers. We encountered relatively more publications on these topics in EU projects and the grey literature. Another explanation might be that these themes concern more recent trends in social media for public security. Academic attention for these initiatives may grow in the upcoming years.

The most studied countries in which social media use for public security has been studied are the US, UK and the Netherlands. While this can be a bias in research choice, it also is indicative of these counties being frontrunners in the uptake of social media by government and police.

Analysis of the social media users named in the studies demonstrates that most studies focus on the LEAs appropriating social media. To gain a more holistic view of social media use for public security, future studies should also focus on the perspective of citizens in general and criminals’ in particular using social media.

Most studies focused on two of the most popular social media platforms: Twitter and Facebook. This signals a rather small definition of social media and a focus on commercial social media platforms. Give the growth in new social media, future studies will have to capture the variety of social media uses for public security. This would include dark web phenomena, social media platforms developed by government organisations, new encryption devices, data analysis and monitoring tools and mobile applications.
4. The use of social media for law enforcement

Social media allows law enforcement agencies and others involved with public security to ask for information from citizens, send information instantaneously to, and interact with, a range of civil society groups, as well as providing a monitoring function. Social media are omnipresent and have become powerful mechanisms driving social, economic and societal change. New and emerging forms of social media (e.g. Twitter, Facebook, YouTube, Instagram and other platforms) are open, distributed, digital communication platforms that enable people and social networks to create and share information and ideas worldwide. Social media allows the fast sharing of user generated content, facilitating communication on a many-to-many basis (Boyd & Ellison, 2007), gives the ability for personalization and allows use anytime and anywhere (De Vries, 2011).

This chapter describes what happens to the domain of public security and policing when the police, citizens and criminals use social media. Looking at the different security task, namely communication and engagement, emergency services and crisis management, surveillance, criminal investigation, community policing and intelligence, this chapter focuses on: how social media are used by different actors; what the impacts are (looking at individual, organizational and societal level); if there are EU or world differences ( frontrunners); and, what future social media use will look like. This chapter looks at the broad range of social media in the domain of public security and thus, beyond the six themes.

4.1 Goals to use social media

Many police departments have started experimenting with using social media, or deploying social media within their daily routines. For example, there are over 2,935 Twitter accounts held by all of UK police together (Foster, 2016). One social media project leader of the Dutch police suggested in a personal conversation that the Dutch police might be using the most Twitter accounts within one organisation worldwide, with well over 2000 accounts.

The most mentioned goals to use social media – often initiated within a communications department - are to increase engagement, reputation (e.g. Denef et al., 2012; Meijer & Thaens, 2013; De Smet, 2012; Meijer et al., 2013), transparency and legitimacy, though to a limited extend, (Grimmelikhuijsen and Meijer, 2015), trust, confidence and relation building (The Police Foundation, 2014; Lieberman, et al, 2013). Other purposes to which social media is put includes increased effectiveness and legitimacy, enhancing transparency (Global Advisory Committee, 2013) collaboration and community participation (Meijer & Thaens, 2013). Usage of social media is likely to be more operational when it initiated outside of the communications department (Meijer & Thaens, 2013). Social media can be a source of intelligence, enhance emergency management (CLEDS, 2013) and it is used to send information to the public. For
example, Foster (2016) noted that 73% of the respondents (over 100 public security professionals) use social media to send information.

Different social media tend to be used for different purposes (Jaitner & Kantola 2014); Twitter is used mostly for real-time purposes, e.g. for monitoring crowds during a protest, while Facebook is more popular for planning activities and blogs are used to express opinions and stories (Jaitner, 2013 in Jaitner & Kantola, 2014). Moreover, different target groups use different social media – knowledge of which is imperative for successful policing with a more complete overview of the platforms used (and for what purposes) being crucial for improving situational awareness (Jaitner & Kantola, 2014). For example during Summer Carnival of July 2012, in Rotterdam, the Netherlands, monitoring and crowd management attempted to utilise Twitter without realising many of the festival visitors were Facebook-users (Broekman & Menkhorst, 2013).

Rosenbaum, Graziano, Stephens & Schunk, (2011) argue that websites should also be used for two-way communication, instead of only pushing information. Their research highlighted that Police departments that implemented the community policing philosophy showed to have more transparent websites and were more likely to ask the community for input through their websites. This research study focuses however on social media, and hence will not explore the possibilities of website utilization.

Introducing social media to the toolset or ‘on the belt’ of police officers is most effective when citizens can also communicate with the police using social media through two-way communication. A study in the Netherlands showed that inhabitants from North-East Groningen appreciate the positive benefits of the police uses social media. Here, Mauritz (2011) found that the image of the police was positively influenced by their using Twitter (especially the transparency it affords).

As well as the overarching goals of social media use – to increase community interaction, improve reputation and enhance situational awareness – social media has been put to use in a range of policing tasks - communication and engagement, emergency services and crisis management, surveillance criminal investigation community policing and intelligence. These will be discussed in turn below.

### 4.2 Communication and engagement

Social media has changed the landscape of policing communication drastically² and redefined how people communicate, both inside and outside LEA’s especially by its employees in their private time (Goldsmith, 2015). It enabled everyone to send information or ask questions to anyone, instantaneously, and at minimal costs. Police communication is rapidly moving beyond the department ‘communication’ anymore. This forms a challenge moving forward on how LEA’s harness and manage the use of social media as a strong public tool amongst their workforce – for crime prevention, tackling crime and increasing the feeling of safety and security.

---
²In this report communication usage and communication challenges are interwoven in the six themes that are the core of the project. Community engagement, although its usage is wider, is incorporated in the theme community policing, since community engagement is at the core of community policing.
Social media has served to increase accessibility of policing services for community members. The two-way engagement with the public is a tangible benefit of social media. In stimulating engagement between police and community, social media adds legitimacy and knowledge to many police tasks. Social media offer a great opportunity to reach target groups who traditionally are hard to reach, e.g. youngsters, ethnic minorities (Meijer et al, 2013). In response to a reduction in 'on the beat' policing, individual police officers are increasingly using social media to enhance their visibility and reassure the public that they are active in an area as well as making it easier for the public to contact them. In this way social media offers a way to interact with people who generally are reluctant, or too busy, to meet police (The Police Foundation, 2014). In this way, increased social media communication, leads to increased transparency and increases perceived police legitimacy (Grimmelikhuijsen and Meijer, 2015). This transparency provides increased accountability and visibility. Whilst at present only a limited number of people actually engaged with the police on social media such a trend, if it continues, is likely to be a core strand of community policing initiatives.

Through the use of social media Police reputation can be affected positively by giving the community more insights in the complex role of policing (The Police Foundation, 2014). For example, in a ‘Tweetathon’ the police of Rotterdam showed the scale and diversity of incoming emergency calls that are acted upon on a daily basis (Broekman & Menkhorst, 2013). Conversely, social media can also damage their reputation, e.g. in cases where the misbehaviour of police officers is recorded and shared through social media. However, according to Siep and Kool (2013) this does not occur often. In general, using social media to communicate with the public enables the police to broadcast messages without interference or need of a third party, e.g. traditional media (Denef et. al., 2012). Through social media extra channels can be created to redirect people online and where they can still be reached and informed (Denef et.al. 2012).

Formal social media strategies for LEA's are not available in most countries. However, in the Netherlands, a social media task force introduced a social media strategy (De Vries & Smilda, 2014) and in the United Kingdom there is no national strategy, but strategies are developed on a force by force basis (The Police Foundation, 2014). The strategy introduced in the Netherlands in 2013 is based on 9 pillars of use: 1) media channel to communicate, 2) active engagement, 3) crisis monitoring and communication, 4) web care, 5) crowd control and event monitoring, 6) real time intelligence, 7) investigation, 8) knowledge sharing and 9) professional private channel within the organization (De Vries & Smilda, 2014).
Though fruitful for different purposes, communication using social media also generates challenges for LEA’s. One challenge with communication via social media, is finding the right tone for the conversation. Information needs to be relevant and useful for the public, otherwise the public might be left with the impression that the police are not spending their time effectively. There are different ways for police forces to communicate via social media; some try to be more personal and others more formal. Both have associated benefits and challenges. The more informal, the closer the relationship with the public, but boundaries in interpersonal relations might not be clear. Being more formal may on the other hand reduce the force’s ability to engage effectively (The Police foundation, 2014). A second challenge is to find a balance between posts that provide information on security and others that can be engaging and fun. The public needs to trust that the content of the police are from high quality sources, because then they are more inclined to engage. Many studies highlight that the public would like to see more engagement (two-way interaction), while current practice in many countries sees the police use social media mostly to send or gather information, and not interact with the public (Heverin & Zach, 2010). This seems to be reality all over Europe, and even worldwide, since police tend to mostly send information on e.g. crimes, traffic accidents, missing people, stolen vehicles, suspects or arrests made (The Police Foundation, 2014). Such social media behaviour has been demonstrated to affect public engagement. When sending messages Van de Velde, et al. (2015) found that chances to be retweeted are affected by both the content of the tweet and its sender. Moreover, the topic of the message, using a weblink, hashtags and mentions increased chances for the tweet being retweeted (ibid). Furthermore, interactions and prior engagement with the community and a personal style have been shown to be related to increased diffusion on Twitter.

4.3 Emergency services & Crisis Management

One of the core police tasks that increasingly utilise social media is responding to emergencies, incidents and crises. In case of an emergency, incident or crisis, community members need to be able to contact and inform the police quickly, and the police needs to get situational awareness in a short space of time. Here social media can be used to report common crime and incidents, as well as emergencies through social media (Johannink & Rensen, 2014). This mode is especially used by youngsters (Vries et al, 2016). Moreover, apps (e.g. SOS alarm app, Dutch app) are being launched to warn bystanders of incidents and enable them to act as first responders and provide first aid in emergency situations. Social media can an effective tool to reach out to a broad audience, but also specific target groups.

Compared to a phone call, communication through social media can also be much richer (and quicker). ‘One picture can save a thousand words’, let alone how much information a live streaming video can give. Using a livestream or sending a picture to the emergency room can save crucial minutes by providing enhanced situational awareness with a precise location in a minimal time. However, using social media for alerting police to an emergency situation or criminal act is not only promising. It is also complex and
challenging and requires the public to respond quickly and for the LEA’s to have appropriate technical system that can interpret and act upon the data received.

In case of larger incidents, police officers can use social media to warn and inform citizens. They can share time-critical information quickly to masses of people by sending one or a small number of messages that get spread. For example, during the Christchurch earthquake in New Zealand and the flooding in Queensland (both 2011) social media were the primary medium to broadcast information (The Police Foundation, 2014; Queensland Police Service, 2011). Also, after the Boston marathon bombings in 2013 social media were used to share information with the community, to keep the community informed about the identification and then search of the suspect. (Davis, et al., 2014). In case of a crisis during an event, social media can also be helpful for crowd management (Fictorie, 2013). For example, during the London riots, and the civil unrest after the NHL final in Vancouver (both 2011) police officers used social media to monitor sentiment, refute rumours and calm the local community (The Police Foundation, 2014).

During a crisis social media are not only a helpful communication tool but also enables police to gather and analyse a lot of information in a short time period. Information can be gathered to increase situational awareness, but also to identify what help is needed in a certain area, or to facilitate help offered and help needed. Foster (2016) found that 52% of the responders use social media for monitoring during events and incidents. Furthermore, analysing messages on social media has the potential to signal potential incidents as an early warning system, before they occur (Vries et al, 2011; Terpstra, et al, 2012). Finally, social media can also be used to find (trusted) volunteers after a crisis, to help in specific tasks that need to be done (Vries et al, 2011).

Crisis communication via social media can also cause problems for police responding to incidents. As we will highlight in chapters 5-1 of this deliverable, the inappropriate posting of information, whilst an event is ongoing, can cause considerable disruption to policing activities and in some cases compromise attempts by police to track suspects as they move away from the scene of an incident.

4.4 Surveillance

Surveillance can be significantly affected by social media. The presence of social media created a cross over between surveillance and intelligence. The police task of surveillance is focused on preventing unrest and signalling suspicious situations. By monitoring social media alongside other monitoring sources such as CCTV, police get to know the community and their behaviours and pick up leads of potential incidents or planned criminal activity. For example, during the London 2012 Olympics social media were monitored for messages suggesting civil unrest (Knibbs, 2013). Analysing large numbers of tweets has been shown to improves crime prediction, help make deployment decisions and increase effective allocation of resources (Police Foundation, 2014; Gerber, 2014)3. For example, the Belgian police use social media for prevention,

3The theme everyday policing will focus on opportunities, and related challenges around utilization of big data.
for instance for incidents or crisis communication and to maintain public order or to make sure things will not escalate (De Smet, 2012).

Police must know how to monitor these types of communications in order to gauge the mood of a crowd, assess whether threats of criminal activity are developing, and stay apprised of any plans by large groups of people to move to other locations. Online organized groups can grow in a short time, consisting of many loose connections. Social media enables them to easily plan meetings in the real world. The diverse Project X gatherings (and threats for gatherings) in several countries worldwide, are striking examples. Unlike before, in these loosely connected networks it is harder to identify key figures in the network (Jaitner & Kantola, 2014). Similarly, in the aftermath of an incident of mob violence, police can "mine" social networking sites to identify victims, witnesses, and perpetrators (COPS, 2011). Getting hold on the provenance of messages, understanding where the information is coming from and if it can be trusted got to a new level due to the introduction of social media.

A new challenge in social media use by LEA’s is online ‘surveillance’, particularly of monitoring terrorist groups (e.g. IS) who use social media to radicalise and recruit (young) people. One of the most influential pro-IS Twitter account has over 17,700 followers and tweets are seen two million times each month (Channel4, 2014).

Another online surveillance challenge is the many death-threats that are being shared everyday on social media. In one incident a 14-year old Dutch girl was arrested after sending a death-threat to American Airlines (copsincyberspace, 2014). Investigating such threats is a time consuming task, because assessment is still mostly done by hand. For example, the Dutch police investigates about 200 (death-) threats out of more than 30,000 each day, sent through Twitter (Couwenbergh, 2013). This is another example that stresses importance, but also the complicatedness of provenance.

### 4.5 Criminal investigation

Investigation refers to the police task of tracking down offenders of crimes. By leaving traces while using social media criminals turn social media into a potentially rich source of information for police. The police can use social media to provide ideas and solutions to improve the quality of service, policing, implementation and monitoring, or to increase control of a situation, and to prevent tunnel vision (De Vries & Kernkamp, 2012). Foster (2016) found that 54% of the police responders in his study receive information through social media from the community. Increasingly, Police officers are seeking to translate existing legal frameworks, developed for police operations in the physical world, into digital legal frameworks, because the crucial legal framework for investigations on social media is missing (Denef, et al., 2012). Departments on a national level are increasingly devoted to investigations on the digital world, whilst at a

---

*The Trolling theme (chapter 9) will, amongst others, focus on such bottom up online and offline herding patterns, new challenges, opportunities and potential solutions for law enforcement.*

*Though radicalization and terrorism is a relevant topic in relation to social media, it is not at the centre of this study. However, the topic is touched-upon in some of the themes, such as the Dark Web and everyday security.*

*The topic of death-threats, and other online norm transgressive behaviours are touched upon in the Trolling theme.*
local level police officers are being trained in order to keep their eyes and ears open online. A challenge for investigation is to obtain data from the different social media networks, which have different methods of sharing data (or not sharing) with the police (ibid.). The challenge is both in legal (e.g. subpoenas) and veracity in technical means (e.g. API’s). For example, a victim of revenge porn from the Netherlands has tried, without success, to force Facebook to share intelligence to find out who put a sex film with her in it online. The trial ended in a disposal (Back, 2016). So no position is taken yet in whether social media are obligated to provide user-information if a user is suspect of violating the law.

Social media has, overall, proved to helpful in solving crimes, and many police departments use them for investigations. In the UK, from 2007 until 2010 crimes that were resolved using Facebook grew by 540%. Crimes resolved using Twitter grew similarly, along with the popularity of the medium (Knibbs, 2013). The UK police for example, increasingly use social media (primarily Facebook and Twitter) for intelligence and investigation (The Police Foundation, 2014). This has often involved regularly visiting and monitoring certain sites that are infamous for being used to facilitate criminal and antisocial activity. Aiming to gather information and evidence police frequently visits these websites, which include for example the dark web, and sites that allow or stimulate hate propaganda, fora which allow for norm transgressive behaviour, such as 4Chan’s /b forum and chat rooms, used to target vulnerable victims for sexual abuse (The Police Foundation, 2014). For example the Victoria police in Australia uses social media for both criminal investigation and enforcement. They have a number of covert operations on social media (CLEDS, 2013). The Dutch national police use Twitter and YouTube to gather information and use this to solve crimes. They have also used social media for high profile cases, such as the Project X riots in Haren, the Netherlands, but also for petty crimes. For example, the police in The Hague could identify the perpetrator of a crime after citizens recognised the perpetrator on a YouTube video the police shared (Meijer, et al., 2013). The Belgium police also regularly use social media to gather information, and enable people to give more anonymous tips so that the police can do their job more effectively with more information (De Smet, 2012).

It is not only the police can use social media for investigations; they can also ask the community to help them. Social media networks consisting of many actors can help in information gathering to support police investigation and prosecution. The investigation on MH17 (Bellingcat, 2015), as organized by Bellingcat, and done with help of the crowd, proves the effectiveness of crowdsourcing crime cases.7

---

7Involving the community in investigations will be further analysed in the chapter DIY policing - chapter 5 of this deliverable.
4.6 Community policing

Social media can stimulate community policing, by enabling all employees in a police organization to have fast and (almost) autonomously contact with citizens (Lieberman et al., 2013; Meijer & Thaens, 2013). Better communication, in theory, enables ‘active citizenship’, which enhances effective community policing. In this situation, citizens are better able to help in reduction of crime and disorder, and improve their self-defence and community members can share their ideas to solve community problems (Lieberman et al., 2013). The community can participate in three ways:

1. citizens give the police information through social media;
2. citizens can put experts or police under pressure through social media;
3. citizens can help with investigations (De Vries & Smilda, 2014).

Neighbourhood police officers for example, use Twitter and Facebook extensively and they get information from their community on for instance drug activities, illegal fireworks or street races (Meijer et al., 2013). Social media can also be used to motivate the crowd to volunteer, for example restoration of public places that were affected by riots or demonstrations as seen in the ‘clean up’ after the London 2011 riots (De Smet, 2012). Another way for the community to stimulate community policing is by organizing ‘neighbourhood watch’ such as through a WhatsApp group, or a commercial service like Nextdoor. Often the neighbourhood police officer is also group member, and can provide tips and help and answer questions (De Vries, 2016).

Such community policing practices are not unproblematic. Challenges may arise around privacy, vigilantism and when citizens employ tasks that are legally bound to the police or other security stakeholders, and therefore cannot be crowdsourced (outsourced to the crowd), e.g. violence, judging or a whole investigation (De Vries & Smilda, 2014). Such activities have also posed critical questions about the roles and responsibilities of citizens who get involved in crime prevention.

4.7 Intelligence

The police use social media to gather information and improve intelligence operations. The speed of social media provides a crucial advantage when appealing for witnesses, or, information or looking for missing persons. Social media, for example, can be used to enable the police to activate citizens to assist with missing persons inquiries. For example in the UK in December 2010 Facebook was used to call for anyone with information to come forward when a woman (Joanna Yeates) went missing and there were serious fears for her safety (The Police Foundation, 2014). A further example comes from the Victoria police who routinely use social media for passive intelligence and internally for intelligence on how their own people are acting (CLEDS, 2013). The Dutch national police also have a real time intelligence centre (RTIC) across the country, based on the real time crime centre in New York, which monitors social media for each

---

*(The theme DIY (Do It Yourself) policing and Everyday Security will also focus on community policing where citizens work together with local police.

*In the chapter 5, everyday policing and chapter 8, dark web intelligence will be further explored.*
MEDI@4SEC
The Emerging Role of New Social Media in Enhancing Public Security
Grant Agreement no 700281

region, including Twitter and Facebook. Social media can also help with intelligence gathering by providing access to the ‘wisdom of the crowd’ (Denef et al., 2012).

Although social media can be helpful in intelligence gathering, it also brings forward challenges. One challenge is filtering and identifying the useful information in the overload of information that is widely and openly available as this creates provenance and trust issues. Potential reputational damage can occur when the police are not able to process and filter all information available and hence miss important information. This happened during the summer riots in London, UK, where there was too much data on social media to process (The Police Foundation, 2014). Another challenge is that the police has to “assess the value and accuracy of any intelligence obtained”. Identifying credible information from rumours and speculation is increasingly difficult (The Police Foundation, 2014). For example, two rumours that could not be refuted, nor confirmed during the Project X riots in the Netherlands were that one girl was killed and that the Hells Angels were on their way to join the riots (Vries, 2013). This created online chaos and a lot of media attention, which in turn put more pressure on the people in charge.

4.8 General Reflections

The introduction of social media in the domain of public security has shown different on conditions for success. Many police organizations adopting social media, consider the usage very fruitful for different purposes in both the operational police tasks, e.g. investigation, crowd control (Knibbs, 2013), organizational purposes, e.g. reputation (Jamieson, 2016) and recruitment (De Smet, 2012). Mauritz (2011) argues that entrepreneurship, employees trying new things within the organization, is crucial for the experimentation with social media. Besides entrepreneurship it seems wise to create a strategy of correct usage of social media, conducting organizational goals and sufficient ICT necessary for successful implementation of social media (Mauritz, 2011).

Furthermore, the more social media are used the more effect and the more response can be expected, which also helps to gain more interaction (De Smet, 2012). Social media usage, in this sense, is self-perpetuating, but must be undertaken with care. Here the tone of the messages is important. Messages sent from a central account should be more formal whilst messages sent from a personal police officer account should be more informal. However, this is a fine line (Foster, 2016). Importantly, engagement requires not only sending information, but also two-way communication (Foster, 2016; The Police Foundation, 2014). Finally, focussing on training and awareness will strengthen the organisation itself, individuals in the organisation need to know what is possible and how to use it appropriately (CLEDS, 2014).

Furthermore, the use of social media has both brought forward tremendous benefits as well as challenges. Being present on social media and using data from social media takes a lot of time, which conflicts with cutting in police-budgets (The Police Foundation, 2014). A second challenge is the large amount of different types of social media which have different characteristics and lead to people being spread over different digital places. Furthermore, anonymity of social media brings up challenges of trust and privacy, because it is not clear who did what and to know if something is trustworthy or
not (De Smet, 2012). Finally, the frequency with which police departments put messages on social media differ substantially (Lieberman, et al., 2013).

4.8.1 Strength and opportunities

The characteristics of social media for public security planning - both positive and negative - can be indicated by making a Strengths, Weaknesses, Opportunities and Threats (SWOT) analyses of social media. Here, instead of a person or company, social media is at the centre of the swot.

Social media enable two-way communication at high speed, anywhere and anytime (strengths). This enables law enforcement agencies to get connected and maintain contact at minimal costs (opportunities). Neighbourhood officers who use social media can get in contact with lots of people they did not know before (Meijer et al., 2013). This, combined with the transparency (strength) that social media bring forward, create opportunities to increase trust and engagement and improve reputation (Denef et al, 2012). Moreover, these strengths, combined with the richness of social media enable law enforcement officers to collaborate with the crowd (opportunity) and so increase effectiveness (Global Advisory Committee, 2013). Furthermore, innovative solutions in emergency response are being developed, making use of these strengths of social media (De Vries et. al, 2016). The speed, richness of information and independency of location and time (strengths) enable law enforcement officers to contact bystanders in case of an accident, either for information (eyewitnesses) or for emergency help (opportunity) and enable crisis communication (De Smet, 2012). The masses of data social media create (strength) also enable opportunities for early warning (Vries, de et al, 2011; Terpstra et. al, 2012) and crowd management (Fictorie, 2013). Analyses of these (combined with other) data (strength) also offer opportunities for more intelligently considered surveillance (Gerber, 2014).

By enabling direct and fast communication (strengths), social media creates opportunities for collaboration between law enforcement officers and community (community policing), for both surveillance and criminal investigation. Moreover, the transparency (strength) of social media, make criminals acting online leave traces, which can help in criminal investigations.

4.8.2 Weaknesses and threats

Social media are decentralized (weakness) thanks to the many diverse platforms. This can, for example, lead to missing out on relevant messages and hence on information (threat), or receiving information late even though social media are being monitored (Broekman & Menkhorst, 2013). This also leads to challenges in acquiring or validating information (threat). It is not only law enforcement agencies that profit from the speed and time and location independency - those who want to organize riots can reach and gather large amounts of people in short time (threat). In these loosely connected groups of people, it is hard to identify key figures (Jaitner & Kantola, 2014). In addition terroristic organizations, like IS can make use of the ability to reach people all over the world (threat), e.g. trying to recruit them to fight the Jihad (Channel4, 2014) and individuals can abuse and harass others anonymously (threat). Transparency of social media can also create both opportunities and threats. Not only criminals leave traces on
the Internet, also law enforcement officers can expose their tracks (threat). Criminals can use these tracks to find out who is after them and plan revenge or make threats. Moreover, criminals could intentionally create false traces, to mislead law enforcement officers. An extra challenge is that criminals find new solutions to hide their tracks, since they moved to the anonymous dark web (threat) where they are increasingly difficult to identify, especially given increasingly sophisticated encryption devices than can be used.

Though social media provides rich information, they can also provide ‘poor’ information, since context is missing. The overload of messages (weakness) contains, for example lots of (death) threats that miss context, and therefore are hard to interpret (threat). Hence, lots of police capacity is devoted to threats that appear to be messages sent by ‘innocent’ teenagers (Couwenbergh, 2013).

Adopting social media also brings forward a range of dilemmas, which include the following:

- a lack of clarity over ethical boundaries and laws;
- how active should the police be with online offenses?
- how best to train the police to use social media effectively and appropriately;
- to what degree should the police take control on social media,
- how transparent should the police be online;
- can the wisdom of the crowd be trusted;
- how best to verify the accuracy of instantaneous social media information before sending it out;
- what social media are next and how will this affect the boundaries of work and personal lives that appear intertwined (De Vries & Smilda, 2014).

Table 4-1: Security tasks versus themes

<table>
<thead>
<tr>
<th></th>
<th>DIY policing</th>
<th>Riots and mass gatherings</th>
<th>Everyday security</th>
<th>Dark web</th>
<th>Trolling</th>
<th>Innovative policing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication and engagement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intake and crisis management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Surveillance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criminal investigation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Community policing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intelligence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Within the tasks we have discussed in chapter 4, multiple themes can be addressed that have been impacted by social media and play a significant role on the current domain of public security and policing (see table 4-1). These will be discussed in chapters 5-10. The table below shows how the different security tasks in this chapter relate to the six themes we focus on in the MEDI@4SEC project: DIY policing, riots and mass gatherings, everyday security, dark web, trolling and innovative market solutions. The next chapters will dive into these six themes to draw out key challenges and opportunities that will for the basis of discussions in our policy and practice dialogue workshops in WP2.
5. DIY policing

The internet, smartphones and social media have become tools for citizens to perform activities that fall within the range of police work and the work of other organizations dealing with public security. As modern Sherlock Holmes they assist the police and go beyond. Citizens investigate crimes, identify suspects, form vigilante groups, hunt paedophiles and report on crimes. Open data sources have proved to be valuable for gathering intelligence and solving crimes and open up professional work to citizens. The information, tools and expert knowledge have spread through the web. Social media-DIY (do-it-yourself) policing by citizens puts pressure on professional security workers that now have people and organisations from all over the world on the side lines or at the centre, doing some or all of their work. Citizens, however, have neither the authority nor the same legal framework for their actions as police forces do. The key questions for many security planners when advancing a social media strategy therefore relate to the consequences of where and how to cooperate with citizens, where to take control and how to avoid negative ethical and legal effects.

5.1 The use of social media in the domain of public security and policing

DIY policing occurs in three main forms. (1) Citizens sometimes act entirely on their own and independently of any public security organization to investigate crimes and punish suspects and offenders. (2) Citizens limit themselves to connecting and finding or checking facts and act as information providers for public security organizations or (3) citizens combine aspects of the two (Huey et al., 2012). As detailed below, beyond such citizen-driven initiatives, there are few examples when DIY policing is actively taken up by public security organisations.

DIY policing is often stimulated by emotive 'local issues and often brings to the fore concerns over how and when citizens should engage with, and be responsible for, public security. For example, motivated by emotional media reports about cyber grooming, online groups have formed where members pose as child victims in cyber grooming and meet suspects. While these groups publicly offer their free services to law enforcement agencies, they also act independently (Huey et al., 2012). Likewise, a phenomenon named "digital vigilantism" describes how citizens engage in offensive acts to counteract actions of other citizens that they do not agree with. This has included extreme terrorist acts and participation in riots, as well as, "mild breaches of social protocol" (Trottier, 2014). For example, after the riots in Vancouver in 2011, people, for example used Facebook to publicly "name and shame" photos of rioters they had taken using mobile phones (ibid.). While this information supported police investigations, it also constituted an overwhelming amount of data that often lacked the required contextual information. The citizen action in this case has also been characterized as an “unintended” DIY-society (Rizza, 2014).

Another form of DIY policing is the use of open data sources to solve 'cold' cases that are no longer actively investigated by the police. For example, in the USA in a case where more than 10, 000 corpses remain unidentified several online communities such as the
Doe Network (named after John Doe’s) have formed to match people from missing lists with unidentified corpses (Halber, 2015).

Citizens also investigate international incidents that go well beyond the scope of a single police force, such as the investigation undertaken by Bellingcat into the airplane crash of MH17. Here, citizen action provided useful insights by collecting information from various sources, including many social media channels (Romein, 2016).

Instead of supporting the police, citizens can also use social media to highlight misconduct of the police (Trottier 2014). As a counter action against recent shootings of black people by U.S. police forces, social media have served as a strong platform for citizens to discuss police actions (Jackson, 2016). DIY policing also takes place in crisis situations or for large events, when citizens such as in situations of earthquakes, where citizens’ social media use support crowd management and emergency relief (Meier, 2015).

Beyond citizen-driven DIY policing and in an attempt to increase the engagement of citizens in public security, some police forces are actively seeking to mobilise citizen investigators. For example, the Dutch police have created citizen networks (e.g. BUGERNET, Politieonderzoeken.nl) where citizens can register as potential volunteers in police investigations (Meijer, 2014). In a further example – a Neighbourhood watch-style WhatsApp project - the police are cooperating with citizens to exchange information and prevent burglaries (Akkermans, et al. 2015). This includes citizens in actively patrolling the streets to prevent crimes and burglaries (Lub, 2016). These projects decrease the boundaries between what can be considered DIY policing and regular policing but are relatively unique to the Dutch context. In other countries, such as the USA and South Africa, volunteer groups have been tested on a much smaller scale involving only small group of social media volunteers (St. Denis, 2011; Omanga, 2015).

5.2 The influence and impact of social media use in the domain of public security and policing

Actions by citizens and the collaboration between citizens and police forces impact public security and policing in many ways. Citizens’ actions can be effective yet controversial. When citizens publish names of offenders and personal details, they can reach hundreds of thousands or millions of people (Trottier, 2014). In the case of a woman who was raped and murdered, civilians on social media advocated for people to “publicly hang” the suspect and included a photo and name of the person who had admitted to crimes (Milivojevic, et al., 2014), establishing a link between the themes DIY policing and Trolling. DIY policing can also produces wrong and misleading information. In the aftermath of the Boston Marathon bombing in 2013, citizen investigations led to misinformation on suspects and rumours being wisely circulated on social media, endangering people that got incorrectly identified as suspects. (Starbird, et al., 2014)

Social media and citizen action have, however, also been shown to be an effective tool supporting the actions of law enforcement agencies. The above-mentioned online communities on cold cases successfully identified corpses (Halber, 2015). In "clean-up" initiatives online activists tracked down sexual offenders and reported their sites to
social media providers and, in one project alone, got 13,000 accounts deleted (Huey, et al., 2012).

Dutch Police initiatives in the area of DIY policing are notable in their success; even though the police only consider 9% of cases for the BURGERNET network, is reported to account for 50% of successful police actions (Meijer, 2014). They allow the police forces and local governments to reduce their efforts while increasing social control and decreasing social problems. (Bervoets, et al, 2016). The active involvement of residents in preventing burglaries, by starting WhatsApp groups, has resulted in a sharp decrease of the number of burglaries. The number of burglaries per 1000 inhabitants decreased by approximately 40% with no evidence of burglaries moving to adjacent or adjoining neighbourhoods where no such WhatsApp group was set up (Akkermans, et al. 2015). Such initiatives also increase the chance of an arrest, as a result of receiving information from citizens (directly or indirectly) (Hoeven, 2011). Citizens also feel safer (Land, et al, 2014).

5.3 Inventory of strengths, weaknesses, opportunities and threats

5.3.1 Strengths
Police forces have data available that, when opened to the public, can support DIY policing (Halber, 2015).

5.3.2 Weaknesses
Several citizen-driven DIY activities are motivated by weaknesses of police forces to respond or operate in a way that citizens consider appropriate. They fall into two categories: The first weakness is the limited resources of police forces, especially in the case of crime happening online. The structure of the forces and the variety of crimes committed online have left police forces in a situation where crime online goes often unnoticed (Huey, et al., 2012). The second weakness of public security organizations are their limited responsibilities and organizational boundaries that cannot address the structure of crimes that cross state or country lines (Halber, 2015).

5.3.3 Opportunities
DIY policing makes available the resources of citizens for public security organization. The police benefits from a networked society, where citizens can join and provide new intelligence or even a ‘theory’ on an ongoing case.

To secure the cyberspace, motivated citizen groups can become a significant partner adding additional manpower to public law enforcement. Citizens provide additional eyes and ears and often also professional expertise from other related fields, e.g. in IT (Huey, et al., 2012). The cooperation of citizens can play an important role in the detection of offenders, since solving a crime largely depends on the quality and quantity of the information that citizens provide to the police immediately after the relevant incident (Sollie, et al, 2013). In kidnapping cases, the extra value for investigative reporting is mainly in the speed and combined intelligence with which a large group can be reached, or that a very specific audience can be targeted (Schoenmakers, et al, 2014).
Beyond these opportunities in policing efficiency and effectiveness, citizen interaction with police forces can have a positive effect on police legitimacy (Meijer, 2014).

### 5.3.4 Threats

A serious threat of DIY policing is vigilantes carrying out retributive actions, often anonymously and therefore with relative impunity. Citizen action taking over the rights are normally transferred to organizations like the police, can endanger fairness, respect and democratic values (Rizza, 2012). DIY policing on social media empowers citizens to bypass existing public security organizations (Trottier, 2014).

Moreover, quality is an issue: evidence posted by citizens lack context and remains unclear, raising the chance for citizens to be wrongfully accused (Penterman, 2012). Misinformation can spread fast and is difficult to identify. (Starbird, et al., 2014). Even when information is correct, social media can increase public awareness and, in consequence, the risk of unfair trials (Milivojevic, et al., 2014).

The distribution of volunteers in DIY policing is also a potential concern. Users in such DIY police support networks commonly underrepresent woman and young people. There have been warnings that initiatives such as BURGERNET can have a negative effect on social cohesion. Turning every citizen into would-be police officers poses the risk of decreasing trust among citizens; citizens are not properly trained to act on behalf of other citizens, nor is it possible to hold them accountable for their actions (Meijer, 2014).

Undefined legal frameworks also threaten police-citizen collaboration and for some DIY policing is described as an activity that is not desired by law enforcement, as the missing authority of citizens and legal consequences remain unclear (Huey, et al., 2012). Additionally, when acting as DIY police officers, citizens on social media often become personally involved through and then, too, might end up linked to a crime (Trottier, 2012). DIY policing on social media also creates a close dependence on corporate social media platforms (Trottier, 2014).

Another threat from DIY policing is that it reveals the limitations and inability of police forces to solve crimes themselves and thus threatens their legitimacy. Journalists covering successful DIY policing in their reports have been raising the question why police forces were not able to do what citizens managed to accomplish. (Halber, 2015).

Finally, there are also practical threats with DIY policing. The involvement of citizens can produce an overwhelming amount of data that is difficult to handle for law enforcement agencies (Trottier, 2012).

### 5.3.5 Conditions for success

Researchers reflecting upon success factors for the Dutch initiatives highlight that for neighbourhood watch programs it is important to take the local context into account (Lub, 2016) in order to better understand how social media use for public security can enhance the degree of collective resilience in a neighbourhood. For the police organization operating in this novel context it is important to have organizational freedom to act differently and tailor the initiative according to local understanding.
(Land, et al., 2014). For police-citizens platforms it is also important to set up a central control point for the deployment of social media (Bogaard, 2012).

5.4 Reflection and conclusion

DIY policing is in many ways a phenomenon of growing relevance for public security planners. On the one hand, we see citizens taking coordinated action in places where public security falls short or fails. Citizens often investigate when the police have given up, do not have enough resources, or cannot respond in a speed that the public expects. Thus the question arises as to whether DIY policing can become an indicator for public security organizations to find the hot spots in which to increase their efforts or to reduce them and allow citizens to take over. On the other hand, it appears that (especially Dutch) police forces are making a concerted effort in co-creating security jointly with citizens. The many platforms and initiatives that are emerging underline the Dutch forerunner role in making best use of and, to a certain degree, encouraging DIY activities. Overall though, DIY policing raises a number of delicate ethical questions. Whilst empowered citizens can be enabled to assist the public security effort, at the same time, they also can create great harm, when acting in irresponsibly. The emergence of DIY policing also questions the general division of responsibilities and power between citizens and LEA’s.

The following key questions have emerged from this topic:

- Can we understand DIY policing activities as signals for missing activities in law enforcement?
- In which areas can DIY policing be a meaningful addition to traditional police work?
- What tools can best manage police-citizens interaction?
- What are the means to contain DIY policing and prevent the negative effects and risks of DIY policing?
- How does and will DIY policing impact the relative roles of citizens and LEA’s?
6. Riots and mass gatherings

A mass gathering is when a large number of people come together in a particular location, indoors or outdoors for a specific common purpose either in an organized and planned way for a defined period of time or in an instantaneous or spontaneous manner, possibly motivated by organizers, participants or third parties or due to an unexpected response to an incident or emergency situation.

Mass gathering can be events of any kind, type, scope and content or protests and demonstrations, immigrant or refugee movements etc.

Due to their nature, mass gatherings are prone to various threats. These include the potential for riots, mass panic that can lead to stampedes or other accidents, violence among participant groups or individuals, etc. In addition, mass gatherings also constitute a very appealing target for terrorist attacks and, at the same time, they can be the direct result of such attacks.

The expansion of social media promotes social movements and mass gatherings both in terms of organisation and coordination of the event itself and by enabling more exposure that leads to increased participation. Importantly, social media can also, conditionally, confer the added capacity of enhancing preparedness against risks that can manifest before, during and after the event and also reduce their potential impact.

6.1 The use of social media in the domain of public security and policing

Social media has emerged as a prominent channel for dissemination of information during real world events. This development gave rise to an online community which has several distinguishing features and expectations: interactivity, immediacy and mass-inclusivity. Law enforcement agencies (LEA’s) cannot hope to realign those expectations to fit their own resources or the traditional modus operandi of the police. Rather, to use social media effectively as part of contemporary community engagement, police will need to adapt to meet the expectations and protocols of the online community (Australian Commissioner for Law Enforcement Data Security, 2013).

6.1.1 Use of social media data gathering (crowdsourcing) – Information Intelligence

During mass disruption events, people digitally converge to generate massive amounts of data within social media networks derived directly from the field. The majority of these communications are derivative and are commonly viewed as a form of noise that must be filtered, verified and aggregated in order to be of use. This is methodologically challenging (Procter et al., 2013; Zubiaga, et al 2015, Panagiotopoulos et al, 2014). Crowd and individual behaviour can serve as a collaborative filter for identifying people tweeting from the field during an event. This hypothesis has been tested using models from machine learning techniques. (Starbird, et al, 2012).

---

10 The main question of how one polices a leaderless organisation (a 'swarm') has traditionally been seen as largely unsolvable. Individuals can be tracked down and arrested, sites can be taken down, services can be blocked or wound up, but others will replace them (Alexander, 2014).
More importantly, social media can be used to monitor a mass gathering event throughout its entire development phase (before, during and after). An example of that can be seen in UK's Metropolitan Police Service which collaborated with Hewlett-Packard (HP) to deploy social media analytics tools (IDOL- Intelligent Data Operating Layer) to manage high volume of data traffic produced throughout the summer of the 2012 London Olympic Games.11

6.1.2 Creating content to communicate and coordinate a safe event/protest/summit

As a general principle, social media used by the Police to send messages and post content in a positive, friendly, instructive and helpful tone tend to encourage safe events and discourage further potential disorders from emerging. As an example, during 2011 Vancouver’s Stanley Cup riots, Vancouver Police Department, using Twitter, included transportation information on closures and routes, instructions to submit photos and videos as evidence, encourage the crowd to stay calm and to get people to allow emergency services to do their jobs (McCann, 2011). Another example is the 2011 riots in England, where the Police engagement with social media included situation reports, retweeting situation reports from other police accounts, appeals to the public not to listen to rumours, updates on police activities, urging people to support the police, condemning rioters, humour and information about clean up events (Procter, et al, 2013). Activists and citizens have used social media to coordinate activities, plan protests, and publicize often high-quality information about their causes. An example of that was the 2010 G20 summit in South Korea where anti-G20 protests took place (Lee, 2015).

6.1.3 Social Media use as organizing tool

Social media can be used as an organizational tool to encourage and form part of both riot and anti-riot forces. Facebook, Twitter and Blackberry Messenger were some of these tools used to organise the by riots of August 2011 in England. Authorities on the other hand relied on open social media sources to observe the course of events and intervene. Two important ways of intervention were the riot clean-up campaign and the initiative to identify looters with a campaign supported by over 60,000 people with #RiotCleanup becoming one of the most popular hashtags on Twitter in the wake of the riots. Social media were also used to organize charity events and fundraising campaigns for small business owners whose properties had to be restored after the riots. (Panagiotopoulos, et al, 2014). Other examples of social media applications being used to organise mass gathering participants include “Sukey”, an information exchange platform which aims to protect protesters from police “kettling” (a strategy used to restrict protesters’ movements and detain them) as well as “Firechat”, a communication platform that can work without being connected to the internet via a localised P2P ad-hoc network which proved to be a significant alternative to Hong Kongers when the government decided to ban the use of Instagram following a protest against it that was organised using that very application. There is also emerging evidence that social media is frequently used to organise irregular migration via networks of various players such

11 HP proposed this trial to help better understand and utilize social media analysis (SMA) for community engagement before the event, look into issues that emerge during the event and assess the aftermath of the event. (Hewlett Packard, 2013).

6.1.4 Social media use in terrorism
The literature on instances of terrorist activity highlights some of the potential problems arising from current approaches to the use of social media under these circumstances. The evidence suggests that clear social media strategies are not yet widely implemented by the authorities. This lack of strategic engagement may often be due to the understaffing and under-prioritisation of social media in emergency services' provision e.g. in the case of the Norwegian authorities, who failed to keep the general public sufficiently informed of the events surrounding the atrocities which occurred in Oslo and the island of Utøya in July 2011, a response which has been criticised as indecisive, disjointed, confusing and inept. Research in this area highlights the importance for the authorities to monitor social media activity during this type of events, and points to the need for interventions of their own to provide accurate, up-to-date and authoritative information, correcting misunderstandings and quashing unsubstantiated rumours (Bartlett and Reynolds, 2015; Mair, 2016; Archie, 2016. This need is illustrated by the outcome of the FBI’s attempts to use social media to identify the perpetrators of the Boston Marathon bombing in 2013. While there were many very positive outcomes of social media engagement under these circumstances (such as the coordination of aid), and some useful information was gathered to help the investigation, this soon got out of control, leading to online 'trials' of innocent people who had been wrongly identified (Project ATHENA WP3_D3, 2014).

6.2 The influence and impact of social media use in the domain of public security and policing

6.2.1 Impacts on identifying individuals
Social media messages produced in mass gatherings can contain significant information that can be indicative of the sender's personal details and her/his location. Impacts on identifying individuals in the field could vary depending on the cause for their participation and actions, in the event e.g. in mass gathering events people might want their accounts to be identified in order to have their personal opinions heard, whereas in political demonstrations, protestors are put in danger to be identified as opponents to the political regime and they try either to avoid the use of social media or provide misleading references to their location or other information. (Starbird, et al, 2012). On the other hand, there are cases where locating individuals is in the best interest of those that seek to be found. Cases of missing persons in the aftermath of disasters or mass gathering incidents have very successfully been facilitated by social media, examples for such initiatives include the “Google Person Finder” project and social media sites for established organisations such as "Amber Alert", UK's "Missing People", or the "Find the Children".

6.2.2 Impacts of data/info/rumours spreading
Information pushed to the crowd is influencing individuals' decisions whether to engage or not in rioting or anti-rioting activities and campaigns. The impact of Twitter during
the riots 2011 in England was significant with 2.6 m tweets related to the events and 7 million Twitter users involved in the riots clean-up campaign. Tweets such as rumour spreading (e.g. a rumour that the London Eye was on fire) either did not attract attention or were re-tweeted so as to be publicly condemned. Tweets also referring to information and warnings about legal actions in progress against potential offenders or those arrested on the spot discourage riots for further actions (Panagiotopoulos, et al., 2014).

6.2.3 Impacts of citizen-generated content
User-generated content on social media can lead to increased pressure on police agencies to appear efficient in dealing with and responding to public concern about crime (Schneider, 2014). On the other hand, people taking and posting photos and videos in social media during the events can encourage others to participate in criminal and/or antisocial behaviour. This influence may also have the effect of peer pressure as a motivating factor especially in youths’ decisions under fear of ostracism and their need for inclusion. The high volume of user-generated content can also play a role in identifying rioters which can lead to disruptions in their personal and family lives. For instance, during the 2011 Vancouver’s Stanley Cup riots, some participants who had been identified, through photos on social media and websites, were subsequently harassed and in at least one case, an entire family was threatened. Some participants lost their jobs, employers suffered backlash, even though they were not involved, whereas others tried to remain hidden (McCann, 2011).

6.3 Inventory of strengths, weaknesses, opportunities and threats

6.3.1 Strengths

• Social media provide immediate and flexible tools to disseminate information and communicate through brief public messages (e.g. Twitter) (Panagiotopoulos, et al., 2014).

• The social media developed by police as trusted and authoritative hub making it a key, valuable and reliable source for a large volume of people. Police media acts as a centralised clearing house including information and details on behalf of other departments, authorities or forces. Information is distributed to people in affected locations who otherwise have no means of communication (Queensland Police Service, 2011).

• Interactive communication platform with low cost. It provides 24/7 access to immediate feedback and information from the public and local authorities at scenes of incidents.

• The collection and analysis of data is perceived to be a more proportionate and fair form of intelligence gathering than other tactics and also provides a substantial resource for situation awareness (Dencik, et al, 2015).

• Social media enable the Police to communicate with often difficult to reach groups such as migrants (Accenture, 2012).

• Citizens’ security feeling and confidence are enhanced interacting and sharing info with police.
6.3.2 Weaknesses

• Due to the large volume and sources of social media coming from the field, data has vast amount of noise and must be filtered in order to end up with the good quality data.\(^{12}\)
• Police are not able to have full control over their public image and can have their legitimate authority challenged and criticized via social media (Schneider, 2014).

6.3.3 Opportunities

• Social media can bridge the communication gap between citizens and police and increase citizen involvement with organized data/information management during a mass gathering.
• Social media interactions with the features applied in mass gathering-rioting can also be used to make local government more responsive to deal with everyday issues in collaboration with citizens (Panagiotopoulos, et al, 2014).
• Retweeting or sharing messages and posts during an event makes an account or profile act as an information redistribution hub, not only for social media but for other sources of traditional and online media (TV, radio, newspapers, blogs, websites etc.) (Procter, et al, 2013).
• Real-time analysis of social media can provide significant additional options for responding to a particular incident and obtaining a detailed and concise operational image.

6.3.4 Threats

• Digital material posted online and the conversations fuelled by riots and mass gatherings facilitates communication among geographically dispersed people in several networks and enable the rapid organization and expansion of rioting finding the crowd and the authorities unprepared.
• The spread of overloaded false rumours, misleading information or even trolling before and during the mass gathering or riot events.\(^{13}\)
• Legal restrictions for collecting, sharing, storing and utilising data harvested from social media during mass gatherings. Public behaviours and expressions of opinions against the promoted narrative themes published before and during a protest event can be subjected to surveillance and punishment (Lee, 2015).

6.3.5 Conditions for success

Data coming from the field through social media platforms due to its large volume and ambiguous quality needs to be evaluated and interpreted correctly. To do so, it must first be collected, filtered and go through an analysis process using appropriate tools and methods that can range from technological solutions and analytics to experience

\(^{12}\) In the context of mass disruption, where veracity of information is vital, machine-only computational solutions are not ideal, and the information resulting from this or any filtering technique must be further combined with human judgment to assess its accuracy. Self-reported location in social media (e.g twitter) can be inaccurate due to on purpose misinformation or due to changing physical location of the Twitterer (Starbird et al, 2012)

\(^{13}\) The rumours created before and during the events emerge the need for development of new tools for their identification and elimination. With the development of tools for collecting, filtering and analysing tweets and comments for inaccurate and misleading information with dangerous implications can be avoided. An example of successful handling of rumours was the U.S. Federal Emergency Management Agency (FEMA) Rumours Control section in their website where they specifically verify or deny the various claims made regarding particular incidents.
based decision making and relevant training. Even if the police use social media there must be specific plans for interpreting and using it in the case of a major crowd disturbance or a riot. More specifically, police forces need to continuously and systematically review their approach to social media so they are always able to escalate readiness, to adopt and engage (and mainly disengage) in a creative - effective way.

One of the main weaknesses when a mass gathering/riot is breaking out is the lack of an Emergency Action Plan (EAP) - a formal written plan which identifies emergencies and describes the measures to minimize impacts and ensure public security. Without one, limited Law Enforcement Forces (LEA) personnel availability, structure and chain of command, dispersion of LEA in key scene - spots and the ability or not to predict the outcome are bound to occur much more often. In addition, the EAP can also be used to determine which platforms are most appropriate for the community. The guidelines should be organised according to three phases of emergency response: preparation, response during the actual crisis, and in the recovery phase.

There are some major challenges in real time social media control and data detection during mass gatherings linked to the need for technological solutions (algorithms, techniques, tools and infrastructure). These are need to filter the large volume of data produced and being monitored in short space of time whilst at the same time balancing this with concerns over anonymity and the protection of privacy (Project ATHENA WP3_D3, 2014).

6.4 Reflection and conclusion

The use of social media in mass gatherings involves various stakeholders such as citizens, riots, police forces, emergency response organizations, digital volunteers etc. involved in different informative and collaborative activities related to information broadcasting, sharing, searching, reporting, status awareness, responding, action coordination, data collection, filtering, aggregation, analysis, visualization and presentation in order to identify and confront crowd, situations, actions, characteristics, behaviours and trends related to public disorders caused by rioting. The entirety of this varied spectrum of stakeholders needs to be taken into consideration for their communication plan.

The incorporation of social media into pre-existing emergency management systems is inevitable, owing to the sheer weight of public usage of such facilities. Moreover, as social networks can be two-way means of communication, they can enable the use of official and unofficial information in tandem. In this optimistic view, the citizenry is viewed as a powerful, self-organising and collectively intelligent force (Gao et al. 2011b).

The literature review has shown riots and mass gathering policing to be a critical issue (and incidentally currently on the rise) which LEA’s need to take into consideration. The use of social media has to be integrated into their daily activities by increasing their efforts to communicate and collaborate within the so called “digitized society” and increasing situation awareness as disruptive events unfold. LEA’s should invest to develop and implement a policy to address such events while retaining their central character and nature, a fundamental expression of human rights in a democracy.
In conclusion, the security questions that need to be addressed with regard to social media in the following years include:

- How best to re-invent the current policing paradigm to incorporate new tools (including message filtering and evaluation technologies), organizational structures, staff, policies and technological infrastructure to support the use of social media?
- How to establish a communication strategy that ensures the appropriate use of social media platforms by authorities in a positive, friendly, instructive and helpful tone that promotes citizen engagement and fosters citizen-police collaboration and trust.
- How to provide targeted communication to specific (and sometimes hard to reach) social groups such as elders, people with disabilities, migrants, etc. to fit their specific needs?
- How best to design, develop and implement plans to establish the protocol for social media use during security-related incidents and investigations?
7. Everyday Security

The concept of “everyday security” refers to the daily management of public security with the aim of preventing and responding to offences which are committed in public spaces and which threaten the security - actual or perceived - of the community in its daily life. The recent massive increase in social media use has drastically transformed people’s communication and information habits, providing authorities with new intelligence sources and platforms for communication. These new opportunities raise numerous questions, for example, in what ways do the data and tools available through social media influence the work of intelligence services and law enforcement agencies (LEA’s)? How do local authorities, which are first in line of defence when it comes to community security, use social media to facilitate and enhance their local crime prevention strategies? How can community policing initiatives supported by social media contribute to the everyday management of security?

7.1 The use of social media in the domain of public security and policing

According to the literature, use of social media in the domain of everyday security is primarily focused on the following aspects: communication (educating citizens, reputation management, public security awareness), enforcement (finding evidence, prosecution, identification of suspects) intelligence (collect and analyse information, crime prediction, crime prevention) and crisis management.

7.1.1 Communication

LEA’s, governments and police forces use social media in their day-to-day activities as a direct channel for communicating with the public, predominantly as a one-way communication tool. They use social media, mainly Twitter, Facebook and Youtube, to reinforce their relationships with citizens by demonstrating greater accountability and transparency (Yavuz et al. 2014). Social media are also used to educate citizens on police work, as seen by the UK police service’s use of Weblogs to educate the public on when to ring 999 (Burnett, et al, 2012). Such channels give police a means of evaluating the spread of information by monitoring the level of engagement (an engagement being defined as a comment, share or like) provoked by posting information (MCCA, 2013). One example is the Metropolitan Police Service Facebook page, which made 17 posts between February 1st and February 18th, 2013. These posts had an average of 115 engagements each, and upon tallying the engagements during this period, the page arrived at a grand total of 222 comments, 1,486 likes, and 253 shares (Bartlett, et al. 2013).

Social media are also used for reputation management. Agencies turn to social media to report success, provide reassurance, promote community activities and deliver statements. The Police Departments in the District of Columbia and Philadelphia use both Facebook and Twitter to connect with the public and answer their questions, this provide reassurance to citizens by informing them (MCCA, 2013).

Police forces also use social media to dispel rumours and conspiracy theories, by proactively intervening in discussions and conversations. The UK police use social
media in this fashion by regularly using Twitter and Facebook to dismiss rumours regarding subjects as diverse as terror threats, riots, demonstrations and abductions, as well as responding to queries from the public and investigating complaints made over social media. For example, during the UK riots in August of 2011, false claims about the army deploying at Bank swept through Twitter, and police used social media to debunk these rumours. West Midlands Police Force also used social media, primarily Twitter, to counter rumours of an attack on their police station by posting ‘twitpics’ of officers standing outside the station (Barlett et al. 2013).

Reputation management is also done using two-way public communication which enables interaction with citizens in new, dynamic, personalized and cost-effective ways. LEA’s use social networking tools such as community list servers, like Tweet-Along. One example is the Arlington police department in Texas (USA). Citizens who had been on a ride-along tweeted their experience to the Arlington PD website, and Arlington then retweeted these accounts to various groups (MCCA, 2013). Through social media, police services encourage citizens to participate in reducing crime and the fear of crime; although such police-citizen cooperation is not new, social media make it much easier to reach citizens and interact with them.¹⁴

7.1.2 Enforcement
During investigations, LEA’s use social media as a tool to report crime, such as in the operations of the Jamaica Constabulary Force (JCF). The JCF has created a crime-reporting website with features such as an instant chat, file uploads and discussion forums. Users can enter details of a crime that they have witnessed and upload any supporting evidence (Donaldson, et al. 2013). Similarly, the Trillion project founded by the European Commission, has conceived a project platform for incident discovery, prediction, reporting and interaction, through which citizens can contribute to better urban security management by reporting crimes, suspicious behaviour and incidents by using the existing social networks and LEA’s can simultaneously benefit by detecting incidents in a more efficient way (Trillion project Brochure, 2015).

In everyday security, the use of social media is closely linked to the concept of community policing. Through social media and mobile apps, citizens can get involved in aiding in investigations and gathering intelligence. Community policing is increasingly accepted as an effective method of improving security. Here social media facilitate the co-production of security through citizens’ cooperation. For example the National Spanish Police, engage citizens using Twitter; with the Tweetredada program, they invite citizens via targeted requests to report various issues, including child pornography, gender violence, and finding the “most-wanted (Accenture, 2013). The Greater Manchester Police have also developed a #Shopalooter campaign at the national level. Thousands of people have interacted with the campaign by tweeting and retweeting screenshots of and links to alleged looters bragging about their exploits, using the ‘shopalooter’ hashtag (Bartlett & Miller, 2013). In the Netherlands, for example, where the adoption rate for social media is particularly high, police forces ask

¹⁴ For example, the Washington DC police department, uses its civilian community outreach coordinators to establish community list servers in all seven police districts to share public security information (MCCA, 2013).
the general public information on Twitter or Facebook. Hints from the public are also requested via SMS broadcast alerts. The 'Burgernet' service organised by the police, informs citizens in real time through mobile phones, when the police reports, for instance, a missing person, a suspect or a stolen vehicle (COMPOSITE Project, 2011).

Even though public participation can be of great help to improve security for example, this can also create problems when investigating, e.g. during the Munich terror attack in 2016, the police tweeted asking people not to upload pictures as the incident was still live. Post event they tweeted to ask them to upload such things for evidence gathering (BBC, 23 July 2016).

According to a study conducted by the Major Cities Chiefs Associates in US (MCCA, 2013), not only are police forces using social networks in criminal investigations, lawyers are also using these tools to support their cases. Prosecuting attorneys use social networking sites to research information about witnesses.15

7.1.3 Intelligence

Social media are used as sources of intelligence: to monitor, investigate and gather evidence. This process can be as simple as searching a name by scrutinizing social media content (Trottier, 2012). Police can also obtain evidence by mimicking how other users access information on the site, since many of the users’ posted information is not protected by privacy settings. Police can also join specific groups and networks. In 2014, police in Cleveland were able to crack down on the Heartless Felons gang after a rapper affiliated with the gang posted videos on YouTube where he seemingly admitted to selling drugs. This result was made possible by observing a visible nexus between the individuals, their social network, and the crime committed (Mattescu, et al. 2015).16

Increasingly so-called ‘Social-Enabled’ policing, is allowing social media and social networking to complement traditional community policing, intelligence-led policing and predictive policing. This idea facilitates community sentiment analysis and the fusion of open source intelligence with traditional data sources for better analysis, aiding prevention or allowing for early detection of crime and disorder (Koh H. E. et al., 2014).17

Legal and ethical questions emerge from some of the police’s use of social media in investigations. In counter-terrorism and public security efforts, the SOCMINT approach (social media intelligence) is frequently used. SOCMINT is a process in which intelligence agencies produce relevant intelligence for national security by identifying, collecting, corroborating data and information from social media (Trottier, 2015). This

15 Trottier (2012) also notes that police can also obtain private information from users on social media through direct requests. Social media companies have established official channels for police to access this information through warrants, court orders and other legal procedures. In Canada, for example, the government is introducing a “Lawful Access” bill which would speed up the process investigators use to obtain this information by eliminating the need for a warrant.

16 In a further example from Ottawa, a hockey player from whom sports equipment was stolen identified one of the suspects using the store’s fan page on Facebook (Trottier, 2012)

17 Another method used by the police to gather evidence from a user’s profile without making their presence known to that individual is by using a fake profile, thereby circumventing the social media privacy settings. According to Kerrigan (2011), mentioned by Trottier (2012), the U.S. government is developing “Persona Management Software” allowing investigators to manage several seemingly authentic “fake” profiles online. However, the terms of service and policies for many social media platforms, like Facebook or Instagram, explicitly ban law enforcement from creating fake identities on their service (Mattescu et al 2015).
approach has been questioned because of the lack of legal clarity over its use. In addition, the SOCMINT approach raises concerns about the origins and circulations of content, as well as the lack of specialized staff (ibid.)

Social media can be also used by police to obtain witnesses and informants. Investigators can also direct their attention to a suspect’s peers in order to obtain information (Trottier, 2015).

7.1.4 Crisis management

By its nature, “everyday security” seems opposed to the concept of “crisis management,” which implies an exceptional and temporary nature but the preparedness phase of the crisis management cycle can be part of the daily management of security. Furthermore, everyday security management also provides for better knowledge of a territory and its security partners; as such, it may contribute to enhancing responses in case of crises through an analysis of ‘early warning tweets’, ‘rumours’ and the ‘self-organization of disaster relief’ on Twitter (Terpstra, et al. 2012). For example, in 2011 the storm incident at Pukkelpop during a festival in Belgium, thousands of tweets were published shortly before, during and after the incident, studies of these tweets determined that automated filtering of information provides valuable information for operational response and crisis communication, as an early warning.

Public authorities (police services, emergency medical services and fire and rescue services) also use applications to inform citizens what to do in case of crisis (Cosmic Project, 2014). Such use of social media during the preparation phase occurred during the monitoring of Twitter and Facebook during the first inauguration of President Obama in 2009, in order to perceive potential situational information that had not yet been obtained by the more formal sources.

7.2 The influence and impact of social media use in the domain of public security and policing

Although the use of social media for everyday security purposes is increasing, there is little research exploring the impact of social media on everyday policing activities (Dunkerley et al. 2014).

**Impact on public satisfaction.** Police work is more visible for the public through social media. When police forces use Twitter, Facebook, Instagram or even Youtube to communicate, inform and educate, citizens. Several analyses revealed that users of social media had more confidence in the police as well as greater overall satisfaction with the police (Ruddell and Jones, 2013). We can observe this in the example of the National Police of Spain, with more than one million of followers that constantly uses social media such as Twitter and Youtube to communicate with citizens, post videos to educate them and even solicit them in investigations.

The two-way communication using list servers and other forms of social media have facilitated not only the communication with citizens, but also between police community. However, this interaction with citizens does not come without risk. In the U.S. Police departments, who use list servers and other email groups, report that
agencies have to continually reiterate that these methods of communication are not a substitute for 911 emergency calls (MCCA, 2013). The 2013 Red Cross Disaster Preparedness Summit shows the public expects emergency responds agencies to respond when calling for help on Facebook (Bernier, 2013) with a failure to do so likely to be counterproductive in terms of citizen-police relations.

**Impact on privacy rights.** Social media analysis and tools allow for far greater surveillance than ever before, with concomitant risks and opportunities (Bartlett and Reynolds, 2015). Public attitudes towards data sovereignty and privacy (even on open platforms) change quickly, and there is a reputational risk if law enforcement agencies are seen to be 'snooping' online. This can generate serious and sustained damage to public trust (Bartlett et al., 2013). Also some police practices in social media can be considered as discriminatory if police target surveillance on a specific group or person, minorities, etc. One example of this is the operation Crew Cut of the New York Police Department, which used social media to crack down on teen “crews”; but which also built a neighbourhood-based group of friends, or clique, without any criminal connection (Mateescu et al. 2015). Another example is when the Department of Homeland Security of the U.S. monitored the #blacklivesmatter hashtag on Twitter during lawful protests across the country, following the acquittal of George Zimmerman in the shooting death of Trayvon Martin (ibid.). This might have a negative impact on the way citizens perceive the police.

**Impact on the police forces agencies.** Law enforcement agencies, become familiar and comfortable using social media into their daily routines and it is clear that police services invest time and resources in developing and maintaining different forms of communication with the general public. Although, the adoption of a social media policy is required, studies reveal that the implementation of a social media use strategy is not a constant in LEA’s (Ruddell and Jones, 2013). While more police forces are starting to incorporate social media data into their investigations, a formal training of law enforcement personnel is slowly becoming mandatory in many counties.19

**Impact on solving crimes and gathering information.** Regarding to investigation, some surveys addressed to law enforcement professionals reveal that social media is a valuable tool to gather evidence and solve crimes as well as assisting in crime anticipation (Lexis Nexis, 2014). The result of a survey addressed to U.S. law enforcement in 2014 reveals how law enforcement increasingly relies on social media tools to prevent crime and to anticipate criminal activity. It was shown that law enforcement officers use real-time social media information to anticipate public gatherings and protests and to prepare in advance of these events (LexisNexis, 2014). For example, burglary data is used by Santa Cruz City in the United States and West

---

18 According with a survey among users of municipal police websites and social media in Canada, social media used in policing has relied on other forms to watch over the public but never so much content has been accessible in a single enclosure. Everyday actions in social media become online content and this content becomes evidence. Many individuals are aware, some refuse to upload content, some other refuse to become users (Trottier, 2012).

19 At the present, self-taught are primarily in their usage of social media (Lexis Nexis, 2014). Philadelphia, for example, provides an 8-hour training for department members who have authorization to provide Twitter updates (MCCA, 2013).
Yorkshire Police in the United Kingdom to identify streets at the greatest risk of burglary and to then increase patrols in those areas (Accenture, 2013). While open source intelligence infused with social media data enables an immediate access to social life for investigators, they also provoke concern with the origins and circulation of this content.

7.3 Inventory of strengths, weaknesses, opportunities and threats

7.3.1 Strengths

- Social Media tools enable public agencies to communicate more frequently and more directly in nearly real time with constituents at little or no cost. Anytime and anywhere there is an internet connection which is easy to use.
- Police services can provide the audience with information and promote accountability through community engagement and empowerment, but also support greater transparency in public service (Ruddell and Jones, 2013).
- Interaction between police and citizens improve citizens’ perception of security.
- A positive interaction with police helps generate and increase feelings of security (Sachdeva, 2015).
- Social media can facilitate an environment in which citizens maintain anonymity in crime reporting (Donaldson, 2013).
- Police understanding of citizens’ behaviour helps measuring the effectiveness of security measures, improving the organisation’s plan to address security issues and involving citizens for collective’s security actions. (Sachdeva and Kumaharu, 2015)
- Social Media allows the police to gather powerful information and sometimes useful intelligence in the interest of public security (Barlett et al. 2013)
- Through social media, Police can dispel rumours e.g. West Midlands Police Force in the UK used Twitter to counter rumours of an attack on the police station by posting ‘twitpics’ of officers standing outside the station.
- Social media promote direct participation of citizens in the security policies (see also DIY policing).

7.3.2 Weaknesses

- A negative interaction with police (e.g. misconduct by police officers) can increase insecurity among citizens (Sachdeva and Kumaharu, 2015).
- The lack of training and knowledge of what they are seeing online could lead to the criminalization of innocent individuals - particularly minors (Mateescu et al, 2015).
- Lack of clear legal and procedural protocols, including jurisdictional boundaries, for the use of social media in investigations.
- Social media surveillance might be focused on certain communities or groups.
- Lack of methods and techniques to measure the effectiveness of the use of social media for policing purposes.
Social media can also disturb other forms of communication and engagement. Due to the large volume of messages received from public through social media, police forces are not able to respond to all requirements or intensity. This may impair the relationship with the police.

Not all people are online or not all people use social media, so information might not be distributed evenly amongst all parts of a population and this might create a digital divide. E.g. senior citizens or people who has not complete high school (Ruddell and Jones, 2013)

7.3.3 Opportunities

- Social media has given to the general audience new awareness of how the police are doing their jobs (Rand corporation)
- The interaction between the police and the public through social media can contribute to better cooperation between police and citizens, to the improvement of their relationship and to mutual understanding
- The popularity of social media provides new opportunities for data collection.
- Social media can be used for community outreach by providing crime prevention tips, offering online reporting opportunities, sharing crime maps and data, and soliciting tips about unsolved crimes.
- Social media can be incorporated into all aspects of core police operations (not just corporate communications but intelligence gathering, crime prevention, public order management, law enforcement, internal affairs conduct investigations and assisting in prosecutions).
- Social media as a source of intelligence can improve the quality and timeliness of decision-making. Open source intelligence, can contribute to understand and learn about potentially violent groups activities, criminal behaviour, signs of disorder, community tension and more (the English Defence League use Facebook to arrange its Demos) (Barlett et al. 2013).
- Social media offers new opportunities to crowd-source intelligence. For example in UK through the app Facewatch ID (online portal enabling Police and communities to work together towards reducing crime) users sort the images via postcode and then inform on those they recognised by sending a name and address to the police.
- Social media traffic analysis could allow for a more rapid identification of events than traditional reporting mechanisms.
- Social media offers a new source of evidence for prosecution and enforcement, i.e. in 2009, Strathclyde Police launched Operation Access, which used social networking sites such as Facebook to uncover criminal activity by identifying weapons carriers.

---

20 Social media is changing expectations and requirements, and raising questions about police force’s communication strategy (Barlett et al. 2013).

21 With the application of geo-location techniques this could lead, for example, to a constantly evolving map showing spikes in possible violence-related tweets (Barlett et al. 2013). Also, putting the social media presence of criminal suspects under surveillance; cross referencing such individuals’ accounts; identifying accomplices; uncovering assumed identities; covertly joining closed social media networks or groups; identifying criminal networks that operate through social media sites; and the provision of social media content suspected of being evidence of a crime to the Crown Prosecution Service (ibid.).
• In the future, social media may further increasingly replace personal contacts between officers and the public.

7.3.4 Threats

• Social Media users may be active participants in crime investigation, however the fact that police are scrutinising citizens social life in these platforms also foster an unwillingness to contribute (Troitter, 2012).

• Using social media for intelligence, there is a risk that this will be done in a way that is unsound and unsafe, radically undermining public trust (Barlett et al. 2013).

• Risk that data collected for intelligence or on-going investigation purposes could be misused.

• By using social media technology for surveillance, investigators have a much better view of citizens’ everyday life. The convergence of so many population and institution means that any single act of surveillance is amplified in its scope (Troitter, 2012).

• Due to social media surveillance of specific groups can generate over criminalization of youth, particularly minority youth (Mateescu, 2015).

• Inaccurate interpretations of social media data. Inaccurate or incomplete information poses significant problems for surveillance technologies and it is unclear how, if at all, existing tools addresses risks of bias, such as in the patterns of language that it flags as suspicious.

• Information broadcast on social media is not verified or proven.

• The use of social media or open source information can be addictive to users and be a continuous firehose of information and contacts demanding action.

7.3.5 Conditions for success

Legal and ethical conditions. As a new technological tool used in daily security management, social media faces some ethical, operational, and technological questions that law enforcement agencies will need clear answers to in order to ensure that civil rights are protected as law enforcement moves increasingly online (Mateescu, 2015), as well as to ensure the success of its use. Particularly with regard to intelligence, investigations and surveillance, social media use must comply with a legal framework. This framework must provide a sound, publicly argued legal footing providing clarity and transparency over social media intelligence use, storage, motivation, regulation and accountability (Barlett, et al. 2013), in order to prevent threats to users’ privacy and to prevent or protect them from unwanted exposure (Trottier, 2012).

---

22 A recent Dutch pilot project, for instance, tests the use of Skype for crime reporting.

23 Social media have heightened surveillance of everyday life. Police are able to access private information with little effort, which is indicative of asymmetrical relations of visibility with the public on social media. Police are able to know intimate details about targeted individuals, who in turn are unaware that they are underwatch, or collaborating in investigations.

24 For example, if an individual who post about drugs and violence on social media is actually engaged on those activities? (Mateescu, 2015) i.e. the NYPD's online surveillance under Operation Crew Cut, for example, included monitoring of black children as young as 10 years of age.
Capability development conditions. The advent of social media has created new offences with which the police have to contend, new spaces for the police to visibly enforce the law, and also increased the number of offences, posing issues of discretion, workload and resources. Police forces must develop specific capacities for proper and effective use of social media and produce specialised training for intelligence analysts and those who will work closely with the Crown Prosecution Service. Such training includes the possible risks of social media use, such as the identification of personal information relating to individual officers (Bartlett, et al. 2013). It is also key that police services consider the technological and methodological development of social media use.

Each constabulary should ideally have a single dedicated, operational lead for social media to integrate its various applications such as: monitoring, managing which jurisdiction takes responsibility for investigations, filtering social media requests and conversations, ensuring the correct use of social media accounts, managing engagement, crowd-sourcing intelligence collection, and managing the public’s expectations of what ‘social media policing’ can and cannot achieve (such as investigating reported trolling, cyberbullying and low-level identity theft) (Barlett, et al. 2013).

7.4 Reflection and conclusion

Today, many law enforcement agencies recognise that social media are important technology to improve the management of daily security. Not only to enable a direct and fast communication with public, but also the opportunities as a source of information that provides from the analysis of big data collected through these platforms for the criminal investigation, anticipating and preventing crimes.

One of the main challenges for LEA’s using social media in policing is the adoption of formal policies and processes within agencies that enable a unified, consistent approach to modern technology usage. As personnel become even more familiar and comfortable using it, they will continue to find robust and comprehensive ways to incorporate emerging social media platforms into their daily routines, thus yielding additional success in interrupting criminal activity, closing cases and ultimately solving crimes (Lexis Nexis 2014).

Law enforcement agencies and leaders need to be able to identify, assess, and evaluate new technology for adoption and do so in ways that improve their effectiveness, efficiency, and evolution without infringing on individual rights (President's Task Force on 21st Century Policing, 2015). Incorporating specialised staff, budget dedicated to innovation and define a clear legal and procedural protocols, become a priority for the agencies and policy planners in the security policy definition (Mateescu et al. 2015).

LEA's are the actors that are most involved in the use of social media in everyday security. Although local and regional authorities are key partners in the definition of the local strategies to fight crime and violence, the literature does not make mention of these actors in the use the social media for police operations. The exception to this is the use of social media to create new channels and means of interacting with citizens to inform them of the cities’ security measures, understanding governance, and more actively participate in policy-making processes.
The analysis of the municipal security strategies and the next phases of MEDI@4SEC will explore the implications of local and regional authorities aside from local police forces in the use of social media for security purposes. Furthermore, there are multiple key questions that can be addressed in the future:

- Can LEA’s guarantee the protection of citizens’ privacy and fundamental liberties when using data from social media for public security purposes?
- How LEA’s can keep the trust of the public when the latter knows that they are scrutinised on social media by LEA’s?
- Is the use of social media for security purposes regulated and operated by trained staff to ensure the correct use of the data collected?
- Is the judicial system (judges, prosecutors etc.) prepared to use social media as a proof to prosecute crimes?
- Are LEA’s prepared to manage the mass data from social media (for investigations, intelligence, monitoring, etc.) in a responsible way?
- Are LEA’s and all public security actors prepared to change/modernize their structures (budget, technology and staff) to adopt social media as a tool to solve and prevent crimes?
- How LEA’s and all public security actors can use social media to better coordinate among them?
- Do local and regional authorities use social media as part of their local security strategy?
8. Dark web

The 2015 Internet Organised Crime Threat Assessment indicates that cybercrime is becoming more aggressive, hostile and confrontational on individuals and businesses. Instead of subterfuge and covertness, there is a growing use of extortion, which boosts the psychological impact of fear and uncertainty on victims. For this reason, cybercrime increasingly bears the signature of organized crime (Europol IOCTA, 2015). This chapter will discuss the Dark Web, one of the digital social spaces particularly facilitating the perpetuation of “high tech” (organized) cybercrimes. Knowledge obtained for this chapter is not only based on scientific and grey literature but included red and blue teaming knowledge as well.

What is the Dark Web?

The internet consists of several layers of accessibility. The first layer is called the Clear web or Surface web. This part is accessible through regular search engines, such as Google or Yahoo and is where social media platforms reside. The second layer, called the Deep web consists of all the data not indexed by traditional search engines; these data can range from bank transactions to closed WhatsApp groups. A small part of the Deep Web is called the Dark web (DW). Here content has been intentionally concealed and users can surf anonymously. In order to reach the DW and to access its content, one needs to install a certain program whose function is similar to that of a web browser or search engine. The most commonly known program is The Onion Browser (TOR).

In this document we refer therefore to DW as online criminal activities, which use a TOR or similar browser technology (e.g., I2P, Freenet) TOR browsers work differently from conventional browsers (Raeesi, 2015).

8.1 The use of social media in the domain of public security and policing

8.1.1 Legal and criminal use of the TOR protocol

The TOR protocol is legally used for several legitimate purposes: to avoid identity theft, for marketing tracking, to circumvent censorship and to perform research on topics that might be sensitive in certain countries. Typical examples of legit users of TOR are listed in the table below:

Table 8-1: Legitimate users of the Dark Web

<table>
<thead>
<tr>
<th>TOR User Group</th>
<th>Purpose of Beneficial Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Political) activists</td>
<td>Operate anonymously in totalitarian regimes; expose business or</td>
</tr>
</tbody>
</table>

25 It is estimated that the Deep web is approximately 4,000-5,000 times larger than the surface web (Finklea, 2015).
26 Other programs are Freenet and the Invisible Internet Project (I2P) (Ciancaglini et al, 2015).
27 Every TOR user becomes a node in the TOR network and all traffic bounces through at least three nodes before reaching its destination; only the previous node and the subsequent node are known by routing nodes. Therefore, past one step, the nodes are literally “in the dark” about other nodes on the network (Tapuri & Shorter, 2015). Bitcoin is the currency which criminals on the DW use most because of the anonymity feature it provides. It is a non-government-controlled peer to peer anonymous crypto-currency (van Hout & Bingham, 2013). It was created in 2009 as an unregulated, alternative method of exchange for online payments and it has been the topic of much media, internet and policy discussion (Wilson & Yelowitz, 2015).
and whistleblowers

<table>
<thead>
<tr>
<th>Role</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Journalists</td>
<td>Protect sources and themselves while publishing non-state controlled articles</td>
</tr>
<tr>
<td>Law enforcement agents</td>
<td>Receive truly anonymous tips, use the internet during surveillance, protect undercover staff</td>
</tr>
<tr>
<td>Businesses</td>
<td>Support corporate spying and market screening operations</td>
</tr>
<tr>
<td>The military</td>
<td>Share confidential data, protect the identity of field agents, gather intelligence</td>
</tr>
</tbody>
</table>

A seventh group of users can be added to these groups, namely criminals. Different sorts of criminal activities and services are exploited on the DW including, criminal trade, child Sex Abuse (CSA) and criminal services, such as murder for hire, human trafficking, hacking services (Ciancaglini et al., 2015; Raeesi, 2015; Tapai & Shorter, 2015; Biryukov et al, 2013; McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker, 2008; Chertoff & Simon, 2015).

Other “grey” services, not necessarily illegal can be exploited for illegal purposes, such as financial transactions – that may facilitate money laundering; the distribution of informative material – typically dealing with illicit content as the “making of a bomb”; fora and chat services, often used for communications that can facilitate the growth of violent extremisms.

Due to the intrinsic properties of TOR, a quantitative analysis of the use of TOR to establish a ratio between the legal and illicit use is very challenging. There is no academic agreement on this question, and no hard numbers are presented. (Biryukov et al., 2013) argues a 50:50 ratio between legal and illegal content.

In the following paragraphs, we focus on a few of the mentioned criminal activities that represent an example of how the “high tech (organized) crime” is nowadays exploiting the DW.

8.1.2 Use of the Dark Web for policing

The use LEA’s make of the DW itself for investigations is mostly not specified in the openly available literature. It is nevertheless generally known that the activities on the DW are object of investigation (a.m., Bryant, 2014), within two operational contexts, as listed below.

Proactive investigation for intelligence, employing the use of TOR and often manual searches of the encountered content; in a few cases, LAE’s are experimenting the use of novel automatic tools to crawl portions of the DW and index their content.\(^{29}\)

Reactive investigations, for example to collect information on the DW on a suspect. These operations are again challenging, mainly because of the difficulty to de-anonymise digital traces on the DW.

\(^{29}\) An example of such tool is the specialized search engine developed by TNO (Spitters et al., 2014). The challenge in this case lies in the difficulty of automatically uncovering new DW pages; the limit of content protected by login also requires a semi-automated approach and the risk to automatically download CSA content (the simple possession of CSA can be illegal in some countries) need to be accounted for.
The perpetuation and impact of concluded operations concerning the DW are instead often mentioned in the media and in official reports; the following sections will focus on these.

*How policing the Clear Web influence the Dark Web.*

Before looking into the policing measures on the DW, noteworthy is that the DW can be influenced by policing and law enforcement efforts on the Clear Web. An example is given by the Internet content regulation from a drug-policy perspective: measures such as the Australian compulsory Internet filtering regime to block drug contents on Clear Web websites would likely drive drug discussions to the Deep or the DW, where digital spaces are not affected by Internet filtering and where governments are actually unable to regulate TOR website content (Barratt et al., 2012). On the other side, this measure might also push violent online extremism into the DW, where monitoring of content is much more difficult and less debate takes place (Hussain & Saltman, 2014; Saltman & Russell, 2014).

*A general policing attitude towards the DW and policing challenges.*

Very little policing studies discuss crime on the DW, let alone studies of the impact of policing measures. This might follow from the novelty of the technology, from the induced and unprecedented move of several crimes into a relatively new transnational context and from the technical challenge posed by the technology itself, not easily accessible for research as open data sources are, and rapidly changing and growing. The exponential growth of the crime specifically on DW market places, for instance, poses a formidable challenge for the foreseeable future, since DW sites proliferate at a rate far greater than law enforcement has been able to intervene. It might become difficult to justify the effort and cost of operations aimed at regulating the DW, especially when there are so many other forms of cybercrime equally deserving of attention (JCAT). All these elements make any LEA’s action for monitoring, investigation or prosecution of criminals very challenging.

Despite cybercrime policing having a typical local characterization, when it comes to the DW similar attitudes appear across law enforcements worldwide: authorities tend to focus on attacking the offender (in the case of CMs, focusing on the supply-side, as discussed in 8.3.4) and on removing the illicit content (as discussed in 8.3.5). The effectiveness of this approach is questioned in the academic literature. Two points are also highlighted: the difference between various cybercrimes perpetuated through the DW might call for different type of measures (e.g., difference between illegal trade and CSA as mentioned earlier); moreover, measures developed to exercise control on phenomena on the Clear Web might bring weak if not counterproductive effects if applied to the DW, as already mentioned in the previous section.

30 Another example is the renaming and rebranding strategy adopted by groups banned from the Clear Web when accused of promoting controversial or violent content (e.g., AM network, Hussain). Government imposed filtering and blocking regulations for content under a specific organization’s name often prove to be futile on the Clear Web itself—the same content is quickly re-proposed under a new name and website data and traffic information becomes no longer accessible for further investigation.
The DW also poses a “policing dilemma”. Anonymity is sometimes a cover for people doing “good” and in need of the protection of technology in order to surf the Web. TOR can be seen as a neutral tool, used for either good or ill (Jardine, 2015). A few examples in literature make a distinction between the TOR technology and the TOR-enforced hidden services, strongly attacking the latter (Guitton, 2013) as promoters of mostly unethical content and calling for a stop to the development of TOR hidden services. Other academics argue that shuttering anonymity networks would not be a viable long-term solution, rather ineffective and damaging to those people that genuinely benefit from these systems. Jardine and Stevens speak about the need of a more active “social policing”, to minimize the socially damaging costs of anonymity-granting technologies, while still allowing the benefits of such systems (Jardine, 2015). Countermeasures to perceived misuse of the DW should be as flexible and adaptable as the technology is, and social policy can provide more capacity for this than relatively “crude” technological regimes (Stevens, 2010).

In this context, it is also worth mentioning the operations of other actors who autonomously infiltrate, disrupt and eventually take down DW websites and services. A popular example is the self-named “Operation DarkNet” of the hacker collective Anonymous, which in October 2011 announced to have accessed a large DW website hosting CAM content and publicly released the login details of more than 1500 users31. A second example, again a campaign launched by Anonymous, is “Operation Paris”, which took down hundreds of websites on the Clear Web associated with ISIS; as a consequence, ISIS’s media outlet, Al-Hayat Media Center, posted a link and explanations on how to get to their new DW site (Weimann, 2016). These cases might be examples of the self-implementation of “social policing measures” (Jardine, 2015) by fractions of the population, who feel the criminal use of technologies might jeopardize the benefits introduced by such systems.

*Focus: the use of cryptomarkets.*

Cryptomarkets (CM), are a relatively new criminological concept, introduced to outline the contours of a new generation of online illicit marketplaces (Martin, 2014). They are a type of website that look similar to regular online market places, such as eBay or Amazon, by allowing their customers to search and compare products and rate vendors, but also employing advanced encryption to protect the anonymity of users. While logged onto a CM, the physical location and identity of all users are masked, creating a completely anonymous marketplace. As a consequence, CMs provide an ideal trading facility to offer and buy illegal good. They gained popularity between 2011 and 2013, with the rise of Silk Road 1, the first major CM on the DW; other popular online market places for illicit goods are Silk Road 2, Agora, Evolution and Alphabay.

*Impact of cryptomarkets on illegal (offline) trafficking.* Marketplaces create new cyber-hotspots serving as places where potential offenders can meet each other, interactions between supply meet demand and relations are built. As a consequence of the CM providing informational and managerial opportunities, today loosely-organized groups

---

and even individuals can be as efficient as old traditional organized groups in drug trafficking, offer their services to a far broader public than traditionally possible (and cutting out several middlemen, if wanted).

Cryptomarket policing. LEA’s efforts against illegal trades on the DW have generally been in place to track the criminal proceeds, to limit the profits of crime and to tighten the global anti-money laundering regime (Raeesi, 2015). This approach follows from the “traditional” line of censorship of drug-related information in online and Internet sources (Barratt, 2012). In this way, LEA’s have completed several operations: the leading law enforcement actors in America and in Europe have taken down several large websites and the operators behind them, amongst which the famous Silk Road 1 and Silk Road 2 (Barret, Farret & Winstock, 2014; Ron & Shamir, 2013; Finklea, 2015; FBI, 2014) and several others within operation Onymous (Europol, 2014). These results were made possible mainly through infiltration operations, classical police investigations and postal interception (Martin, 2014).32

Focus: child pornography

Criminals who are present on the DW appear more comfortable offending and discussing their sexual interest in children than those using the Surface Web. The greater level of anonymity and strong networking may be favouring their sexual urges, which would not be revealed in any other environment lacking such features. Hidden services within the DW are therefore often used as a platform for the distribution of child abuse material (CAM). The nature of these services drives the abuse of new victims because the production of fresh material is demanded for membership on child abuse forums and it reinforces the status of the contributors. Furthermore, child abuse offenders are facilitated by many of the financial services and products used by more “mainstream” cybercriminals; a continuation of migration from traditional payment mechanisms to those offering a greater degree of anonymity, such as Bitcoin, is observed. (Europol, IOCTA 2015). This might be evidence that offenders with a sexual interest in children who produce and distribute CAM are becoming more entrepreneurial and “innovative”, exploiting developing technologies.

This might ensure that LEA’s apply questionable policing policies, which can be inducement for ethical, legal and privacy discussions on a global level. According to information leaked to media sources, the federal bureau of investigation (FBI) hosted a Child Porn hidden service for 13 days after obtaining control of the site. The operation allowed to gather IP addresses and deposit malware to collect data about the site’s users to the FBI. A hurdle not only difficult for Law Enforcement Agencies but also for researchers trying to study CSA is the “share-to-join” rule some CSA hidden services use. In order to join the site researchers need to obtain an invite from a member, often by proving themselves as paedophiles and providing material in order to join.

Focus: possible use for terrorists, violent and hate extremists

32 Another example of successful operations have been achieved in the Netherlands within the project ITOM (OM NL, 2014). Thanks to the resources (economical and in terms of personnel), the focus on cryptomarkets investigation and the transnational integral approach setup by the project, three big drugs sellers have been identified. The operation allowed to recover more than 1 M €. The project does not present prospects on effective strategies for policing the DW; alternative (not social media related strategies) are mentioned such as the “Naming and Shaming” approach.
Often, especially in recent times, claims are made about the terrorist use of the DW. Violent extremists are believed to be using the DW in the same way as they were using the Clear Web, but with exploitation of “added capabilities” (Weimann, 2016). Among the examples, step-by-step instructions to guarantee anonymity and hindering of geolocations from counter terrorism agencies are made available on the DW; a secret network of communications on the DW have been used between leaders of al-Qaeda to plan attacks in 2013; a DW page promotes donations in bitcoins to support the jihad (Weimann, 2016). Several of the criminal uses mentioned in section “Legal and criminal use of the DW” can indeed apply to activities that can lead to terrorism, such as money laundering, cyber-attacks to collect funds, fund raising, and weapon trafficking.

Multiple authors also mention that the hidden ecosystem of the DW can be particularly conducive not just for financing, trafficking and planning, but also for propaganda and recruitment (Chertoff & Simon, 2015). The “cold” recruitment of new supporters by the hand of radical groups and the promotion of extremist ideas are activities likely to display their message in locations much more easy to find and access than the DW (Bryant, 2014).

On the other side, communication phases subsequent to a first “contact” might seek more secluded digital spaces, such as closed for a, apps and chat services on the Clear Web. With the tightening of policies that ban extreme violent ideological content and services from the Clear Web, as well as private citizens initiatives of hacking, see 8.2, fanatics particularly motivated are driven on to the DW, where they are even harder to track (Hussain, 2014). Few data analytics research studies have attempted to collect and analyse fora of extremist content (e.g., Zhang, 2010) to pose a base for law enforcement operations. The challenge in this field is the “ephemeral nature” of content: fora emerge quickly and in many cases seem to disappear by changing name and location but retaining much of the same content.33

8.2 The influence and impact of social media use in the domain of public security and policing

Very little policing studies discuss crime on the Dark Web, let alone studies of the impact of policing measures. This might follow from the novelty of the technology, from the induced and unprecedented move of several crimes into a relatively new transnational context and from the technical challenge posed by the technology itself, not easily accessible for research as open data sources are, and rapidly changing and growing. The exponential growth of the crime specifically on DW market places, for instance, poses a formidable challenge for the foreseeable future, since DW sites proliferate at a rate far greater than law enforcement has been able to intervene. It might become difficult to justify the effort and cost of operations aimed at regulating the DW, especially when there are so many other forms of cybercrime equally deserving of attention (Reitano et al., 2015).

33 There is therefore yet little ability to assess the extent of terrorism-related content on the Clear and on the DW (Stevens, 2010), hence subsequent policing interventions are still far away.
All these elements make any LEA’s action for monitoring, investigation or prosecution of criminals very challenging.

Despite cybercrime policing having a typical local characterization, where it comes to the Dark Web similar attitudes appear across law enforcements worldwide: authorities tend to focus on attacking the offender (in the case of CMs, focusing on the supply-side, as discussed in 8.3.4) and on removing the illicit content (as discussed in 8.3.5). The effectiveness of this approach is questioned in the academic literature. Two points are also highlighted: the difference between various cyber crimes perpetuated through the DW might call for different type of measures (e.g., difference between illegal trade and CP as mentioned earlier); moreover, measures developed to exercise control on phenomena on the Clear Web might bring weak if not counterproductive effects if applied to the DW, as already mentioned in the previous section.

The DW also poses a “policing dilemma”. Anonymity is sometimes a cover for people doing “good” and in need of the protection of technology in order to surf the Web. TOR can be seen as a neutral tool, used for either good or ill (Jardine, 2015). A few examples in literature make a distinction between the TOR technology and the TOR-enforced hidden services, strongly attacking the latter (Guitton, 2013) as promoters of mostly unethical content and calling for a stop to the development of TOR hidden services. Other academics argue that shuttering anonymity networks would not be a viable long-term solution, rather ineffective and damaging to those people that genuinely benefit from these systems. Jardine and Stevens speak about the need of a more active “social policing”, to minimize the socially damaging costs of anonymity-granting technologies, while still allowing the benefits of such systems (Jardine, 2015). Countermeasures to perceived misuse of the DW should be as flexible and adaptable as the technology is, and social policy can provide more capacity for this than relatively “crude” technological regimes (Stevens, 2010).

8.3 Inventory of strengths, weaknesses, opportunities and threats

In the previous paragraphs we already mentioned the most relevant literature discussions concerning how the Dark Web can introduce elements of strength, weakness, opportunity or threat in the context of law enforcement policing. These elements are discussed in the following sections.

8.3.1 Strengths

For the goal of law enforcement online surveillance, the Dark Web is a digital space where LEA analysts and researchers can conduct investigation anonymously, without leaving an online footprint. For specific contexts, the use of the DW as a space favouring online trade and e-commerce might induce a better “quality” of products due to self-regulation mechanisms of the market. Additionally, traders on the DW encounter less physical risks than if they would trade “on the street”. These arguments are particularly relevant with respect to the drugs trade.

Linked to the previous point, the cryptomarkets on the DW might lead to a disruption of traditional local organized crime networks. For instance, loosely-organized groups or individuals become nowadays as efficient as old traditional organized groups. This can
be seen as an element of strength for LEAs in the disruption of strong locally organized criminal networks.

8.3.2 Weaknesses

Various elements of strength, if exploited by criminals, become elements of weakness for law enforcement goals. For the LEA’s goal of identifying criminals, for instance, anonymity and untraceability of the online footprint of criminal users definitely poses a challenge to investigation and policing.

The DW is also a relatively novel and very rapidly innovating (changing) technology, hence it requires faster and more automatized investigations than the current state of operations. The content on the DW is neither easily accessible nor findable, it is a strong transnational context and is not met by adequate cybercrime detection capabilities. Standard infiltration operations (e.g., moles operating in a hidden service) have proved weak and shown little impact.

8.3.3 Threats

The general threat of the Dark Web is that its anonymity favours criminal activities. In particular, it poses a threat to the society through the proliferation of trade of specific products (e.g., drugs, counterfeit medicines, weapons) and services (e.g., murder for hire, data theft, CP). Media narratives describing the DW as “a place for criminals” do not help to counter this threat, but may be rather driving a bigger number of outlaws to it.

Additionally, the DW is intrinsically an economically-regulated environment: the DW financial methods attract a lot of capital and crypto markets naturally show resilience to intervention from LEAs on the supply side. The proliferation of criminal DW sites proceeds at a higher rate than the actual interventions and strategies can do.

Finally, being the Dark Web based on a highly complex, innovative and creative technology, the effects of both its legal and illegal exploitation are generally unknown and unpredictable on the long term.

8.3.4 Opportunities

Policing proposals

The DW is challenging law enforcement and policing capacities in an unprecedented way, and demands a greater (transnational) cooperation, more effective investigations (Reitano et al., 2015) and better technology tools targeting issues as the traceability and attribution of criminal transaction and criminal communications on the DW (Europol IOTCA, 2015).34

Christin (Christin 2012) suggests that an opportunity would lie in strategies focusing the “offense” of law enforcement and policing on the demand of DW products, instead of the supply. He mentions four strategies for intervention on DW crypto markets: disrupting the network; disrupting the financial infrastructure; disrupting the delivery model; or

---

34 An already ongoing initiative targeting the first mentioned need in the case of transnational cybercrime is J-CAT, a task force led by EU member states, facilitated by Europol’s Cybercrime Centre and running prioritized joint investigations (Reitano et al., 2015). This initiative proposes its platform, its efforts to partner with the private sectors and with universities and its mechanism for trust and intelligence sharing (governed by the Europol body) as opportunities for a successful fight against cybercrime.
“laissez-faire”, i.e. tackling the issue by detachment. He argues though that the first two would be technologically impossible, while the latter would be unlikely adopted by governments due to the existing normative agenda on the war on drugs.

Opportunities: technological research developments that can form a base for policing

The last ten years have seen a progressive growth in the technological research around the features characterizing the DW. We list below a collection of the most interesting research efforts that could lead to methodologies, techniques or tool to be used by the authorities to support policing choices. It is important to note that the efficacy of these efforts has not been tested in a policy context yet, but each potential opportunity springs from an element of weakness in the DW phenomenon.

Identify top-sellers in crypto markets. The crypto markets provide fora and spaces for customer feedback (such as reviews); this information, if automatically analysed, can provide an interesting base to assess the network of sellers and identify top-sellers – potentially “top targets” in an intelligence operation. Deep learning sentiment analysis (Li) seems to outperform other methods in the context of malware and carding sellers.

Disrupt the system of trust. The presence of reviews on sellers on the DW can also be exploited for a more pro-active intervention. LEAs might be able to interfere with the businesses on crypto markets by manipulating buyer reviews. The goal can be that of provoking the failure or the reduction of profitability of the seller. (Markopoulos, 2015) uses a game theoretic model to derive an optimal strategy for a LEA to achieve market interference.

De-anonymise. A central question that would enormously support LEAs operation is the “attribution of identity” question on the Dark Web. To answer this questions, advanced data mining and analysis technologies are required to perform DW users profiling. To actually determine the identity of a trader on the Dark Web, it is firstly important to trace anonymous transactions; data mining techniques are a powerful method to analyse large payment systems and publicly available transaction graphs of the type provided by the Bitcoin scheme (Ron & Shamir, 2013). Linking of heterogeneous data across different sources to a certain cyber identity is then needed.

The simultaneous analysis of the content of posts on the Clear and Dark web might pose clues for an identity connection, relevant for both CP content and violent extremism content. Methods based on the homophile principle (two individuals are as close as their interests are in common) in combination with network analysis (two individuals are as close as their reference networks overlap) can help determining if a profile on the Clear Web matches a user on the Dark Web (Cristani, 2015).

---

35 Different variables are balanced in the research, e.g., the budget to be “injected” in the market, the risk of exposure of the LEA operator and the risk of counterproductive effects such as increase in the profit of the seller. Review manipulation is shown to be a highly promising method, if LEAs have accurate information on the cost structure of market participants, on the effectiveness of the review mechanism, as well as on the details and the effectiveness of potential review manipulation countermeasures set by the market operator.

36 Technologies like text mining can be used to analyse the communication between traders and customers; the choice of words, subtle indicators of style and even systematic spelling mistakes can form a “textual fingerprint”. Analyzing temporal patterns can provide additional information (Raajmakers, 2016). Ultimately it is the incidental connections of the Dark Web with the Clear Web (or the real world) that can lead to effective identification of individuals. These connections are often based on inaccuracies or accidents, such as mentioning accidentally an email address, or unintended visible swapping bitcoins (Raajmakers, 2016).
Exploit user's errors and TOR vulnerabilities. As mentioned above, LEAs can exploit inaccuracies or accidents on the use of the DW. Some researchers also believe that a lot of DW users still show a certain degree of “naivety” (Bryant, 2014), by using TOR through a web browser. Standard web browser might have a JavaScript running or cookies enabled; both elements would assist a digital forensics investigator, testing whether a suspect accessed illegal material (Bryant, 2014). It is estimated that over 90% of regular TOR users would be sending their traffic from a non-TOR IP location at least once (Hurley et al., 2013).

Other researchers argue that vulnerabilities of the TOR network can also be exploited (Bradbury, 2014). Examples can be “hacking TOR” by breaking cryptographic keys – not impossible with an older version of the TOR key, running an own TOR relay, analysing the (clear) text traffic entering and leaving the network. Since TOR is continuously innovating, the sustainability of such methods is not obvious. A maybe more sustainable option is proposed by the director of the TOR project himself. He pointed out that the authorities could just as easily monitor Internet communications with the complicity of major ISPs, which would enable them to watch those communicating with TOR nodes before their traffic reached the DW, or after it left (Bradbury, 2014).

8.3.3 Conditions for success
The main condition for success in the case of the Dark Web is a transnational LEA effort focusing on quickly adaptable innovations, at the same level of technological progress and with the same flexibility that the same technologies governing the Dark Web propose. Awareness and understanding of how the criminal processes and the economy facilitated by the DW are also essential perquisites.

8.4 Reflection and conclusion
Technology is more than a new handy tool. It alters the way we think, the way we see the world and the world itself (Chan, 2001). Historically, technology has revolutionized policing practices (Chan, 2001), but it did the same for criminal ones. Technologies developed on the Internet introduced a new spectrum of capabilities and features, in terms of volume, velocity, interactivity, transnationality and dynamical evolution (Stevens, 2010). Therefore, cybercrime has become increasingly sophisticated, both technologically and psychologically (Grabosky, 2014).

The world of cybercrime on the DW is in particular a rapid changing world in which professionalization and commercialization are being implemented at a high rate (Verburgh, 2016). This is both a consequence of the technology “features” named above, and of self-adaptation measures in response to policing strategies or law enforcement operations.

The rapid development of DW cybercrime creates difficulty for researchers to keep track of new innovations; past research might soon be out-dated due to the fluidity of cybercrime. Even greater is the difficulty of policy makers and law enforcements, to identify and apply proper and timely innovations, reducing the possible DW misuses but at the same time maintaining the benefits of this technology.
We list below a number of reflections emerged from the literature review and that should be taken into account in the discussion on policing against DW-facilitated crimes.

- Policies should rely on flexible and adaptable innovations, to avoid limited applicability in a cybercrime community that is instead capable to quickly develop countermeasures.
- No “size-fits-all” measures: strategies should differentiate between the types of crime (e.g., CP vs crypto markets vs violent extremism activities).
- No “total-block” strategies: policies should seek balance between freedom of speech and crime solving.
- In the case of crypto markets-related crimes, strategies should focus on the “economical game”. Policies should be able to tackle the ecosystem, instead of single targets, and focus on the demand first, instead of the vendor’s side only. Disrupting a full economical system can bring a bigger and more sustainable impact than taking down single operators.
- In the case of violent extremism, strategies should rather focus on the producers, rather than the consumers of extremist material. Empowering the “good” and the “grey” users with spaces for open debate allows extremisms to be blended and debated.
- In general, for all types of crimes, strategies should consider the potential of the “good side” of the community, a little explored DW policy direction, by empowering “good users” for positive counter actions and stimulating “social policing”.
- The options of applying social media strategies from the Clear Web to the Dark Web might be explored, being aware of the differences between the two digital dimensions. If Clear Web strategies are technically not applicable or practically not effective on the DW, attention should be given to the differences and to the exploration of possibly new methods.

Strategies should build on the experience and awareness of initiatives such as ITOM and JCAT, where transnational collaboration, coordination of joint and simultaneous operations in different locations around the globe have successfully been tested.
9. Trolling

Trolling can be usefully defined as the targeting of defamatory and antagonistic messages towards users of social media (Williams and Pearson, 2014:4).\(^{37}\) Trolling broadly understood includes: cyberbullying; cyberhate; cyberstalking; cyberharassment; revenge porn; sextortion; naming and shaming; and flaming. Cyberhate is trolling targeted towards those with minority status.\(^{38}\) The term ‘flaming’ is used by different actors to refer to different activities: some use it to refer to extremely provocative language, designed to start a fight (Hardaker 2010; Herring et al. 2002; Williams and Pearson, 2014:11); others use it to refer to those who post offensive or provocative material for their own entertainment or gratification (Bishop, 2013). Most of these acts take place within a context of wider abuse, including offline, but some trolls, in particular those who belong to the sociologically distinct group of individuals who self-identify as trolls, carry out the vast majority of their abuse online. The legal status of all the trolling-related acts just listed differs from jurisdiction to jurisdiction and from act to act. An impressive and varied array of preventive, counter-trolling, and criminal justice approaches to combatting trolling are currently employed by public security providers broadly understood.

9.1 The use of social media in the domain of public security and policing

9.1.1 Who are the Trolls?

Our ability to generalise with respect to this question is limited by the paucity of empirical studies undertaken outside of North America. However, the results of the few examples of existing research are both interesting in themselves and may prove indicative of trolling trends internationally.

‘Subcultural trolls’ or those trolls who explicitly identify with the term ‘troll’ to describe their online identity, are distinct in that they tend to be indiscriminating in their choice of targets, and that they are motivated by a desire to get kicks, or ‘lulz’, a kind of enjoyment in the face of the suffering of others (Phillips, 2015). That same study hypothesizes that trolls enjoy economic comfort, as their activities require a reliable internet connection, a personal device, and a private space from which to troll; that they are white; and that they are between the ages of 18-30 (ibid, p.53-4).

In 2014 Canadian scholars undertook a psychological study of individuals self-identifying as internet trolls (5.6% of respondents to their initial survey). They found significant correlation between subcultural trolling and narcissism, psychopathy and Machiavellianism and a strong correlation between trolling and sadism (Buckels et al., 2014). They also claim that trolls engage in antisocial behaviour offline as well as online, a fact that could be significant for LEAs developing strategies to deal with antisocial behaviour offline.

\(^{37}\) Relatively innocuous forms of trolling also exist, like the use of troll bots programmed to deliver marketing messages automatically on behalf of companies or the use of social media to deliver mocking and sometimes infantile but mostly humorous messages. This summary addresses forms of trolling that challenge or undermine public security.

A separate category is that of politically and morally-motivated individual perpetrators of online aggression, many of whom, unlike subcultural trolls, are motivated not by enjoyment but by a desire to highlight and oppose what they see as immoral behaviour. These forms of aggression are directed typically at public actors such as politicians who disregard norms of political correctness, corporations that violate human rights, or academics who violate scientific norms by engaging in plagiarism. A recent study of online aggression of this sort on political sites found that, contrary to common assumption, anonymity did not increase online aggression (Rost et al, 2016). Rather, a greater proportion of aggressive posts were made by non-anonymous than by anonymous commenters.

This should be distinguished from a further category of politically-sponsored trolling, namely that of organised groups representing political agents (sometimes even national governments) who use aggressive and defamatory language to counter and harass those who criticise the positions of those agents. Examples include the trolling by professional pro-Russian commenters of political threads on journalistic media sites during the Ukraine crisis of 2014.39

Those who post abusive content online are as likely to be women as they are to be men. Challenging commonly-held assumptions about the behaviour of different genders, a recent study, which provided a snapshot of misogynistic internet trolling globally on Twitter over 3 weeks, found that 50% of those tweeting aggressive and misogynistic messages are women.40

Some trolls are bots. Many troll bots are employed for marketing purposes. The numbers of aggressive or offensive troll bots operating online is unknown. Little research exists on the identities of the agents funding and coordinating such bots. But the extent of bot use is impressive: research from 2013 suggests that 9% of Twitter accounts are fake and that many of these are bots.41

9.1.2 Who are the targets and victims of trolling?
While anyone can become a target of trolling, victims of abusive trolling online include in particular, young people, women, LGBT people, ethnic minorities and celebrities or anyone with a public-facing role. A US-based Pew Research Center survey published in 2014 found that 70% of 18-to-24-year-olds who use the Internet had experienced harassment, and 26% of women that age said they’d been stalked online.

9.1.3 Where does Trolling occur?
All forms of trolling and online abuse described here happen on all kinds of regular social media sites as well as on specialist online forums. They occur in particular as well in online spaces that exhibit technological features which make them attractive sites for positing illicit material. For example 4chan/b/ deletes most threads in a matter of minutes, while anonymity-granting tools like TOR make the dark web a hotspot of...
Abusive sites (Jardine 2015). An estimated 40 revenge porn websites exist in the USA, enabling the posting of explicit online material and then charging a fee to remove material, thus exploiting the position of victims for profit (Citron in Think Progress). Apart from attractive technological features, some sites are targeted for their high shock-and-outrage value. For example, memorial pages on Facebook are heavily targeted by trolls seeking to upset grieving friends and relatives (Phillips, 2016).

9.1.4 Which actors have a role in countering trolling through social media?
Front running public security planners in counter-trolling are the UK (Individual/regional police forces; central government; local government; national LEAs e.g. UK’s National Crime Agency). Businesses (telecoms and social media providers) and campaign groups also feature significantly in efforts to counter this activity. Parents and schools have a special role to play in educating young users of social media. The press and online journalistic media has an equally important role in raising awareness of trolling and how victims can protect themselves. Self-styled ‘troll hunters’ often work in tandem with journalists to identify and expose trolls. Public figures such as celebrity victims of trolling can also use their position as role models or their public platform to play an important role in this respect. Finally, social media providers and the communities that use them are uniquely well-placed to counter trolling.

9.1.5 How is social media used by public security actors to counter trolling?
Social media providers have a range of digital techniques for detecting illegal content and blocking it, but they also make use of codes of conduct and community rules to promote respectful communication on their platforms as well as educational material. Police use social media as a source of evidence and intelligence of trolling, and also as a tool of communication with which to inform and educate the public. A range of NGO and campaign groups develop tools and sites to educate people about the risks of social media use. Possibly because of their relative lack of power, actors who are not public security authorities sometimes use the techniques used by trolls in order to identify, combat, and punish trolling. Thus, in Sweden, Germany and the USA some groups find and expose the identities of, thus naming and shaming, those posting online racism and hate speech (Chen, 2014; De Vries, 2016; Webb et al, 2016). Similarly, counter-speech is employed by online communities to challenge offensive trolling.

9.2 The influence and impact of social media use in the domain of public security and policing

Impacts on individuals of cyberbullying: cyberharassment and cyberstalking
Cyberbullying can be more harmful to people than offline bullying because it can occur 24 hours a day, 7 days a week and can be experienced each time a person goes online. Specific psychological effects cited in the literature include: isolation and relationship problems; fear; depression; loss of confidence; self-harming; suicide (Various, cited in

Danielle Citron is quoted in an “The Trolling Epidemic, Quantified” on the site Think Progress, October 23rd, 2014, at: https://thinkprogress.org/the-trolling-epidemic-quantified-c44e58a10047#.ranyw4q9p

See, for example, a Dutch site educating young people about the risks of sexting www.onuitwisbaar.nu. More examples are given in the best practice list below.
Williams and Pearson, 2014) loss of employment, paranoia (Citron and Franks, 2014) and serious harm to a person’s reputation (Webb et al, 2016).

**Impact of revenge porn, sextortion; sexual naming-and-shaming:**

A US study suggests that 1/10 former partners threatens to post explicit images of exes online and of those who threaten an estimated 60% follow through (Dawkins, 2014) The impact of these forms of online abuse is gendered, because women and girls tend to be the victims (Ibid.). In the Netherlands, a 13 year old girl committed suicide after her name was published on a ‘banga list’, a list of girls identified maliciously by local boys as being sexually promiscuous.44 The risks of sexting in this context are made clear by a study by the UK Safer Internet Centre, which showed that 88% of sexting pictures or videos are put on other websites, sometimes even on porn sites.45

**Impact of online hate towards minority/disadvantaged groups**

- **Women:** Though some research suggests men are subject to more mild forms of online harassment, women suffer most persistent and harmful abuse (Pew, 2014). UK research from 2016 showed that, over a three-week period 80,000 twitter users were targeted for aggressive misogynistic abuse (DEMOS).

- **LGBT community:** In Russia social media is used to entrap LGBT individuals into meeting groups of self-proclaimed ‘paedophile hunters’ who video the meetings which are used to humiliate and shame them online (De Vries, 2014).

- **Trans people:** UK research shows that trans people are significantly more likely than non-trans LGB people to have been a direct victim of hate crime involving online abuse. Anti-LGBT hate crime is highly repetitive in nature for trans people, meaning that most trans individuals experience multiple incidents of abuse each year.46

- **Black & Minority Ethnic Groups:** Racist abuse online is widespread. Islamophobic hate speech is a category of specific concern. A recent report on Islamophobic hate speech in the UK found that victims of online abuse were afraid that the abuse would migrate offline into violence, especially if their online profiles were public.47

9.3 Inventory of strengths, weaknesses, opportunities and threats

9.3.1 Strengths

National police agencies in some jurisdictions have the resources, technological know-how, national overview, and strategic coordination functions that can prove vital in operations of national or international scale, and even in challenging environments. For

---

44 https://www.rnw.org/archive/dutch-girl-commits-suicide-over-banga-list
44 Further statistics illustrating the risks in the USA are given in a report by a campaign called ‘the national campaign’, http://thenationalcampaign.org/resource/sex-and-tech - 21% of teen girls and 18% of teen boys have sent/ posted nude or semi-nude images of themselves. - 61% of all sexters who have sent nude images admit they were pressured to do it at least once. - 15% of teens who have sent nude pictures of themselves, send these images to people they have never met, but know from the internet. - 17% of sexters share the message they receive with others, and 55% of those share them with more than one person.
45 VKontakte article on LGBT Hunters in Russia, at http://socialmediadna.nl/homolokkers/
example, in the USA the FBI have conducted highly successful operations in the dark web, subverting encryption tools like Tor.

Local police forces often have excellent parochial knowledge that can feed into national strategies and action and can prove crucial for interpreting hate speech (Jardine, 2015).

Online community members know and interact with their communities very proficiently. This means they can be effective at detecting trolling and countering trolling immediately, in real-time, via moderation but also via exclusion and counter-speech. With respect to the latter, some have suggested that online hatred provides an opportunity to consolidate a counter-movement challenging the view and providing a productive defence of more inclusive and tolerant forms of cultural identification (McClosker, 2015).

Social media providers are also very well-placed to react to online abuse, because it happens on their platforms and because they have the discretion to remove material that police may not have the power to. Recent years have seen a growing awareness among social media providers of their responsibilities with respect to abuse and hate crime online. Between 2014-5, Reddit, Twitter, Google and Microsoft also announced tools people can use to request the removal of information. In May 2016, the European Commission published, in collaboration with a range of mainstream providers, a Code of Conduct on Illegal Online Speech, providing guidance on preventing and responding to such abuse.

9.3.2 Weaknesses

**Police: poor police knowledge and understanding of the acts, their impacts, and protective and preventive strategies**

A recent report by the UK police watchdog found that police are inadequately informed about what trolling is, dismissing illegal behaviour as ‘just kids on Facebook’ (Her Majesty’s Inspectorate of Constabulary, 2015). Similar findings in relation to US police are reported by hate crime expert Danielle Citron, who says: “law enforcement just often dissuades people. They don’t take it seriously. They say, ‘we don’t get how to figure out how to find these people. Turn the computer off, boys will be boys.’ They often just don’t get the technology, and they don’t get the law... I think law enforcement often just doesn’t have the expertise and training, and they get intimidated by technology, so they discourage victims from reporting” (Citron in Think Progress, 2014). In the UK a lack of awareness amongst police on what actions are available to victims, leading to failures to give good advice has been flagged up. For example, officers were cited as asking victims: ‘what do you expect us to do about it?’ (Ibid.). Police chiefs should make sure officers understand the significance of online anti-social behaviour and that they are equipped with the knowledge to provide good advice to victims and investigate crimes adequately (Ibid.). This is especially important for local forces, which tend to lack the access to

---

48 For example, in 2015, Pornhub, the largest pornography site on the internet, introduced a reporting option for victims of revenge porn to report non-consensual posting of images (Henry and Powell, 2016, 404).

information, technical expertise and coordination role of national bodies (Jardine, 2015).

**Police: Inadequate police capacity/resources/technical knowhow**

There are inadequate criminal justice resources to police the volume of communications that travel through computer networks (Gianassi 2014). The technology to identify hate speech on social media networks is yet not widely adopted by authorities charged with protecting the public (Henry and Powell, 2016:404)

**Police: lack of confidence in policing from victims of cyberhate and the communities within which they live**

The combination of the growing prevalence of cyber hate and the lack of sufficient police capacity/knowledge, especially at a local level, can lead to frustrations and disappointment among victims. This can translate into reluctance to report and/or a greater openness to vigilante or digilante anti-tring acts. Police have been shown to be less effective at dealing with reports from certain sections of the population.  

**Community counter-speakers and troll hunters: sinking to similar depths**

A weaknesses with counter-speech online is that in some cases it can itself become abusive, creating a cycle of hate, worsening the problem (Williams and Pearson, 2014). As mentioned above, a range of groups exist to detect and expose or otherwise punish online trolls. In Germany and Sweden, such groups harness the power of both social and journalistic media to expose and thus name and shame racist trolls (de Vries, 2016; Chen, 2014). Concerns have been raised that efforts along these lines can end up becoming almost as ugly and abusive as those they aim to expose.

**Victims and offenders: unrealistic expectations of the law and police**

Henry and Powell, (2016) argue that both victims and potential offenders need better information sources on the law pertaining to cyber hate in England and Wales. Otherwise some borderline trolls may unwittingly find themselves criminalized, while some victims may take excessive risks online, believing themselves to be protected from abuse by the law. Also, if expectations of police powers and capacity exceed reality, police may be seen to be failing where in fact they merely lack sufficient powers, and this may damage trust in the police (Mason et al, 2015).

**Social media providers: poor prevention, slow reaction**

The measures adopted by many online social forums are reactive rather than preventive. For example, Facebook’s troll-detection technology is highly effective at identifying trolls and blocking their IP addresses, but only once they have behaved like

---

50 For example, UK research shows that both direct and indirect experiences of anti-LGBT hate crime effect trans individuals’ attitudes towards the police, CPS and the government more broadly. Specifically, most trans people believed the Government should do more to combat anti-LGBT hate crimes, they felt that the police are less effective and respectful, and they have less confidence in the CPS to prosecute anti-LGBT hate crimes (Walters and Paterson, 2014).

51 For example, the sites, ‘Yes, you’re racist’ and ‘Yes, you’re homophobic’ and even ‘Racists getting fired’ are controversial because they are intended to humiliate and damage online ‘haters’ (Webb et al, 2015).

52 For example, sites such as Pornhub have introduced ‘report abuse’ buttons, but they have not yet gone the extra mile and obliged posters of material, even explicit sexual material, to verify that it is consensually obtained and posted (Henry and Powell, 2016:404).
trolls long and hard enough for trolling patterns to be detected (Phillips, 2015: 72). Some sites can be slow to respond to calls from the public to remove quite obviously racist posts. For example, at the time of writing the UK charity devoted to measuring and reporting anti-Muslim hatred and attacks is criticising Twitter for ignoring requests to remove such material (TellMAMA, 2016).\textsuperscript{53}

**Victims and social media providers: cycle of weak reporting-weak response**

A study by Bullying UK found that parents are reluctant to report incidences of cyberbullying. Only 30\% of parents have reported bullying online and in these cases only 50\% of social networks responded (Bullying UK 2014). When reporting bullying to a social network site, only 8.8\% of respondents said that the network took any action. Better reporting would give providers a better overview of the scale of the problem and may drive greater investment (and public and political pressure for investment) in solutions.

9.3.3 **Opportunities**

**Building police/community trust through negotiation**

Police can build police/community trust by negotiating, rather than assuming, a common understanding of hate crime, especially where the law is unclear. The literature reveals that successfully policing hate crime is impeded where the approach to defining and categorising hate crime is over- or under-inclusive. Over-inclusive approaches focus on community expectations (which often reflect a desire for greater criminalisation) while under-inclusive approaches are oriented towards prosecution (which is often difficult to secure, given that the law leaves much to the interpretation of the judge) (Mason et al., 2015).

**Social media users’ self-regulation and counter-speech**

Initiatives to promote social media users’ self-regulation, by being more circumspect about what is posted online, include WAM 2014; UK Safer Internet Centre, 2015 (Webb et al., 2016). Counter hate-speech initiatives can be effective at overshadowing or drowning out hate speech if used tactically, as reported in an international comparative context in research by DEMOS and Facebook.\textsuperscript{54} Recent research from the RAND Corporation suggests that an effective form of counter-speech could take the form of warnings by social media providers to social media users to be aware of and attuned to aggressive or hateful sponsored propaganda trolling masquerading as genuine political expression (RAND, 2016).

**Initiatives to enable cross-border public security action**

Some examples of these include MLAT-mutual legal assistance treaties, aiding efforts to police the internet across borders, and Interpol’s Global Complex for Innovation, which builds relationships and mutual understanding between national police forces (Jardine, 2015).


Harnessing the power of anonymity on social media for public security aims

Anonymity is a challenge to identifying abusers, but also an opportunity as abusers don't know and cannot verify the identity of those they are dealing with, which is how the host of the Silk Road 01 website was identified and ultimately arrested (Jardine, 2015).

Legislative guidance for public security providers

Recent legislative activity and guidance to police in the UK is providing further clarify on the status of social media sites as ‘public spaces’ and on the distinction between legal and illegal content (Williams & Pearson, 2014:5). The European Commission’s Code of Conduct on Countering Illegal Hate Speech Online, drafted in collaboration with mainstream providers, is another example of authoritative guidance on how to.

Best practice for social media providers

For social media providers, the UK Anti-Defamation League and several major internet companies established ‘Best Practices for Responding to Cyberhate’ (ADL 2014). This recommend timely and proportionate responses from social media providers, and for the internet community to explore avenues for counter-speech as a viable alternative to criminal sanctions. Similarly, the UK Council for Child Internet Safety published the report Child Safety Online: A Practical Guide for Providers of Social Media and Interactive Services (2015).

Police-initiated alternatives to traditional forms of crime reporting

Public reluctance to use traditional crime-reporting mechanisms to report online abuse has prompted the development of alternative tools. True Vision, an online hate reporting tool launched by the UK’s Association of Chief Police Officers has been a big success because people report much more often than they would directly to police (Home Office, 2014). A new initiative by London’s MET police, the Online Hate Crime Hub does something similar.55

Harnessing knowledge and tech advances from academia and the not-for-profit sector

Public security planners can look to technological resources from outside the world of business. For example, the University of Cardiff has developed an online automated cyber hate detection tool (Williams and Pearson, 2014). Similarly, DEMOS, a UK think tank, has developed tools to identify specific kinds of hate crime (e.g. misogyny) on specific social media sites.56 Finally, troll-hunting groups have sophisticated methods of evidence collection and tracing of online abusers that could be useful to police. The Berlin-based Peng! Collective uses bot technology used by spammers to detect misogynistic language on Twitter and then to counter-troll it with humorous messages in an attempt to disrupt trolls (Barlett, 2015).

Public-private-third sector partnerships

55 http://bit.ly/2aLwPPm
56 DEMOS and Cardiff are also working to examine the relationship between hate speech online and hate crimes offline, developing theories that could be of significant use for LEAs seeking to pre-empt and prevent hate crime offline. See ‘Social Media and Hate Crime’ project, DEMOS, at http://www.demos.co.uk/research-area/centre-for-analysis-of-social-media/
The literature points to public-private-third sector partnerships as a great opportunity (Jardine, 2015 p.17; Henry and Powell, 2016:411; World Economic Forum Report on 2013). Many examples of good practice are given, including:

- Telecoms company O2 partners with the UK’s National Society for the Prevention of Cruelty to Children to train one member of O2 staff in every shop to advise young people about staying safe.
- Crown Prosecution Service Hate crime schools project [http://www.cps.gov.uk/northwest/working_with_you/hate_crime_schools_project/](http://www.cps.gov.uk/northwest/working_with_you/hate_crime_schools_project/)
- Safety project funded by Welsh government and Welsh police forces to educate pupils by 85 specially trained police officers
- National Crime Agency Cyber Crime week of action- events in schools, pop up stall in shopping centre
- The e-safety Zone is a forum for information, police and public authorities can pass this on to schools and directly to citizens and it is used as part of training for local authority staff.
- A Cyber-Bullying Information Sharing Point has been proposed to facilitate inter-agency collaboration and best-practice exchange (Williams and Pearson, 2014).

### 9.3.4 Threats

*Lack of police understanding of different experiences of victims*

A failure to respond to the needs of communities reduces trust and legitimacy and hampers the effort to counter hate-speech online and offline. For example, it is shown that people’s experiences of anti-LGBT online hate crime affect their attitudes towards the police, CPS and the government more broadly.\(^57\)

*Lack of clarity on moral/corporate/legal responsibility for responding to trolling*

A challenge is identifying where responsibility- both legal and moral- for intervening and preventing trolling lies- (Webb et al., 2016). Deciding whether something is criminal is not always easy (Rudkin, 2014) as, at least in UK law, it involves interpretation of how offensive a post is. Police considering whether to prosecute abuse or offensive speech online will be cognizant of the risk, in such a nebulous legal context, of having a case rejected by the Crown Prosecution Service or even thrown out of court. Unless prosecuting trolling cases becomes less of a high-risk activity, trolls will continue to benefit.

*Lack of broad national picture on hate crime online*

Both government and academic sources of evidence and monitoring are weak in providing evidence on the impact of cyber hate (Williams and Pearson, 2014: 21). The Crime Survey for England and Wales does not currently include questions on hate crime,

---

\(^57\) In a recent UK study most trans people believed the Government should do more to combat anti-LGBT hate crimes, they felt that the police are less effective and respectful, they felt police should have special policies to deal with anti-LGBT hate crimes, and they have less confidence in the CPS to prosecute anti-LGBT hate crimes (Walters and Paterson, 2016).
let alone hate crime on social media, so it is difficult to plan and direct resources effectively.

**Cross-border cooperation to fight online hate crime**

Most hate content is stored on US servers, but ever-changing technology makes cross-border law enforcement and civil actions significantly more difficult (ICCA 2013). Henry and Powell (2015: 405) also point out that many sites are hosted outside the victim’s home country and this can hamper efforts to deal with the problem. Trolls benefit from the lack of international cooperation.

### 9.3.5 Conditions for success

A strong and clear message emerging from the literature is that coordinated action, involving a range of public security planners and providers is essential for trolling of any kind to be effectively prevented, countered, and punished. This includes legislators because a lack of legal clarity is an obstacle to effective criminal justice operations. It also includes diplomatic agents as cross-border cooperation and coordination is likewise essential for effective operations. Upskilling and educating police officers is also identified as a prerequisite for effective responses to victims of the most serious kinds of online abuse.

### 9.4 Reflection and conclusion

While the literature suggests that organic, community-driven counter-trolling actions are cheaper, faster, more effective and more responsive to trolling than the actions of public authorities, these cannot substitute the strong arm of the law in cases of serious harassment, stalking, and abuse of individuals online. There is some current literature examining the nexus between online and offline abuse, but this is scant and rudimentary. Further research in this area would be beneficial to public security providers and victims of trolling. Key issues to be addressed in the next 5 years include:

- How to develop and improve cross-border cooperation between LEAs in different jurisdictions and social media providers to ensure that the most serious kinds of trolling do not occur with de facto impunity?
- How to ensure that self-styled troll hunters and online community groups use counter-speech, peer pressure, naming and shaming and online investigation to counter trolling in ways that are both legal and ethically defensible?
- How social media and other online tools can be used by LEAs to provide innovative forums for victims of trolling to report their abusers to LEAs effectively and quickly has well as to provide victims with guidance for how to protect themselves?
- How best to achieve greater legal clarity on the definition and scope of hate crimes, harassment and abuse online to empower victims and create clear channels for effective preventive measures or prosecution?
- How to achieve greater understanding of the link between online abuse and offline events so that public security authorities can better predict and plan responses to both?
10. Innovative market solutions

The use of new technologies in policing and public security in general is not a new phenomenon. Social media and applications used aim to better the effectiveness of public authorities, with fast and accessible data in multiple formats (for example photos, videos, geolocations, voice and text). From tweets to serious gaming, social media has pushed public security and policing to advance their investigative processes as well as interaction with citizens. Social media do provide actionable information in real time, but coping with the amount of data received during an event can be challenging. According to Thom (2014), 500 million tweets are produced every day and approximately 15 million of those have geo-coordinates. To digest, analyse, expand and share the valuable information to the domain of public security and policing, constant innovations are required in order to meet needs.

An innovative market is considered a specific branch, which researches unarticulated needs or niche requirements of practitioners and end-users. For example there is no one single app in the EU that informs all citizens about potential ongoing crisis. The need is information exchange among end-users throughout Europe for better response. Identifying such a need, focuses R&D funding and mobilises the supply side.

However technologically advanced a solution may be, there is also need for balancing between needs of public authorities and the rights of the people. Solutions should advance but what also advances is the need for respect of personal data. Data protection regulations have also opened a new market dealing with the protection of that data and their potential misuse.

Innovative market solutions thus refer to new or better product, concepts, methods and ideas that have been developed with the aim to fulfil a defined (or yet unknown) need and operational requirements for public security.

10.1 The influence and impact of social media market solutions use in the domain of public security and policing

In the case of innovative market solutions, the main impact derives from the collection, processing, analysis and diffusion of information is data. When gathering and processing data, even LEAs have to comply with laws and Regulations in place. Every individual has the right to his/her privacy and the appropriate and discreet handling of his/her data according to the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights that defines rules for data collection and data processing.

Positive Impact

The use of social media for crime investigations and surveillance of suspects is a novel method used more and more often by public authorities. Social media and the information deriving from these platforms are considered paramount for criminal investigations. The real time availability of the data creates a continues cycle of possible crimes committed and have assisted evidence gathering as well as arresting individuals.
or groups engaged in organised crime. Hence, enhancing situational awareness by using what is the richest pool of information available.

**Negative Impact**

Gathering and processing data however come with a responsibility for those handling the data. Public authorities cannot store the massive amount of data gathered every day and thus employ external companies to hold the data in their private databases. The police of Birmingham as one example purchased storage space from Amazon’s Web Service in 2015 to store videos from their body cams (Mearian, 2015). That raises many questions on how that data is secured and if it is has been used by the company as a competitive advantage.

Questions of oversight also emerge, in fact who is to say that the data gathered do not target a specific profile and who is the one responsible to define such a profile. How do we distinguish between a peaceful protests and a mass shooting attempt. These variables raise many questions for the origins of surveillance and the motives of public authorities (Kumar, 2013).

10.2 The use of social media market solutions in the domain of public security and policing

**Information gathering and filtering**

Information sharing is key for public authorities to gather intelligence. Now with social media the pool of that incoming information is vast but meaningless unless sorted. Innovations in social media mining and filtering have had a rapid growth the past five years. In this section we address recent innovations on gathering of the information available on social media and the process of sorting and sense making as well as the challenges of rumours and fake data present online.

With the overload of information in all stages of a crisis, computational methods are of extreme importance for the comprehension of the data received (Hiltz et al. 2013); social media does not reduce information overload. LEAs would need to deploy enough man power in order to sort the valuable information from for example rumours which exist during a big crisis, while at the same time re-engaging with citizens. Engagement with the audience can be crucial for diffusing necessary information in real time but definitely challenging. Some public authorities (Belgian Crisis Centre Twitter account) respond to questions posed to them online, that in fact precious time but at the same time real time diffusion of information compensates for it. Platforms like Hootsuite were built to make this engagement easier and more efficient (Hootsuite, 2016).

Twitter related solutions with regards to information gathering and filtering have now been integrated to web and mobile services; these solutions are commonly referred to as “Twitterservers” (Hiltz et al. 2013). To further stress the importance of Twitter, during the Haiti earthquake in 2010 the Red Cross introduced the idea of Twitter micro syntax proposals, designed to mark-up twitter feed and filter information in regards to the situation on the ground. Such a lexicon can significantly improve the detection of crisis related tweets. The Pattern software (Clips 2012) also uses a parser in addition to
a lexicon. Even though both methodologies and lexicons exist, there is no mapping of particular lexicon to specific ontology classes (Jahankhani et al., 2015). Crisis ontologies have advanced significantly during the past years. Some of the solutions on the market are, Vieweg, the humanitarian exchange language (HXL), the management of crisis ontology (MOAC) and the integrated data for Events Analysis (ibid).

In recent years several researchers have incorporated in their filtering analysis “geo-analytics”. This solution allows for visual representation in a form of a map (McEachern et al. 2011). Maps, like Senseplace2, can be used to understand when, where and what is the incident at hand as well as the nature of the incident (Hiltz et al. 2013). Solutions like RiskMaps provide intelligence and security in real time (RiskMap) and Geotime provides the option of depicting crimes online over time. Different solutions have different timelines and specifications depending on the needs they tackle.

Facebook has also been increasingly involved in public security during the last years. It’s first solution the Safety Check (Zuckerberg, 2014), was used by citizens throughout Europe and the Americas to inform if they were safe in different sets of crisis, the Paris bombings, the Brussels attacks, and the Orlando shootings among others. Now Facebook has introduced feature called the “community-generated Safety Check”, where it monitors trending posts within a specific community and then initiates a Safety Check (Karsten and West, 2016).

For all the aforementioned solutions constant engagement with the supply side (industry and SMEs) is necessary in order to identify needs of public authorities and competencies of the market. Either through European funded projects or other initiatives the engagement of the supply and demand side push innovation.

**Monitoring behaviour, sentiment analysis and surveillance**

In addition to information gathering, innovation potential also rises with emotionally charged social media content. This is an attempt to not only rely to what could be an incident but also understand who is potentially involved. It is basically sophisticated software that reads and processes texts of social media content; it bases its analysis on positive or negative sentiment and puts forward an appropriate breakdown for the user (Morrison). These solutions complement information sharing and assist public authorities in their decision-making processes.

In addition to the ‘unofficial’ sharing of information between LEAs and citizens, social media are also widely used for surveillance purposes. To identify criminal behaviour, either online or in the real world, authorities request new technologies for monitoring (Mateescu, et al. 2015). A lexicon-based sentiment analysis is one of the tools used for these purposes. It requires a lexicon labelled words, possibly with weights of their intensity, and use of recurrence of these words in texts to compute the sentiment value of the text (Jurafsky & Martin, 2015). Surveillance of course after the Snowden leaks (BBC, 2014) and the unlawful use of programmes such as Prism from the US National Security Agency have become challenging for national authorities. Enigmabox, released in Switzerland in 2013, the Blackphone released in The Netherlands with pre-installed apps for secure communication; ProtonMail as a secure email service and the best
encryption software so far, which its complexity does not permit wide use, PGP (Technologist, 2014).

In regards to crime investigations nowadays any innovative solutions need to consolidate an approach for the end-user to be able to access not only data from free-to-use sources like Facebook and Twitter as well as the deep or dark web. Different solutions are now available to gather data required for combating physical but also online crime and turn it into valuable intelligence (BrightPlanet, 2013). Systems like BlueJay and Beware are used by law enforcement not only to monitor the behaviour of individuals or groups, but for decision making purposes during a crisis by evaluating all relevant data instantly.

With the pattern deriving from such tools single class classifiers detect what is considered abnormal rather than stating the norm. Classifiers discern between what is similar to something ‘normal’ and what deviates from it being ‘abnormal’ (Daniel & Sushil, 2002). However, what is normal in one context can be abnormal in another, thus the classifiers need to be trained with ‘normal’ portions in each possible context in order to detect changes and the ‘abnormalities’ in that specific context. What is used for training ‘normal’, are trends. In order thus to analyse new data would require considerable amount of historical ‘commonalities’.

All the above-mentioned solutions work with ontologies or lexicons and extract words and phrases which are within the parameters of ‘abnormal’. Solutions like EMOTIVE monitor the strong sentiment behind words and phrases through the ontology. The monitoring can evolve around incidents which have already occurred or reactions from individuals or groups. Visual analytics can be embedded in such solutions and do in most cases incorporate geo-location metadata that show the traffic of a topic within an area or community. Some of the Sentiment tools for twitter include Twitter search, twitter sentiment, Social mention, Sysomos, Tweetzi, Twendz, Statsit, Twitrrart, Evri, AnalyzeWords, and Moodviews (Bouma et al. 2012).

**Network Forensics**

As mentioned before, the plethora of information on social media could potentially be valuable for law enforcement to track patterns, to realise a potential threat or to even use them to gather evidence. Network forensics is the main method to accomplish that. It has been one of the booming innovative markets during the past years (Wright, 2010). However, frameworks build for network forensics like PyFlag and Xplico, cannot access all the needed data; especially sensitive data that operators cannot and should not release. For a special investigation beyond the visible social pages they need special permission, and for that the facts have to be aligned with the claim of misconduct of a person or group (Mulazzani et al., 2013). A more in-depth investigation will need to examine, patterns, history, photos, access to the dark web among others (Wright, 2010). As mentioned in the section of the Dark Web, its exponential growth has caused a formidable challenge since the sites open in a rate much greater than law enforcement can handle.58 Two of the most prominent methods to enhance forensic analysis include,

---

58 Still, Article 10 of the European Convention on Human Rights maintains that "everyone has the right to freedom of expression" and that that right may only be qualified in narrowly limited circumstances. Those circumstances include...
event tracking and differential snapshots. Event tracking is one of the tools that can be used for better investigations. Within Google Analytics, there is a feature named Event Tracking available in the ‘ga.js’ method code. LEAs can use this element to collect and cluster types of interactions in a certain web page (Google Analytics). Tools like CapAnalysis filter data also according to IP, GeoIP and/or Ports, Protocols, countries and data volume (CapAnalysis). In addition, differential snapshots and snapshot backups, like ’diffsnapshot’, is a “specialized backup that is created almost instantaneously by using a split-mirror solution obtained from an independent hardware and software vendor” (Microsoft). These backups help control very large databases. Analysis of these backups can provide a pool of historical data.

10.3 Inventory of strengths, weaknesses, opportunities and threats (for use of social media market solutions)

10.3.1 Strengths
Requirements can be easily identified when law enforcement share information. When using innovative solutions law enforcement identify threats faster and can request new solutions from providers. If the specific threat however is not widespread throughout other agencies it is more difficult. Efficient requirement analysis as well as sharing of lessons learned can be valuable resources for the gathering of data and data patterns (Zhao, 2013). With this in mind decision making for law enforcement can be allocated in a more efficient way in line with predictive policing approaches (Gerber, 2014). With the help of innovative solutions data can be gathered in real time and shared with the relevant law enforcement in all crisis stages.

10.3.2 Weaknesses
A big challenge that develops with social media is misuse. LEAs have to be trained in order to make use of the full potential of social media. The lexicon used on social media by citizens complicates the understanding of messages from law enforcement; this is why automated sorting is important in their day-to-day work. In addition to that the language itself is seemingly a pattern, #tags, abbreviations and slang but does not stand on its own. For these challenges that have emerged with social media but also for market reasons, public authorities are dependent on industry and SMEs to build solutions for them. Most of the times the security market is so fragmented that the solutions build are not needed or redundant. To access further information, data that would be potentially used for forensics, service operator would need to give access to them (Mulazzani et al., 2013). Operators cannot and will not share such information unless probable cause if proven. Law enforcement agents thus need to find new ways to obtain such data. The lack of forensics APIs and standardised operators processes an additional challenge.

10.3.3 Opportunities
Usage of Visual Analysis (VA) can be a valuable resource in combination with machine learning, language processing, and interactive interfaces. They can be utilised to cope
with large amount of data. If the gathering of data becomes more efficient, their analysis and distribution becomes faster and preventive mechanisms can be placed. Novel features like geotagging and location need to be included especially in forensic examination in social networks (Mulazzani et al., 2013).

Lens-like tools also generate interesting data for law enforcement since they can tag over a map and observe frequently use messages in a specific area. A combination of focus and contextual analysis in visual analytics is in fact used both to social media and news agencies (Thom, 2013). From the data collected from these media patterns can be detected which can also indicate anomalies. With these in place and the integration of ‘unsupervised algorithms’ for event detection, promote visual representations of potential and ongoing crisis (ibid.).

10.3.4 Threats

When using innovative solutions, botnets and malware are currently one of the most significant threats existing in social media. They can manipulate information according to the perpetrator’s needs and produce or exploit a story line with false information. Bots “mislead, exploit, and manipulate social media discourse with rumours, spam, malware, misinformation, slander, or even just noise” (Ferrara et al., 2015) and “rumours are pieces of information that cannot be verified in real time, especially when there is a strict gag order. Despite this, many people accept them as true and share them further” (Crisis Response, 2016). In fact the usage of instant messaging has increased rumours during emergencies more than ever (ibid.). The diffusion of wrong information can lead to reception of misinformation of law enforcement and stalling of emergency response.

10.3.5 Conditions for success

The real time information that social media provide public authorities, has introduced a much needed source of information. New solutions adapting to needs also create new challenges on a societal and ethical level. Innovative market solutions as important as they are for the analysis of data gathered and processed from social media have limitations. For this reason a balance between what is needed by public authorities and what is right for citizens has to be maintained.

The first condition that we consider for the successful use of those tools is training. Not simply training on how to share information with citizens, but training on legal frameworks for the gathering and processing as well as data retention; on triangulating information throughout different sources; on cultural sensitivity and avoidance of unwanted bias; and appropriate operationalisation of the data gathered with the sensitivity and respect required. The technical as much as the legal components on the usage of social media are critical for LEAs to achieve their goals. This is why serious gaming is one of the most significant innovations that have resulted from the use of social media. It is considered at the moment the best technology-mediated learning tool (Derryberry, 2017).

Some of the features of the categories described in the first section – information gathering and filtering, monitoring behaviour, sentiment analysis and surveillance as
well as network forensics – need to be combined, always according to needs, in order to deliver the most accurate data possible. Thus, combining data gathering with a multilevel analysis of the information and secure delivery of the trends deriving from that data to the respective authorities.

In addition, in order for innovative solutions to reach the market on time, standards have to be in place. Thus, a consolidated end-to-end approach starting with the needs of end-users ending with the evaluation of the product from end-users. To further this aspect, the demand and supply sides need to communicate their needs and their capabilities accordingly. In this regards, when needs and operational requirements are known the R&D funding will be distributed to necessary research and the development of appropriate solutions.

10.4 Reflection and conclusion

This part of the literature review was based on academic research, R&D project results and white papers from the supply sector. Our main observation from this research derives from the fact that there not one consolidated study on the use of innovative market solutions from public authorities. There exist studies tackling specific solutions, operational needs of law enforcement and even certain challenges present from the use of social media; thus the literature is fragmented and inevitably certain aspects, like the storage of data in the private domain, are not well documented.

Nevertheless, innovative market solutions used on social media have revolutionised the way public authorities conduct their basic everyday operations, making them more efficient and cost effective. This niche field has created a new ground for further innovations in investigations, monitoring, understanding behaviour and training. The technical capacity of those investigating online should be that that would respect citizens and secure their data. Ethical and societal considerations thus need to be at the forefront of new solutions; security cannot be above the law.

For public authorities, practitioners and end-users to be aware of their limitations on data collection, information sharing and surveillance capabilities, a critical component is training. The introduction of serious gaming has expanded training capabilities, but for that to function properly training facilities should be well known and allow external persons to be able to train and be trained with the most advanced solutions available.

The three main questions deriving from this chapter linked to the development of innovate market solutions are:

- What can be done to facilitate communication between the supply of and demand for new innovative social-media solutions?
- What is the future of training capabilities and how to use it best for public security?
- How do we balance between security and rights in advancing new security solutions?
- What are the challenges with data been collected from third parties? Should there be pan-European requirements for the usage of that data?
• Should we have calls for funding specifically on development of further sophisticated solutions for social media?
11. Conclusions

This report has provided an overview of the state of the art on the emerging role of (new) social media in enhancing public security. It has specifically focused on the current uptake of social media by public security bodies, the different daily uses of social media within various security tasks, the impact and influence of its use as well as the challenges and opportunities ahead. Our analysis has paid particular attention to six security themes to illustrate the weaknesses, strengths, threats and opportunities of social media in the public security domain. This analysis has identified a series of questions which will be explored further through the dialogue workshops which form the backbone of the MEDI@4SEC project.

11.1 Strengths and Opportunities

First of all, the strengths and opportunities of social media in enhancing public security are enormous with specific characteristics of social media making it a powerful medium within the security domain:

- By enabling two-way communication at high speed, anywhere and anytime (strengths) social media allows law enforcement agencies to connect with end-users and citizens and maintain contact at minimal costs (opportunities), improving the reach of these organisations within neighbourhoods and local communities (Meijer et al., 2013).

- Improved communication combined with the transparency (strength) that social media bring forward, create opportunities to increase trust and engagement and improve reputation (Denef et al, 2012).

- Moreover, these strengths, combined with the richness (strength) of social media, enable law enforcement officers to collaborate with the crowd (opportunity) and so increase effectiveness (Global Advisory Committee, 2013). For example, innovative solutions in case of an emergency are being developed, making use of these strengths of social media (De Vries et al, 2016) and social media creates opportunities for collaboration between law enforcement officers and community (community policing), for both surveillance and criminal investigation.

- The speed, richness of information and independency of location and time enable law enforcement officers to contact bystanders in case of an accident, either for information (eyewitnesses) or for emergency help (opportunity) and enable crisis communication (De Smet, 2012). The masses of data social media create (strength) enable opportunities for early warning (Vries, de et al, 2011; Terpstra et al, 2012) and crowd management (Fictorie, 2013). Analyses of this data (in some cases combined with others) (strength) also offer opportunities for intelligently considered surveillance (Gerber, 2014).

- Finally, the transparency (strength) of social media makes criminals acting online leave traces, which can help for criminal investigations.
11.2 Weaknesses and Threats

The use of social media also introduces weaknesses and threats for public security.

- Social media are decentralized via diverse platforms (weakness) which can for example lead to missing out on relevant messages, and hence missing out on information (threat), or receiving information late even though social media are being monitored (Broekman and Menkhorst, 2013).
- There are challenges in acquiring or validating information (threat).
- The speed and time and location independency of social media are of benefit to those breaking the law as well as law enforcement agencies, e.g. those who want to organize riots can reach and gather large amounts of people in a short time (threat). In these loosely connected groups of people, it is hard to identify key figures (Jaitner and Kantola, 2014).
- Social media enables individuals and groups to reach people all over the world (e.g. International terrorist organisations) (threat).
- The transparency of social media can create also expose the tracks of law enforcement officers which can aid the criminal (weakness).
- Criminals have found new solutions to hide their tracks, since they moved to the anonymous dark web (threat) where they are difficult to identify.
- Social media can also provide ‘poor’ information, since context is missing. The overload of messages (weakness) contain for example lots of (death) threats that miss context, and therefore are hard to interpret (threat).

11.3 MEDI@4SEC Themes

11.3.1 DIY (Do-It-Yourself) policing

DIY policing questions the general division of responsibilities and legitimate power between citizens and law enforcement agencies. The key questions for many security planners are about where and how to cooperate with citizens, when to take control and how to avoid negative effects. We highlight how, on the one hand, we see citizens taking coordinated action in places where public security falls short or fails. This leads to the question: can DIY policing become a factor for public security organizations to use in targeting where their resources are best deployed and where citizens can aid their operations? On the other hand, it appears that some (especially Dutch) police forces have taken these concerted efforts in co-creating safety jointly with citizens. The many platforms and initiatives that were studied, underline the Dutch forerunner role in encouraging DIY activities. DIY policing does raise a range of delicate ethical questions. Empowered citizens have the means to fight injustice and produce desirable change, while at the same time, they can also create great harm when acting irresponsibly.

11.3.2 Mass Gatherings

The rapid adoption of social media has enabled social movements and mass gatherings in two ways: 1) in organization and coordination of the event itself, and 2) by providing wider exposure that leads to increased participation. This report shows that policing of riots and mass gatherings is a critical issue for law enforcement agencies that poses key
question. How to re-invent the current policing paradigm to incorporate new tools, organizational structures, staff, policies and technological infrastructure to support the use of social media in such situations? Here the focus should be on both, monitoring potential mass gatherings on social media as well as preparing for one and communicating with community. Moreover, in such instances it is vital to advance a communication strategy to ensure the uniform use of social media by authorities in a positive, friendly, instructive and helpful tone to promote citizen engagement, collaboration and trust. Such interactive communication can provide a substantial resource for situation awareness but should be done in an ethically aware way.

11.3.3 Every day Security

The recent massive increase in social media use has drastically transformed people’s communication and information habits, and provides authorities with new opportunities for intelligence sources and platforms to communicate. These new opportunities raise numerous questions, for instance, in what ways do the data and tools available through social media influence the work of intelligence services and LEA’s? How do local authorities use social media to facilitate and enhance their local crime prevention strategies? Or, how can community policing initiatives supported by social media contribute to the everyday management of security? One of the main challenges for law enforcement agencies using social media in policing is the adoption of formal policies and processes within agencies that enable a unified, consistent approach to modern technology usage. Incorporating specialized staff, budget dedicated to innovation and defining a clear legal framework and procedural protocols, become a priority for the agencies and policy planners in the public security domain.

11.3.4 The Dark Web

Historically, technology has revolutionized policing practices but it has also facilitated criminality with the Dark Web emerging as a key space for “high tech” (organized) cybercrimes. The analysis presented in this report raises a number of issues which should be taken into account in the discussion on policing against Dark Web: How to avoid limited applicability in a cybercrime community that is instead capable of quickly developing countermeasures with flexible and adaptable innovations policies? Furthermore, there should be no “size-fits-all” measures: strategies should differentiate between the types of crime, nor should there are “total-block” strategies: policies should seek balance between freedom of speech and crime facilitation. In the case of cryptomarket-related crimes, how to be able to tackle the ecosystem, instead of single targets, and focus on the demand first, instead of the vendors side only with strategies that focus on the “economical game”? Moreover, with violent extremism, how to set out strategies that focus on the producers, rather than on the consumers of extremist material? And also, how to empower the “good” and the "grey" users with spaces for open debate that allows extremisms to be blended and debated? Finally, what are the options of applying social media strategies from the Clear Web to the Dark Web, being aware of the differences between the two digital dimensions?
11.3.5 Trolling

Trolling broadly understood includes cyberbullying, cyberhate, cyberstalking, cyberharassment, revenge porn, sextortion, naming and shaming and flaming. The legal status of all the trolling-related acts just listed differs from jurisdiction to jurisdiction and from act to act. An impressive and varied array of preventive, counter-trolling, and criminal justice approaches to combating trolling are currently employed by public security providers broadly understood. While the literature suggests that organic, community-driven counter-trolling actions are cheaper, faster, more effective and more responsive to trolling than actions of public authorities, these cannot substitute the strong arm of the law in cases of serious harassment, stalking, and abuse of individuals online. There is some current literature examining the nexus between online and offline abuse, but this is scant and rudimentary. Further research in this area would be beneficial to public security providers and victims of trolling.

11.3.6 Innovative Market Solutions

To digest, analyse, expand and share the valuable information on social media to the domain of public security and policing, constant innovations are required in order to meet these needs. An innovative market solutions focus on social media and applications used, aiming to increase the effectiveness of public authorities, with fast and accessible formats. From tweets to serious gaming, social media have pushed public security and policing to advance their investigative processes as well as their interaction with citizens. One key question that arises is what can be done to facilitate communication between the supply of and demand for new innovative social-media solutions? Furthermore, how can the training of public security planners in social media use be facilitated by new innovations? Overall, one of the most important question with new technology solutions is, how do we balance between security and rights in advancing new security? Solutions should advance, but the respect of personal data must advance as well. Data protection regulations have opened a new market dealing with the protection of data and their potential misuse. This raises questions like; what are the challenges with data been collected from third parties? And should there be pan-European requirements for the usage of that data? Ethical and societal considerations thus need to be at the forefront of new solutions; security cannot be above the law.

The questions, challenges and opportunities raised in this report provide insight for future research, and will be the focus of the upcoming policy and practice workshops in the MEDI@4SEC project.

The questions, challenges and opportunities raised above, provide insight for future research, but especially input for the upcoming thematic workshops of this EU MEDI@4SEC project the upcoming years.
Bibliography


Bartlett, J., Miller C. (2013), @metpoliceuk How Twitter is changing modern policing the case of the Woolwich Aftermath. London: Demsos.


IBM Knowledge Center (IBM). Diffsnapshot. IBM. Retrieved at 09-13-2016 via http://ibm.co/2cKr7Lh.


Mauritz, A., (2011). Be Connected, be Social, be Polite; Sociale Media, de Verbindende Factor tussen Politie en Burger. Onderzoeksrapport NOG.


NBC News (2013), ‘1 in 10 Twitter Accounts is Fake, Say Researchers’ Nov 25th, at http://nbcnews.to/2dxsDR


Procter R., Crump J., Karstedt S., Voss A. & Cantijoch M.,(2013). Reading the riots: what were the police doing on Twitter?. Policing and Society, 23(4).


TellMAMA (2015) ’We fear for our lives: offline and online experiences of anti-muslim hostility’ at http://bit.ly/1LeOM1l.


Appendix 1  Flow chart of PRISMA steps

*Flow chart Systematic Literature Review according to the PRISMA method.*

<table>
<thead>
<tr>
<th>Step 1 Define</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Step 2 Collect and assess</th>
</tr>
</thead>
<tbody>
<tr>
<td>Academic literature plus conferences</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3 Analyse and report</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
</tr>
</tbody>
</table>
Appendix 2 Search strings PRISMA method

A search string was developed in cooperation with all partners to be sensitive as well as selective in searching databases and using search engines. Relevant search terms were extracted from the project proposal and complemented with search terms that were provided by all project partners during the kick off meeting of the project. A generic search string was defined including variations of keywords on (1) social media and (2) policing and public security. In addition, seven thematic search strings were developed with keywords relating to the six project themes and possible other themes. By the use of search operators and wildcards, variations of keywords are included. Different variations of the search strings were created for various databases and search engines.

Search strings academic literature

Generic search string:

('social media' OR "Facebook" OR "Twitter" OR "web 2.0" OR "web 3.0" OR "cyber*" OR "user?generated content" OR "new media" OR "social network" OR "blog*" OR "weblog*" OR "online discussion forum*" OR "SOCMINT" OR "SMI" OR "open source" OR "app" OR "apps" OR "smartphone*" OR "website") AND ("police" OR "policing" OR "law enforcement" OR "LEA" OR "LEAs" OR "public security" OR "everyday security" OR "public safety" OR "early warning" OR "crime prevention" OR "crowd control" OR "homeland security" OR "intelligence agency" OR "prosecut*" OR "securiti?ation" OR "crime")

Thematic search string Trolling:

("troll*" OR "4chan" OR "Reddit" OR "hate crime*" OR "cyberbully*" OR "flaming" OR "naming?shaming" OR "hate speech" OR "do?ing" OR "banga" OR "cyberstalk*" OR "revenge porn*" OR "hoax*" OR "cyberflashing" OR "hugging" OR "hussi*" OR "N00b") AND ("police" OR "policing" OR "law enforcement" OR "LEA" OR "LEAs" OR "public security" OR "everyday security" OR "public safety" OR "early warning" OR "crime prevention" OR "crowd control" OR "homeland security" OR "intelligence agency" OR "prosecut*" OR "securiti?ation")

Thematic search string DIY Policing:

("crowdsourc*" OR "crowdsearch*" OR "cybervolunteer*" OR "copwatch*" OR "doe network" OR "neighbo?hood watch" OR "websleuth" OR "crimestopper*" OR "serendip*" OR "vigilant*" OR "crowdmap*" OR "red?team") AND ("police" OR "policing" OR "law enforcement" OR "LEA" OR "LEAs" OR "public security" OR "everyday security" OR "public safety" OR "early warning" OR "crime prevention" OR "crowd control" OR "homeland security" OR "intelligence agency" OR "prosecut*" OR "securiti?ation")

Thematic search string Everyday Security:

("smart cit*" OR "open data" OR "big data" OR "social media monitor*" OR "social media analy*" OR "datamin*") AND ("police" OR "policing" OR "law enforcement" OR "LEA" OR "LEAs" OR "public security" OR "everyday security" OR "public safety" OR "early warning" OR "crime prevention" OR "crowd control" OR "homeland security" OR "intelligence agency" OR "prosecut*" OR "securiti?ation")

Thematic search string The Dark Web:

("dark web" OR "dark net" OR "Onion Router" OR "TOR" OR "I2P" OR "bitcoin*" OR "dark market" OR "deep web" OR "crimesourc*" OR "hacking") AND ("police" OR "policing" OR "law enforcement" OR "LEA" OR "LEAs" OR "public security" OR "everyday security" OR "public safety" OR "early warning" OR "crime prevention" OR "crowd control" OR "homeland security" OR "intelligence agency" OR "prosecut*" OR "securiti?ation")

Thematic search string Riots and Mass Gatherings:

("riot*" OR "mass gathering*" OR "slacktivis*" OR "cyberacti?is*" OR "crisismap" OR "public event") AND TITLE ("police" OR "policing" OR "law enforcement" OR "LEA" OR "LEAs" OR "public security" OR "everyday security" OR "public safety" OR "early warning" OR "crime prevention" OR "crowd control" OR "homeland security" OR "intelligence agency" OR "prosecut*" OR "securiti?ation") AND ("social media" OR "Facebook" OR "Twitter" OR "web 2.0" OR "web 3.0" OR "user?generated content" OR "new media" OR "social network" OR "blog*" OR "weblog*" OR "online discussion forum*" OR "SOCMINT" OR "SMI" OR "open source" OR "app" OR "apps" OR "smartphone*" OR "website" OR "cyber*")
**Thematic search string Innovative Market Solutions:**

('app' OR "apps" OR "nextdoor" OR "social media monitor" OR "social media analyzer" OR "datamin"') AND ('police' OR "policing" OR "law enforcement" OR "LEA" OR "LEAs" OR "public security" OR "everyday security" OR "public safety" OR "early warning" OR "crime prevention" OR "crowd control" OR "homeland security" OR "intelligence agency" OR "prosecut" OR "securitiation")

**Thematic search string Other themes:**

(['radicalis"' OR "terroris" OR "counterterrorism" OR "cyberterrorism" OR "terror" OR "gang" OR "grooming" OR "sexting" OR "clickbait" OR "counter\narrative" OR "social movement" OR "counter\nmovement" OR "crisis management" OR "social influencing" OR "identity theft") AND TITLE ('police' OR "policing" OR "law enforcement" OR "LEA" OR "LEAs" OR "public security" OR "everyday security" OR "public safety" OR "early warning" OR "crime prevention" OR "crowd control" OR "homeland security" OR "intelligence agency" OR "prosecut" OR "securitiation") AND("social media" OR "Facebook" OR "Twitter" OR "web 2.0" OR "web 3.0" OR "user\ngenrated content" OR "new media" OR "social network site" OR "blog" OR "weblog" OR "online discussion forum" OR "SOCMINT" OR "SMI" OR "open source" OR "app" OR "apps" OR "smartphone" OR "website" OR "cyber")

**Search strings grey literature**

**Generic search string:**

"Social media" AND police
"Social media" AND policing
"Social media" AND "public security"
"Social media" AND "public safety"

**Thematic search string DIY policing:**

Crowd AND "social media" AND "criminal investigation"
Crowd AND "social media" AND Surveillance

**Thematic search string Riots and mass gatherings:**

Riot AND "social media" AND "public security"
Riot AND "social media" AND "public safety"
"mass gathering" AND "social media" AND "public security"
"mass gathering" AND "social media" AND "public safety"

**Thematic search string Dark web:**

Dark web" AND "public security"
"Dark web" AND "public security"
"dark web" AND "crime"

**Thematic search string Everyday security:**

"social media" AND "everyday security"
"social media" AND "early warning"
"social media" AND "crime prevention"

**Thematic search string Trolling:**

Trolling AND "social media" AND "public security"
Trolling AND "social media" AND "public safety"
"Cyber stalking" AND "social media"

**Thematic search string Innovative Market solutions:**

"social media" AND app AND "public safety"
"social media" AND app AND "public security"
Appendix 3 Eligibility criteria

- Publication needs to be from 2010 or more recent;
- Publication should address current issues of social media and policing/public security and not only historical events that are no longer relevant to the current situation;
- The full publication needs to be publicly available via the university and company accounts of at least one of the partners. Only the most relevant payed publications were purchased and included in the review;
- The full publication needs to be in English;
- Additional non-English suggestions from partners and experts are added when they provide an English summary;
- Publications from newspapers or popular magazines are excluded;
- Publications that were wrongly selected because of misspelling of 'policies' as 'polices' are excluded;
- Publications related to one of the six themes should not only describe the phenomenon, but also specify a role for the police/public security.
- Publications should be about public security monitoring/early warning, meaning that articles about disease or natural disaster monitoring/early warning etc. are excluded;
- Publications applying a sociological definition of 'policing' /'surveillance' behavior of people on social media without attention for police/public security issues are excluded;
- Publications on crisis management are only taken into account when a role for the police/public security is outlined;
- Publications on social influencing in general are excluded, but social influencing within security domain is in scope.
- Publications on cybercrime and cybersecurity need to take into account a role for police and criminal investigation, they are excluded when they are only describing the phenomenon or legal framework;
Appendix 4 PRISMA flow diagrams

- Academic publications: N=423
- Grey publications: N=223
- European publications: N=108

Screening for eligibility: N=754
Ineligible articles removed: N=372

Full publications included in meta-synthesis: N=382
### Appendix 5 Analytic framework of codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Please list surnames and initials of all authors of the publication. Separate authors by using a comma. If no authors are listed, please list the organization which published the document.</td>
</tr>
<tr>
<td>Year of Publication</td>
<td>Please note the year of publication (2010-2016). Earliest publications we take into account are 2010. If the year of publication is unknown, please note.</td>
</tr>
<tr>
<td>Title</td>
<td>Note full title and subtitle of the publication.</td>
</tr>
<tr>
<td>Type of publication</td>
<td>Select the relevant type of publication from the list. (see for categories paragraph 2.2 of this deliverable)</td>
</tr>
<tr>
<td>Source/publisher</td>
<td>Please note the source or publisher of the publication. For example the journal or book series, conference or publisher or publishing organization. Do not enter an URL to the publication: do this under column L.</td>
</tr>
<tr>
<td>Language</td>
<td>Select the language the full publication is available in. Options are: English, Dutch, Other, Unknown. When the publication is available in multiple languages, please select the language in which the publication was reviewed.</td>
</tr>
<tr>
<td>Full text available?</td>
<td>Please note whether the publication is available in full tekst (yes, no, unknown). If not, the publication is not eligible for further review. Do not enter an URL to the publication: do this under column L.</td>
</tr>
<tr>
<td>Link to full publication</td>
<td>Please provide the URL of the full publication. If the publication is not easily/publicly available online, please store the file on the Google drive.</td>
</tr>
<tr>
<td>Abstract</td>
<td>Copy-paste the full abstract of the publication. For non-academic publications a management summary or introduction paragraph can be copied here. If not available please note n.a.</td>
</tr>
<tr>
<td>Type of research/content</td>
<td>Please note the timeframe in which the research took place. E.g. riots of June 2011; Facebook interactions from January 2013-June 2013.</td>
</tr>
<tr>
<td>Timeframe research</td>
<td>Please note the timeframe in which the research took place. E.g. riots of June 2011; Facebook interactions from January 2013-June 2013.</td>
</tr>
<tr>
<td>Country setting research</td>
<td>Note in what context the research took place. E.g. The Netherlands, Nordic countries, South America or 20 French municipalities.</td>
</tr>
<tr>
<td>Level of government</td>
<td>Select from list on what level of security/policing governance the publication focuses. If not applicable, please select n.a.</td>
</tr>
<tr>
<td>Data</td>
<td>Note what type of data was collected. E.g. Quantitative survey data; Semi-structured</td>
</tr>
<tr>
<td><strong>Type of social media</strong></td>
<td>Note whether the publication addresses any specific types of social media. E.g. Twitter, Youtube, Online reviews.</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Public security/policing task</strong></td>
<td>Note whether the publication addresses any specific public security/policing tasks for which social media are appropriated. Please be as specific as possible. E.g. crowd control during riots, information mining for criminal investigation; communication for reputation management.</td>
</tr>
<tr>
<td><strong>Public security organizations/actors/stakeholders identified</strong></td>
<td>Note whether the publication addresses any specific public security/policing tasks for which social media are appropriated. Please be as specific as possible. E.g. crowd control during riots, information mining for criminal investigation; communication for reputation management.</td>
</tr>
<tr>
<td><strong>How are social media used for public security/policing</strong></td>
<td>Provide a description of the social media uses for public security/policing that are under scrutiny in this study. Please be as specific as possible.</td>
</tr>
<tr>
<td><strong>Strengths, Weaknesses, Opportunities and Threats (SWOT) and Conditions for successful use</strong></td>
<td>Summarize any identified Strengths, Weaknesses, Opportunities and Threats (SWOT) and Conditions for successful use.</td>
</tr>
<tr>
<td><strong>Impacts/results of social media use</strong></td>
<td>Describe what impacts or results of social media appropriation for policing/public security are defined in the publication. These may concern police organisations but also larger societal impacts. E.g. Efficient police work; trust of citizens in police, more crimes solved, new types of criminal activities.</td>
</tr>
<tr>
<td><strong>Relevance to six themes (primary theme)</strong></td>
<td>Does this publication have relevance for any of the six themes of Media4Sec? Please select the theme that this publication is relevant to. If it has relevance to another theme, please select 'other' and elaborate this in column AB. If the publication has no relevance to any specific theme, please note n.a. If the publication has relevance to multiple themes, note these in the next columns in order of relevance (primary, secondary, tertiary theme).</td>
</tr>
<tr>
<td><strong>Relevance to six themes (secondary theme)</strong></td>
<td>Does this publication have relevance for any of the six themes of Media4Sec? Please select the theme that this publication is relevant to. If it has relevance to another theme, please select 'other' and elaborate this in column AB. If the publication has no relevance to any specific theme, please note n.a. If the publication has relevance to multiple themes, note these in the next columns in order of relevance (primary, secondary, tertiary theme).</td>
</tr>
<tr>
<td><strong>Relevance to six themes (tertiary theme)</strong></td>
<td>Does this publication have relevance for any of the six themes of Media4Sec? Please select the theme that this publication is relevant to. If it has relevance to another theme, please select 'other' and elaborate this in column AB. If the publication has no relevance to any specific theme, please note n.a. If the publication has relevance to multiple themes, note these in the next columns in order of relevance (primary, secondary, tertiary theme).</td>
</tr>
<tr>
<td>Table:</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Explanation of relevance to themes</strong></td>
<td>Please elaborate how the publication is relevant to one or multiple of the six themes. If it has relevance to another theme, please note what theme this is &amp; why. If it has no relevance to any specific theme, note n.a.</td>
</tr>
<tr>
<td><strong>Eligibility? (Yes/No)</strong></td>
<td>Please note whether the publication is eligible for the literature review (Based on eligibility criteria)</td>
</tr>
</tbody>
</table>
| **Assessment of relevance for T1.2** | Please assess the relevance of the publication for T1.2  
Enter 1-3 stars for relevance for eligible articles. If necessary, further specify in Column H. When Eligibility = no, note here why not without ranking stars. |
<p>| <strong>Who added and assessed? (Step 2)</strong> | Type your organization's name (TNO, UoW, EFUS, UU) |
| <strong>Who will analyze and report? (Step 3)</strong> | Type the name of the partner who will analyze this document (TNO, UoW, EFUS, UU) |
| <strong>Concrete/best practices named for T1.3?</strong> | Are any concrete or 'best' practices identified that are relevant for T1.3? Please select Yes, No, Unclear, n.a. |
| <strong>Ethical or legal considerations named for T1.4?</strong> | Are any ethical or legal considerations for social media appropriation named that are relevant for T1.4? Please select Yes, No, Unclear, n.a. |</p>
<table>
<thead>
<tr>
<th>Type of Literature</th>
<th>Relevance to Six Themes</th>
<th>Author(s)</th>
<th>Year of Publication</th>
<th>Title of Publication</th>
</tr>
</thead>
<tbody>
<tr>
<td>grey</td>
<td>The dark web</td>
<td>Abdelghani, H., M. Mans, and Mohamed Ali Kaafar</td>
<td>2010</td>
<td>Digging into anonymous traffic: a deep analysis of the tor anonymizing network</td>
</tr>
<tr>
<td>grey</td>
<td>General</td>
<td>Accenture</td>
<td>2012</td>
<td>Preparing police services for the future: six steps toward transformation</td>
</tr>
<tr>
<td>grey</td>
<td>Hints and mass gatherings</td>
<td>Accenture</td>
<td>2013</td>
<td>Are police forces maximizing technology to fight crime and engage citizens</td>
</tr>
<tr>
<td>grey</td>
<td>Other</td>
<td>avid</td>
<td>2012</td>
<td>Jihadien on the Web</td>
</tr>
<tr>
<td>academic</td>
<td>Innovative market solutions</td>
<td>Athgar, B. &amp; Gibson, H.</td>
<td>2015</td>
<td>Processing Social Media Data for Crisis Management in Atheira</td>
</tr>
<tr>
<td>grey</td>
<td>DIY policing</td>
<td>Akkerman, M., Volkard, R.</td>
<td>2015</td>
<td>Effect of the WhatsApp-project in Tilburg on the amount warningbrakers - an evaluatie</td>
</tr>
<tr>
<td>grey</td>
<td>The dark web</td>
<td>Alberto Muñoz</td>
<td>2015</td>
<td>Klue al lado ociso de internet</td>
</tr>
<tr>
<td>grey</td>
<td>The dark web</td>
<td>Alberto Muñoz</td>
<td>2015</td>
<td>Klue al lado ociso de internet</td>
</tr>
<tr>
<td>grey</td>
<td>The dark web</td>
<td>Alex Broukhov, Ivan Pustogarov, and Ralph-Peter Wissmann</td>
<td>2013</td>
<td>Content and popularity analysis of tor hidden services</td>
</tr>
<tr>
<td>academic</td>
<td>DIY policing</td>
<td>Alexander, B.K. &amp; Jackson, R.</td>
<td>2016</td>
<td>If they gunned me down and crying white white: An examination of twitter campaigns through the lens of citizens’ media</td>
</tr>
<tr>
<td>academic</td>
<td>Hints and mass gatherings</td>
<td>Alexander, D.E.</td>
<td>2014</td>
<td>Social Media in Disaster Risk Reduction and Crisis Management</td>
</tr>
<tr>
<td>grey</td>
<td>Innovative market solutions</td>
<td>ALEXANDRA RATESCU, et al.</td>
<td>2015</td>
<td>Social Media Surveillance and Law Enforcement</td>
</tr>
<tr>
<td>academic</td>
<td>Other</td>
<td>Almenas, S.</td>
<td>2014</td>
<td>The criminalisation of identity theft under the saudi anti-cybercrime law 2007.</td>
</tr>
<tr>
<td>grey</td>
<td>General</td>
<td>Ackerman, N.</td>
<td>2013</td>
<td>The Internet Police: How Come West Online, and the Cop’s Followed</td>
</tr>
<tr>
<td>academic</td>
<td>The dark web</td>
<td>Alexi Lavning</td>
<td>2014</td>
<td>Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics</td>
</tr>
<tr>
<td>academic</td>
<td>The dark web</td>
<td>Alexi Lavning</td>
<td>2014</td>
<td>Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics</td>
</tr>
<tr>
<td>grey</td>
<td>General</td>
<td>Bartlett, J.</td>
<td>2013</td>
<td>Cyberpractises for the use of social media in public safety communications</td>
</tr>
<tr>
<td>academic</td>
<td>Everyday security</td>
<td>Aymer, A.</td>
<td>2014</td>
<td>Big data and innovation in the delivery of public services: The case of predictive policing in Kent</td>
</tr>
<tr>
<td>grey</td>
<td>Trolling</td>
<td>Awan, I. &amp; Blakemore, B.</td>
<td>2012</td>
<td>Policing cyber hate, cyber threats and cyber terrorism</td>
</tr>
<tr>
<td>grey</td>
<td>Hints and mass gatherings</td>
<td>Bähr, E., Broek, van den B.</td>
<td>2013</td>
<td>Project X-Haven: monale panel over jeugd technologie en crisis</td>
</tr>
<tr>
<td>academic</td>
<td>Hints and mass gatherings</td>
<td>Baker, S.J.</td>
<td>2012</td>
<td>The dark web: From the criminal crowd to the ‘mediated crowd’: The impact of social media on the 2011 english riots.</td>
</tr>
<tr>
<td>grey</td>
<td>Other</td>
<td>Barisett, J., Krasadatomi-Jones, A.</td>
<td>2015</td>
<td>Online anonymity: Islamic State and surveillance</td>
</tr>
<tr>
<td>grey</td>
<td>Everyday security</td>
<td>Bartlett, J, Miller, C.</td>
<td>2013</td>
<td>@MeteoUK: How Twitter is changing modern policing</td>
</tr>
<tr>
<td>grey</td>
<td>Everyday Security</td>
<td>Bartlett, J., Reynolds, L.</td>
<td>2015</td>
<td>The state of the art 2015 A literature review of social media intelligence capabilities for counterterrorism</td>
</tr>
<tr>
<td>grey</td>
<td>The dark web</td>
<td>Bartlett, Jamie</td>
<td>2014</td>
<td>The Dark Net: Inside the Digital Underworld</td>
</tr>
<tr>
<td>grey</td>
<td>Hints and mass gatherings</td>
<td>Beekers, V., Edwards, A., de Koot, J.D.</td>
<td>2013</td>
<td>Social media monitoring: Responsive governance in the shadow of surveillance?</td>
</tr>
<tr>
<td>grey</td>
<td>Innovative market solutions</td>
<td>Berger, J.M., Morgan, J.</td>
<td>2015</td>
<td>The ISIS Twitter Census</td>
</tr>
<tr>
<td>grey</td>
<td>DIY policing</td>
<td>Bervoets, E., Van, Ham, T.</td>
<td>2016</td>
<td>Samen signaleren: burgerparticipatie bij sociale veiligheid</td>
</tr>
<tr>
<td>academic</td>
<td>Other</td>
<td>Bleekam, D.</td>
<td>2010</td>
<td>Bikowra: The fight against criminal cyber networks.</td>
</tr>
<tr>
<td>grey</td>
<td>DIY policing</td>
<td>Bignon, Van den</td>
<td>2013</td>
<td>Social media in de opsporing Ben-veenken onderzoek naar de mogelijkheden van het betrekken van burgers bij de opsporing via sociale media in de korpse Gelderland/Zeeland</td>
</tr>
<tr>
<td>academic</td>
<td>Everyday Security</td>
<td>Brarland L.</td>
<td>2015</td>
<td>Top 10 U.S. Municipal Police Departments and Their Social Media Usage</td>
</tr>
<tr>
<td>grey</td>
<td>General</td>
<td>Braekel, van C.</td>
<td>2010</td>
<td>facebook-internet oppeen doen onbekend naar betachtschik die gebruik van internet bij opsporingsoondeheden door politie-gemeente Kennemerland</td>
</tr>
<tr>
<td>grey</td>
<td>Trolling</td>
<td>Brand, M.</td>
<td>2015</td>
<td>Cyberbullying in social networks: Phenomenology and police measures. [Cybermobbing in soziaal netwerken: Phenomenologie en politieke Maatregelen]</td>
</tr>
<tr>
<td>academic</td>
<td>Other</td>
<td>Breenam, T.</td>
<td>2013</td>
<td>Cybercrime: Re-thinking crime control strategies</td>
</tr>
<tr>
<td>grey</td>
<td>Everyday Security</td>
<td>Broekman, C.C.M.T. &amp; M. Menkhorst</td>
<td>2013</td>
<td>Burgermelding signalering - invoepsignalering met behulp van sociale media</td>
</tr>
<tr>
<td>academic</td>
<td>Social Media Investigation for Law Enforcement</td>
<td>Brown, J., K., Helenek</td>
<td>2013</td>
<td>Social Media Investigation for Law Enforcement</td>
</tr>
<tr>
<td>grey</td>
<td>General</td>
<td>Buruma, T.</td>
<td>2012</td>
<td>Walking the Social Media Beat - The Police and Law Enforcement Basic Guide to Twitter</td>
</tr>
<tr>
<td>academic</td>
<td>Everyday Security</td>
<td>Campego, M. &amp; Zavlink, A.</td>
<td>2013</td>
<td>Should cyberbullying be criminalized?</td>
</tr>
<tr>
<td>academic</td>
<td>Other</td>
<td>Chambers-Jones, C.</td>
<td>2013</td>
<td>Cybercrime economic and comonwealth laws.</td>
</tr>
<tr>
<td>academic</td>
<td>Other</td>
<td>Chang, L.</td>
<td>2013</td>
<td>Cybercrime in the greater china region: Regulatory responses and crime prevention across the taiwan strait.</td>
</tr>
<tr>
<td>academic</td>
<td>Other</td>
<td>Chang, Y. C.</td>
<td>2012</td>
<td>Combating cybercrime across the taiwan strait - Investigation and prosecution issues.</td>
</tr>
<tr>
<td>academic</td>
<td>Other</td>
<td>Chatravadi, M., Urai, A., Aagaraw, P., Satt, S., &amp; Mak, S.</td>
<td>2014</td>
<td>International cooperation in cyber space to combat cyber crime and terrorism.</td>
</tr>
<tr>
<td>academic</td>
<td>Hints and mass gatherings</td>
<td>Chauhan, A., Hughes, A.L.</td>
<td>2015</td>
<td>Facebook and twitter adoption by hurricane sandy</td>
</tr>
<tr>
<td>grey</td>
<td>The dark web</td>
<td>Chien, Hsinchun</td>
<td>2012</td>
<td>Dark Web - Exploiting and Data Mining the Dark Side of the Web</td>
</tr>
<tr>
<td>grey</td>
<td>Hints and mass gatherings</td>
<td>Cheong, M., Ray, S., Green, D.</td>
<td>2012</td>
<td>Interpreting the 2011 London Riots from Twitter Metadata</td>
</tr>
<tr>
<td>grey</td>
<td>The dark web</td>
<td>Cioceaghi, V., Balsuuzi, M., McArdle, R., &amp; Roter, M.</td>
<td>2015</td>
<td>Below the surface: exploring the deep web</td>
</tr>
</tbody>
</table>
MEDIE@SEC
The Emerging Role of New Social Media in Enhancing Public Security
Grant Agreement no 700281
The Emerging Role of New Social Media in Enhancing Public Security

MEDI@4SEC
Grant Agreement no 700281

92
Thematic Review of New Social Media in Enhancing Public Security

Grant Agreement no 700281


academic General Meier, A.J. & Topoleski, R. 2015 Social Media and the New Organization of Government Communications: An Empirical Analysis of Twitter Usage by the Dutch Police

grey General Meier, A.J.; G.O. Grimmethunjes; D. Ritters, M. T. Thomsen & P. Step 2012 Police & social media: Van hype naar onderbouwde keuzes

grey The dark web Michail Chatzifotis and Tobias Simon 2015 The IMPACT OF THE DARK WEB ON INTERNET GOVERNANCE AND CYBER SECURITY

academic Gift giving Mininovic, J., & McGovern, A. 2014 The death of jil mulheer: Crime and punishment on social media

grey General Ministry of Defence Police 2013 GUIDELINES ON THE SAFE USE OF THE INTERNET AND SOCIAL MEDIA BY MPD OFFICERS

academic Trolling Misheli, K., J. Freehoffer, D., Jones, L. M., & Wilke, J. 2015 Use of social networking sites in online sex crimes against minors: An examination of national incidence and means of utilization.

academic The dark web Monica J. Battail, Simon Lemm, and Matthew Allen 2013 Internet content regulation, public drug websites and the growth in hidden internet services

academic The dark web Monica J. Battail, Simon Lemm, and Matthew Allen 2013 Internet content regulation, public drug websites and the growth in hidden internet services

academic Everyday security Morssell, C., & Décary-Hits, D. 2013 Crime facilitation purposes of social networking sites: A review and analysis of the "cyberbanking" phenomenon

grey General Murphy, J.P., Polischuk, A. 2013 Social media evidence in government investigations and criminal proceedings: a frontier of new legal issues


grey General Nederhoed, N. 2012 Wijzigen 2.0 Een onderzoek naar de invloed van sociale media op de dagelijkse werkzaamheden van de wijzigant

grey General Neven, A. 2013 Burgemeesterast in 140 tekens. Een onderzoek naar het Tweetgebruik van de burgemeesters in Nederland.

grey General New South Wales Police Force 2013 Official Use of Social Media Policy

grey The dark web Nicola Christin 2012 Traveling the silk road: a measurement analysis of a large anonymous online marketplace

grey The dark web Nicola Adami, J.P. Barak 2013 Criminalisevan de verkoop van illegale dieren

academic Trolling SLOB, W. 2016 Trolling: The ugly face of the Social Networks

grey Everyday Security Not specified 2014 La Policía Nacional e las Redes Sociales: Un nuevo servicio de atención al ciudadano

grey General Not specified 2015 The police on Twitter: image management, community building, and implications for policing in Canada

grey Everyday Security Oetelina's; J.J. Koops, B.J. 2011 Nulwetlen en opvoeden in een internetstomme

academic Trolling Olasy, M. K. 2012 Have no fear (of "spying inference upon inference"): How UNITED STATES V. COMSTOCK can save the matthee shepard and james byrd, jr. hate crimes prevention act.

grey The dark web OM NL 2014 Verantwoording aanpak peinganiseerders criminaaliteit 2014

academic Other Omand, D. 2015 The dark net: Policing the Internet's underworld.

academic Everyday security Omand, D.; Bahrkoltz, J. & Miller, C. 2012 Introducing social media intelligence (SOCIAM)


academic DIY policing Omana, D. 2012 Challenging the social media space: Community policing in a twitter converged baraza

grey General Omana, D. & Counts, S. 2015 Social Enablers of Policing. The power of social media on dermamoon outcome


academic Rorts and mass gatherings Palfy, D.U., Leonard P., Cahl H., Makelth, J. & Crosby S., Brunton D. W. 2016 Police took my home I dedicate my life to his revenge - Twitter tensions between gang-involved youth and police in Chicago

academic Everyday security Pedersen, S.; Brunsttil, S.; Smith, R. & Grimnes, A. 2014 The impact of the escalation of blogs within the UK blogosphere

grey DIY policing Pentemann, P. 2012 Bredemansiaan in de opsporing: privacyinhoud van rel? Onderzoek naar de grenzen van het gebruik van bestelmaterial in de opsporing via de social media


grey General Pijpers, Z.P. 2013 De kracht van online opsporing. Een onderzoek naar het gebruik van Twitter binnen de opsporing

grey General Police Executive Research Forum, Police and Community Relations Commission 2011 Social Media and Tactical Considerations for Law Enforcement

grey Rorts and mass gatherings Postmes, T.; Bezuow, M. van 2013 Stamps & sociale onrust in Nederland?


academic Rorts and mass gatherings Proctor R.; Crump J.; Karstedt S., Voss A., Cantliph M. 2013 Reading the riots: what were the police doing on Twitter?

academic Rorts and mass gatherings Proctor R.; Vds. F. & Voss, A. 2013 Reading the riots on Twitter: methodological Innovation for the analysis of big data

grey Rorts and mass gatherings Queensland Police Service 2011 Disaster Management and Social Media - a case study, 2011

grey Everyday Security Raad van der. L. 2015 Twitterropolis

academic The dark web Ranier Böhm, Nicolas Chrsin, Benjamin Edelman, and Tyler Moore 2015 Bitcom: Economics, technology, and governance

grey General Rand 2015 Respect and Legitimacy—A Two-Way Street. Strengthening Trust Between Police and the Public in an Era of Increasing Transparency

academic Innovative market solutions Rasim, M. & Jahnian, A. 2013 A new algorithm to estimate the similarity between the intentions of the cyber crimes for network forensics.

academic The dark web Reiato, Orelting, and Hunter 2015 Innovations in International Cooperation to Counter Cybercrime

academic Trolling Reytas, B. W. 2010 A situational crime prevention approach to cyberstalking victimization: Preventive tactics for internet users and online place managers.

academic The dark web Rezza Kæsli 2015 The Silk Road, Bitcoins and the Global Prohibition Regime on the International Trade in Illicit Drugs: Can this Storm Be Weathered?

grey Rorts and mass gatherings Rezak, Kæsli 2015 The Silk Road, Bitcoins and the Global Prohibition Regime on the International Trade in Illicit Drugs: Can this Storm Be Weathered?

grey Rorts and mass gatherings Rianne Decker, Godfried Engbersen 2012 How social media transform migrant networks and facilitate migration

grey General Rianne Decker, Godfried Engbersen 2012 A situational crime prevention approach to cyberstalking victimization: Preventive tactics for internet users and online place managers.

grey Trolling Ridder, c. de 2012 Pesten in een cyberwereld. Een onderzoek naar de vraag waarom kinderen cyberprestat


The Emerging Role of New Social Media in Enhancing Public Security

Grant Agreement no 700281

 solutions


grey Everyday Security Rottenburgh, Robert Schulte 2013 Online handhaving in de basissettings

grey Everyday security Ruddell, R. Jones N. 2013 Social media and policing: Matching the message to the audience


academic The dark web Sarah Meiklejohn, Marjorie Pomarole, Grant Orange, Geoff My Voeller, and Stephen Savage 2016 A fistful of Bitcens: characterizing payments among men with no names.

academic The dark web Sarah Meiklejohn, Marjorie Pomarole, Grant Orange, Geoff My Voeller, and Stephen Savage 2016 A fistful of bitcens: characterizing payments among men with no names.


academic The dark web Sarah Meiklejohn, Marjorie Pomarole, Grant Orange, Geoff My Voeller, and Stephen Savage 2016 A fistful of bitcens: characterizing payments among men with no names.


academic Roots and mass gatherings Schneider, C.J. 2014 Police image work in an era of social media: You’ll see and the 2017 montebello summit protest

grey General Schreuder, D.C. 2014 policing and social media: social control in the age of new media

grey City picking Schalkwijk, T., van der Knick, J., Koster, J. 2014 Tussel hulp en tyfus: de invloed van opsommering en gerucht in openbare ruimte

grey General Schuurs, Fogg, T. 2012 Police and Social Media: Written Evidence to the Independent Police Commission


academic Everyday Security Siersema, D.G., Sherman, R.A. 2015 Situations in 140 characters assessing real world situations on twitter

grey General Seep, P., Kool, D. de 2013 Himeende burgeren en politie. De betekenis van GSM-risico's van burger voor de uitvoering van politieacties en de reputatie van de politie

grey General Siersema, D.G. 2013 lie, damn lies, and viral content

academic Other Sindh, K. Kombade, K., Gadge, R., & Measham, B. B. 2014 Forensic investigation processes for cyber crime and cyber space.

grey General Snel, G., Tops, P. 2011 Ein weerd te wenen: sociale media en de politie, een eerste verkenning

grey City picking Serrbrot, F. 2013 Burgersparticipatie bij opsommering en geruchten: politie inzetten en de mening van burgers

grey General Serrbrot, F. 2012 Het gebruik van sociale media in de opsommeringtaktiek

academic Trilling Sorel, Tom 2015 Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous

academic City picking Marbit, R., Muzny, G. Palen, L. 2014 Learning from the Crowd: Collaborative Filtering Techniques for Identifying On-The-Ground Twitter Trends during Mass Disruptions

academic City picking Stabrook, K., Jim Maddock, Mark, Brand, Peo Achtenman and Robert M. Mason 2014 Rumours, False Flags, and Digital Villagers: Mass Information on Twitter after the 2013 Boston Marathon Bombing

academic Innovation market solutions Stephens, P. 2012 An evaluation of linux cybercrime forensics courses for european law enforcement.

academic General Stewart Benham and Keith Edmonson 2014 Sub Saharan African Terorst Groups: use of the Internet

academic Other Sthilwasser, L. 2014 Should virtual cybercrime be regulated by means of criminal law? A philosophical, legal-economic, criminological and constitutional dimension.

grey General Suy, K. en P. Daleman 2010 Burgerlijk en anders vormen van burgerparticipatie in de veiligheid

grey General Sweerby-Nurje, J. 2015 Social Media under investigation

grey Everyday Security Taal, W. 2015 Maatschappelijk Politiebestuur

academic Other Telck, J. 2010 Policing social networking sites and online grooming

academic Roots and mass gatherings Temminkova, I., Varga, A., Bykle, D. 2014 Building a Crisis Management Temp Source for Social Media: The Case of Floods and Protests gatherings

academic Everyday security Yewellerr, D. 2012 Cyberbullying homeland security: The texas virtual buettenpolity and participatory citizenship.

academic General Thureau, M. & A. Maoer 2012 Social Media: War can en must de Politie eren? - Voor vor kwartiermeesters

academic General The Police Foundation 2014# SM @OOV? Visie op sociale media in openbare orde en veiligheid

grey The dark web The Means to Justify the End: Combating Cyber Harassment in Social Media'.

academic The dark web The Briefing. Police use of social media

academic The dark web The Briefing - Sociale Media: Wat kan en moet de Politie ermee?

academic Innovation market solutions Theodson, R., Kruiger, R., & Eft, T. 2016 Can twitter save lives? A broad-scale study on visual social media analytics for public safety.

grey Trilling Thomas Hudon 2014 Social media, trolling and the law: a 9 point guide

academic Everyday Security Tobler, J. 2013 Scales Medien – Must Get the Police (no authors)

grey The dark web Tim Stevens 2010 REGULATING THE DARK WEB

academic General Tsy, K. 2012 Capt Watr: Spectators, Social Media and Police Reform

grey Trilling Yavuz, E. 2010 Following you home from school a critical review and synthesis of research on cyberbullying

grey The dark web YORK authors 2016 Inception

academic Innovation market solutions York, P. 2016 Comparatieve Review of Social Media Analysis Tools for Preparedness

academic City picking Trottier, D. 2012 Policing Social Media

academic City picking Trottier, D. 2012 Cybercrime and power users: Police and user led investigations on social media

academic Everyday security Trottier, D. 2015 Open source intelligence, social media and law enforcement: Visions, constraints and critiques

academic Roots and mass gatherings Trottier, D. & Fuchs, C. 2014 Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the age of Facebook, Twitter and Youtube

grey General Unknown 2012 use of internet for lenterit purposes

grey General Unknown 2014 Veldje Politieke Taak websiteover social media

Other Upton, P., Schrum, D.J., & Butler, D.A. 2013 Internet boring: New trends in social media and gang violence

grey Other Uvis, Dgov 2015 the President's task force on 21st Century Policing

academic General Ustlin, Politi, R., & Graber, P. 2015 Police message diffusion on Twitter: Analysing the reach of social media communications

grey General Stopera, D. 2015 How to Means to Justify the End: Combating Cyber Harassment in Social Media

grand City picking Vasos Lub 2016 Die burger op wacht

academic Roots and mass gatherings Vasterman, Peter; Vlifes, Hub 2015 Project X Harer research revisited. A critical analysis of the research project about the role of the media in the Facebook riots in September 2012

grey The dark web Verhuy, Y. 2016 Weet wat je tweet. Onderzoek naar het gebruik van Twitter door wijkagenten en welke bijdrage dit kan leveren aan het verwezenlijken van de burger.

grey The dark web Verhuy, Y. 2016 Profiles of cryptomatemarket arrestees: an exploratory study

grey General Wies, A. & Smidt, P. 2014 Social media: the new dna

grey General Wies, A. de e.a. 2011 RSM ©DO! Visie op sociale media in openbare orde en veiligheid

grey General Wies, A. de; Koch, K. 2012 opposing 2.0 Met massa meer massa. Een whitewrap over crowd sourcing in opposing


grey General Wall, D. S. 2014 Copyright trolling and the policing of intellectual property in the shadow of law

94
| academic | Other | Wilt, D.S. et al. | 2013 | Policing cybercrime: networked and social media technologies and the challenges for policing |
| academic | Everyday Security | Warwick AirForce | 2013 | Social media: A security challenge and opportunity |
| academic | Webbo, C., & Yi, M. | 2013 | Gaming on and off-line: Humanizing the cyber criminal |
| academic | The web dark | Weikung Li | 2015 | Identifying top sellers in underground economy using deep learning-based sentiment analysis |
| academic | The web dark | Weikung Li | 2015 | Identifying top sellers in underground economy using deep learning-based sentiment analysis |
| academic | Other | Weizmann, U. | 2010 | Terror on Facebook, Twitter and YouTube |
| grey | Everyday Security | Wendy Fink | 2014 | Can Twitter Be Used to Predict Crime? |
| academic | Trail | Wijayaratne, A.W., & Tawstr. | 2014 | Fighting cyber crime in email spamming: An evaluation of fuzzy clustering approach to classify spam messages |
| grey | General | Wipf, J. | 2015 | Analyse twitterverkennings UTwente rond het NOS incident |
| academic | Rats and mass gatherings | Xilija, K. | 2018 | Police lijdenswaarden: communicatie op Twitter. Een beschrijvend onderzoek naar de communicatieve rol van de politie op Twitter tijdens de rellen in Haren |
| academic | Other | Wile, M. & Novickij, J. | 2016 | The use of specialised cybercrime policing units: An organisational analysis |
| academic | Everyday security | Xiong, J. & Zhou, Y. | 2015 | Suggestions for public privacy protection in policing based on big data |
| grey | Other | Yar, M. | 2012 | E-crim e 2.0: The criminological landscape of new social media |
| academic | General security | Yarby, B., & Wilson, G. | 2014 | Making Sense of Facebook Market? Social Networking Sites and Contemporary Homocide |
| academic | Everyday Security | Yavuz, N., & Welch, E. W. | 2014 | Factors affecting openness of local government websites: Examining the differences across planning, finance and police departments |
| academic | Other | Yu, S. | 2014 | Fear of cyber crime among college students in the united states, An exploratory study |
| academic | The dark web | Yume Zhang, et al. | 2010 | Developing a Dark Web Collection and Infrastructure for Computational and Social Sciences |
| grey | Other | Zebel, S., Wijaya, P. de, Giebels, E., Kuttschreuter, M. & Spil, W. | 2014 | Jeugdlider van cybercrime: Nationale, Een ethische verkenning |
| academic | Other | Zhang, Y., Xiao, X., Ghafoor, K., Zhang, D., & Deng, H. | 2012 | A survey of cyber crimes |
| academic | Innovative market solutions | Zhao, S., & Huang, K. | 2013 | Context modeling for developing a database system of authentic case in training cyber police |
| academic | General | Zigang, Y. | 2011 | Cyber variants of traditional crimes and criminal law responses |
| academic | Rats and mass gatherings | Lohag, A., Lukata, M., Procter, N., Bontcheva, K., & Tomsic, P. | 2015 | Towards detecting rumors in social media |
| grey | General | Zılmali, W. | 2015 | Burgemeester in cyberspace |
| grey | Other | Zulkifli | 2014 | Critical infrastructure protection: More comprehensive planning would enhance the cybersecurity of public safety entities’ emerging technology |
| european | DIY policing | BRIDGE | 2014 | D4.1: BRIDGE Summary of Technologies and Standards of Existing Emergency and Crisis Management Systems |
| european | DIY policing | BRIDGE | 2014 | D4.2: Functional View on the BRIDGE Architecture |
| european | DIY policing | BRIDGE | 2014 | D6.3: Information and Infrastructure View on BRIDGE Network Architecture |
| european | DIY policing | BRIDGE | 2014 | D6.4: Demonstration of Collaboration Technologies (BRIDGE; Demonstration II) |
| european | DIY policing | BRIDGE | 2015 | D15.4: Integrated Demonstration in Real-Scale Networks under Crisis Conditions (BRIDGE Demonstration III; Final Demonstration Scenario) |
| european | DIY policing | BRIDGE | 2015 | D13.2: BRIDGE 21st Century Social, Legal and Ethical Emergency Collaboration |
| european | DIY policing | BRIDGE | 2014 | D14: BRIDGE Awareness of Wider Sectoral Implications |
| european | DIY policing | BRIDGE | 2015 | D14: BRIDGE Awareness of Wider Sectoral Implications |
| european | DIY policing | COMPOSITE | 2011 | D4.1 - K2T Trends in European Policing |
| european | Everyday security | COMPOSITE | 2012 | D4.2 - Best Practice in Social Media Adaptation |
| european | Everyday security | COSARC | 2013 | Deliverable D8.1 & D8.2: Guidelines for the use of new media in crisis situations |
| european | Everyday security | COSARC | 2013 | Deliverable D2.3: Report on the adverse use and reliability of new media |
| european | Everyday security | COSARC | 2013 | Emerging technologies in crisis situations |
| european | Everyday security | Emergent | 2014 | Usage Patterns of Social Media in Emergencies |
| european | Everyday security | Soteria | 2014 | D4.1 Theoretical and expert-driven classification of emergencies on the impact of social media |
| european | Innovative market solutions | CityRisks | 2016 | Deliverable D2.2: Analysing factors influencing the fear of crime from the citizens’ perspective |
| european | Innovative market solutions | CityRisks | 2015 | Deliverable D2.2: Analyzing participants influencing the fear of crime from the citizens’ perspective |
| european | Innovative market solutions | CityRisks | 2016 | Deliverable D2.2: Analyzing factors influencing the fear of crime from the citizens’ perspective |
| european | Innovative market solutions | CityRisks | 2015 | Deliverable D2.2: Analyzing factors influencing the fear of crime from the citizens’ perspective |
| european | Innovative market solutions | SUPER | 2016 | D8.1 - Best practices and policy development guidelines |
| european | Innovative market solutions | CAPITAL | 2015 | D3.3 Cyber security market analysis D4.4 Cyber Security and Privacy Agenda |
| european | Innovative market solutions | CAPITAL | 2015 | D2.3.3 List of current and future cyber security threats |
| european | Rats and mass gatherings | DRIVER | 2014 | D4.21 - Vision on Response 2025 Keywords |
| european | Rats and mass gatherings | ATHENA | 2014 | D3.3 – A REVIEW OF BEST PRACTICES FOR SOCIAL MEDIA IN CRISIS COMMUNICATION |
| european | Rats and mass gatherings | MOSAIC | 2014 | D2.2 Ethical Framework |
| european | The dark web | COURAGE | 2016 | A Theoretical Categorization and Sub-Division of Cyber Crime & Cyber Terrorism |
| european | The dark web | COURAGE | 2015 | D5.6 - Final Research Agenda, including the roadmap of recommendations for a system of horizon scanning of new CC/CT threats |
| european | The dark web | COURAGE | 2015 | D5.6 - Final Research Agenda, including the roadmap of recommendations for a system of horizon scanning of new CC/CT threats |
| european | The dark web | COURAGE | 2015 | D5.6 - Final Research Agenda, including the roadmap of recommendations for a system of horizon scanning of new CC/CT threats |