Workshop 4 Report:
Everyday Security
Deliverable 2.6

European Forum for Urban Security (EFUS)

Co-funded by the Horizon 2020 Framework Programme of the
European Union
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

Executive Summary .................................................................................................................. i

1. Introduction ......................................................................................................................... 1

1.1 MEDI@4SEC .................................................................................................................... 1

1.2 Work Package 2: Implementation: Improved Dialogue, Collaboration and Practices ................................................................. 1

1.3 Deliverable #.# .................................................................................................................. 2

2. Workshop Objectives, Setup and Method ........................................................................... 3

2.1 Everyday Security Workshop ............................................................................................ 3

2.2 Workshop themes .............................................................................................................. 5

2.3 Method ............................................................................................................................. 6

2.4 Side events ....................................................................................................................... 9

3. Everyday Security ............................................................................................................... 11

3.1 Definition ......................................................................................................................... 11

3.2 The use of social media in Everyday Security – Defining some common activities 11

3.3 Opportunities, challenges, legal and ethical considerations ........................................... 12

4. Stakeholder analysis from the workshop ......................................................................... 14

4.1 Identifying Stakeholders in Everyday security ................................................................. 14

5. SWOT Analysis ................................................................................................................. 20

5.1 Theme: Communication & Engagement Activities ....................................................... 20

5.2 Theme: Monitoring Activities ....................................................................................... 24

5.3 Theme: Enforcement Activities ..................................................................................... 28

6. Relevant Methods, Procedures, practices, and Recommendations ................................... 33

7. Practices analysis .............................................................................................................. 35

8. Conclusions ...................................................................................................................... 37

References ............................................................................................................................ 39

Appendix 1 Workshop Agenda .............................................................................................. 40

Appendix 2 Participant List .................................................................................................. 42

Appendix 3 Workshop Evaluation ......................................................................................... 44
Executive Summary

This document provides results from the workshop on Everyday Security: social media uses to enhance public security, held on November 14, 2017 in Barcelona, Spain as a part of the European research project MEDI@4SEC. The workshop brought together 62 people from 15 countries across various sectors including local authorities’ representatives, academic research, industry, social media business and other authorities, as well as law enforcement agencies, to discuss the uses of social media as a tool or information resource during the daily activities of all security providers.

Although the field of work is fairly widespread when talking about Everyday Security, the workshop focused on 3 main topics, specifically:

Communication & Engagement: social media use to increase engagement, reputation, transparency and legitimacy and to communicate and interact directly with citizens.

Monitoring: social media use in preventing unrest and flagging suspicious situations (intelligence) and as a tool to analyse a large number of open data to improve crime prediction and prevention.

Enforcement: Social media information used by the police to track down criminal offenders. Social Media as a potentially large source of information for LEAs.

Based on 16 discussion groups, the authors have derived a SWOT analysis, description of stakeholders and their potential roles in public security, as well as a list of recommendations to improve the use of social media in the daily activities of security actors.

More specifically, this document comprises a detailed description of the workshop and its methodology (Section 2), an introduction to the topic of Everyday Security (Section 3), and the following analyses:

i. SWOT analysis for using social media before, on everyday security activities, for each theme (Section 4);

ii. Analysis of the stakeholders involved in each theme with their roles and responsibilities (Section 5);

iii. Analysis of relevant methods, procedures, practices, and recommendations that can help set out a roadmap to improve the use of social media in everyday security (Section 5).

The document ends by presenting the main conclusions taken from analysis of the discussions held during the workshop on the three themes discussed (Communication-Engagement, Monitoring and Enforcement). Some important transversal topics, stakes and needs were uncovered. The need for common knowledge and shared guidelines at the European level; training for all actors; cooperation and coproduction were highlighted. The recognition of social media companies’ vital role was also a fruitful area for discussion. Finally, ethics and legal issues were also a topic of concern in order to improve the existing framework.
1. Introduction

1.1 MEDI@4SEC

MEDI@4SEC focuses upon enhancing understanding of the opportunities, challenges and ethical consideration of 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.


Following the results of the first work package, which focused on providing a state-of-the-art overview and identifying best practices, the second work package in the MEDI@4SEC project aims to identify opportunities and challenges in social media use, analyse available technologies and the need for standards, distributing the above findings and engaging in discussion with the wider public security community.

The core component of work package 2 is a series of policy and practice dialogue workshops, one on each of the themes, in order to address key issues related to social media use for security purposes.

The workshop on Everyday Security with the use of social media that we report on in this document is the fourth in the series, marking yet another important milestone for the growth of the community created by MEDI@4SEC in the social media field. Interested parties can follow the project’s activities and register for upcoming workshops on the
project's website at www.media4sec.eu, as well as in our LinkedIn group (https://www.linkedin.com/groups/12000103)

1.3 Deliverable 2.6

This document provides results from the workshop on Everyday Security: social media uses to enhance public security, held on November 14, 2017 in Barcelona, Spain as a part of the European research project MEDI@4SEC. The workshop brought together 62 people from 15 countries across various sectors including local authorities' representatives, academic research, industry, social media business and other authorities, as well as law enforcement agencies, to discuss the uses of social media as a tool or information resource during the daily activities of all security providers.
2. Workshop Objectives, Setup and Method

2.1 Everyday Security Workshop

The workshop took place on November 14, 2017 in Barcelona, Spain. The project was organized by MEDI@4SEC’s partner, the European Forum for Urban Security (Efus), with the collaboration of the project consortium.

Participation was limited and interested parties had to apply to the workshop by filling in and submitting an online application form on the MEDI@4SEC webpage. After the submission deadline, applicants were selected based on their relevance to the topic and their background. In addition, gender and country coverage were also factored into the selection process.

In total, 62 people participated in the workshop, of which 38 were external (not part of the MEDI@4SEC project consortium). Participants came from 16 countries (Austria, Belgium, Denmark, France, Finland, Germany, Greece, Italy, Ireland, the Netherlands, Poland, Portugal, Slovenia, Switzerland, United Kingdom and the United States of America) from backgrounds such as local and national police, social media business and industry, researchers, civil servants and consultants from both the private and the public sector, please see Appendix 2 for more details.

<table>
<thead>
<tr>
<th>COUNTRIES</th>
<th>Participants</th>
<th>COUNTRIES</th>
<th>Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>1</td>
<td>Italy</td>
<td>4</td>
</tr>
<tr>
<td>Belgium</td>
<td>5</td>
<td>Netherlands</td>
<td>8</td>
</tr>
<tr>
<td>Denmark</td>
<td>1</td>
<td>Portugal</td>
<td>1</td>
</tr>
<tr>
<td>Finland</td>
<td>1</td>
<td>Slovenia</td>
<td>3</td>
</tr>
<tr>
<td>France</td>
<td>5</td>
<td>Spain</td>
<td>13</td>
</tr>
<tr>
<td>Germany</td>
<td>3</td>
<td>Switzerland</td>
<td>1</td>
</tr>
<tr>
<td>Greece</td>
<td>4</td>
<td>UK</td>
<td>8</td>
</tr>
<tr>
<td>Ireland</td>
<td>3</td>
<td>USA</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>62</td>
<td></td>
</tr>
</tbody>
</table>

*Table 2.1 Participants per country*


2.2 Workshop themes

The workshop examined the uses of social media in everyday security activities. Although the field of work is fairly widespread when talking about Everyday Security \(^1\), the workshop focused on 3 main topics, specifically:

2.2.1 Communication & Engagement:

As mentioned in the Report on the Current State of the Project (MEDI@4SEC, 2016), social media is mostly used in order to increase engagement, reputation, transparency and legitimacy and to communicate and interact directly with citizens. It also allows trust and confidence of citizens in the police to improve, albeit to a more limited extent. Some other purposes that social media are used for include increasing effectiveness and legitimacy, enhancing transparency (Global Advisory Committee, 2013) collaboration and community participation (Meijer & Thaens, 2013).

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), 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. Thanks to social media. Better communication could also mean 'active citizenship', which enhances effective community policing. In this situation, citizens can better assist with reducing crime and general disorder by providing information, and improve security strategies by sharing their ideas to solve community problems (Lieberman et al., 2013).

Described in the in the Report on the Current State of the Project (MEDI@4SEC, 2016), social media has served to increase accessibility of policing services for community members. Two-way engagement with the public is a tangible benefit of social media, although this is not always implemented yet. By stimulating engagement between police and the community, social media adds legitimacy to many police tasks. Social media offers a great opportunity to reach target groups who are traditionally hard to reach, e.g. youngsters and minorities (Meijer et al, 2013) who feel more comfortable using social media, or vulnerable groups who prefer anonymity in their interactions with authorities.

2.2.2 Monitoring:

Monitoring entails social media uses in preventing unrest and signalling suspicious situations (intelligence), and as a tool to collect and analyse a large quantity of open data to improve crime prediction and prevention (MEDIA4SEC, 2016).

LEAs are using social media analysis in an effort to stop crime before it starts. Predictive policing is a part of intelligence that is focused on what is likely to occur. By using this tactic, police can identify a suspect’s social network and map how information flows between various people. Police can use data from a wide variety of social media to try to

---

\(^1\) As it was shown in the Report on the Current State of the Project (MEDI@4SEC, 2016). In which all the activities identified during the research on the use of social media and everyday security were examined in detail. For a more in-depth look at the content please visit http://media4sec.eu/downloads/d1-1.pdf. For this report, a summarised version of the three themes selected for the workshop is mentioned
predict phenomena, such as where gun violence is likely to occur, where a serial burglar is likely to commit his next crime, and which individuals a suspect is likely to contact for help.

This analysis can be also used for other security actors rather than police forces. For example, local authorities can use social media information to better understand criminal phenomena, crime perception and develop strategies. Social media and apps provide new tools to collect a tremendous amount of data, which can include the collection of relevant data on security and perceived security. Smartphone apps are particularly interesting tools because they can usually attach geo-data to reports of incidents or to map perceptions.

Indeed, even if predictive policing is great news for the future of security and freedom, it also creates threats to individual freedom. One can imagine that data collected for security purposes could also become a tool for undemocratic or unauthorised surveillance of citizens.

### 2.2.3 Enforcement:

This theme focuses also on the potential uses of social media in solving crimes and tracking down criminal offenders, as well as what the implications are in terms of professional cultures and practices and the ethical and legal impacts.

Social media information is used by the police to track down offenders. Social media is a potential source of information for police when criminals leave traces while using it. There are plenty of examples where social media has proved to be helpful in solving crimes, and many police departments use them for investigations. Police frequently visit websites such as those on the dark web, sites that allow or promote hate propaganda, or forums that allow anti-social behaviour in order to gather information and evidence.

### 2.3 Method

With the aim of thinking beyond the current situation and to plan for the future of policing, the workshop's design was based on the 5-D method\(^2\) (Define, Discover, Dream, Design and Develop) on the topic of Everyday Security, allowing for an interactive exchange to build a sense of community. In this way, participants in eight groups of seven were able to discuss the various issues around Everyday Security (three themes were selected: 2 groups on Communication & engagement, 3 groups on monitoring and 3 groups on enforcement). Overall, the workshop programme included:

1. Introduction to the workshop.
2. Introduction to the MEDI@4SEC Project
3. Introduction of the topic: Everyday security
4. Presentations related to various real case studies on three themes from key note speakers and different stakeholders' perspectives
5. Focus Group discussion sessions on the three themes

6. Discussion including participants' testimonials
7. Conclusions and presentations of thematic summary results

Initially, to set the tone and introduce the project and the workshop itself to the participants, a plenary session was designed. Efus’ Executive Director presented the role of Efus within the project, and highlighted its role as an organization composed of local authorities in Europe, and why in-depth knowledge on the use of social media as a tool or resource in daily activities to preserve security is also important at the local or municipal level. Professor Jon Coaffee from University of Warwick then introduced the MEDI@4SEC project including its aims, ongoing activities and upcoming events.

Later, in order to provide participants with a comprehensive overview of the workshop's main topics, a presentation on the uses of social media for security purposes was made by a consortium. representative.

Following that presentation, in order to provide participants with thinking material on the range of the topics at hand, keynote speakers from various standpoints and backgrounds gave presentations on a number of relevant topics. In total, 9 presentations were given:

1. Mossos d’Esquadra (regional police in Catalonia, Spain) presented their experience of social media communication and analysis during the terrorist attacks in Catalonia, with particular focus on the large quantity of fake news.
2. The M7 Citizen Security group presented an app designed to involve municipalities, the police, the local private sector and citizens in local responses carried out to maintain security.

3. The Soteria project consortium presented their FP7 research project, whose main objective is to develop software solutions to improve the situational awareness of LEAs, by using techniques applied to social media for locating and communicating with citizens.

4. The IDIAP research institute from Switzerland showed how analysis of social media can be applied to urban security specifically by improving the policing of night life.

5. The Hague police presented a real-time connection platform called BART, through which citizens are encouraged to support police to maintain safety and security within their neighbourhood.

6. Facebook presented its experience supporting law enforcement agencies in cases of harassment of women, pedo-pornography, missing children and terrorism.

7. A Professor from the University of Paris-Est Marne la Vallée gave a presentation on social media data and predictive policing ("The case of predpol") with a sociological approach.

8. London’s Metropolitan Police gave a presentation on how to create open source intelligence and investigation capability through social media.

9. KIVU, an Austrian tech company, presented its analytical software to tackle terrorist propaganda & recruitment on social media, based on a network approach and targeted analysis, a more effective way to collect social media intelligence.

The afternoon program was an open, interactive exchange of ideas concerning the question “How could LEAs and other security actors use social media to maintain everyday security?”. The discussion was focused around the three themes selected to be developed during the workshop (1) Communication & Engagement, (2) Monitoring and (3) Enforcement. The workshop sessions were organized as follows:

- Two sessions of 50 minutes were held on 8 different tables (2 tables for communication & engagement, 3 tables for Monitoring and 3 tables for Enforcement).
- Each table hosted 5 participants and 2 hosts/moderators from the project consortium.
Each participant was assigned to one theme/table per session based on their areas of interest declared on the initial application.

Each table/theme went through the Dream, Design and Develop steps of the 5-D method through a set of questions first regarding the current roles of all actors involved, the methods, procedures, practices, regulations and social media tools used today. Subsequently, participants were asked to ‘dream’ what the ideal future would look like, taking into consideration the current situation and existing restrictions as well as the strengths, weaknesses, opportunities and threats of social media’s characteristics and its use for each theme.

Based on 16 discussion groups, a SWOT analysis, description of stakeholders and their potential roles in public security were derived, as well as a list of recommendations.

After the focus group discussions, the session that followed was dedicated to Q&A and allowed all the participants to gather and share their ideas and insights. A key point raised by the participants was the necessity to frequently meet and exchange ideas between professionals from different sectors. Also, the idea of the creation of a common culture could only exist through that kind of event. Eventually, a participant noted that non-social media-friendly professionals and more high-level representatives should participate in such events.

The workshop’s last session included three presentations of the most important points from the focus group discussions on each theme. The tables discussed each topic among themselves, selected the most important point arising from the discussion, then one of them presented to the participants. The workshop’s conclusion included a social event where participants had the opportunity to mix and increase the chances of networking among Community members.

2.4 Side events

Furthermore, the workshop was followed by the Efus international conference. The MEDI@4SEC project was represented during this event through an open workshop on the use of technologies for prevention. The three-hour workshop was divided into two sessions. The first session focused on the use of new technologies to improve efficiency in urban management and foster safer cities, and the second one on the vulnerabilities and risks of these new technologies for end users and city security providers. The main concerns resulting from the exchange between the panellists and the public were, looking at the most important points: what opportunities are offered by new technologies in terms of urban security and crime prevention? How do open data and social media reshape prevention policies? Is there a need to guarantee ethical use while ensuring the security of virtual spaces?

More than 10 speakers from the Netherlands, UK, Spain, France, Germany and Italy representing local authorities, as well as law enforcement agencies, private sector and research participated in this workshop. Around 140 participants attended. The workshop was co-led by MEDI@4SEC and members of the consortium were involved in these sessions as helpers or speakers. The exchanges between speakers during these two
sessions, as well as insights from the consortium, contributed to the new Efus manifesto³, which has a section dedicated to technology.

In order to widely disseminate the project, a stand for the project was installed during the three-day conference to take advantage of the significant number of people who participated. Efus and members of the consortium were at the stand to present the project, offer insight on the project, publications, and answer questions and concerns.

³ Efus Manifesto political document on urban security which brings together all the values and principles that form the foundations of Efus’ and its members’ actions. It constitutes a continuation of the principles and recommendations of the Naples Manifesto (2000) and the Saragossa Manifesto (2006), Aubervilliers and Saint-Denis (2012), yet it also forms a future action plan for local authorities that can be followed during the years to come. The last version was presented on 17 November 2017 during the closing session of the international conference “Security, Democracy and Cities: coproducing urban security policies”, organised by Efus
3. Everyday Security

The concept of Everyday Security has been described and challenged in previous MEDI@4SEC publications.\(^4\) In this part, we present evidence collected from the first stage of the project based on the best practices and current state of the project as an introduction to the topic of everyday security.

3.1 Definition

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 sources for intelligence, investigations, crime prediction and prevention and with new platforms to communicate and interact with citizens.

3.2 The use of social media in Everyday Security – Defining some common activities

The following patterns, identified during the first stage of the project\(^5\), describe the use of social media for Everyday security activities:

**Analysing social media:** Social media can help solve crimes. Therefore, LEAs monitor and analyse data on social media that is relevant for criminal cases. This practice is similar to social media monitoring and analytics, but in this case is specific to one criminal investigation.

**Answering Citizens:** Citizens have questions for law enforcement agencies but typically do not ask, because it is complicated to do so. Therefore, LEAs answer citizens’ questions in special (mostly chat) sessions and provide answers to frequently asked questions online or through an app.

**Crime Prevention:** Therefore, LEAs use social media to share information to explain to citizens how they can improve their own safety.

**Educating Citizens:** People don’t know the risks of social media to their safety. Therefore, LEAs offer teaching, particularly to children and parents on how to use the internet in a responsible way.

**Informing Citizens:** Many police forces provide regular information to the public through their local and corporate social media channels about crime, policing successes, daily policing experiences, human experiences and local events.

---

\(^4\) For a more in-depth description please consult MEDI@4SEC D1.1 ‘Report on State of the Art Review’

**Intake:** People are used to using social media to communicate with each other and to contact and interact with organizations. Also, for reporting crime, crime tips or other relevant information.

Therefore, LEAs use social media channels such as apps or Twitter (DM’s) to have people submit information about incidents or crimes.

**Intelligence:** Social media contains a large amount of data that might be relevant to public security. Therefore, LEAs use social media to gather intelligence.

High volumes of unstructured data and traffic are generated from various social media sites before, during and after an event or an emergency incident period.

Therefore, LEAs use software tools for data analysis of unstructured data with machine learning that lets you search and analyse text, image, audio, and video from virtually any source uncovering trends, patterns and relationships.

**Monitoring:** Social media provides a sense of what is going on for public security planners (before, during or after incidents for example). Therefore, LEAs monitor social media on various security topics.

**Refuting Rumours:** On social media, especially during crises, rumours spread easily.

Therefore, LEAs use social media to refute rumours, as they have a strong voice in social media that can be treated as trustworthy.

### 3.3 Opportunities, challenges, legal and ethical considerations

Social media represents an opportunity to law enforcement agencies and other security providers to improve the management of daily security. The opportunities for the use of social media as a tool include direct and fast communication with the public. This can contribute to better cooperation between police and citizens, the improvement of their relationship and to mutual understanding.

Social media also offer opportunities as a source of information. For example, contributing to criminal investigations, and anticipating and preventing crimes through the analysis of data collected on these platforms. Social media as an intelligence source can improve the quality and timeliness of decision-making. Open source intelligence can contribute to understanding and learning about potentially violent groups activities, criminal behaviour, and more.

One of the main challenges for LEAs and other security providers 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. The advent of social media has created new offences with which the police and other security providers such as local authorities and mediators have to contend with, new spaces for the police to visibly enforce the law, and increased the number of offences, creating issues with discretion,

---

*See MEDI4SEC (2016). Ethics and Legal Issues Inventory: Positive and Negative Societal Impacts of the Adoption of Social Media Across the Public Security Community Deliverable 1.3*  
workload and resources. Police forces must develop specific capacities for proper and effective use of social media and produce specialised training.

As a new technological tool used in daily security management, social media faces some ethical, operational, and technological questions. Law enforcement agencies will need clear answers to these questions 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. With particular 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 ultimately protect them from unwanted exposure (Trottier, 2012).
4. Stakeholder analysis from the workshop

The aim here is to provide a summary of the work reported above:

4.1 Identifying Stakeholders in Everyday security

During the workshop discussion, participants identified a number of actors involved or that should be involved in each of the proposed topics:

<table>
<thead>
<tr>
<th>Communication and engagement:</th>
<th>Role / responsibility</th>
</tr>
</thead>
</table>
| **Police forces** *(National and local level)* | The police already use social media as a direct channel to communicate with the public. It is currently being used as a constant and reassuring contact, sharing accurate information and dispelling rumours. It can also allow citizens and the police to work together to make society safer.  
  
  In terms of communication and engagement LEAs, play an important role. They use social media to keep citizens informed in real-time about the security situation during crises, as well as at normal times. The use of these platforms is not only restricted to informing and interacting with citizens through creating direct channels of communication (respond to their concerns, complaints, etc). Police forces also use social media to inform people about their activities (which are their competences and belong to another kind of public service).  
  
  Communication with citizens is important in two ways. Police forces should be able to respond to citizens. Police should ensure that communication is based on mutual respect, trust, open communication channels, and the provision of information that is accurate and relevant. |
| **Citizens** | Citizens have an active role in information sharing, contributing to the work of police forces. Their responsibility is to share useful information and educate themselves about the right and wrong way to use social media. |
| **Local Authorities** | Local authorities mainly have the role of carrying out crime prevention policies using social networks to educate and bring citizens’ attention to different aspects. For example, prevention of drug and alcohol consumption, tips to avoid becoming a victim of urban crime, what to do in case of a crisis etc.  
  
  Education and stimulating debate on issues relating to online hate as a means of promoting the prevention of emotional and |
physical abuse are also important responsibilities of local authorities.

<table>
<thead>
<tr>
<th>Social Media Platforms</th>
<th>Social media companies are also responsible for educating citizens about the correct use of social media, as well as raise awareness to the threats that these platforms can embody</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private security</td>
<td>Private security services are increasingly present in places that were previously exclusively for law enforcement (providing security at large events, including as security guards in shopping centres and other public spaces). These actors have information that can be valuable to the police forces. Consequently, their role is to share information in real-time with the corresponding security actors through social networks.</td>
</tr>
<tr>
<td>Schools</td>
<td>Schools play an important role in the education of young people on the responsible use of social networks, informing them of the potential risks and dangers found in these networks.</td>
</tr>
<tr>
<td>Press</td>
<td>Journalists and reporters have an important role to play when finding breaking stories online, and they have the responsibility to go to the police for verification that they are ready, or at least have taken the required measures to confirm or deny it.</td>
</tr>
</tbody>
</table>

Table 4.1 Stakeholders Communication and engagement

<table>
<thead>
<tr>
<th>Monitoring:</th>
<th>Role / responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polices forces (National and local level)</td>
<td>The analysis of information is useful for different LEA activities where an incident has not necessarily occurred, covered under the “Monitoring” title. LEAs try to understand data in order to anticipate, predict and prevent:</td>
</tr>
<tr>
<td></td>
<td>- In terms of anticipation, LEAs use real-time social media information to anticipate potential disturbances that may occur and prepare and mobilise their response in advance to maintain the peace.</td>
</tr>
<tr>
<td></td>
<td>LEAs can also use social media data to understand some phenomena and to predict future trends, for example by using social media to ‘crowd-source’ information is an important way of gaining valuable intelligence.</td>
</tr>
<tr>
<td></td>
<td>- LEAs also identify, collect and analyse data and information from social media that concerns national security (but not only) by using social media. Through these analyses, LEAs can determine behavioural patterns that could mean a security risk. It is also a</td>
</tr>
</tbody>
</table>
source of real-time information and an important element in security management.

LEAs have a responsibility to use Social Media for monitoring activities mentioned above, bearing in mind confidentiality and consent issues and the identification of the boundary between what is public and what is private. Analysts collecting information must have a solid and a legitimate reason for resorting to intrusive actions that violate some privacy issues and such methods must meet the principle of proportionality and necessity.

Officers and staff members responsible for social media campaigns can use that knowledge to develop more effective communication strategies.

**Local Authorities**

Local authorities (LA) also have a role to play, especially with respect to crime prevention. LA use social media information to better manage crime prevention policy and to communicate about their offline security strategy. Also, social media is an ideal space to disseminate counter-narratives and alternative narratives created at the local level, meaning they are adapted to specific situations.

LA such as municipalities can also play an important role in educating citizens in the correct use of social media and verifying the origin of the information before disseminating it.

In addition, in the management of security at a local level, the role of local authorities will include the designing of local security policies for social media analysis. This means data mining and predictive analytics – the statistical analysis or ‘mining’ of unprecedentedly large ('big data') data sets, including social media and other 'big' or open data sets (such as census data, crime, health, environmental and transport data), to find the dynamics, interactions, feedback loops and causal connections between them. Also, social media big or open data can be used to design security diagnosis and audits.

**Private companies**

Social media companies also play a role, especially in identifying, monitoring and censoring content which could be considered as a protentional risk in terms of security (Terrorism, sexual abuse, child pornography...).

**Academy**

Scientists and researchers are responsible for developing knowledge, methods and tools based on the needs of security providers and stimulating capacity building. A special role is played by experts able to translate technical information into intelligence.
innovation centres)  that can be understood by security providers. Another role for experts is to assist with ethical and legal challenges.

Industry (Developers)  The sheer amount of data produced through social media that needs to be analysed, coupled with the rapid speed with which decisions need to be made, requires computing capacity to select accurate data so it can be quickly filtered and analysed, and then transformed into practical intelligence. Industries have the responsibility to provide security actors with models and algorithms to facilitate data collection.

National governments  National government have the important role of allocating resources to technological development, supporting research institutes to develop new technologies and encouraging public-private partnerships to facilitate transfer of knowledge. Governments also have the responsibility to come up with a legal and ethical framework that can manage and clarify every aspect of information taken from social media and used for security purposes.

Open Source Social Media Intelligence will become an increasingly important source of intelligence for the police. However, it requires a clear set of guidelines and regulations to ensure it is proportionate and based on broad public consent.

Table 4.2 Stakeholders Monitoring

<table>
<thead>
<tr>
<th>Enforcement:</th>
<th>Role / responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Police forces</td>
<td>Law enforcement agencies continue to play a fundamental operational role when using social media in investigations. LEAs use social media to solve crimes quicker. Police take evidence from social media and also use it to help find missing, endangered or distressed people, identify criminals, identify criminal networks and identify witnesses. LEAs will also use social media to improve communication with colleges and the community. It is important to work on finding more ways to put applications/platforms within everyone’s reach. To continue obtaining valuable information from social media used in enforcement activities, the adoption of formal policies and processes within agencies will lead to a unified, consistent approach to modern technology usage. Personnel will require the correct experience to manage social media and to become 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 when interrupting criminal activity, closing cases and ultimately solving crimes.</td>
</tr>
</tbody>
</table>
Citizens play an important role by providing information to police (pictures, videos and also scenarios, hypotheses, or even complete case dossiers) and giving consent to data collection. Citizens have the responsibility to report incidents and at the same time make themselves aware of legal/ethical issues and take an active role in one's personal security.

The role of local authorities is to strengthen and diversify their use of new technology and invest in training for local police as well as other local services (mediators, support victims, social services, tourism providers, etc) to manage social media, and with these actors being closer to citizens they can collect valuable information for investigations.

Local authorities should include social media analysis as part of local security policies and also consult citizens over rules for gathering and analysing social media data as it directly involves their personal data and individual freedoms.

Social media is an increasingly important public space where crime can be both committed and spotted. The role of social media companies is to provide information to LEAs in case of emergencies and to prevent illegal activity.

Social-media companies use standard legalese to spell out their policies for granting access to individuals' online accounts.

In the future there needs to be more interaction with social media companies, to ensure commercial companies share required data with LEAs. A structured approach to an interface between commercial companies and LEAs is required.

Specialized prosecutors should be put in place and work towards international coordination and common international legislation.

Legislation for social media offences will need to be reviewed in order to provide guidelines that will ensure decision making in cases when social media has been used, for example, as a piece of evidence.

Governments have a role in developing processes and procedures to be implemented at EU level, which define international coordination and a common international legislation, as well as a European Network (LEAs cooperate).

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citizens</td>
<td>Citizens play an important role by providing information to police (pictures, videos and also scenarios, hypotheses, or even complete case dossiers) and giving consent to data collection. Citizens have the responsibility to report incidents and at the same time make themselves aware of legal/ethical issues and take an active role in one's personal security.</td>
</tr>
<tr>
<td>Local Authorities</td>
<td>The role of local authorities is to strengthen and diversify their use of new technology and invest in training for local police as well as other local services (mediators, support victims, social services, tourism providers, etc) to manage social media, and with these actors being closer to citizens they can collect valuable information for investigations. Local authorities should include social media analysis as part of local security policies and also consult citizens over rules for gathering and analysing social media data as it directly involves their personal data and individual freedoms.</td>
</tr>
<tr>
<td>Private companies (Social Media Platform Providers)</td>
<td>Social media is an increasingly important public space where crime can be both committed and spotted. The role of social media companies is to provide information to LEAs in case of emergencies and to prevent illegal activity. Social-media companies use standard legalese to spell out their policies for granting access to individuals' online accounts. In the future there needs to be more interaction with social media companies, to ensure commercial companies share required data with LEAs. A structured approach to an interface between commercial companies and LEAs is required.</td>
</tr>
<tr>
<td>Judges and prosecutors</td>
<td>Specialized prosecutors should be put in place and work towards international coordination and common international legislation. Legislation for social media offences will need to be reviewed in order to provide guidelines that will ensure decision making in cases when social media has been used, for example, as a piece of evidence.</td>
</tr>
<tr>
<td>Governments at national and European level</td>
<td>Governments have a role in developing processes and procedures to be implemented at EU level, which define international coordination and a common international legislation, as well as a European Network (LEAs cooperate).</td>
</tr>
</tbody>
</table>

Table 4.3 Stakeholders Enforcement

During the workshop, participants discussed the roles and responsibilities of the different stakeholders involved in everyday security activities in the three selected topics. Police forces, citizens, local authorities and social media are the most important actors. However, other stakeholders, depending on the day-to-day security activities, need to be considered.
In terms of communication and engagement, on the one hand LEAs and other public authorities have the most important role. They should use social media to inform and interact with citizens in a timely manner, although on the other hand citizens can also play a part by communicating and contributing to policing with reliable information. Workshop discussions also highlighted the role of other stakeholders such as social media companies, schools and local authorities in educating people on the responsible use of these platforms.

In the area of monitoring activities - whose purpose is to analyse social media information to try and understand behaviour and anticipate and prevent criminal acts - LEAs are the most important stakeholder. Nevertheless, it is necessary to involve other actors for fully effective monitoring activities. For instance, providing companies in the industry with adequate technology can facilitate the identification of data to be analysed by LEAs. Social media companies also contribute to these activities by sharing information of high importance.

When talking about enforcement activities, new actors can intervene such as judges and prosecutors. The need for specialised and trained legal representatives was raised. Indeed, the actions and knowledge provided by prosecutors and judges is key to the success of such projects.

For all these daily activities to maintain security, the intervention of national and European governments is necessary to define clear frameworks in the use of these tools. This means they can be responsibly integrated into the operational work of both the police and other actors that contribute to keeping the peace.

The cooperation and collaboration of the actors mentioned during the discussions on their specific role and responsibility is necessary for the effective use of social networks in everyday security activities.
5. **SWOT Analysis**

Part of the discussion session was dedicated to identifying Strengths, Weaknesses, Opportunities and Threats (SWOT) for everyday security activities. The core idea of SWOT is to look at an issue from an internal and an external perspective, understanding internal strength and weaknesses, based on the organisations’ capacity (LEAs in this case), as well as external opportunities and strengths posed by the organisation's background or environment. The goal then is then to benefit from strength and opportunities while mitigating weaknesses and threats.

Below, we present the SWOT analyses on the use of social media for each of the themes that were identified during the workshop. They came up at several of the round tables. Some of the items discussed were part of all topics, however they have been included in just one theme.

As different kinds of actors took part in this analysis, this is addressed to security providers in general and not just LEAs.

5.1 **Theme: Communication & Engagement Activities**

<table>
<thead>
<tr>
<th>STRENGTHS</th>
<th>WEAKNESSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promoting collaboration between citizens and LEAs</td>
<td>Disruptions to communications</td>
</tr>
<tr>
<td>Reaching people that are not normally easily reachable</td>
<td>Difficulties adapting to rapid technological changes</td>
</tr>
<tr>
<td>Informing citizens about the role of local police</td>
<td>Lack of willingness to share information through social media on sensitive topics</td>
</tr>
<tr>
<td>Fast way to reach a lot of people</td>
<td>Lack of human capacity to respond in real time</td>
</tr>
<tr>
<td>Informing citizens with trustworthy real time information</td>
<td>Different levels of experience in social media use</td>
</tr>
<tr>
<td>Promote Prevention</td>
<td>Lack of willingness</td>
</tr>
<tr>
<td>Adapting language when engaging with citizens</td>
<td>Risk of bad reputation</td>
</tr>
<tr>
<td>Dispelling rumours</td>
<td>Social media replaces traditional policing</td>
</tr>
<tr>
<td>Learn from peers</td>
<td>Lack of training</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OPPORTUNITIES</th>
<th>THREATS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent crime by influencing people's behaviour</td>
<td>Negative content on security providers</td>
</tr>
<tr>
<td>Better reputation for police among (young) citizens</td>
<td>Decreasing number of citizens engaged</td>
</tr>
<tr>
<td>Co-produced safety</td>
<td>Digital divide</td>
</tr>
<tr>
<td></td>
<td>Increasing feeling of insecurity</td>
</tr>
</tbody>
</table>
Encourage innovation
Gaining the citizens’ trust
Inform/communicate on the local crime prevention strategy

Simplification of complex crime prevention matters

5.1.1 Strengths
1. Promoting collaboration between citizens and LEAs: social media facilitates two-way communication, enabling LEAs to establish close, trusting relationships with citizens, increasing their contribution on security issues.

2. Reaching people that are not normally easily reachable: demographic analysis of social network users that shows young people are likely to use these tools actively.

3. Informing citizens about the role of local police: Sometimes problematic relations between police and citizens are due to a lack of knowledge on what the police actually do. Through social networks, citizens can be educated in this regard. Also, LEA do communicate and disseminate their activities in text, image or video for example via Twitter.

4. Fast way to reach a lot of people: social media means a larger number of people can be reached, in case of emergency these platforms are helpful to inform citizens on what to do.

5. Informing citizens with trustworthy real time information: social media can be used to inform citizens rapidly and directly. LEAs and other security providers can report successfully and provide reassurance, to promote community activities and delivering statements.

6. Promote Prevention: through social media, LEAs and other security actors such as local authorities can educate and empower citizens to protect themselves by providing them with security tips and appeals for collaboration, listening and monitoring.

7. Adapting language when engaging with citizens: LEAs should communicate using citizens’ language when communicating via social media.

8. Dispelling rumours: The viral nature of social media allows exaggerated, fake and malicious information to spread very rapidly. In response, security providers must use social media to dispel rumours.

9. Learn from peers: Security providers are willing to share their experience using these platforms. Many LEAs are already sharing their insights, enabling them to better coordinate with other departments.

5.1.2 Weaknesses
1. Disruptions to communications: social media can also disrupt regular forms of communication and engagement normally used to reach security providers.
2. **Difficulties adapting to rapid technological changes**: technological advances in social networks are faster than the ability of LEAS and other security providers to integrate these platforms into their daily social activities (e.g. LEAs start using certain SM platforms when they are already “out of fashion”).

3. **Lack of willingness to share information through social media on sensitive topics**: Information dissemination through social media could be a very touchy subject as some topics, such as radicalisation, are very sensitive. This explains why some senior managers or directors of LEAs and other public security organisations are very reluctant to use these tools.

4. **Lack of human capacity to respond in real time**: social media is becoming a real communication channel, but LEAs are not capable of responding to all messages and complaints. This can mean an adverse result vis-à-vis citizens’ confidence.

5. **Different levels of experience in social media use**: LEAs lack the proper tools and knowledge for online collaboration. Digital devices are not standard equipment, which hinders cooperation between different police forces in different countries and even in the same country there is division between the different police services.

6. **Lack of willingness**: especially at a management level, there is a lack of willingness to integrate these tools into everyday security activities. The fear of the risk of using these technologies in policing is an obstacle to embracing opportunities that SM technology offers. There is scepticism on the part of senior officers about the value of social media.

7. **Risk of bad reputation**: Social media has significantly increased officers’ community exposure. Police are often surrounded by cameras and amateur reporters who broadcast everything they see and their opinion of it to a worldwide audience.

8. **Social media replaces traditional policing**: Even though social media is becoming an important tool for LEAs and public safety agencies, embracing social media does not devalue traditional police work.

9. **Lack of training**: on the use of social media and the behaviour guidelines on social media (they have no instructions or rules about what should be shared and what should not). Some individuals (LEAs) are using social media in their professional lives in the same way they use it in their private lives.

5.1.3 **Opportunities**

1. **Prevent crime by influencing people’s behaviour**: LEAs and local authorities in particular can use social media to educate and raise awareness.

2. **Better reputation for police among (young) citizens**: social media can help police with legitimacy and reverse the image of ‘the police aren’t doing anything’.

3. **Co-produced safety**: social media can facilitate inclusion of a large number of different actors in public security. All-community involvement from the police, social support services, charities, youth groups, local churches, parents’ organizations, rehabilitation centres and schools. There is great potential for the police to create and curate networks of citizens cooperating to keep their society safe.
4. **Encourage innovation:** The use of social networks is an opportunity for LEAs and other security providers to innovate regarding policing, integrating new technologies and promoting the participation of actors other than justice and security.

5. **Gaining the citizens’ trust:** Local authorities and LEAs to be more approachable so they can get closer to their citizens. This closeness allows for the identification of priorities and an improved adaptation of services to citizens’ needs.

6. **Inform/communicate on the local crime prevention strategy:** Local authorities can use social media to inform citizens about their crime prevention strategy on a more regular basis (such as about its implementation) and offer better follow up concerning local actions that have been implemented.

### 5.1.4 Threats

1. **Negative content on security providers:** Malicious content posted by the general public or clumsy content posted by LEAs can create a reputation crisis.

2. **Decreasing number of citizens engaged:** Citizens may not use social media in the future due to privacy reasons. Citizens might have the feeling that they are under surveillance all the time.

3. **Digital divide:** Difficulties reaching groups of citizens who don’t use social media. For example, senior citizens, who are normally active in general social life can be set left out when using these platforms.

4. **Consent of information:** Citizens are not informed when police intervene on social media.

5. **Increasing feeling of insecurity:** Continuously informing citizens about crimes and suspects via social media can trigger feelings of insecurity in society.

6. **Improve reporting by vulnerable groups:** Thanks to its anonymity, social media can facilitate the reporting of hate crime.

7. **Simplification of complex crime prevention matters:** Crime prevention and urban security are very complex issues that are transversal and involve many different actors. Social media uses simple and fast communication that could lead to misinterpretation.

LEAs can engage with citizens well through social media. In this regard, it is very important to carry out complete two-way communication, which means answering all questions raised by citizens, using the same networks that they use and the kind of language that people will understand. LEAs have reached various levels of maturity in adopting social media. It was stressed that there is a difference between countries in which Social Media is only in the hands of the Communication department and countries where law enforcement officers are involved and have their own accounts. This second way of managing social media seems more likely to achieve greater engagement, but poses a challenge to social media policies and training. There is also a difference between using social media for broadcasting and social media for engagement purposes. Several
best practices of engagement were discussed, for example social media quizzes and Tinder matching with suspects.

Social media is an excellent tool to build good relationships with citizens. The main aim must be to reduce crime. On this point, it is very important to engage, educate, and inform people in order to prevent crime. Also, monitoring social media can strengthen the police’s information and can help build a good relationship with citizens. Besides, LEAs must take care about the way in which they communicate because they can provoke feelings of insecurity, for instance by sending too many messages related to crime.

5.2 Theme: Monitoring Activities

<table>
<thead>
<tr>
<th>STRENGTHS</th>
<th>WEAKNESSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>New source of information/improved data</td>
<td>Lack of collaboration with social media companies</td>
</tr>
<tr>
<td>Innovation on the methods used by police when collecting intelligence</td>
<td>Lack of effectiveness evaluation</td>
</tr>
<tr>
<td>More two-way/targeted information</td>
<td>Lack of funds for acquiring technology</td>
</tr>
<tr>
<td>Development of new jobs</td>
<td>Lack of knowledge and experience using social media</td>
</tr>
<tr>
<td>Improve legal statements and procedures</td>
<td>Lack of certified and approved applications for LEAs and citizens</td>
</tr>
<tr>
<td></td>
<td>Barriers between legal frameworks and technology</td>
</tr>
<tr>
<td></td>
<td>Stigmatisation of urban areas and/or groups of population</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OPPORTUNITIES</th>
<th>THREATS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crowd-sourced intelligence</td>
<td>Hacking risk</td>
</tr>
<tr>
<td>Influence the decision-making process</td>
<td>Competition with other actors</td>
</tr>
<tr>
<td>Increasing knowledge</td>
<td>Lack of storage policy</td>
</tr>
<tr>
<td>Anticipation</td>
<td>Violation of privacy</td>
</tr>
<tr>
<td>Cost reduction</td>
<td>The lack of legal clarity over the use of SOCMINT</td>
</tr>
<tr>
<td>Possibility to improve privacy on social media</td>
<td>Lack of organisational processes to make full and proper use of information</td>
</tr>
<tr>
<td>Enrich criminal behavioural research</td>
<td>Stigmatisation of specific individuals or groups</td>
</tr>
<tr>
<td>Sharing best practices</td>
<td>Presence of international platforms</td>
</tr>
<tr>
<td>Improving crime prevention policies</td>
<td></td>
</tr>
<tr>
<td>Coordination between police departments</td>
<td></td>
</tr>
</tbody>
</table>
EU projects
Improve information collection methods in local security audits

Automatic judging of algorithms used by Facebook or other platforms could be problematic
Social media data is becoming a business
The lack of EU-wide legislation
Obstacles of Data Protection Legislation
Private Power
API access restriction to LEAs

5.2.1 Strengths
1. **New source of information/improved data:** LEAs and security providers have found a new source of intelligence with different social media platforms. By using analytics tools, they can help the police to identify emerging events, piece together networks and groups, discern public behaviour and promote social awareness.

2. **Innovation on the methods used by police when collecting intelligence:** LEAs can modernize/improve/diversify their methods to collect, store and analyse data. Social media's possible uses can contribute to understanding and learning about potentially violent group activities, criminal behaviour, disorder, community tension and more.

3. **More two-way/targeted information:** direct contact with citizens enables LEAs to get better information during incidents.

4. **Development of new jobs:** new specialised teams for doing more open source and online investigation are springing up in various LEAs, mostly being good at managing officers’ expectation and at ensuring that only information that is necessary is sought. This is good both for privacy and for police because it doesn't overload them with data.

5. **Improve legal statements and procedures:** The scheme used by the London Metropolitan police could be improved. Their actions must follow P L A N: Proportionate, Legal, Accountable, Necessary.

6. **Increasing cyber bullying and hate speech:** due to the anonymity and the principle of non-censorship on some social networks, SM contributes to increasing cyber bullying and hate speech.

5.2.2 Weaknesses
1. **Lack of collaboration with social media companies:** social media policies are sometimes not in tune with the needs of LEAs. It is difficult to improve cooperation and collaboration when the companies are wary about being too close to LEAs.

2. **Lack of effectiveness evaluation:** inexistent methods and techniques to evaluate the effectiveness of SM use in collecting, classifying and enlisting data that are applied across the forces.
3. **Lack of funds for acquiring technology:** the industry has developed software, applications, algorithms, etc. to facilitate the effective analysis of the masses of information on social networks to which LEAs do not have access due to lack of funds.

4. **Lack of knowledge and experience using social media:** not all LEAs and other security providers are aware of social media technology, not all of them have the background, knowledge and experience to use social media. Lack of trained security professionals: insufficiently equipped to gather intelligence with social media.

5. **Lack of certified and approved applications for LEAs and citizens:** apps that are certified and approved to allow safe and ethical sharing of information could help monitoring activities. Citizens could, legitimately, be suspicious about how their data will be used when in the hands of private companies.

6. **Barriers between legal frameworks and technology:** Law makers are not always aware of technology and the speed at which it changes.

7. **Stigmatisation of urban areas and/or population groups:** If the information about crime is concentrated on the same groups of people or same urban areas, these could be stigmatised as “dangerous and unsafe “with negative impacts in terms of reputation”.

5.2.3 **Opportunities**

1. **Crowd-sourced intelligence:** new opportunities to crowd-source intelligence. Several sporadic successes have demonstrated the ability of crowd-sourcing to offer effective contributions to intelligence when directly solicited.

2. **Influence the decision-making process:** SOCMINT Intelligence can improve the quality and timeliness of decision-making against organised crime and terrorism.

3. **Increasing knowledge:** social media can contribute to understanding and learning about potentially violent group activities, criminal behaviour, signs of disorder, community tension and more.

4. **Anticipation:** There is an opportunity for LEAs and other security providers to be more proactive and less reactive, analysing data and predicting crime.

5. **Cost reduction:** Tools for automation will help reduce labour costs for analysis, which are currently too high.

6. **Social media companies investing in securing their platforms and their users:** social media companies are investing in improved identification/biometrics tech to better protect individuals from nefarious photoshopping. This can be useful for helping LEAs to identify criminals.

7. **Possibility to improve privacy on social media:** Privacy features incorporated by companies are at the client’s request. Because of the cost, small companies are not able to develop them. Raising awareness in policing procurement or buying departments, and perhaps introducing some standardisation, would improve privacy by design (PbD) technology compliance.
8. **Enrich criminal behavioural research:** social media analysis can enrich criminal science with new parameters / indicators to identify criminal behaviours.

9. **Sharing best practices:** Platforms can facilitate communication and interaction between different stakeholders from various sectors (police, academics, researchers, practitioners,), enabling them to exchange knowledge, experiences and best practices used in their organizations.

10. **Improving crime prevention policies:** Local authorities can use information from social media to enhance their regular source of information. This data will help LA to identify priorities and implement more accurate programmes based on local needs.

11. **Coordination between police departments:** Better coordination between intelligence and operations and executive levels.

12. **EU projects:** Participation of LEAs in more EU-relevant projects will contribute significantly to a change in attitude and mentality, bringing new ideas into their organizations and facilitating the resolution of Change Management issues.

13. **Improve information collection methods in local security audits:** Social media are an opportunity for local authorities to collect extra information for the local security audits.

### 5.2.4 Threats

1. **Hacking risk:** Risk that criminals might hack into these infrastructures and access criminal intelligence was a concern.

2. **Competition with other actors:** LEAs cannot compete with private security companies when hiring the best graduates with a tech background. Additionally, outsourcing of intelligence to commercial companies and ‘black-boxed’ tools reduces the accountability of LEAs.

3. **Lack of storage policy:** Social media produces a very large volume of data, so it is necessary to include a storage policy for both intelligence and evidence. Social media information that is collected but not used for intelligence or on-going investigation purposes should be discarded safely and quickly.

4. **Violation of privacy:** Collection of social media users’ data can be considered as a violation of privacy. The increasing use of software to collect and analyse information creates additional risk of misuse. Public attitudes towards data ownership and privacy (even on open platforms) can change quickly, and there is a reputational risk if law enforcement agencies are seen to be watching people online.

5. **The lack of legal clarity over the use of SOCMINT:** Governments can be confronted by legal and reputational issues when using social media for intelligence. Some organizations are launching a series of Freedom of Information requests about LEAs’ use of social media analysis.

6. **Lack of organisational processes to make full and proper use of information:** People with bad intentions can also monitor others, so who monitors the monitors?

7. **Stigmatisation of specific individuals or groups:** Social media surveillance of specific groups can lead to over-criminalization of youth, particularly minorities.
8. **Presence of international platforms:** Platforms from China, Russia (WeChat, Telegram, VKontakte) or other countries may become bigger in the European Union. It poses a challenge if they expand in the future (issues when trying to ask for data, data leaks...)

9. **Automatic judging of algorithms used by Facebook or other platforms could be problematic:** humans are left out of the equation.

10. **Social media data is becoming a business:** social media companies as owners of data may sell their data to the highest bidder. Data is giving more and more power to social media companies and the LEAs' surveillance powers are limited in comparison. Social media could substitute LEAs when investigating crime.

11. **The lack of EU-wide legislation:** giving LEAs equal access to social media data is an obstacle that reflects the fact that laws continue to lag behind and be out of step with practice. Currently, requests for access to servers and so forth undergo a slow, lengthy process and this is a hindrance to efficient law enforcement action to tackle crime.

12. **Obstacles of Data Protection Legislation:** Overly restrictive data protection legislation is a real barrier to open source police work in certain countries. It prevents organisations sharing vital information.

13. **Private Power:** increasingly centralised information in the hands of private companies. Also, private companies have more advanced tools, but using them poses a controversial issue regarding trust.

14. **API access restriction to LEAs:** APIs (Application Programming Interface) from social media are in many cases restricted for LEAs. These applications help police officers identify and monitor protesters based on their public social media posts.

This discussion reflects the influence of a significant degree of uncertainty about how effective monitoring activities currently are and what the prospects are for its future development. The robustness of social media monitoring (and other intelligence gathering) infrastructures means the possibility that criminals might hack into them and access criminal intelligence. LEAs will need to implement very thorough security protection measures and ensure infrastructures are properly maintained (e.g. don’t use software that is out-of-date and no longer supported). Comments that did seem to reflect a consensus view included the lack of training, tools and support from more senior members of the organisation.

### 5.3 Theme: Enforcement Activities

<table>
<thead>
<tr>
<th>STRENGTHS</th>
<th>WEAKNESSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Find partners</td>
<td>1. Lack of European tools and procedures at EU level</td>
</tr>
<tr>
<td>2. Rapid incident identification</td>
<td>2. Lack of technical skills among police officers</td>
</tr>
<tr>
<td>3. Faster, more effective and more flexible emergency response</td>
<td>3. Resource limitations</td>
</tr>
<tr>
<td>5. New evidence</td>
<td>5. Problem of jurisdiction</td>
</tr>
<tr>
<td>7. Sharing practices</td>
<td></td>
</tr>
</tbody>
</table>
Networking between European Police Forces and local authorities

**LOCATION IN REAL-TIME**

**OPPORTUNITIES**

1. Working with SM companies
2. Better engagement with Internet Service Providers (ISPs)
3. Collaboration with justice actors
4. Collaboration with other public-sector organizations
5. Collaboration with the private sector
6. Collaborating internationally
7. Policing by consent
8. General Data Protection Regulation (GDPR)
9. Community-oriented policing
10. Develop an SM strategy
11. Citizen engagement
12. Collaboration with journalists
13. Develop European legislation

**THREATS**

1. Lack of clarity around LEAs practices on SM
2. Infringing on the right to privacy
3. Fake News
4. Legitimate reasons for online anonymity
5. Lack of formal exchange mechanisms with SM companies
6. Technology is not designed for the requirements of LEAs

5.3.1  **Strengths**

1. **Find partners:** With the right partnership, officials can gain the support they need to evolve quickly and use the benefits that are available to them.

2. **Rapid incident identification:** Social media traffic analysis could allow for a more rapid identification of events than traditional reporting mechanisms.

3. **Faster, more effective and more flexible emergency response:** With the application of geo-location techniques this could lead, for example, to a constantly evolving map showing spikes in possible violence-related tweets.

4. **Citizens aiding LEAs:** Citizens provide LEAs with information about terrorism, organised crime or missing people, among others. Additionally, citizens can provide municipality services if they have been victims of an civil issue (noise, garbage problems, lack of street lights, etc.)

5. **New evidence:** Social media offers a new source of evidence for prosecution and enforcement. Posts, videos and photos that are uploaded to SM by criminals can be used as valuable evidence of criminal activity.

6. **New police function:** new unit which has the main responsibility of tracking criminals on Facebook, Myspace, Twitter and other social media.

7. **Sharing practices:** industry can share best practices with LEAs to enhance SM policing.

8. **Networking between European Police Forces:** Create a structure for cooperation between police and outside expertise.
9. **Location in real-time:** ability to connect social media activity to location. For example, there is Geofeedia, a company that offers products using the location data of social media posts, when available, and then maps them.

### 5.3.2 Weaknesses

1. **Lack of European tools and procedures at EU level:** it is not clear how data should be sourced, or which authority is responsible. There is a lot of reluctance between Member States for European cooperation.

2. **Lack of technical skills among police officers:** LEAs usually do not have the correct profile to deal with the huge amount of information that social media can provide (lack of background and training in social media and IT).

3. **Resource limitations:** SM has increased the number of offences, creating issues with workload and resources. The police may find themselves unable to investigate all the cases reported to them, mainly internet trolling.

4. **New risks:** The amount of personal information posted on social media increases individuals’ risk such as personal addresses.

5. **Problem of jurisdiction:** when a criminal uses SM in a police department’s jurisdiction, the company operating the platform may be based in another city or even a different country. This makes it difficult to obtain records and also makes it difficult to determine whose legal jurisdiction the content falls under. This can be more problematic if every piece of content could be subject to different countries and their national laws are different.

6. **Lack of training:** Interpreting behavior on social media is a difficult task for LEAs, with many inaccurate interpretations of social media data. Lack of training for understanding by investigators on what they are seeing online could lead to the criminalization of innocent individuals – particularly minors.

### 5.3.3 Opportunities

1. **Working with SM companies:** using SM information as evidence for solving cases can mean better engagement for LEAs with Internet Service Providers.

2. **Better engagement with Internet Service Providers (ISPs):** ISP companies want to ensure their users assume more responsibility by educating customers, building useful filter systems, and encouraging more community policing of material and reporting of material that breaches terms and conditions. There is an opportunity for LEAs and companies to work together to share findings.

3. **Collaboration with justice actors:** working closely with justice actors can help speed up investigations and convictions.

4. **Collaboration with other public-sector organizations:** local governments and public-sector organizations could work closely with police services to deal with matters they are best placed to address themselves. This can help police services monitor criminal activity and develop a more responsive service. Formalized cooperation with schools
and social services by sharing information about people who have committed or are likely to commit a crime.

5. **Collaboration with the private sector:** Collaborating with the private sector to reduce crime in areas such as cybercrime and corporate fraud is in the interest of both the police and the relevant organizations concerned. In fraud prevention, private sector companies are often better placed to protect themselves and gather evidence of crime which can be passed on to the police.

6. **Collaborating internationally:** Expanding collaboration from a national to international level can provide a new dynamic in fighting today's borderless crime.

7. **Policing by consent:** Consent is very important in order to minimize harm, and to ensure that research subjects can make an informed and free decision on their involvement in an investigation.

8. **General Data Protection Regulation (GDPR):** contained a Directive on the processing of personal data for authorities responsible for preventing, investigating, detecting and prosecuting crimes. It ensures that police forces can do their work efficiently, using technological means while preserving the fundamental rights of citizens.\(^7\)

9. **Community-oriented policing** to a new level by providing quick, cheap and easy ways to get important information out to followers and concerned citizens.

10. **Develop a social media strategy:** for LEAs and other security actors, using SM means they have the opportunity to develop effective social media policies that balance organizational needs and free speech.

11. **Citizen engagement:** Improving communication between police and citizens (discussions among citizens and police about security issues, digital community policing/online patrol).

12. **Collaboration with journalists:** Journalists who use the web for their first line of research exchanging information with LEAs could be an interesting source of information.

13. **Develop European legislation:** The law must take into account the current and upcoming changes to offer some tools and possibilities for public actors to lead effective activities.

14. **Balance human/machine activity:** Understanding what is the right balance operationally and ethically between human and algorithm-driven decision-making.

### 5.3.4 Threats:

1. **Lack of clarity around LEAs practices on SM:** creating fake profiles to further an investigation can be considered as a violation of people's right.

2. **Infringing on the right to privacy:** serious concerns regarding the protection of personal data, right to privacy and freedom of expression.

3. **Fake News:** publicly providing fake information through social media can disturb an investigation and can cause social panic.

---

4. **Legitimate reasons for online anonymity**: the public increasingly uses the internet in an encrypted way and makes use of the dark web, making it difficult to monitor and enforce for police forces.

5. **Lack of formal exchange mechanisms with SM companies**: there is no structured interface with between the social media industry and LEAs.

6. **Technology is not designed for the requirements of LEAs**: tools are tailored by private companies and there is too much data in hands of the private sector.

During the discussion in general, the participants feel they understood what they can and cannot do regarding collecting information. However, it is not always clear how data should be sourced and which authority is responsible. Jurisdictions are also a big issue, because there is a lot of reluctance between Member States regarding European cooperation.

As seen in the SWOT analysis, social media pose new challenges to law enforcement agencies as well as to other actors involved in the co-production of security. Nevertheless, at the same time, it offers numerous opportunities which can be utilized by harnessing it for further capacity improvements.
6. Relevant Methods, Procedures, practices, and Recommendations

In this section we present the analysis of the various tools, methods, practices and organisational issues that limit security providers’ engagement with social media that can contribute to the setting out of a roadmap for future improvement.

<table>
<thead>
<tr>
<th>Current issues/limitations</th>
<th>Future recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lack of expertise</strong></td>
<td>Training for security providers on how to communicate using social platforms (what to and what not to communicate, not including personal information, using appropriate vocabulary and other codes of conduct for personal use)</td>
</tr>
<tr>
<td></td>
<td>During operational task, produce specialised training for intelligence analysts as well as for criminal investigators.</td>
</tr>
<tr>
<td></td>
<td>Training might be necessary for judges, prosecutors, and defense attorneys for responsible use of social media data in cases.</td>
</tr>
<tr>
<td></td>
<td>It is also necessary to train and raise awareness to other public actors, such as mediators, social services, hospitals, prison or traffic data on the use of this tool for security purposes, as they are important allies for police forces.</td>
</tr>
<tr>
<td><strong>Weak security, data protection and infrastructure</strong></td>
<td>LEAs need to implement security protection measures and ensure infrastructures are properly maintained.</td>
</tr>
<tr>
<td><strong>Lack of formal legislation on the use of social media for security purposes</strong></td>
<td>The existing legislation for social media needs to be reviewed in order to provide a clear ethical, legal and regulatory framework that allows the police to use social media in policing, ensuring that the law is not being infringed upon or any rights are being violated.</td>
</tr>
<tr>
<td></td>
<td>The Right not to have your data analysed, or the right for it not to be collected could become manifest, blocking social media companies or law enforcement from doing this (as companies protect their customers). It could be a fundamental right not to be able to monitor social media. “Serve &amp; protect” could have consequences, such as to block a platform in some countries or let them simply pay fines if they do not abide by the law.</td>
</tr>
<tr>
<td>Lack of technology</td>
<td>Police forces and local authorities should integrate technologies that enable police officers and other relevant security actors to respond more quickly to citizens, improving investigations and preventing crime and other kind of problems that affect the feeling of security.</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Lack of social media culture</td>
<td>The creation of new departments with specialized skills and knowledge on priority tasks could support special investigation and intelligence units.</td>
</tr>
<tr>
<td>Weak level of coordination and collaboration with other actors</td>
<td>Police forces need to reinforce cooperation, nationally and internationally, with other police forces, justice organizations, public sector, private sector organizations, civil society organizations, and citizens in order to be more efficient at preventing and fighting crime.</td>
</tr>
<tr>
<td>Lack of a formal social media policy</td>
<td>This is necessary to provide internal guidelines that will ensure decisions are made with interim guidance having already been set out.</td>
</tr>
<tr>
<td>Very different levels of maturity in using social media</td>
<td>Moving to a wider range of tools, more bottom up use by individual police officers, and from broadcasting to more reciprocal communication.</td>
</tr>
<tr>
<td>SM are being used in policing, but there is no evaluation of their effectiveness</td>
<td>Evaluation of the effectiveness of the uses of social media analytics for policing.</td>
</tr>
</tbody>
</table>
7. Practices analysis

During the workshop several existing practices were discussed, some of them described in MEDI@4SEC deliverable D1.1 (State of the Art Review) and classified in D1.2 (Best Practice) into patterns, see Section 3.2.

In the table below, we present the analysis of the current practices discussed on everyday social media security, along with their limitations and propose some recommendations that can contribute to the creation of a roadmap for future improvement.

<table>
<thead>
<tr>
<th>Current issues/limitations</th>
<th>Future recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current apps or social networks that enable cooperation between citizens and LEAs are mainly about “cadre de vie” and keeping the peace. Lack of cooperation/collective intelligence and tools in the field of investigation.</td>
<td>A social network where citizens would help LEAs identify and track down wanted criminals or missing persons by sending locations where they were seen.</td>
</tr>
<tr>
<td>Data collection is focused on creating individual data profiles</td>
<td>Create patterns for generalization of profiles and behaviour from individuals’ data that has been collected and processed instead of creating individual data profiles, which have social and legal implications.</td>
</tr>
<tr>
<td>Lack of social media data analytics to make primary and secondary prevention more accurate</td>
<td>Develop a system that collects social media data and connects with victims or first offenders, analyses it and provides warnings and advice to involve citizens and prevent crime.</td>
</tr>
<tr>
<td>Law enforcement platform for Open Source Intelligence (OSINT), is starting to work well</td>
<td>In order to improve their performance, it would be useful to have a tool that collects all OSINT data in the world (in all languages), filters and analyses it to make it relevant, and provides them with automated evidence collection. On this matter, it would be useful to work towards an international database standard to share law enforcement’s social media data (for intelligence/investigations) within Europol/Interpol.</td>
</tr>
<tr>
<td>LEAs do not have the proper knowledge to deal with the huge amount of information</td>
<td>To connect different platforms which can provide them with different kinds of knowledge and therefore improve the quality of the information. In this regard,</td>
</tr>
<tr>
<td>that social media can provide</td>
<td>the provided information should be treated and &quot;cleaned&quot;.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Different tools developed in every country</td>
<td>Implementation of guidelines at European level that allow the use and analysis of the information of the different tools developed to be integrated.</td>
</tr>
<tr>
<td>LEAs don't have the required knowledge to create their own tool</td>
<td>Develop tools according to LEAs needs with proper and relevant training.</td>
</tr>
<tr>
<td>Need of closer cooperation between LEAs.</td>
<td>Set up tools at a European level to ensure better intelligence gathering and interoperability.</td>
</tr>
<tr>
<td>Need to better coordinate with other actors</td>
<td>Adapting analytics for wider intelligence, or broadening the scope of analytics — to include hospital, prison or traffic data — can offer richer intelligence. Sophisticated analytics techniques can quickly process a wide variety and volume of data sources — from video cameras, sensors, and biometrics — and thus dramatically transform policing.</td>
</tr>
<tr>
<td>Lack of knowledge and awareness of municipalities and local actors</td>
<td>Create a guidebook that highlights the threats and opportunities of social media use and data analytics with basic guidelines.</td>
</tr>
<tr>
<td>Need to better understand the needs and feedback of citizens regarding social media and apps created in order to ensure safety</td>
<td>Develop local diagnoses on (1) citizens' needs, (2) citizens uses and knowledge of technologies – e.g. senior (3) citizens’ trust in these apps (4) citizens’ will to cooperate with LEAs in general, and through tech apps in particular</td>
</tr>
</tbody>
</table>
8. Conclusions

Actors clearly use social media for LEAs' communication activities throughout Europe. Nevertheless, for other activities such as monitoring or intelligence, which means more operational activities, there is no a standard or generalized knowledge on social media use. Moreover, in Europe there are many differences between countries, cities or LEA units regarding their use and knowledge of social media.

Senior managers or directors of public or private organizations – especially LEAs and governments - are not fully aware or at ease with social media stakes, threats or opportunities. It highlights the need for training of all kinds of actors involved in public security. However, the requirements for each type are different: senior managers should be aware on the need of new departments with specialized skills and knowledge that could support special investigation and intelligence units, agents and practitioners should be trained on more operational or technical insights.

Social media platforms embody new threats or reinforce existing weaknesses as a new public space (hate speech, extremist propaganda…) they can harm individuals and society as a whole very badly. To tackle these emerging threats and weakness, not just LEAs alone should work to mitigate these risks. Cooperation is key:

New security actors or providers appeared or were revealed through massive social media use. Indeed, social media companies, industrial companies, local authorities or citizens have an important role to play in security - by holding data, powering end users’ solutions, preventing security threats or voicing their concerns. Since all these actors have different roles and knowledge, their partnership is key to enhance public security on a day-to-day basis. This partnership should be orientated towards coordination of public security to make the most of each other’s roles and responsibilities in society.

Social media companies are key actors in this procedure. It continually came up throughout the workshop that their collaboration should contribute to ensuring safety for all. Indeed, social media companies could pursue and, in many countries, reinforce collaboration with LEAs by sharing useful information in specific cases such as child sexual abuse, terrorism, suicide and organised crime among others. Social media cooperation can be also extended to improving knowledge by sharing anonymised information and trends with researchers. In general, it appears that social media companies - even if they are key actors - are not very well known by the more traditional security actors. Also, building and reinforcing knowledge-sharing with this specific actor is necessary considering the tremendous increase in the number and size of social media companies over the past few years.

Local and public authorities in their role of prevention or social media companies as data holders can play a part in educating people on how to use social media and in leading prevention actions.

Participants also highlighted the central role of data itself. For all security providers, data represents a new type of evidence, new sources for security diagnosis and audits and
effective and crucial data for researchers to understand criminality. Data access, property and analytics is a subject of concern for every security provider.

**LEAs and other security providers’ activities on social media raise issues on legal and ethical frameworks.** The respect of individual freedoms, the need for anonymity in their use, mass data analysis, or the gap between an online activity and its area of jurisdiction pose limitations. In addition, data protection and privacy should be reinforced as fundamental rights and procedures should be reviewed to effectively protect citizens. There is also a need to formalize and homogenize legal frameworks throughout Europe to facilitate coordination.
References


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


MEDI@4SEC (2016). Report on State of the Art Review Deliverable D1.1

MEDI@4SEC (2016). Worldwide Mapping of Best Practices and Lessons Learnt Deliverable D1.2

MEDI@4SEC (2016). Ethics and Legal Issues Inventory: Positive and Negative Societal Impacts of the Adoption of Social Media Across the Public Security Community Deliverable 1.3


Appendix 1  Workshop Agenda

09.00-09.30 Registration

09.30-10.00 Welcome (Plenary Room)
Introduction to the workshop (Elizabeth Johnston, Executive Director, Efus – FR)
MEDI@4SEC project (Jon Coaffee, University of Warwick – UK)
Everyday security overview (Sebastian Denef, Fraunhofer – DE)
Practical Information (Myassa Djebara, Efus – FR)

10:00 -10:40: Social media use in security actors communication tasks (Plenary Room)
Mossos d’Esquadra: communication of the terrorist attacks in Catalonia (Jordi Peña,
Social media Officer, Mossos d’Esquadra – ES)
M7 Citizen Security: Local response to the citizen’s global security needs (Gemma Navarro
Vallès & José Antonio Gallego Director Einsmer Business Designer – ES)
SOTERIA: A journey into the use of social media for urban security purposes (Alessandro
Zanasi, President Security Research and Advisory – IT)
Cities through the lens of social media: basic insights (Phan Thành Trung , Researcher, Idiap
Research Institute –CH)

10:40 - 10:50: Q&A

10:50-11:10 Short break (Plenary Room)

11:10 – 12:00 Social media use in policing tasks (Plenary Room)
We are BART! (Richard Vriesde, Police the Hague – NL)
Facebook collaboration with civil society to prevent IRL harm (Sarah Yanicostas, Public
Policy Facebook – FR)
Predictive policing is a moral technology. The case of predpol (Bilel Benbouzouid,
Sociologist, Professor at University of Paris-Est Marne la Vallée – FR)
Creating an Open Source Intelligence and Investigation Capability (Jonathan Oram,
Metropolitan Police of London – UK)
How to tackle terrorist propaganda & recruiting on social media - A network approach
(Daniela Klimpfinger, Kivu technologies – AT)

12:00 – 12:10: Q&A

12:10 – 13:10: Focus Group Discussions on themes: Communication & Engagement,
Monitoring (Intelligence, prediction and prevention) and Enforcement Session 1
(different rooms)

13:10 - 14:30: Lunch Break (Plenary Room)
14:30 - 15:30: Focus Group Discussions on themes: Communication & Engagement, Monitoring (Intelligence, prediction and prevention) and Enforcement Session 2 (different rooms)

**15:30 - 16:15:** General table / Hosts meeting

**16:15 – 17:00:** Conclusions of Theme Sessions

**17:00 - 17:40:** Drinks - End of the Workshop
<table>
<thead>
<tr>
<th>Category</th>
<th>Country</th>
<th>Organization</th>
<th>MEDI@4SEC Consortium or external delegate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Police/ENLETS</td>
<td>Denmark</td>
<td>Police of Denmark</td>
</tr>
<tr>
<td>2</td>
<td>Police/ENLETS</td>
<td>Greece</td>
<td>Hellenic Police</td>
</tr>
<tr>
<td>3</td>
<td>Police/ENLETS</td>
<td>Finland</td>
<td>Police of Finland</td>
</tr>
<tr>
<td>4</td>
<td>Police/ENLETS</td>
<td>Netherlands</td>
<td>Ministerie van Defensi</td>
</tr>
<tr>
<td>5</td>
<td>Police/ENLETS</td>
<td>Netherlands</td>
<td>Dutch Police</td>
</tr>
<tr>
<td>6</td>
<td>Police/ENLETS</td>
<td>Netherlands</td>
<td>Dutch Police</td>
</tr>
<tr>
<td>7</td>
<td>Police/ENLETS</td>
<td>UK</td>
<td>Metropolitan Police of London</td>
</tr>
<tr>
<td>8</td>
<td>Police/ENLETS</td>
<td>Netherlands</td>
<td>Dutch Police</td>
</tr>
<tr>
<td>9</td>
<td>Police/ENLETS</td>
<td>Italy</td>
<td>Guardia di Finanza</td>
</tr>
<tr>
<td>10</td>
<td>Police/ENLETS</td>
<td>Denmark</td>
<td>Police of Denmark</td>
</tr>
<tr>
<td>11</td>
<td>Police/ENLETS</td>
<td>Greece</td>
<td>Hellenic Police</td>
</tr>
<tr>
<td>12</td>
<td>Local Police</td>
<td>Spain</td>
<td>Police Zaragoza</td>
</tr>
<tr>
<td>13</td>
<td>Municipality</td>
<td>Portugal</td>
<td>Setúbal Municipality (Câmara Municipal de Setúbal)</td>
</tr>
<tr>
<td>14</td>
<td>Private Company</td>
<td>Spain</td>
<td>Einsner</td>
</tr>
<tr>
<td>15</td>
<td>Local Police</td>
<td>Italy</td>
<td>Police Regione Emilia-Romagna</td>
</tr>
<tr>
<td>16</td>
<td>University</td>
<td>France</td>
<td>Researcher Université Marne La Vallée</td>
</tr>
<tr>
<td>17</td>
<td>Local Police</td>
<td>Greece</td>
<td>Hellenic Police</td>
</tr>
<tr>
<td>18</td>
<td>Local Police</td>
<td>Germany</td>
<td>Bayerisches Landeskriminalamt</td>
</tr>
<tr>
<td>19</td>
<td>Local Police</td>
<td>Spain</td>
<td>Municipal police of Terrassa</td>
</tr>
<tr>
<td>20</td>
<td>Local Government</td>
<td>Spain</td>
<td>Ajuntament de L’Hospitalet</td>
</tr>
<tr>
<td>21</td>
<td>Government</td>
<td>Netherlands</td>
<td>Ministry of Security and Justice</td>
</tr>
<tr>
<td>22</td>
<td>Regional Government</td>
<td>Spain</td>
<td>Generalitat de Catalunya - Gabinet de Seguretat</td>
</tr>
<tr>
<td>23</td>
<td>Regional Government</td>
<td>Belgium</td>
<td>Brussels Prevention and Security department</td>
</tr>
<tr>
<td>24</td>
<td>Police</td>
<td>UK</td>
<td>College of Policing</td>
</tr>
<tr>
<td>25</td>
<td>Local Police</td>
<td>Germany</td>
<td>Police of Lower Saxony</td>
</tr>
<tr>
<td>26</td>
<td>Local Government</td>
<td>Netherlands</td>
<td>City of Rotterdam</td>
</tr>
<tr>
<td>27</td>
<td>Private</td>
<td>International</td>
<td>Atos</td>
</tr>
<tr>
<td>28</td>
<td>Regional Police</td>
<td>Spain</td>
<td>Policía de la Generalitat - Mossos d’Esquadra</td>
</tr>
<tr>
<td>29</td>
<td>Regional Police</td>
<td>Spain</td>
<td>General Police Directorat</td>
</tr>
<tr>
<td>30</td>
<td>Government</td>
<td>Netherlands</td>
<td>Ministry of Interior</td>
</tr>
<tr>
<td>31</td>
<td>Local Police</td>
<td>Italy</td>
<td>Local Police Dept. in Parma</td>
</tr>
<tr>
<td>32</td>
<td>Private</td>
<td>USA</td>
<td>iThreat® Cyber Group</td>
</tr>
<tr>
<td>33</td>
<td>Research center</td>
<td>Switzerland</td>
<td>IDIAP</td>
</tr>
<tr>
<td>34</td>
<td>Local Police</td>
<td>Netherlands</td>
<td>Police the Hague</td>
</tr>
<tr>
<td>No.</td>
<td>Type</td>
<td>Country</td>
<td>Name</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------</td>
<td>---------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>35</td>
<td>Social Media Company</td>
<td>International</td>
<td>FACEBOOK</td>
</tr>
<tr>
<td>36</td>
<td>Private</td>
<td>Italy</td>
<td>Zanasi &amp; Partners</td>
</tr>
<tr>
<td>37</td>
<td>Police</td>
<td>Slovenia</td>
<td>General Police Directorate Slovenia</td>
</tr>
<tr>
<td>38</td>
<td>Private</td>
<td>Spain</td>
<td>Eisner</td>
</tr>
<tr>
<td>39</td>
<td>other</td>
<td>Spain</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>Civil Organisation</td>
<td>France</td>
<td>Efus</td>
</tr>
<tr>
<td>41</td>
<td>Civil Organisation</td>
<td>France</td>
<td>Efus</td>
</tr>
<tr>
<td>42</td>
<td>Research</td>
<td>Netherlands</td>
<td>TNO</td>
</tr>
<tr>
<td>43</td>
<td>Research</td>
<td>Netherlands</td>
<td>TNO</td>
</tr>
<tr>
<td>44</td>
<td>Industry</td>
<td>Belgium</td>
<td>EOS</td>
</tr>
<tr>
<td>45</td>
<td>University</td>
<td>Netherlands</td>
<td>UU</td>
</tr>
<tr>
<td>46</td>
<td>Local Police</td>
<td>Spain</td>
<td>Police de Valencia</td>
</tr>
<tr>
<td>47</td>
<td>Local Police</td>
<td>Spain</td>
<td>Police de Valencia</td>
</tr>
<tr>
<td>48</td>
<td>Local Police</td>
<td>Spain</td>
<td>Police de Valencia</td>
</tr>
<tr>
<td>49</td>
<td>Industry</td>
<td>Belgium</td>
<td>EOS</td>
</tr>
<tr>
<td>50</td>
<td>Research</td>
<td>Germany</td>
<td>Fraunhofer IAO</td>
</tr>
<tr>
<td>51</td>
<td>Research</td>
<td>Greece</td>
<td>KEMEA</td>
</tr>
<tr>
<td>52</td>
<td>Research</td>
<td>Greece</td>
<td>KEMEA</td>
</tr>
<tr>
<td>53</td>
<td>Local Police</td>
<td>UK</td>
<td>Police Services of Northern Ireland</td>
</tr>
<tr>
<td>54</td>
<td>Local Police</td>
<td>UK</td>
<td>Police Services of Northern Ireland</td>
</tr>
<tr>
<td>55</td>
<td>Local Police</td>
<td>UK</td>
<td>Police Services of Northern Ireland</td>
</tr>
<tr>
<td>56</td>
<td>Research</td>
<td>Slovenia</td>
<td>XLAB</td>
</tr>
<tr>
<td>57</td>
<td>Research</td>
<td>Slovenia</td>
<td>XLAB</td>
</tr>
<tr>
<td>58</td>
<td>University</td>
<td>UK</td>
<td>Warwick</td>
</tr>
<tr>
<td>59</td>
<td>University</td>
<td>UK</td>
<td>Warwick</td>
</tr>
<tr>
<td>60</td>
<td>University</td>
<td>UK</td>
<td>Warwick</td>
</tr>
<tr>
<td>61</td>
<td>Civil organisation</td>
<td>France</td>
<td>Efus</td>
</tr>
</tbody>
</table>
Appendix 3 Workshop Evaluation

All participants were asked to complete an evaluation questionnaire at the end of the event. An overview with the average scores (n=28) is provided below.

The overall rating of the workshop, on a scale of 1 (very poor) to 10 (excellent) was 8.5. In addition, the level of agreement was quite high for almost all critical parts of the workshop assessment (5-Strongly agree, 1-Strongly disagree).

Furthermore, participants expressed their great enthusiasm about the workshop program and organization. Among other things, delegates appreciated the quality of the presentations, the interactivity of the group discussions, and the diversity of backgrounds. A few practical suggestions for improvement were also given. In addition, the consortium has begun a debrief following the event. The information collated through this exercise has been used in the planning of the next workshop.