Innovative Approaches and Solutions to Understand, Identify and Tackle Social Media Crime

Bernhard Jäger
SYNYO Research
Vienna, Austria
bernhard.jaeger@synyo.com

Peter Leitner
SYNYO Research
Vienna, Austria
peter.leitner@synyo.com

Abstract

The dramatic rise of social media sites like Facebook, Twitter and YouTube in the last decade have also led to a marked increase in criminal activities and offences in such interactive spaces. These so called social media crimes include a wide range of phenomena such as spamming and defrauding thousands of people or arranging sexual contacts with minors. The authors of this paper developed a classification scheme based upon four clusters: Social Hacking, Social Scamming, Social Insulting and Social Agitating. Built upon and supported by an extensive analysis a framework was built which allows to group particular phenomena and built the mentioned clusters in a comprehensible way. Resulting from this classification scheme this paper elaborates further on a) how social media is mainly used within a particular crime phenomenon and b) prevention and identification strategies for social media crime.

Keywords: social media crime, crime prevention, crime identification, social media, taxonomy

Introduction

Criminal activities in social media have been increasing ever since social media platforms and channels emerged. Doubtlessly, social media channels are advantageous because they offer a relatively uncomplicated, interactive and collaborative form of communication. However, they also provide space for criminal activities (Frank et al., 2011; Loizou, 2012). New social media-specific forms of delinquency arose in the last years, which can generally be defined as follows: *Social media crime comprises criminal activities committed against individuals or groups of individuals where social media such as social networking, microblogging or media sharing sites play a crucial role (Leitner, 2013).*

Due to the high dynamics of social media crimes, law enforcement agencies and legal actors in charge, permanently face new challenges in handling respective cybercrime-related phenomena such as Cyber Mobbing (e.g. Fawzi, 2009), Cyber Bullying (e.g. Hinduja et al., 2008), Cyber Grooming (e.g. O'Connell R., 2003), Cyber Stalking (e.g. Thapa and Kumar, 2011), Social Phishing (e.g. Coronges et al., 2012). Therefore, a case-related treatment and analysis of social media crimes and respective phenomena was conducted. The result of it was, as proposed in "A flexible categorization model for contemporary crime types in social media" (Leitner et al., 2014), a scientifically sound, case-related, and flexible taxonomy for the systematic classification and evaluation of social media crimes.

However, this comprehensive taxonomy of social media crimes and related phenomena requires further investigation on crime classification. Furthermore, practice-oriented strategies and methods to prevent and counteract social media crimes, including legal evaluation and advice, are still needed and therefore addressed in this paper.

Methods

The categorisation, approaches and solutions which are presented in the following chapters are outcomes and side products of the Social Media Crime project which was funded through the Security Research Funding Programme (KIRAS) by the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT). To gain a better understanding on potential crime phenomena in social media a comprehensive desk research was conducted. The research included systematic analysis of literature, statistical data, country specific references, press articles, websites and blogs. Especially for web-based search extensive keyword lists were used to identify relevant content. For further analysis a structured overview of existing cases was needed. Therefore over 200 particular cases were collected from the found materials. Finally more than 50 cases were selected based on minimum criteria including information about offence, offender, victim and evidence. Important for the selection was also a high variety between the cases which were systematically categorised and analysed. The given information allowed to compare cases, identify differences according approaches of offenders and characteristics of victims and criminals. This approach allowed also to take a closer look on actions and methods of offenders when making use of social media. Based on this information and a clustering of the found cases the first social media crime taxonomy was developed. In addition also the legal situation (in Austria) was analysed for each case. In a later step this was crucial to identify legal loopholes and make recommendations for updating existing laws. Furthermore semi-structured interviews were conducted with members of police forces and organisations such as NGOs that work together with the law enforcement agencies to ensure public awareness on cyber crime. The interviews aimed to gain a better understanding on the current state of knowledge of the interviewees and their

https://aisel.aisnet.org/pajais/vol7/iss4/2
DOI: 10.17705/1pais.07401

organisations about criminal activities in social media, how they deal with it and if there was any form of categorisation they currently use internally for such cases. With a questionnaire a general understanding on the current understanding of social media crime among police forces as well as researchers and NGOs revealed feedback from over 12 countries and showed that social media crime in general is hardly recognised in any statistics. However, the questionnaire also asked if law enforcement agencies (as well as connected organisations and researchers) would need a better understanding about criminal phenomena that take place in social media. The analysed feedback revealed that a majority of respondents sees the need for more information that may help to identify such phenomena and develop prevention strategies. The size of the project did not allow creating sample sizes for interviews and questionnaires that enable statistical significance testing. Interviews and the questionnaires were of explorative nature and designed to set-out the research field, especially for further research activities that may take a closer look on particular problems (e.g. improving crime statistics, need for trainings and materials for professionals dealing with social media crime, supporting public awareness on the issue and foster organizations that work together with law enforcement agencies to report criminal activities in social media). However, the information gathered in the interviews and questionnaires combined with the created taxonomy allowed to draft new approaches to prevent and act against social media crime. Further research of the presented approaches will be needed to evaluate their practical applicability.

Categorization of Social Media Crime

Due to the rapid dissemination and emerging use of social media in recent years, the number of criminal actors misusing social media services has been on the rise, and a further increase of offenses is to be expected (Marinos and Sfakianakis, 2012). These actions are labeled as isolated or grouped phenomena and various synonyms are often used incorrectly by different stakeholders. The proposed taxonomy is built upon and supported by extensive analysis and experimental study clustering techniques (Leitner et al., 2014). Thus, the following four crime types (clusters) were defined in the field of social media:

Social Hacking: This cluster and its containing phenomena are defined by the need for information on victims and potential targets. Offenders may use both legal and illegal methods. Former can be simple searches for public available information, while the latter deals with account hacking, password theft, likejacking, fake apps or social engineering.

Social Scamming: Offenders try to trick or blackmail their victims into financial transactions, and executing illegal tasks or linking them to doubtable online offers. In most cases there exists no previous relationship between victims and offenders. Social media within this cluster is used to find and lure victims, but not for the actual transactions. Some examples include love scams, gift carding or skype blackmailing.

Social Insulting: Phenomena in this cluster specifically target single individuals with the aim to inflict harm on the victim. Well-known phenomena include cyber mobbing, cyber stalking or cyber grooming. Acquired evidence has shown that even within one phenomenon there is a vast amount of different techniques used.

Social Agitating: This includes phenomena like cyber radicalism, criminal hacktivism or crime mobs. Cases in this cluster are focused on civil obedience and social disturbance. In most cases there is more than one offender who use social media for distributing content and to mobilize the crowd.

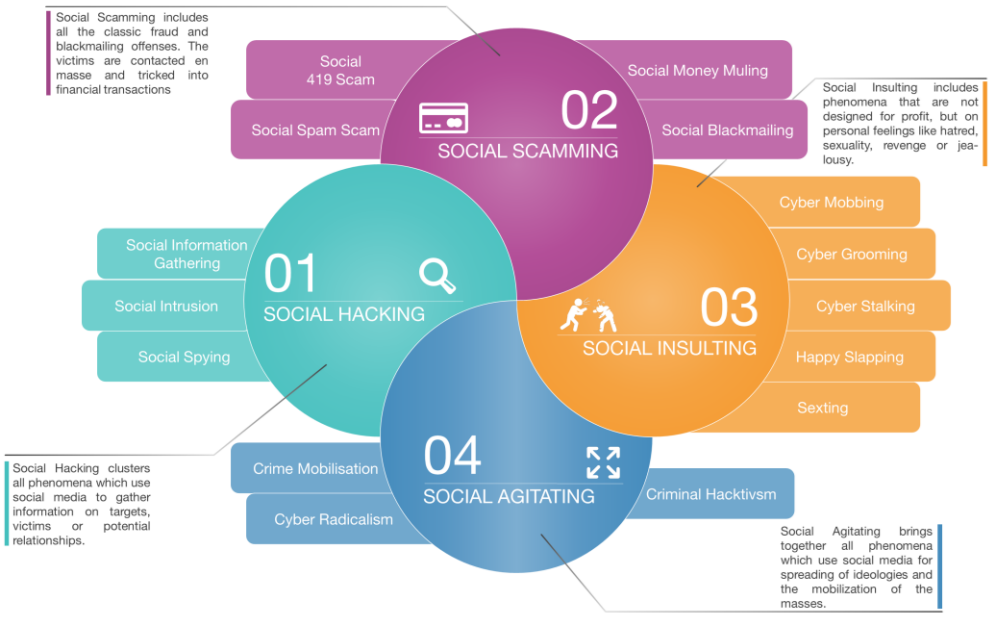

Figure 1 - Social Media Crime Taxonomy (prepared by SYNYO)

To create the taxonomy shown in figure 1 a comprehensive analysis of particular phenomena and underlying actions was performed. As there was no existing standard how criminal phenomena in social media can be structured a novel so called Social Media Crime Framework was established. This framework is based on the idea that each of the identified phenomena is based on a set of actions that are performed by criminals. Singular actions don't have to be criminal acts per se but can appear together with criminal actions. For instance 'mass distribution' (e.g. of messages) is an action that usually is utilised by Scammers. Further actions used in this phenomenon may be 'identity faking' and 'manipulation of individuals to transfer money'. Based on breaking down each phenomenon to particular actions the Social Media Crime Framework allows to compare found phenomena and make them comparable. Thereby it can be shown that some phenomena make use of similar actions. Such phenomena can be grouped and presented as clusters (as shown above). To isolate particular actions, find similarities and differences, build phenomena and group them to clusters over 200 reported crime cases were identified and analysed. Social Media Crime is a highly dynamic field and it is very likely that new phenomena will appear. The current approach allows experts to easily extend the current taxonomy on all levels (add new actions, define thereby new phenomena and build new clusters if relevant).

Figure 2 shows in detail which of the 21 identified actions were allocated based on the analysis to the 15 isolated Social Media Crime Phenomena. There is also a more detailed list of actions available which shows different modifications of actions. To allow a better overview figure 2 only focuses on the main actions and their relation to particular phenomena.

https://aisel.aisnet.org/pajais/vol7/iss4/2
DOI: 10.17705/1pais.07401

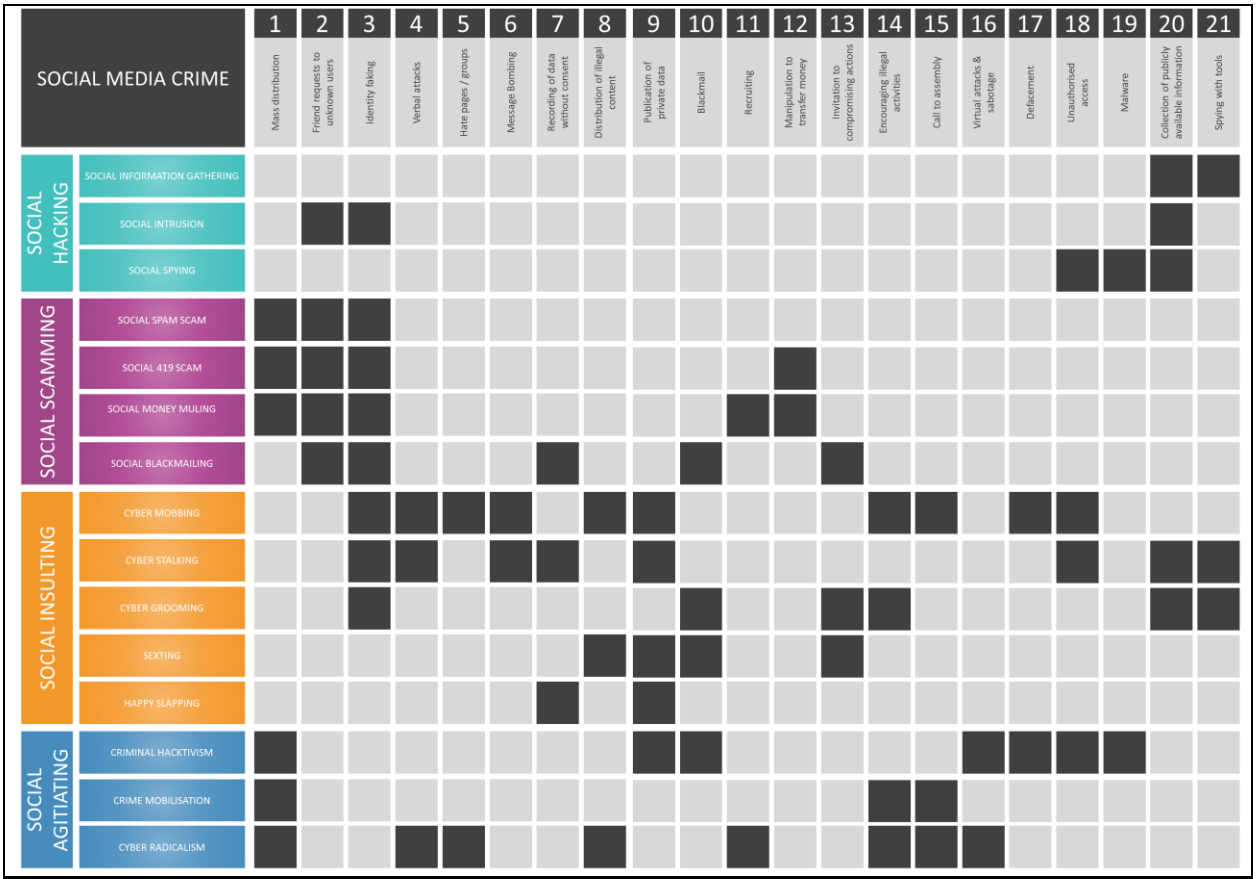

Figure 2 - Social-Media-Crime-Matrix (prepared by SYNYO)

The described approach does not only allow to structure existing phenomena but shows also how social media is mainly used within a particular crime phenomenon. The method presented below elaborates how social media is used within a crime phenomenon. The following four types for media usage were identified:

- **Information**: Social Media is used to gather information about a person / group / movement.
- **Contact**: Social Media is used to get in touch with a person / group / movement.
- **Execution**: Social Media is used to commit offenses.
- **Distribution**: Social Media is used to spread information to a wider audience.

Based on the discovered social media crime types different trends and approaches of social media usage for criminal activities are identified and structured:

- **Social Hacking** uses social media mainly for information gathering. However in cases of Social Intrusion and Social Spying Contacting (C) and Executing (E) are also significant components.
- **Social Scamming** is the cluster including classic fraud offences. As a result Contacting (C) and Distributing (D) are prevalent characteristics of this cluster.
- **Social Insulting** is classified by having a strong Execution (E) component. However, a notable crime known as Happy Slapping differs from the other

types of Social Insulting crimes. Happy Slapping, defined as a phenomenon where one or more people attack a victim for the purpose of recording the assault, primarily focuses on using social media for distribution.

- **Social Agitating** describes itself clearly as a cluster using the dissemination component of social media.

Figure 3 shows the four possible usages of social media for 15 different social media crime phenomena.

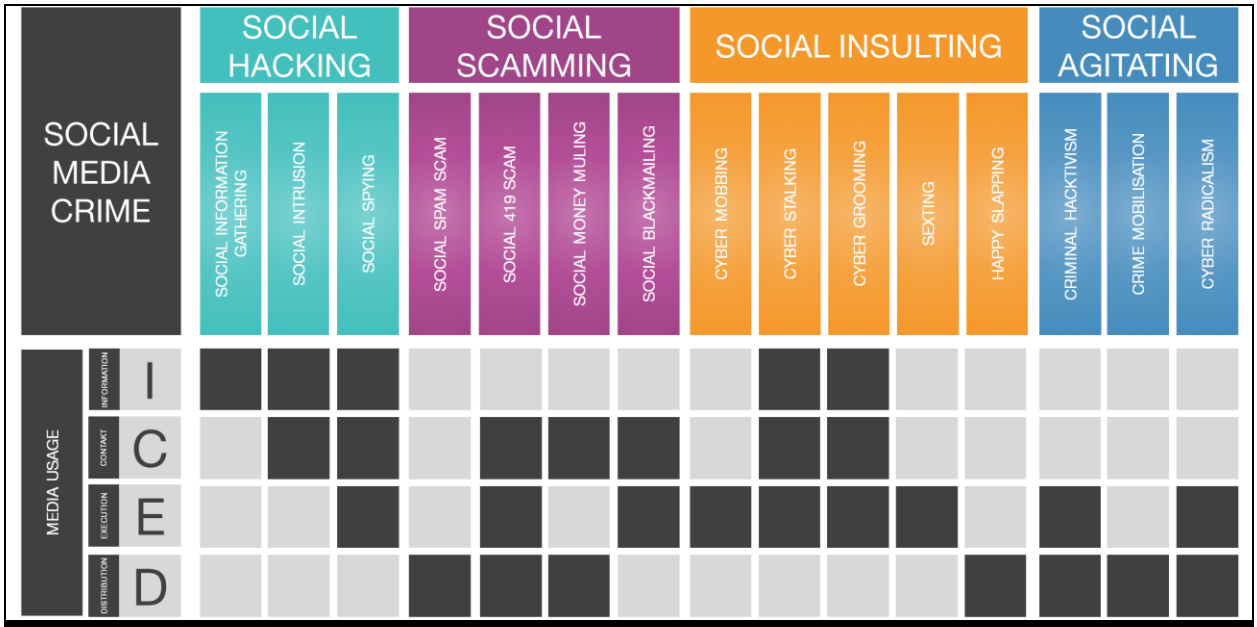

Figure 3 - Categorization of social media crime phenomena (prepared by SYNYO)

Approaches and Solutions Against Social Media Crime

As police and law enforcement agencies see themselves constantly faced with new challenges regarding social media crimes, strategies and measures for fighting them are urgently needed. Two levels of solutions are proposed: a) Approaches and solutions to **prevent** social media crimes and b) Approaches and solutions to **identify** social media crimes. Overseeing these two levels would be the presence of an expert platform to identify emerging threats and share knowledge between all affected stakeholders (Nosrati et al., 2013). Figure 4 shows an overview of all suggested approaches and solutions.

Approaches and solutions to prevent social media crime

E-Campaigning is an effective adoption of social and tradition media to raise awareness and knowledge about specific topics. Social media with its potential of fast and uncomplicated information distribution is doubtlessly a new crime scene, but vice versa its potential might also be useful to counter social media crime, for example for launching campaigns and for widespread awareness building. For crime prevention it can be used to target two main audiences: a) reducing the number of potential victims, and b) deterring offenders. Publicity directed at the potential victims include new ways to report crimes, general information about new crime phenomena, techniques offenders use (fraud, employment/business opportunities, identity theft), workshops, brochures and contact information about

https://aisel.aisnet.org/pajais/vol7/iss4/2
DOI: 10.17705/1pais.07401

crime prevention departments (Federal Bureu of Investigation, 2013).

Intelligent Filters and Warnings could be used by platform providers and social media hosts to inform the users during the process of posting if they are headed in the direction of producing social media crime relevant contents. Especially in the field of written user generated content this would be an effective way to reduce and prevent social media crime. Very often end-users are not aware on their production of forbidden content and actions against national laws. In combination with contextual information, automated scripts and algorithms could be used to warn the action persons before making their content public.

Technical and Legal Advisory for raising privacy and data awareness is a crucial step to keep data on the Internet private and therewith prevent social media crimes. Preventive educational measures on usage of various online identities or the knowledge of settings on social media networking sites should be established for different age groups. Furthermore this educational measure should also involve a legal standpoint including topics like image rights, detailed documentation, when suspecting a crime or immediate deletion of naked pictures received (Berson, 2003).

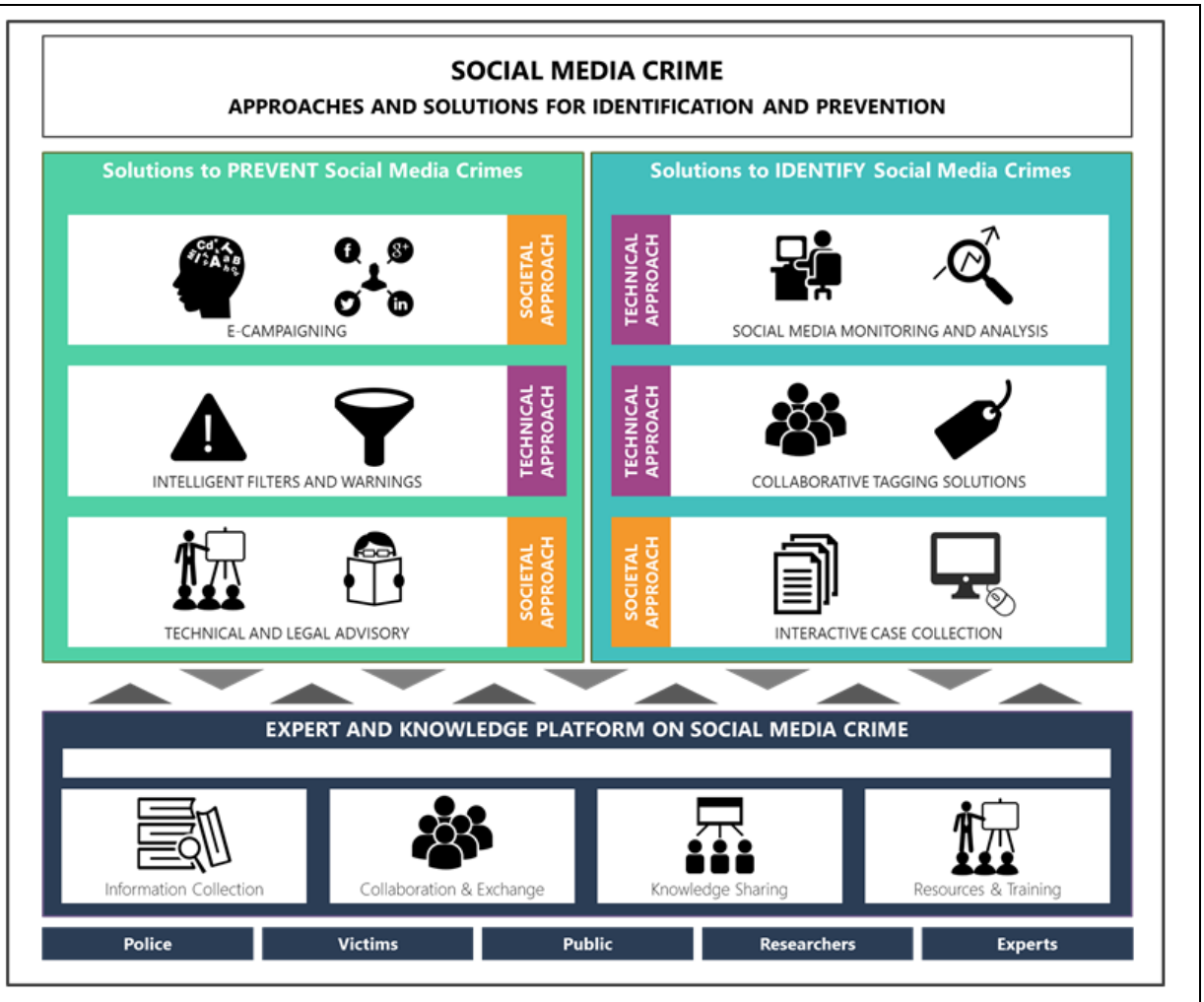

Figure 4 - Approaches and solutions for the identification and prevention of social media crime (prepared by SYNYO)

Approaches and solutions to identify social media crime

Social Media Monitoring Tools / Network Analysis is a viable solution to conquer the information overflow due to the rising user-generated content in Social Media. In recent years, marketing strategists, political decision-makers, NGOs, entrepreneurs and other groups have become increasingly aware of the information capacities arising from social media and the demand for tools, which support them in overviewing the unstructured but valuable user-generated information. Therefore a variety of social media monitoring tools have been developed to manage, channel, aggregate and analyze user generated content and open data. Established social media monitoring tools often provide real-time or near real-time analyses and will become an important resource to detect social media crime at an early stage. Such tools can for example analyze the behavior of users (likes, posts, keywords) on social media sites. (Kontaxis, 2011) Based upon this the detection of aggressive or illegal demonstrations, riots, crime mobs or any other form of crime mobilization is possible. Additionally monitoring tools offer an opportunity for identification of groups and persons with histories of criminal activity (COPS, 2013). However, more research on legal and especially privacy implications is needed before using social media monitoring tools for crime detection.

Collaborative Tagging Solutions are especially useful in the field where automated algorithms and technologies will not work. New approaches are necessary to include human intelligence on detecting social media crime. Collaborative tagging solutions are an essential approach to identify and report crime in social networks and other sites in the WWW. Similar to already implemented reporting functionalities by the platform hosts, more powerful platforms are needed to include the crowd in a stronger way for intelligent social media crime identification and reporting. Gamification approaches may also be implemented as an additional trigger to use such new tools and platforms.

Interactive Case Collection can not only improve the general awareness and knowledge of the public, but also of experts. Moreover, potential and actual victims can verify if any actions against them are illegal. For example case collections on scam and spam can be helpful for the identification and verification of such crimes (Loizou, 2012).

Conclusion

Over the last years a dramatic raise of criminal activities that make use of social media was detected. This paper describes a new approach to structure and compare criminal activities in social media and which solutions would be needed to fight these new phenomena in various ways. The presented approaches and solutions could be implemented to prevent social media crime in an early stage or to identify and report it at a later stage when already published. The created Social Media Crime Taxonomy and Matrix build an important basis for all further approaches, as it allows solutions that make use of it for the first time to categorise and analyse criminal activities in social media in a comprehensible and systematic way. The shown preventive concepts should be implemented by providers of social media platforms to reduce the amount of crime-related content and to warn unaware end-users at an early stage. Reactive approaches and solutions could be used by many stakeholder groups (companies, NGOs, law enforcement agencies, lawyers, media etc.) to identify issues quickly and develop mitigation strategies. Besides that it is of utmost importance to raise awareness among end-users on current social media crime phenomena and new trends. Well-informed end-users can minimize their own risk to become victims and support law enforcement in detecting crimes. Thereby

https://aisel.aisnet.org/pajais/vol7/iss4/2
DOI: 10.17705/1pais.07401

they play a crucial role in fighting social media crime in the long run.

Acknowledgements

The project "Social Media Crime" was funded through the Security Research Funding Programme (KIRAS) by the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT).

References

Berson, I. (2003). "Grooming Cybervictims The Psychosocial Effects of Online Exploitation for Youth," *Journal of School Violence*, 2(1), pp.5-18.

U.S. Department Of Justice (2013). *Social Media and Tactical Considerations for Law Enforcement*. COPS (Community Oriented Policing Services).

Coronges, K., Dodge, R., Mukina, C., Radwick, Z., Shevchik, J., and Rovira, E. (2012). "The Influences of Social Networks on Phishing Vulnerability," *Proceedings of the 45th Annual Hawaii International Conference on System Sciences*, 4-7 January 2012, Maui, Hawaii, pp.2366-2373.

Fawzi, N. (2009). *Cyber Mobbing: Ursachen und Auswirkungen von Cyber Mobbing im Internet.* Baden-Baden.

Federal Bureu of Investigation. (2013). "2013 Internet Crime Report" Retrieved from http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf on April 23, 2015.

Frank, R., Cheng, C. and Pun, V. (2011). *Social Media Sites: New Fora for Criminal, Communication, and Investigation Opportunities.* Public Safety Canada.

Hinduja, S. and Patchin, J. W. (2008). "Cyberbulling: An Exploratory Analysis of Factors Related to Offending and Victimization," *Deviant Behavior,* 29 (2), pp.129-156.

Kontaxis, G., Polakis, I., Ioannidis, S. and Markatos, E. P. (2011). "Detecting Social Network Profile Cloning," *Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pp.295-300.

Leitner, P. (2013). "Social Media Crime: Towards a Common Understanding of an Emerging Phenomenon," *Proceedings of the IADIS International Conference Internet Technologies & Society 2013*, Malaysia, IADIS Press, pp.119-124.

Leitner, P., Jäger, B. and Weiss, M. (2014). "A Flexible Categorization Model for Contemporary Crime Types in Social Media," *IADIS WWW 2014*.

Loizou, V. (2012). "To what extent has Facebook become a conduit for criminal activity?," *Journal of Criminology*, pp.1-36.

Marinos, L. and Sfakianakis, A. (2012). *Thread Landscape.* Heraklion: Greece.

Nosrati, M., Hariri, M. and Shakarbeygi, A. (2013). "Computers and Internet: From a Criminological View," *International Journal of Economy, Management and Social Sciences*, 2(4), pp.104-107.

O'Connell, R. (2003). *A typology of cybersexploitation and on-line grooming practices.* Cyberspace Research Unit/University of Central Lancashire.

Thapa, A. and Kumar, R. (2011). "Cyber Stalking: Crime and Challenge at the Cyberspace," *Research Cell: An International Journal of Engineering Sciences*, 4, pp.340-354.

About the Authors

Bernhard Jäger is Research Manager at SYNYO. He holds a master's degree in sociology and a bachelor of arts in communication studies. During his career he worked on projects in the fields of Criminology, Youth Delinquency, Labour Market and Health Care. He gathered extensive knowledge on deviant and criminal behaviour of individuals and masses, youth delinquency, policing, crowd control, criminal justice and crime prevention. Besides his profound expertise on qualitative and quantitative social research methods he also gained experience in web-usability, accessibility, user experience methods, user interface prototyping and design.

Peter Leitner is the Head of Research and Development at SYNYO. He holds two masters and received his Ph.D. from the Vienna University of Technology. Dr. Leitner has extensive experience in the field of software engineering, complex web platforms, innovative applications and analytical solutions. As well he is architect for large IT systems and has a broad know how on innovative frameworks and information visualisation engines. He has extensive project and risk management skills combined with 13 years of practical experience. Beside his activities at SYNYO Dr. Leitner is a lecturer for project management and software engineering at the Vienna University of Technology.

https://aisel.aisnet.org/pajais/vol7/iss4/2
DOI: 10.17705/1pais.07401