Eze, T, Speakman, L. & Onwubiko, C. (eds.) Proc. of the 19th European Conference on Cyber Warfare and Security ECCWS 2020, 25-26 June, 2020, pp. 278-283, ACPI

Young People and the Dark Side of Social Media — Possible Threats to National Security

Teija Norri-Sederholm[1], Reetta Riikonen[1], Panu Moilanen[2], Aki-Mauri Huhtinen[1]
[1]Department of Leadership and Military Pedagogy, National Defence University, Helsinki, Finland
[2]University of Jyväskylä, Finland
teija.norri-sederholm@mil.fi
reettariikonen1@gmail.com
panu.moilanen@jyu.fi
aki.huhtinen@mil.fi
DOI:10.34190/EWS.20.064

Abstract: Social media is increasingly becoming a forum for criminality, misuse, and hate speech, as there are no filters or other controlling mechanisms to filter user-generated content. Furthermore, disinformation and propaganda are becoming more sophisticated and harder to track. Hence, this dark side of social media can pose a viable threat to national security. Future generations will be born into an environment of polluted and polarised online information networks. Consequently, young people, many of whom use social media on a daily basis, will have to find ways to survive in these circumstances, often without the help, knowledge, or experience of earlier generations. Thus, young people are at risk of becoming predisposed to all kinds of harmful material, which, in turn, can affect their thinking and behaviour. This can lead to many new threats to national security. This study focuses on the observations of police officers on the current trends and threats youngsters face on the dark side of social media. The aim was to examine possible threats to national security related to young people's social media use based on data from three semi-structured interviews with police officers working in Preventive Measures Units. The analysis was done using inductive content analysis. Based on the analysis, there are three main threats to national security concerning young people's social media use: the amount of false information available online, the glorification of violence and crime, and large-scale gatherings and swarming. The results indicate that although most young people's social media use is harmless, social media platforms can also be used in a way that threatens national security. Many of the threats posed by young people's social media use have not yet been realised. However, it is important to be aware of the risks and be prepared for any possible negative outcomes in order to maintain national security.

Keywords: information influence, national security, police, social media, young people

1. Introduction

Social media is a core part of young people's everyday life. For example, in Finland three quarters of all 16–24 year–olds use social media on a daily basis (Statistics Finland, 2020). The core elements of social media consist of interactive services, user-generated content, user-specific profiles, and online social networks with other individuals and groups (Obar & Wildman, 2015). The dark side of social media can be defined as a "collection of 'negative' phenomena that are associated with the use of IT that has the potential to infringe on the well-being of individuals, organisations and societies" (Tarafdar et al., 2015, 161). Social media has multiplied the risks of misinformation, disinformation, propaganda, and hoaxes (Posetti & Matthews, 2018), and it is increasingly a hub for criminality, misuse like trolling and bullying, hate speech, and harassment (Jutterström 2019, 207; López-Fuentes 2018). Thus, social media does pose threats to national security.

One of the threats to national security by social media is information influencing. Social media can be used to alter and manipulate the social, cognitive, and psychological dynamics of a given social network or community. This is often referred to as influence or psychological operations. (Chandramouli, 2011.) These operations are often based on spreading disinformation. Disinformation can be defined as false information disseminated with the intent to deceive people, whereas misinformation does not include any malicious intent (Fetzer, 2004, 228; Lazer et. al. 2018, 1094). The ease with which disinformation can be spread is one of the properties linked to the essence of social media: it is based mainly on user-generated content and has none of the editorial controls of traditional media (Allcott and Gentzkow 2017, 211; Jensen et. al. 2010; Livingstone 2019, 6). In

addition, it is easy to gain information of users and influence them in social media by using programmed algorithms, bots, which can also create filter bubbles because they present users with information that is similar to their previous behaviour in social media (Burkhardt 2017, 12; Spohr 2017, 152–153). This can lead to ideological polarization among users as the content they encounter aligns with their pre-existing beliefs (Spohr 2017, 153). The success of disinformation is based on an understanding of human psychology: it appeals to people's minds and their beliefs. Therefore, it has been successfully used for creating rifts between citizens and polarising society. (McGeehan, 2018.) Because of the nature of rhizomatic information networks, we cannot eliminate disinformation on social media. Hence, there will always be new applications to attract audiences into distributing disinformation. In addition, applications are developed to be more sophisticated and challenging to control by institutional regulations. (Napoli, 2019.) Overall, information influencing activities can be described as having four characteristics: they are deceptive, have bad intentions, "seek to disrupt constructive debate", and "interfere in debates or issues in which foreign actors play no legitimate role" (Pamment & Agardh-Twetman, 2018, 6-7).

Social media can also be used to create incidents and events. For example, swarming, unexpected gatherings of large numbers of people in particular places, is a phenomenon strongly linked to communication on social media (White 2006). Probably the best-known form of swarming is a flash-mob, in which a group of individuals normally unknown to each other meet in a certain place to do something silly and then disperse within ten minutes (Solecki & Goldschmidt 2011; Seo et. al. 2014). However, there also exists more serious forms of swarming, such as gatecrashings, riots and mobs (White 2006; Wasik 2011). Whereas traditional flash-mobs are positive and funny, these other forms of swarming might pose serious security threats. In addition, social media can be used to catalyse incidents, which have their origins in the virtual world, but which then spill over into the real world, possibly having serious consequences (Chandramouli, 2011; Irwin-Rogers & Pinkney 2017). Typically, the ultimate goal of influence or psychological operations is to cause effects in the real world. In addition, it is not uncommon that minor real-world incidents become catalysed in social media and result in more drastic real-world events.

Another threat to national security is the availability of violent content in social media. The link between social media content and real-world violence was originally identified as being related to gang violence in particular (Irwin-Rogers, Densley & Pinkney 2018), but it is actually a more common phenomenon. Among young people, spreading and consuming violent content is not rare: this can be in the form of extremely graphic videos and pictures for the purpose of thrill-seeking and entertainment, for example. In some cases, this kind of behaviour can be linked to a phenomenon called appetitive violence, in which violence and other forms of delinquency are admired and, in some cases, actually carried out. (Ching, Daffern & Thomas, 2012.)

In this paper, we focus on police officers' observations regarding current trends and threats associated with young people and the dark side of social media. Our aim is to examine possible threats to national security related to young people's social media use. In addition to the more traditional threats, it is important to understand these new threats related to social media in order to enhance national security comprehensively. The results will serve as a pilot for our future studies concerning young people, social media, and national security.

2. Material and Methods

This paper is based on a qualitative study design. The data was collected using semi-structured interviews. The interview themes relating to social media were present and future threats, new technology, the relation between the real world and the virtual world, and the communication environment. The empirical data included three interviews from three different police districts representing different geographical areas in Finland and different sized organisations in order to obtain sample diversity. The voluntary interviewees were chosen based on their role and knowledge in the Preventive Measures Unit. The purpose of preventive measures undertaken by the police is to improve public security and combat crime. Two interviews were one-to-one interviews and the other was a group interview with three police officers. Before the interview, all participants were informed about the study and signed an Informed Consent Form that included the description of the study, its intended use, the confidentiality of the study, and the rights of the participant. The interviews were conducted by the first, second, and third author, and were audio-recorded. The mean duration of each interview was approximately 74 minutes.

Interview data was transcribed verbatim and analysed (Figure 1) using a qualitative inductive content analysis (Krippendorff, 2013). In the first stage of the analysis, data was coded using Atlas.ti 8.4.22 qualitative data analysis software. Eight code groups were created: disinformation and information influencing, swarming, polarisation and strong language, transitions between social media and the real world, the generation gap, social media as an information source, glorification of violence and crime, and a channel to the dark side. In the second phase of the analysis, data not related to national security was excluded and a mind map used to regroup the remaining data. Following this, three groups were formed: false information in social media, the glorification of violence and crime, and large-scale gatherings and swarming.

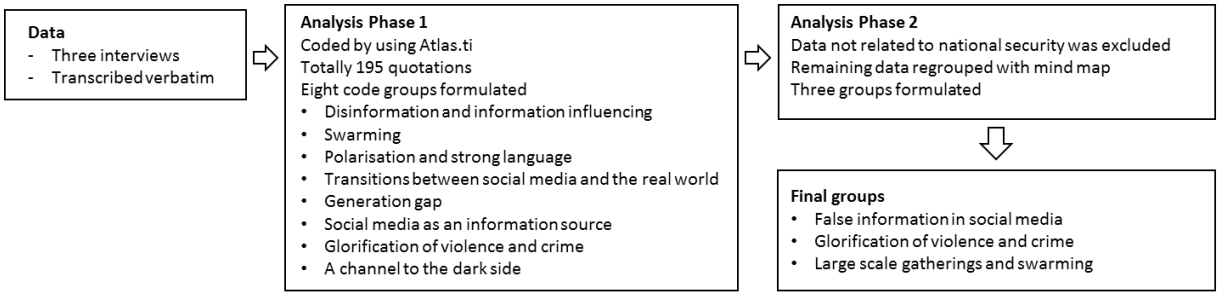

Figure 1: Analysis process

3. Findings

According to the police officers, the main threats to national security in the context of young people and the dark side of social media are the amount of false information in social media, the glorification of violence and crime in social media, and large-scale gatherings and swarming. Young people, sometimes just out of curiosity, can be exposed to things that have a bad influence on them. Social media offers everything for everyone and even so-called decent youngsters can stray onto the dark side of social media. The ease of buying drugs, surfing on the Tor-net, and joining groups with polarised thinking have been seen in police officers' work. The problem with the internet and social media is that a much larger group of youngsters is exposed to bad influences than before. For example, it is obvious that social media has had a great influence in the process of radicalisation and the number of radicalised people.

Spreading mis- and disinformation is very easy on social media as the information flow is enormous. This poses daily challenges to young people. According to the interviewed police officers, young people do not always have the ability to critically evaluate the information, the source, and the trustworthiness of the information they come across in social media. The interviewees noted that if the information comes from a reliable source from the youngsters' point of view, such as a friend or relative, they seem to assume that the information is true, even though it may not necessarily be so. This "blind" acceptance might be due to the mental immaturity of youngsters. Another challenge in the context of disinformation is the simplification of messages and the lack of reasoning behind statements and arguments in social media. This makes information influencing easier, as you only need the right timing for your provocative intervention.

When there is an incident, such as a school threat, it is typical that rumours, misinformation, and disinformation fill social media. As a result, the police must intervene and try to correct the information. However, the vast amount of rumours and disinformation makes it impossible for police to respond to them all. When such an incident happens, it is important that the police delivers the true information as quickly as possible in social media before someone fills the communication vacuum with rumours and misinformation. In recent years, police officers have detected a new phenomenon related to disinformation. As an attack happens, fabricated stories begin to spread on social media sometimes even within ten minutes of the first official news of the attack. The speed and the quality of the false material is such that, in addition to curious citizens, there has to be an organised group behind the disinformation. The look and feel of the fake news can be so similar to the official news channels that it is very hard to notice the difference and realise that these news reports are not true.

From the point of view of national security, the interviewees emphasised that what is more concerning is long-term influences and opinion formation. Extremist and other players know how to use incidents to their advantage and affect public opinion by creating negative impressions related to society and public authorities.

In general, their messaging includes systematic communication and material. Target groups, sometimes including youngsters, are planned in advance, focusing on having more supporters and visibility in the media. It is notable that some young people seek this kind of action and they look for groups where people share, sometimes even quite polarised, ideas.

All the police officers in the interviews noted that lack of consideration and attention seeking are noticeable phenomena within youngsters on social media. Youngsters may create rather provocative pictures, texts, videos, or memes, for example, to gain more followers or to emphasise their belonging to a group. Lack of consideration can also be seen in the messaging between youngsters, as the messages sometimes even include threats of violence. Occasionally it is just a rhetorical way of messaging. However, sometimes the threat transforms into an act of violence in real life. These kinds of incidents happen as social media enables youngsters to indulge in faceless forms of behaviour they would never engage in when face-to-face with others. Nevertheless, it is possible that the changes in the youngsters' messaging and behaviour are due to some sort of turning point in society. The increase of polarisation and threatening messaging on social media are phenomena that concern youngsters and adults alike. This is also reflected in the level of security in society and in the citizens' feeling of safety.

The interviewees also highlighted the role of the internet in radicalisation processes. Young people spend a lot of time there looking for like-minded friends and people. In case young people are looking for these kinds of polarised groups to strengthen their own identity, it may cause cognitive distortion and increase a black and white worldview. Moreover, idolising violence and criminality has been identified as a phenomenon in some youngsters. Young people can watch exceptionally violent videos, including brute force being used on real people and this has become everyday entertainment. An example of this is the mosque shooting video in New Zealand, which the following day, children were watching on their phones as it was freely available on social media.

According to the police officers in the interviews, there are opinion leaders and influential individuals among young people in social media. Having thousands of followers, some of these youngsters post pictures and videos where, for example, they are carrying weapons or doing something criminal, such as stealing. The problem is that the followers of such influential individuals, ordinary young people, admire them and might want to copy this behaviour. Thus, this phenomenon of idolising crime can create a feeling of insecurity among young people and affect their mind set. Social media has also made swarming and organising gatherings easy and opinion leaders in particular can easily organise gatherings or mass brawls with many of their followers as bystanders out of curiosity. There can be tens or even hundreds of young people participating in such gatherings. Often these gatherings are harmless as the aim is simply to attract many people in the same place at the same time, but on other occasions the aim is to organise a mass brawl, for example. This pattern of behaviour and the way of influencing includes the traditional elements of being young wanting to be part of a group and to be accepted and recognised. One positive aspect is that for most youngsters there are no sinister intentions behind this kind of behaviour, but it is may be down to thoughtlessness or their will to gain visibility. On the other hand, this may cause young people to look for acceptance in such a way that they may actually become victims.

4. Discussion

The aim of this study was to examine possible threats to national security related to young people's social media use. This was done through a series of interviews with police officers from the Preventive Measures Unit. The results indicated that the main threats to national security concerning young people and the dark side of social media were the amount of false information, the glorification of violence and crime, and large-scale gatherings and swarming.

False information, whether it is mis- or disinformation, can have many negative outcomes for national security. In the case of sudden attacks and incidents, rumours as such can affect people's feeling of safety. In addition, it is possible that false information even leads to violent action in real life. For example, a manipulated picture or video shared at the right time can lead to a clash between groups with pre-existing contrary worldviews. This is one way of doing information influence. (Pamment & Agardh-Twetman, 2018.) However, the biggest risk to national security is the long-term information influencing on social media, which can diminish youngsters' trust in public authorities and the government. Local communities are also affected by false information as it can

cause tension and communal dissolution. Information influence has many serious consequences in society, such as radicalisation and polarisation (see McGeehan, 2018).

Social media plays an essential role in young people's everyday life and mostly its usage is harmless. However, the same features, increasing communication and joy, are used for harmful purposes (Jutterström, 2019; López-Fuentes, 2018) posing threats to society. With the vast amount of false information in social media (Posetti & Matthews, 2018), the problem is that it is impossible for the police to detect and correct it all. The task is becoming even more difficult as new technologies and applications are constantly being developed (Napoli, 2019) and typically youngsters are the first ones to use new applications. Hence, it is hard for the police to keep up with the constant changes in social media platforms. This requires active participation and constant training from police in the use of social media. Furthermore, the role of specialised police teams and the use of artificial intelligence in data mining will increase in the near future. Therefore, it is crucial that the police adapt to this new environment. This may require changes in the selection and training of new police officers because the traditional qualities of a good police officer may not be enough in combatting crime in the virtual world.

Harmful content, available daily on social media, poses another threat to national security, as more and more youngsters become predisposed to detrimental material, such as strong language, violent content, drugs, and radicalised groups. In the context of national security, the glorification of violence and crime is an especially worrying phenomenon, as the admiration and consumption of violent content can turn into concrete action (Ching, Daffern & Thomas, 2012). The problem is that it is impossible to erase all the harmful content in social media. Hence, there will always be bad influences in social media regardless of the action of authorities. Another problem is that as more people than before become exposed to this kind of material there is the possibility that the content gradually becomes more common, accepted, and normal. Thus, the role and responsibility of parents in monitoring their children's social media use and educating their children in social media are more important than ever. Youngsters should learn at home where the line between normal and abnormal is. However, it is a fact that many parents are ignorant of the material their children are watching and sharing on social media.

The police officers' examples of swarming and other organised gatherings by young people showed how easy it is to organise large-scale gatherings on social media (see White 2006). This leads to at least two risks. First, it would be possible to organise massive gatherings or mass brawls of even thousands of people on social media. These events could lead to actual danger towards bystanders and threaten the sense of security of citizens. Secondly, although the gatherings organised by youngsters in Finland have not had outside actors or influencers so far, it is possible that some malicious actors would try to exploit the gatherings for their own purposes in the future.

The immensity of social media is, in itself, a threat to national security, as the total amount of information it contains is so enormous that it is impossible for the police to follow it all. For this reason, international police cooperation and citizens' awareness and willingness to share their knowledge are crucial elements in enabling successful preventive work and operations. This will be even more important in the future. In order to obtain information from citizens, the police must gain their trust and maintain a good relationship with them. In the case of young people, the police must adopt new ways of communication to reach them. For example, there should be more police officers working and chatting to youngsters on social media as this is a natural way of communication for youngsters. To reach youngsters, the police must also have a presence on the newest social media platforms the youngsters use. This requires a familiarity with the latest technological developments and applications and a willingness to learn how to use them. In addition, the police need an efficient way to organise all the information they acquire because not all citizens can accurately evaluate the importance and meaning of the information they share with the police.

Issues concerning the limitations and the validity of the study must also be considered. In particular, the study is small-scale with only three interviews. For this reason, the findings cannot be generalised. Having few more interviews would have ensured a better saturation in the data and thus increased the validity of the results. However, during the coding, data from each interview were part of each code group. This means that the themes of all three final groups came up in every interview. To increase the validity, the analysis was conducted in two phases by two of the authors. It should also be noted that the interviews were made in different parts of Finland to ensure a wider perspective. In addition, each interview represented a slightly

different aspect of the Police Preventive Measure Units and all the interviewees were experienced police officers. Notwithstanding these limitations, the interviews provided data that describe current trends and threats of young people's social media use well. The study also served its purpose of forming a background for our future studies.

To conclude, the results of this study indicated that there are risks to national security that concern young people in social media. Nevertheless, further studies are required to discover what kind of experiences young people themselves have of the dark side of social media. The diversity of the social media platforms young people use is one of many challenges the public safety authorities face. To be able to secure national security in a constantly changing and transiting virtual environment, new kinds of skills and abilities are needed. Furthermore, there must be a willingness and a capability to adapt to these changes in order to be prepared for new threats arising from the dark side of social media.

5. Acknowledgements

This study is part of a research project funded by the Academy of Finland.

6. References

Allcott, H. and Gentzkow, M. (2017) "Social media and fake news in the 2016 election", *Journal of Economic Perspectives*, Vol. 31, No. 2, pp. 211–236.

Burkhardt, J. M. (2017) "Combating Fake News in the Digital Age", *Library Technology Reports*, Vol. 53, No. 8, pp.1–33.

Chandramouli, R. (2011) "Emerging social media threats: Technology and policy perspectives", *Proceeding of the 2011 Second Worldwide Cybersecurity Summit (WCS 2011)*, pp. 70–73.

Ching, H., Daffern, M., and Thomas, S. (2012) "Appetitive Violence: A New Phenomenon?", *Psychiatry, Psychology and Law*, Vol. 19, No. 5, pp. 745–763.

Fetzer, J. H. (2004) "Information: Does it Have To Be True?", *Minds and Machines*, Vol. 14, No. 2, pp. 223–229.

Irwin-Rogers, K., and Pinkney, C. (2017) *Social Media as a Catalyst and Trigger for Youth Violence*. Catch 22 / University College Birmingham, London.

Jensen, M. L., Burgoon, J. K., and Nunamaker Jr, J. F. (2010) "Judging the credibility of information gathered from face-to-face interactions" *Journal of Data and Information Quality*, Vol. 2, No. 1, pp. 3:1-3:20.

Jutterström, M. (2019) "Problematic Outcomes of Organization Hybridity: The Case of Samhall", in S. Alexius and S. Furusten (eds.) *Managing Hybrid Organizations Governance, Professionalism and Regulation,* Palgrave MacMillian Cham, pp. 199–214.

Krippendorf, K. (2013) "Content Analysis: An Introduction to Its Methodology", 3rd edition, SAGE, Los Angeles

Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S. A., Sunstein, C. R., Thorson, E. A., Watts, D. J., and Zittrain, J. L. (2018) "The science of fake news", *Science*, Vol. *359,* No. 6380, pp. 1094–1096.

Napoli, P. M. (2019) *Social Media and the Public Interest. Media Regulation in the Disinformation Age*. Columbia University Press, New York.

Livingstone, S. (2019) "EU Kids Online", The International Encyclopedia of Media Literacy, Wiley Online Library.

López-Fuentes, F. de A. (2018) "Decentralized Online Social Network Architectures", in T. Özyer, S. Bakshi and R. Alhajj (eds.) *Social Networks and Surveillance for Society,* Springer*,* Lecture Notes in Social Networks. pp. 85–100.

McGeehan, T.P. (2018) "Countering Russian Disinformation", *Parameters*, Vol. 48, No. 1, pp- 49–57.

Obar, J. A., and Wildman, S. (2015) "Social media definition and the governance challenge: An introduction to the special issue" *Telecommunications Policy*, Vol. 39, No. 9, pp. 745–750.

Pamment, J. and Agardh-Twetman, H. (2018) *The role of communicators in countering the malicious use of social media,* NATO Strategic Communications Centre of Excellence.

Posetti, J. and Matthews, A. (2018) "A short guide to the history of ´fake news´ and disinformation", A learning module for journalists and journalism educators. ICFJ International Center for Journalist.

Seo, H., Houston, J. B., Knight, L. A. T., Kennedy, E. J., and Inglish, A. B. (2014) "Teens' social media use and collective action", *New Media & Society*, Vol. *16,* No. 6, pp. 883–902.Solecki, S. and Goldschmidt, K. (2011) "Adolescents texting and twittering: the flash mob phenomena", *Journal of Pediatric Nursing* Vol. 26, No. 2, pp. 167–169.

Spohr, D. (2017) "Fake news and ideological polarization: Filter bubbles and selective exposure on social media", *Business Information Review*, Vol. 34, No. 3, 150–160.

Statistics Finland (2020) *The use of information and communication technology*, [online], Statistics Finland, http://www.stat.fi/til/sutivi/2019/sutivi_2019_2019-11-07_tau_021_fi.html.

Tarafdar, M., Gupta, A., and Turel, O. (2015) "Editorial: Dark side of information technology use", *Information Systems Journal*, Vol. 25, No. 3, pp. 161–170.

Wasik, B (2011) "#Riot: self-organized, hyper-networked revolts – coming to a city near you", [online], *Wired Magazine,* https://www.wired.com/2011/12/ff_riots/.

White, R. (2006) "Swarming and the social dynamics of group violence", *Trends & Issues in Crime and Criminal Justice*, 326.