Conducted as a part of the SOMEP project, which aims to provide vocational improvement in training services regarding the use of social media by the police:

Social Media and the Police – an Austrian Picture

Maria Schrammel, Centre for Social Innovation

March 2014

Content

Table of Figures

SOMEP has been funded with support from the European Commission. This website reflects the views only of the authors, and the Commission cannot be held responsible for any use, which may be made of the information contained therein.

Education and Culture DG
Lifelong Learning Programme

Abstract

Conducted as a part of SOMEP project, which aims to provide vocational improvement in training services with regard to the use of social media by the police, this report discusses the Austrian approach and strategies to implement social media use into Austrian police practices, since social media systems caused a societal change that cannot be ignored by the police. Hence it outlines the Austrian Cyber Security Strategy, followed by an illustration of the Austrian security research programme KIRAS and two topic-relevant projects by KIRAS. Moreover the report summariyes a number of newspaper articles, which address concrete examples of social media use by the Austrian police as well as the "social media guidelines" of the police of Wels, who use social media in daily practice.

1. Introduction

Social media systems have become interwoven with people's everyday lives, a societal change that cannot be ignored by police forces. In Europe there is little consensus on how best to integrate social media into existing police practices (Denef, Bayerl, Katein 2011:11). This report discusses the Austrian approach and strategies to implement social media into Austrian police practices.

In general social media are a bottom-up phenomenon, which means "people adopt the technology as needed, figuring out how to use it on the way" (Denef, Bayerl, Katein 2011:12). Police forces who follow this bottom-up approach enable their officers to use e.g., Twitter or Facebook mostly without restrictions and provide them with a high degree of freedom. However it allows some control over who uses social media and how (Denef, Bayerl, Katein 2011:12). The other approach would be a top-down strategy, which would require general guidelines to be put in place before social media are rolled out. Denef et al. explain: "These guidelines target the entire force and prescribe how officers can (or should) deal with social media in their daily work" (Denef, Bayerl, Katein 2011:12). This way of using social media aims to safeguard police against the potential threats of unfettered and uncritical use. But such guidelines do have some disadvantages. Developing such guidelines can take a long time and "require continuous updates to keep in line with social and technological developments" (Denef, Bayerl, Katein 2011:13).

The social media landscape is constantly changing. Consequently police offices are picking only the most popular services such as Facebook or Twitter (Denef, Bayerl, Katein 2011:13). A selection of Austrian newspaper articles seem to imply that the Austrian police seem to follow this selective approach and pick only the most popular social networks to work with (Kurier, DiePresse, Krone, derStandard, Kleine Zeitung).

Denef et al. (2011) emphasise the fact that the most common purpose of social media is still the informational use. It enables police to spread information about recent crimes, traffic accidents, and missing people among Austrian citizens in real time. "Generally, these messages are linked to a request for help from the public – with often very positive results" (Bayerl, Denef, Katein 2011:13f.).

With the focus on the interlink between social media and police, this report discusses first the

Austrian Cyber Security Strategy (ACSS) followed by an illustration of the Austrian security research programme KIRAS, which carries out future research on social media and crime and the use of social media services for crime prevention (URL 1; URL 2). The description of two projects by KIRAS will provide insight into Austrians' research on social media crime and the preparation of study results to develop new police investigation strategies to prevent cyber-crime or use cyber space and social media services to fight crime in general. After discussing these projects, the report outlines a summary of newspaper articles, which address concrete examples of social media use by the Austrian police. This is followed by a demonstration of a police department in Wels, Upper Austria, which already officially started to use social media in its daily practices.

2. Supporting Policy Framework

2.1 Action Field - The Austrian Cyber Security Strategy

About three quarters of Austria's population use the internet regularly, half of this group on a daily basis (Bundeskanzleramt 2013: 4). Attacks from cyberspace pose not only a direct threat to Austria's safety, but also to the proper functioning of the state, economy, science and society. Cyberspace may be misused for various purposes by non-state actors, like criminals, organized crime or terrorists, as well as by state actors, like secret services and the military. Because threats in cyberspace as well as productive use of it are practically unlimited, it is a top priority of Austria to make this space sufficiently safe and secure at national and international level (Bundeskanzleramt 2013:4).

The concept of "Cyber Security" has taken on great significance. Threats caused by the new cyberspace have increased enormously over the past years. These risks affect individuals and state or economic institutions alike in Austria. Moreover new types of criminality have developed, which leads to a need for increased juridical and technical knowledge requirements of staff and, as a consequence thereof, new training requirements in professional environments (Sicherheitsbericht 2012:220).

The resolution of the Council of Ministers in May 2012 delegated the Federal Government to provide a national Cyber Security Strategy by the end of 2012. The acquired draft was adopted by the Federal Government in March 2013. The planning of the implementation followed. Every two years, an implementation report has to be prepared (Sicherheitsbericht 2012:220).

The Austrian Cyber Security Strategy (ACSS) is a comprehensive and proactive concept for protecting cyberspace and the people in virtual space while guaranteeing human rights. But above all it will build awareness and confidence among the various levels of Austrian society (Bundeskanzleramt 2013:4f.).

The ACSS includes opportunities and risks in cyberspace, principles of cyber security, strategic

goals, fields of action, as well as measures and implementation of these strategies.

The ACSS cites five main opportunities that cyber space enables:

- Information and communication space
- Space for social interaction
- Economic and trade space
- Space for political participation
- Control space

Besides these opportunities cyberspace provides, there are several risks and threats ranging from "operating errors to massive attacks by state and non-state actors using cyber space as a venue for their activities" (Bundeskanzleramt 2013:6). Cyber-crime such as identity fraud, cyber-attacks or misuse of the internet for extremist purposes is a serious new challenge facing all of the stakeholders affected. Governmental and non-governmental bodies need to cooperate at national and international level (Bundeskanzleramt 2013: 6)

The spectrum of these risks and threats is presented in the Cyber Risk Matrix in figure 1.

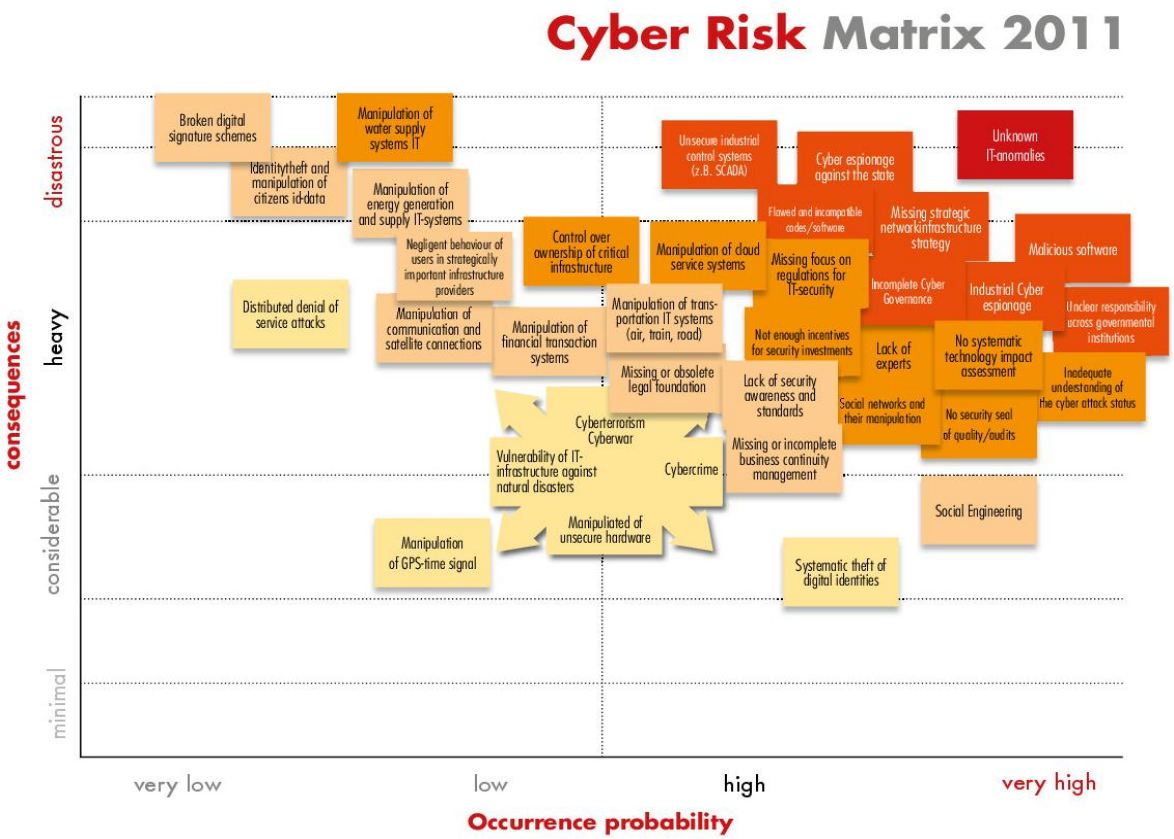

Figure 1 Cyber Risk Matrix 2011

2.1.1 Strategic goals

In a continuously developing digital society like Austria's, it is vital to ensure compatibility with the fundamental values of an open society. The dynamic and virtual space serves as a basis for information exchange and social and political participation. It facilitates social prosperity and economic benefits in the framework of e-government and e-commerce (Bundeskanzleramt 2013:9).

Within the scope of the Cyber Security Strategy, Austria pursues the following goals (Bundeskanzleramt 2013:9):

- Availability, reliability and confidentiality of data exchange as well as integrity of data themselves can only be ensured in a secure resilient and reliable cyber space. ICT systems should be as redundant as possible.
- Austria will ensure that its ICT infrastructures are secure and resilient to threats
- The legal asset "cyber security" will be protected by the Austrian authorities in cooperation with non-governmental partners.
- Austria will implement a "culture of cyber security" by taking a number of awareness measures.
- Austria will act as a pioneer in implementing measures to secure the digital society.
- Austria will play an active role in international cooperation at European and global level.
- The Austrian administration's e-government is secure and will be continuously further developed.
- All Austrian enterprises will protect the integrity of their own applications and the identity and privacy of their customers.
- The Austrian population should be aware of the individual's personal responsibility in cyber space.

2.1.2 Implementation

After the adoption of the ACSS by the federal government, a Steering Group developed an Implementation Plan to carry out the horizontal measures laid out in the ACSS within three months. The competent bodies are responsible for implementing these measures within their respective mandates. The implementation is coordinated by the Cyber Security Steering Group. Every two years the Cyber Security Steering Group will submit an Implementation Report to the federal government. Moreover the Austrian Cyber Security Strategy will be continuously reviewed and updated if necessary (Bundeskanzleramt 2013:17).

One of the strategies, as mentioned above, will be to strengthen Austria's research in the area of cyber security. In the framework of Austrian and EU security research programmes, cyber security must be among the key research priorities (Bundeskanzleramt 2013:15). Austria strives for an active thematic leadership in EU security research programmes: the Austrian security research

programme KIRAS, which is described in the following chapter, is considered as a forerunner in European security research. It also carries out projects which will be essential in developing police investigation methods for cyber-crime prevention in Austria (URL 1).

2.2 Policy Framework - Austrian Security Research Programme KIRAS

Austrian's security research programme is called "KIRAS". The name is derived from Greek and means "circle of security". KIRAS, an interdisciplinary, multidimensional and integrative programme is a pioneer in the field, having become, in 2005, the first security research programme in Europe. Hence the European security research programme was essentially modelled after KIRAS (Reiter 2007:84; KIRAS 2011: 5).

KIRAS is coordinated as a national framework programme and distances itself from military armaments research but includes social and cultural as well as scientific aspects in its programme. Thus the term "security" in the programme refers to non-military, economical, ecological, cultural and social dangers and risks (Reiter 2007:84). It also refers to measures of public authorities to preserve and enhance public security (KIRAS 2011:4).

Strategic goals of KIRAS (Reiter 2007:84; KIRAS 2011:4f.):

- Enhancement of security and security awareness
- Production of for security policy required knowledge
- Growth of national safety economy
- Establishment and development of excellence in the field of security research
- Consideration of social issues in all aspects of security research

To reach these goals, already established governance structures led by the "Federal Ministry of Transport, Innovation and Technology" (bmvit) and including Federal Ministries, social partners and "Research Technology and Innovation (FTI) actors" are used (KIRAS 2011:5).

2.2.1 Social Media Research Projects

As in the Austrian Cyber Security Strategy outlined above, cyber security issues must increasingly be taken into account in applied cyber research and in security research programs such as KIRAS (Bundeskanzleramt 2013:15). Consequently a number of cyber-relevant research projects are emerging.

KIRAS carried and carries out a total of 45 projects. There are only two regarding social media crime and the use of social media by the police and other security organisations. These projects will be presented in the following sections. The first project plans to outline a structural analysis of criminal investigation-relevant aspects in social media (URL 1). The other, which for the purposes of this report is the more important one, "SMD4Austria identifies and analyses international experience,

outstanding projects, as well as risk of social media services and creates concept models for implementation" (Rainer et al. 2013: 115). In addition, they focus on chances, opportunities and risks in the use of social media by the security sector (URL 2).

2.2.1.1 KIRAS Project: Social Media Crime

The rapid spread and use of social media (e.g. microblogs such as Twitter, social networks like Facebook and video sharing portals like YouTube) lead to an increase of criminal activities in this dynamic interaction space. On the one hand, a displacement of known offences like fraud can be identified; on the other hand, new types of crime caused by social media arise. "Criminal mobs" or "identity theft" are only two examples. According to the experts of this study the list of legal relevant activities expands continuously. Police and juridical authorities are confronted with new challenges and terms such as "cyber-grooming", "profile cloning", "social engineering", "cyber-stalking", "cyber-bullying", "crime mobs", "identity theft", and more.

Currently in Austria there is no structural foundation available for the criminal investigation of the aforementioned phenomena made possible through the use of social media. To conceptualise appropriate strategies for this new field of criminality, proponents of this project advocate for structured analysis and categorisation combined with the development of a "method grid" as essential to filling this void.

The project "Social Media Crime" is going to accomplish a comprehensive study of the topic area in its entirety. The study will be of importance for the Austrian Ministry of the Interior and especially the Austrian Federal Crime Police Office. Through scientific research and surveys the researchers will prepare a thorough analysis of single instances of social media crime and activities. The results will give information about the manifestation, reasons and consequences of social media crime as well as characteristics of victims and perpetrators. They will be structured and categorized according to the needs of Austrian criminal investigations. Furthermore this categorisation will outline prevention and counter-measures which are already introduced or planned at international level. The gained insight will lead to the preparation of concrete recommendations for action, and criminal investigation in Austria will be supported to sustainably stem social media crime. The Austrian Centre for Law Enforcement Sciences (ALES) will be a project partner and contributes extensive juridical expertise to the project. Concrete statements about the legal situation concerning these phenomena in Austria will be made and conspicuous gaps in law will be spotlighted. At the end of the study the grid together with the collected case studies will be interactively edited and will be made available for the target groups (URL 1). This project is currently under implementation and will be finished by September 2014.

2.2.1.2 SMD4Austria – Social Media Services for Security and Prevention in Austria

SMD4Austria is concerned with opportunities social media services provide, such as strategic acquisition and exploitation of information, communication and interaction of security organisations with citizens, media and other crisis management organisations, to support security

and criminality prevention (URL 2). SMD4Austria planned to make these opportunities usable for the Federal Crime Police Office and other organisations for security and crime prevention in Austria (URL 2). On behalf of KIRAS and the Federal Ministry of Transport, Innovation and Technology the projects goal is to obtain results that can shed light on the advantages of social media services by taking into account international experiences of them and an overview of the technical possibilities, the opportunities for validation through verifying user acceptance and juridical aspects, a potential decision basis for effectiveness, the potential economic uses of resources for social media services and the presumed innovation jump regarding prevention, investigative and explanatory work (Rainer et al. 2013a; URL 2). Moreover they developed appropriate implementation concepts and thus developed the requirements for further usage of social media services by Austrian security organisations (Rainer et al. 2013 115; URL 2).

SMD4Austria has found that social media can basically be applied in three major fields. Each of them has its specific opportunities and risks. These three major fields of application in crisis interaction are discussed in the following section (Rainer et al. 2013: 115f.):

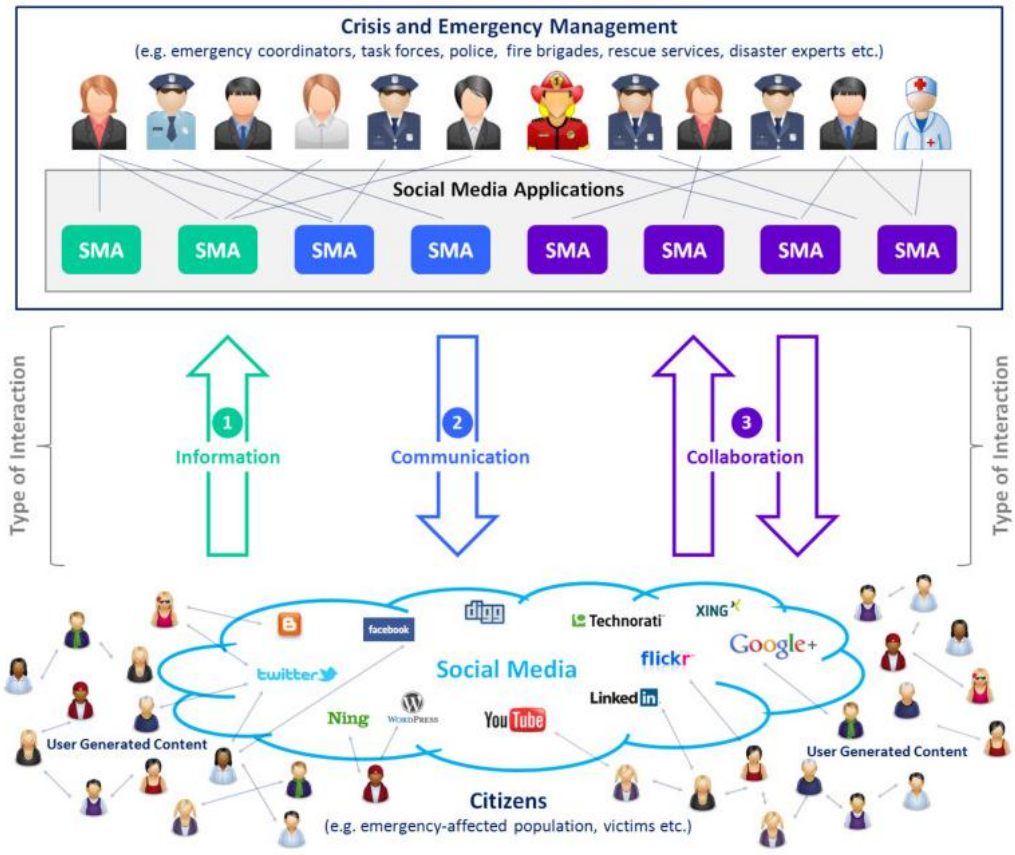

Figure 2 Crisis and Emergency Management

- Information
  Relevant information from the social media cloud is gathered and used by security organisations. This involves the collection, filtering, aggregation, and visualisation of data.

- Communication
  Social media is mainly used as a simple communication channel. Its purpose is the mere dissemination of information. In times of crisis this channel plays an even more important role "since traditional infrastructures might be damaged and the advancement of the mobile broadband has made social media sites almost available from any place", according to Rainer et al. 2013.

- Collaboration
  The third form of interaction, enabled by social media, points out the bidirectional information exchange between emergency managing organisations and citizens. Rainer et al. 2013 argue: "The services aid in making the interaction more systematic, but yet the collaboration activities are characterized by a comparable high demand for human resources, since the responses to individual entries cannot be automated and in many cases multiple feedback loops are necessary."

These three fields of social media application are complementary. A holistic crisis communication strategy needs to incorporate all three. According to Rainer et al. 2013, the information-gathering function is the most fundamental one even though it is the most neglected one (Rainer et al. 2013: 118).

In Figure 3, SMD4Austria shows Austria's actual situation and the future of modern security organisations based on these three fields of social media application:

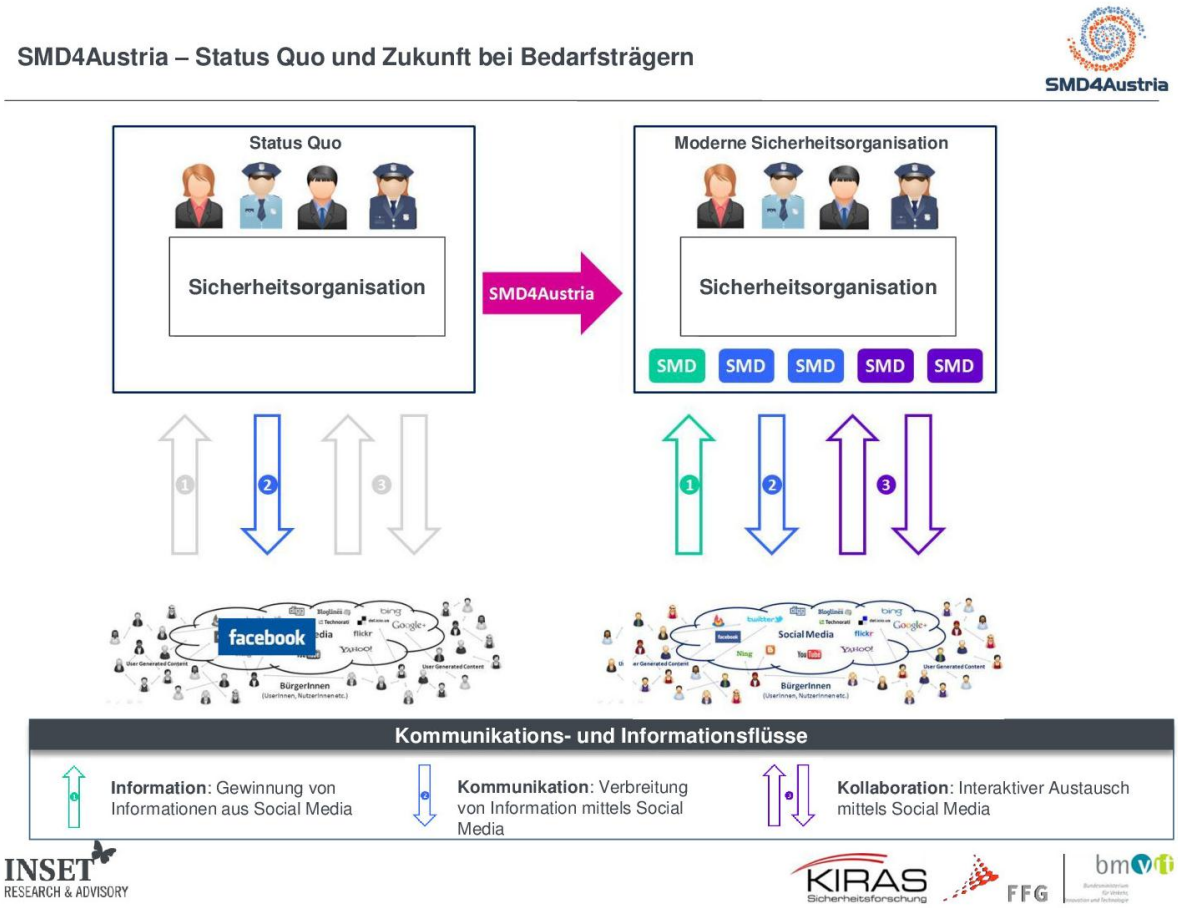

Figure 3 SMD4Austria – Status Quo und Zukunft bei Bedarfsträgern

To develop a comprehensive list of criteria to evaluate social media services, which could then be applied in different security organisations, SMD4Austria compiled the data through a survey distributed to experts, citizens, and the Federal Crime Police Office (Rainer et al. 2013a.).

SMD4Austria emphasises that only through a detailed analysis of different social media services can potential threats and difficulties, such as a lack of citizen acceptance of the use of social media by security organistaions, be minimised. Hence it is necessary to carry out pre-analyses of the services from the ethical, juridical and user-centered perspectives (Rainer et al. 2013a).

3. Social Media and the Austrian Police

However, by now any systematic evaluation or any other research in this field exists, the following section relies purely on anecdotal evidence gathered from newspaper articles. Furthermore, evidence was gathered from one police office in Upper Austria that officially uses social media in

investigations (URL 3). This chapter will present a summary of the cases outlined in different newspapers, as well as a short presentation of the Upper Austrian police office's social media investigations.

3.1 Austria's police officers using social media

The Austrian newspaper "Die Presse" (Feb. 2014) considered the question to which extent the Austrian police are using social media and what legal limitations are currently in place. According to this news outlet, compared to the United States or Great Britain, where official news is immediately published on Twitter or Facebook, the Austrian police do not much rely on social media. But the Austrian police do use social media for investigations. For example, the Federal Criminal Police Office as well as the police of Vienna opened their own Facebook accounts, which are used to search for criminals by the use of photos from security cameras or by personal description. The Austrian citizens appreciate the social media presence by the police, according to the newspapers (DiePresse 02.02.2014).

From this article one can deduce that Austrian police indeed are using social media, especially social networks for investigations. But the article outlines that when it comes to using social media for professional purposes on private police officers' accounts, there are narrow limits (DiePresse 02.02.2014). The case of a young police officer who posted a missing person notice on the internet – including on her private Facebook site - led to discussions about Austrian's privacy policy. The article emphasises the fact that the notice had previously been published by the police, so she did not break the law. However, besides infringements against penal law, she could have been blamed for malpractice (up to five years in prison) or violation of official secrecy (up to three years). But in the end, she was not blamed for anything; instead she was praised as a dedicated police officer, according to the sources (DiePresse 02.02.2014).

Another article from the newspaper "Die Presse" (2013) also concerns the case of the police officer who posted the missing person notice. This article emphasises that the problem of the use of social media by the Austrian police is a "grey area" and is not clearly defined, pointing out that this was a particularly delicate situation because of the need for data privacy and the allegations of malpractice (DiePresse 29.12.2013). Furthermore the article discusses Austrian police officers' access to social media. According to this article, police spokesman Furtner assured journalists that Facebook is inaccessible on police computers throughout Austria, especially after the case of the Upper Austrian police officer. Today, only 150 police computers are unlocked, which is, however, sufficient for hidden investigations using social networks (DiePresse 29.12.2013).

Besides the story about criminal investigation on social media, the prohibition for Austrian's police officers to use social networks is discussed in the next article from "Kleine Zeitung" (2010). Kleine Zeitung emphasises the efficient usage of social networks for crime investigation in Austria's neighbor countries, and coincidently they cavil about the Austrian police being locked out of Facebook, Twitter & Co. They point out that around 16,000 police computers were locked in 2010. Kleine Zeitung cited Rudolf Gollia, spokesman of the internal affairs ministry in 2010, who argued

that the Federal Criminal Police Office prevents private use of social media by police officers during working hours. For example, they aim to prevent possible misunderstandings, which could be caused by private postings. (Kleine Zeitung 23.02.2010).

Another article published in August 2013 in the newspaper Kurier is concerned with social network pages by the police and their use for manhunts. This article outlines the former use of social networks by the police to provide security tips or links to citizen service institutions as well as events by the police. Moreover there have already been concrete hints concerning Internet criminality or burglary – but daily happenings are not supposed to be told through Facebook, Twitter and Co., according the article. What changed in August 2013, was that from then on there have been direct links to actual manhunts of missing persons and alleged criminals by the Federal Criminal Police Office, according to Kurier. Moreover they reported that users can find pictures of missing(?) people and a short description of the record as well as the link to the investigation site of the Federal Criminal Police Office (Kurier 2013).

The Upper Austrian police office in Wels uses social media for their investigation work and developed a social media guideline for their police officers. The next chapter summarises this guideline. .

3.2 Social Media use by the police of Wels, Upper Austria

The Upper Austrian police in Wels aim to react to the changes in society caused by social media. So they developed a guideline in social media usage for their officers, which states how police officers can and should use social media and what the limits are. Thus the guidelines illustrate chances and risks and demonstrate some of the possibilities police officers in Wels have discovered through the appropriate use of social media (URL 3).

The police of Wels see a great opportunity arising through new media. They highlight the participative character of social media, which allows for contact between different groups inside and outside of the police through feedback channels (URL 3).

According to the police of Wels, there is no need to designate a spokesman for social media, as each message sent by police officers is the responsibility of the whole police bureau. Nevertheless, it is important that the "official communication" of the police of Wels is divided from informal information, or the personal opinion of individuals. The online and social media activities of the police involve information, communication and interaction with all relevant target groups in the web. They work with the following channels: the social media newsroom (www.cop4wels.at) as well as the social media platform Facebook (www.facebook.com/cop4wels), Twitter (www.twitter.com/cop4wels) and Google+ (pluy.google.com/cop4wels). Through these activities the police aim to become connected with target groups and to provide relevant information and services through social media (URL 3).

Regarding private and vocational use, the guideline points out that postmodern communication

blurs borders between private and vocational communication. The Police station of Wels emphasises that they choose to trust the police officers to distinguish when to post private messages and when it is appropriate to do so vocationally; to choose the right language and right pictures; and to retain data privacy. Moreover the guidelines for the police officers in Wels outline communication strategies which, for example, explain how to deal with criticisms and how to react to them (URL 3).

The social media guidelines of the police station in Wels also discuss data privacy and copyright law. They underline that data privacy and confidentiality are essential elements they always consider. Not only data privacy, but also copyright law plays an important role in the use of photos, texts or videos. The guidelines underline the need to always consider these laws (URL 3).

4. Summary and Conclusion

Threats caused by the new cyberspace and risks that affect not only individuals but also state and economic institutions in Austria have caused the issue of cyber security to take on greater significance on the national stage. Thus, in May 2012 the council of ministers delegated the Federal Government to develop a national Cyber Security Strategy (Sicherheitsbericht 2012:220), which is called the "Austrian Cyber Security Strategy" (ACSS). This strategy is a comprehensive and proactive concept developed to protect people in cyberspace and to continue to ensure human rights. Moreover it builds awareness and confidence among Austrian society (Bundeskanzleramt 2013:4f.). The ACSS takes into account the opportunities and risks in cyberspace, principles of cyber security, strategic goals, fields of action and measures for implementation of these strategies (Bundeskanzleramt 2013).

Among the seven fields of action, one focusses on research and development. In the framework of the scope of research regarding Social Media and Police in Austria, this field plays an important role. The paragraph regarding this field emphasises the importance of increasingly taking cyber security into account in applied cyber research and in security research programmes like KIRAS (Bundeskanzleramt 2013:15). As previously mentioned KIRAS, the Austrian security research programme, which is said to be a forerunner for European research programmes, is of particular importance. Besides cyber security research projects, KIRAS implemented two projects regarding social media and crime as well as social media service use for security organisations (URL 1; URL 2). These projects outline strategies to help Austria react to the societal changes caused by social media. SMD4Austria even talks about a "modern security organisation" that effectively uses social media services in all three fields of action (information, communication, collaboration) (Rainer et al. 2013a). The results as well as the aim of their study outlined that Austria's security organisations do not use these possibilities yet. Hence international best practice examples have been adduced to develop security and prevention strategies through the usage of social media services for Austrian security organisations (Rainer et al. 2013a).

Some newspaper articles provide insight into the ongoing discourse about how Austrian police uses

social media in their occupational daily routines and which problems they face. From the newspaper articles, one can deduce that the Austrian police follow a top-down approach, which requires a clear guideline similar to the one that the police bureau of Wels has developed (URL 3). In 2010 the Austrian Federal Criminal Police Office decided to lock all but 150 police computers. According to Austrian newspapers, they tried to prevent misunderstandings caused by private usage of social media and they underlined that 150 authorized police officers are enough to use social media for crime investigation (DiePresse 2014; Kliene Zeitung 2010; Kurier 2013).

Besides the information of these newspapers there is one police office in Wels which already uses social media for their police work. The guideline for their officers, which outlines risks and opportunities social media provides for them and how the officers should act when using new media (URL 3), points out an top-down approach of Austrian's police.

In conclusion it can be said that Austrian police, compared to other European countries that have already implemented social media in their police forces, has just started to develop clear strategies, methods and guidelines to use social media in their practice. The security research programmes, which support this development, focus on international best practice examples to reach an optimal implementation strategy for Austria. In Austria a detailed analysis of social media services, which include a pre-analysis from the ethical, judicial and user-centralised perspective, plays an important role and should prevent potential threats and difficulties.

5. References

Bundeskanzleramt (Hg.) 2013: Austrian Cyber Security Strategy. BM.I Digitalprintcenter. Vienna http://www.bmi.gv.at/cms/BMI_Service/cycer_security/130415_strategie_cybersicherheit_en_web.pdfR

BAYERL, Petra Saskia; DENEF, Sebastian; KAPTEIN, Nico 2011: Cross-European Approaches to Social Media as a Tool for Police Communication. In: European Police Science and Research Bulletin. Issue 6. 2011/12. European Police College. Published Online. https://www.cepol.europa.eu/fileadmin/website/Research_Science/Bulletin/06_EPSR_BULLETIN.pdf

DiePresse: Was die Polizei auf Facebook macht. 02.02.2014. http://diepresse.com/home/panorama/oesterreich/1556990/Was-die-Polizei-auf-Facebook-macht

DiePresse: Vermisstensuche über Facebook: Konsequenzen für Polizistin? 29.12.2013 http://diepresse.com/home/panorama/oesterreich/1511680/Vermisstensuche-uber-Facebook_Konsequenzen-fur-Polizistin

HUBER, Edith 2011: Cyberstalking. Österreichweite Studie zum Cyberstalking Verhalten. In: KIRAS 2011: KIRAS Sicherheitsforschung. Wissenschaf(f)t Sicherheit Fachtagung Sicherheitsforschung 2011. Tagungsband. http://www.kiras.at/fileadmin/dateien/allgemein/tagungsband/KIRAS2010Ansicht.pdf

KIRAS 2011: KIRAS Sicherheitsforschung. Wissenschaf(f)t Sicherheit. Geförderte KIRAS-Projekte 2009-2011. www.kiras.at/fileadmin/dateien/2011Kiras_kl.pdf

Kleine Zeitung: Facebook-Verbot: Polizei sperrt Freunde weg. 23.02.2010 http://www.kleinezeitung.at/allgemein/multimedia/2299474/facebook-verbot-polizei-sperrt-freunde-weg.story

Kurier: Wiener Polizei fahndet ab sofort auf Facebook. 08.08.2013 http://kurier.at/chronik/oesterreich/wiener-polizei-fahndet-ab-sofort-auf-facebook/22.116.982

RAINER, Karin; JÄGER, Bernhard; POLT, Wolfgang 2013: Social Media und Social Media Analysen im Spannungsfeld von Sicherheit, Ethik und Datenschutz – Anwendungspraxis im Projekt SMD4Austria. 13. Österreichische TA-Konferenz. Österreichische Akademie der Wissenschaft http://www.oeaw.ac.at/ita/fileadmin/redaktion/Veranstaltungen/konferenzen/ta13/praes/ta13-rainer.pdf

RAINER, Karin et al. 2013a: Social Media Application in Crisis Interaction. Systema. 2013. Volume 1. Issue 1. p. 111 – p-127

REITER, Erich et al. 2007: Sicherheitsforschung in Österreich und in Europa. Vergleichende Studie

europäischer Sicherheitsforschungsansätze. In: KIRAS 2009: KIRAS Sicherheitsforschung. Wissenschaf(f)t Sicherheit. Ergebnisse bisheriger Untersuchungen. http://www.kiras.at/fileadmin/dateien/allgemein/studien/KIRAS%20Studien%202009.pdf

Sicherheitsbericht 2012: Bericht des Bundesministeriums für Inneres über die innere Sicherheit in Österreich. http://www.bmi.gv.at/cms/BMI_Service/SB_2012/1_Sicherheitsbericht_2012.pdf

URL 1: http://www.kiras.at/gefoerderte-projekte/detail/projekt/social-media-crime/

URL 2: http://www.kiras.at/gefoerderte-projekte/detail/projekt/smd4austria-social-media-dienste-fuer-sicherheit-und-praevention-in-oesterreich/

URL 3: http://www.cop4wels.at/social-media-guideline-cop4wels/