PROBLEMY MECHATRONIKI
UZBROJENIE, LOTNICTWO, INŻYNIERIA BEZPIECZEŃSTWA

PROBLEMS OF MECHATRONICS
ARMAMENT, AVIATION, SAFETY ENGINEERING

ISSN 2081-5891; E-ISSN 2720-5266 https://promechjournal.pl/

Threats to Military Institutions Arising from Operating in the Social Media Environment

Renata KOWALIK* (kowalikr@witu.mil.pl)
Ewa ZAWÓŁ (zawole@witu.mil.pl)

*Corresponding author
ORCID: https://orcid.org/0009-0000-4850-6965

*Military Institute of Armament Technology,
7 Prymasa Stefana Wyszyńskiego Str., 05-220 Zielonka, Poland*

Received: July 15, 2022 / Revised: November 15, 2022 / Accepted: November 25, 2022 / Published: September 30, 2023.

2023, 14 (3), 131-148; https://doi.org/10.5604/01.3001.0053.8824

Cite: Chicago Style

Kowalik, Renata, and Ewa Zawół. 2023. "Threats to Military Institutions Arising from Operating in the Social Media Environment". *Probl. Mechatronics. Armament Aviat. Saf. Eng.* 14 (3) : 131-148. https://doi.org/10.5604/01.3001.0053.8824

Abstract. The purpose of this paper is to present the scale of the effect that using the Internet can have on national security, and to raise awareness about the use of social media. The lack of security on the Internet or any regulations of law applicable to it must make us aware of the types of threats that originate from using the mobile apps, social media, and instant messengers that play a major role in our lives. Information security, construed as protection of information against inadvertent or wilful disclosure, modification, or enabling its processing or destruction, can be viewed from a technological and cognitive standpoint. The phenomenon of social media is driven by the human need for belonging, respect, and recognition. We seek acceptance from others, and not necessarily from our closest circles. This, in turn triggers a stimulus to share everything we do in the public space. The latest electronic devices make it possible to precisely locate their users. Online posts that we publish without understanding what could be garnered from them can be useful to a potential adversary. With the problem characterised like this, it can be anticipated that exploitation of social media can be a source of threats to national security. The hazards are becoming increasingly pertinent to the security of the military institutions that use the attributes of social media. This paper is an overview aimed at structuring and presenting the collected knowledge and raising awareness of social media in the context of the national security of military institutions. This paper uses theoretical research methods that include generalisation, analysis, synthesis, and inference.

Keywords: social media, online security, technological progress, hazard, information sources

.

1. INTRODUCTION

The importance of social media cannot be overestimated in the modern world, which is not unlike national security. The rise of the Internet has created a multitude of novel opportunities which, once made real, forever changed the mechanisms used by people as work tools, for entertainment, and for communication. Computer techniques are now used daily. Every day, we use electronic signatures, social networks, and popular online apps for sports, generally construed fitness, or banking. The feasibility of easy and inexpensive publishing and exchange of information between people entails multiple consequences, of which two are very important to ICT security. The first consequence is the growing impact of social media on information sharing and social behaviours. The second consequence is that users of the Internet leave digital footprints [1].

Given the specific nature of this paper, its authors took up the challenge to collect the source material for studying the problem mostly from online sources.

On 2 May 2011, a resident of Abbottabad, Pakistan, posted on Twitter that there were helicopters hovering over his home at 1 a.m. Later on, the same person commented on one of the helicopters being struck down.

As he found out later, the night’s incident concerned a major military operation, the neutralisation of Osama bin Laden, a high-profile terrorist. Although unintentionally, the top-secret mission of the U.S. special forces was put at high risk from the tweets of a complete stranger [2].

On 22 March 2022, a blogger posted a TikTok video of Ukrainian military technical assets parked outside a shopping Centre in Kiev. Not long after the online post, the Russian military bombed the mall. Eight people died [3].

In June of 2015, the photo of a militant outside of an ISIS camp was posted in social media, helping the U.S. military to locate and effectively strike the location [4].

On 9 May 2018, a Dutch soldier began his training at the International Airport in Erbil, northern Iraq. The soldier covered 2.9 miles in 29 minutes and 34 seconds. His progress was tracked by Polar V800, a fitness app. The service makes a map publicly available online to view the route of every run, bicycle ride, or swimming distance of the app users since 2014. The data can be analysed to discover the identity of the user of interest, their current location, and, going deeper into the data, learn the names of their partner and children. Experts state that it was easy to acquire personal data, profile pictures and location data of 6400 high-level military employees from 69 countries [5].

In July of 2015, a group of bankers posted an Instagram video from a mock execution of their Asian colleague in the style of the Islamic State. The video was posted after the bankers had training in Birmingham, UK, and quickly deleted afterwards. All those involved in the prank were fired from their jobs [6].

This paper defines and studies security hazards, especially those pertinent to military organisations, which emerge from the use of social media, and proposes certain recommendations to reduce the risks of security hazards given the phenomenon of social media.

2. GENESIS, DEFINITION AND REGULATIONS OF THE MAJOR SOCIAL NETWORKS

Social media, or social networks, also known as social network services or social network sites, are abbreviated to SoMe. SoMe are Web 2.0, which means new media.

The users of social media become both their consumers and creators. According to the definition in the Polish PWN Encyclopaedia, a social network (site) is an online service co-created by a community of Internet users who share similar interests. It enables contact between friends on the social media, and sharing information, interests, and more [7].

Currently, each social network is different, and it is virtually impossible to build a single, consistent definition of SoMe. Among such diversity, there are some similarities that link all social networks [8]:

- social networks are driven by online apps;
- social content is generated by SoMe users by posting content online;
- using a social network requires the user to create their profile;
- social network services allow users to expand their connections with other users by building a 'network' of stakeholders or by forming common features of a specific group of people.

The basic functionalities provided by social media include:

- communication – this functionality enables contact with users individually (by private messaging) or *en masse* (by discussion forums);
- information – this functionality means access to information and the ability of users to transmit information by themselves (both in public and private domains);
- publishing – this functionality is the facility for presenting one's views and discussing them with other users.

Considering regulations of law, social networks have become one of the essential and ubiquitous tools for the pursuit of rights and liberties guaranteed by the Constitution of the Republic of Poland [9]. Polish legislation has no laws dedicated to the operation of social media, and this entails the risk of many different kinds of abuse. Given that the operation of social networks is largely based on the exchange of content from different authors, an important question that arises concerns the protection of intellectual property online, especially copyrights and related rights. More importantly, the growth of social networks is currently outpacing the prevailing regulations of law, which by principle should regulate social network operations, especially today, when online services have become the most important mass communication medium. There are issues related to this: first, the primary objective of SoMe is to provide a fast and simple method of content distribution, by which the stakeholders can expand the reach to their audience; because of this, however, it becomes virtually impossible to effect any control over how content is used, and by whom. The growth of the Internet results in an inevitable shift in how information security is perceived.

Polish regulations do not cover the specifics of SoMe functioning, whereas the European laws have fallen behind the technological growth and only regulate a selection of issues that mostly relate to copyrights.

Considering the genesis of social networks, the first ones were not created only in the USA. When Mark Zuckerberg created his Facebook.com, Grono.net was entering the Polish web, a network with identical features and which, at its inception, was to be exclusively elite in nature [10].

Two years later, the social network Odnoklassniki.ru emerged in Russia (currently known as Ok.ru), the first objective of which was for the users to find common friends [11]; in this regard, the network was counterpart to the Polish network *Nasza Klasa* (Our classroom)

SoMe technologies have different formats, such as blogs, team projects, business social networks, discussion forums, microblogs, and services for posting photos or reviewing products and services, social media bookmarks, online SoMe games, social networks, and video and virtual reality streaming services [12]. 27 million Poles use SoMe, with 1.3 million new SoMe users signed up each year [13].

Facebook was created in 2004 and has been open to all Internet users since 2006, ranking among the networks which have dominated the global SoMe market. Facebook is a global corporation which owns Instagram and applications such as WhatsApp. Facebook users provide data to the social network voluntarily, where it is collected and analysed. It is enough for a Facebook user to post a photo from their summer vacation to gather information about the user: whether the user likes to travel or not, the user's financial status, whether the user has family or not, and the duration of absence of the user from their workplace or duty [14].

Twitter was established in 2006 and is called a microblog. This is because of the character limit in the posts written on user profiles [15]. The network is extremely popular among politicians and journalists. Unless the user opts in by changing a setting for their Twitter account to be private, all information about them is publicly available, including to people who do not have a Twitter account.

Instagram is a social network established in 2010 and purchased by Facebook in 2012 [16]. Aside from its core feature of posting photos, Instagram facilitates a lot more. Since being taken over by Facebook, Instagram has been expanded with numerous features that have made it one of the most popular social networks in the world; what is more, there is a growing number of users willing to give up their activity in other SoMe in favour of Instagram. Instagram users can post videos called 'reels' that the user's followers can view for 24 hours only.

YouTube is one of the oldest online video services and was opened as early as 2005. According to statistical data from Gemius (Gemius/PBI, May 2019), YouTube.com is the third most often visited website in Poland (19 million users). The platform allows users to organically post videos and discussions concerning them, empowering marketers with many opportunities for communications, from a personal channel to partnering with YouTube influencers and paid media, with diverse advertising formats (such as pre-rolls). All expert forecasts suggest video content consumption will continue to grow in the coming years, which means YouTube's position seems to be stable.

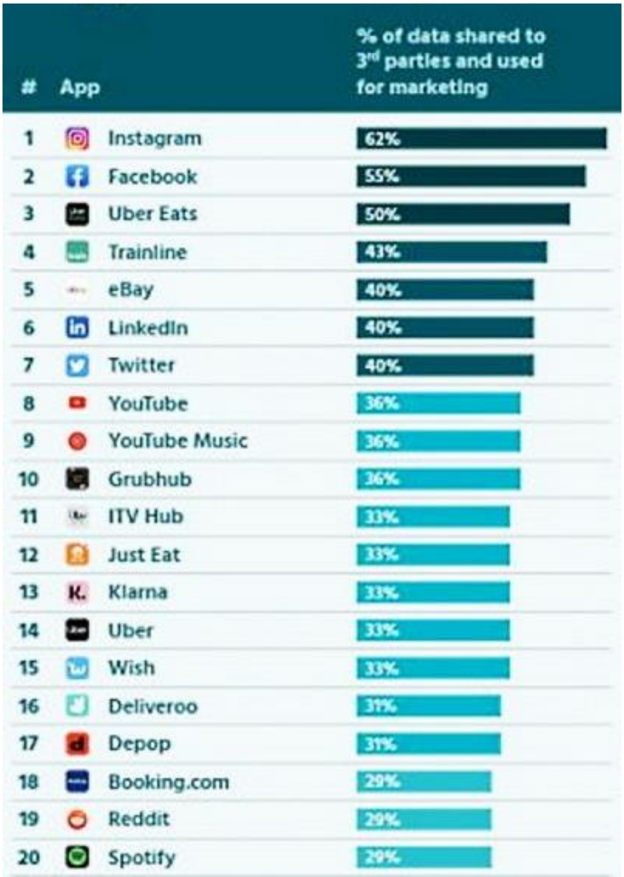
The operation of social networks largely depends on user activity, who in turn access the network's contents via user accounts. Registering a SoMe user account requires submission of personal data in most cases. Social networks are thus vast repositories of personal data.

There are many other apps available on the market; some monitor the quality of sleep, while others monitor the quantity of water consumption, or keep track of the user's physical workout progress. Apps dedicated to healthy eating are popular and feature menus and calorie counters. Everyone can find an app that satisfies their expectations. Health and fitness apps help with monitoring health and staying healthy.

Their reminders, customisable goals and a comparative chart allow boost every user's motivation to make changes to lead a healthier lifestyle [17].

Apple has recently updated its privacy policy, demonstrating how some corporations collect and use their users' data. Researchers from The Cloud Blog compiled a list that shows exactly which apps collect the most user data.

The graphic below shows exactly what such data collection looks like in the 100 most popular applications.



#	App	% of data shared to 3rd parties and used for marketing
1	Instagram	62%
2	Facebook	55%
3	Uber Eats	50%
4	Trainline	43%
5	eBay	40%
6	LinkedIn	40%
7	Twitter	40%
8	YouTube	36%
9	YouTube Music	36%
10	Grubhub	36%
11	ITV Hub	33%
12	Just Eat	33%
13	Klarna	33%
14	Uber	33%
15	Wish	33%
16	Deliveroo	31%
17	Depop	31%
18	Booking.com	29%
19	Reddit	29%
20	Spotify	29%

Fig. 1. 20 popular apps which collect the most data about users and share it with third-party companies.(Source: The Cloud Blog press materials)

Instagram takes the lead, followed by Facebook with the third place being taken by the popular online food ordering app, Uber Eats. The rest of the top of the list includes LinkedIn, Twitter, YouTube, YouTube Music, and apps such as Reddit, Spotify and Snapchat.

The research used new privacy labels available in the App Store, which classify all information collected by apps into 14 different categories. The information sections scrutinised by App Store include ‘third-party ads’, ‘developer ads or marketing’, and more. As we can see, a great number of apps collect more data about us than anyone would suspect. What can be done about it? All users should use their devices with more awareness and not simply grant permissions to every app [18].

3. SoMe RISKS

Although no official statistics exist that document the use of SoMe in the Polish Forces or Polish military institutions, it can be safely assumed that soldiers and non-uniformed personnel follow the same usage patterns as the average Pole.

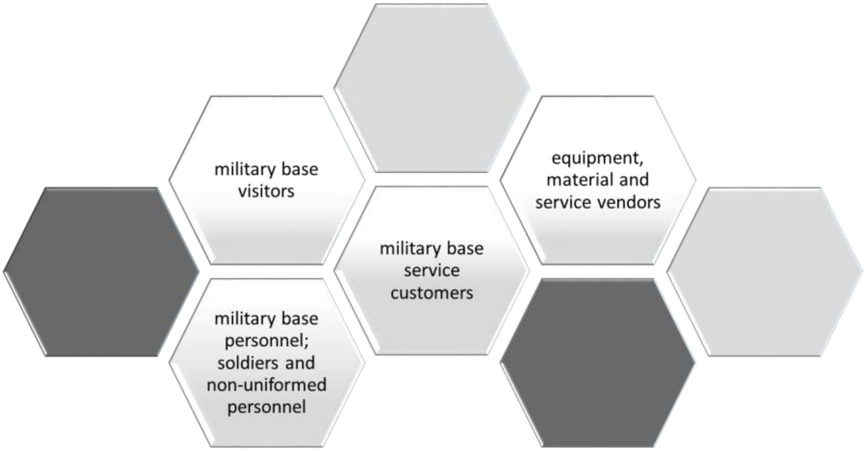

military base visitors
equipment, material and service vendors
military base service customers
military base personnel; soldiers and non-uniformed personnel

Fig. 2. Potential SoMe users posting sensitive information about military institutions on SoMe. (Source: Proprietary research work)

Figure 2 defines the potential SoMe users wilfully or unwittingly posting sensitive information of military institutions – they include soldiers and non-uniformed personnel, and military institute contractors, such as vendors of services, materials or equipment, as well as customers who take part in research, employ the services of military institutions, and the whole host of people visiting military bases.

There are five key security hazards which can emerge from using SoMe: direct disclosure risk, location disclosure risk, user anonymity risk, system design risk, and information aggregation risk. These hazards can be broken down into two broad types: user-attributable risks and systemic risks [19].

User-attributable risks are generated by actions of the people categorised above (Fig. 2); systemic risks stem from inherent features of SoMe platforms. The diagram below summarises the risks.

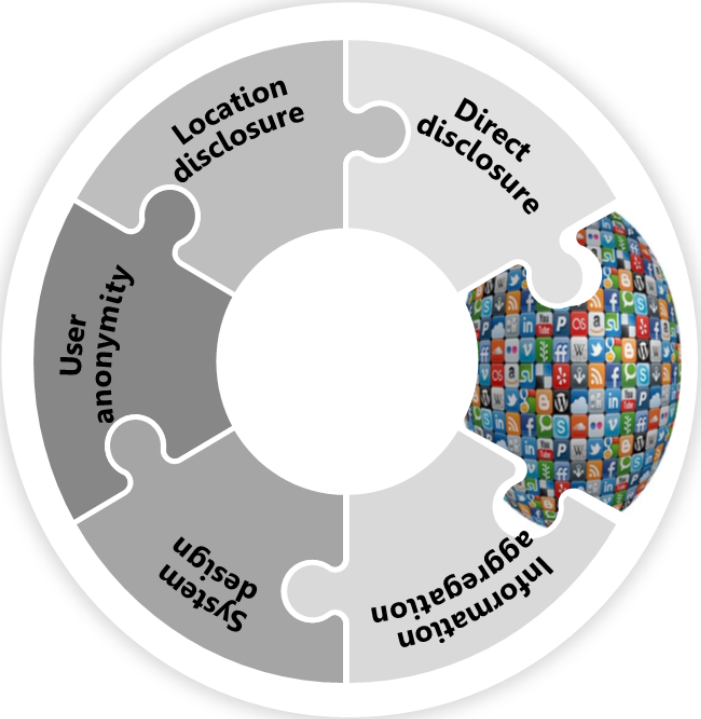


Fig. 3. Security hazards from using SoMe. (Source: Proprietary research work)

3.1. Direct disclosure risk

Considering the nature of SoMe which depends on user-generated content creation and exchange, users are encouraged to share information about them, what they do, where they are, what their interests, achievements, failures, and opinions on specific topics are, and are asked to comment if they like something or not. Military institution stakeholders –usually doing so without second thought or in ignorance of the consequences – share their private thoughts via SoMe accounts, unwittingly disclosing sensitive information to other users, which has posed a hazard to operational security more than once.

Some sensitive information that can be published online may feature confidential data about the military organisation, tactics, or operational potential. These breaches can go much further, affecting national security or the security of ongoing military operations.

In March of 2020, the Israel Defense Forces were forced to abandon their planned raid on militants in a Palestinian village after one IDF soldier posted the location and time of the attack on his Facebook profile. The soldier updated his status with: 'On Wednesday, we are cleaning out Qatanah – today an arrest operation, tomorrow an arrest operation and then, please God, home by Thursday' [20]. The consequences would have been catastrophic had the raid not been cancelled, and the militants had learned about the IDF attack. When it comes to military institution operations, a thoughtless post, photo, or comment made online can provide knowledge of the specification and performance of the technical asset of interest, tactics, operational plans, or commercial relationships.

The second risk in this domain is the extent of the effect SoMe posts can have on employers. No online post can directly physically harm the employer or their company, but comments from a member of the workforce may result in financial loss, damage to goodwill, or exposure of trade secrets. The scale of a potentially negative post depends on the job level of the poster at his or her company, the time of posting and the visibility of the post online, as well as the potential audience, the content, and, naturally, the comments posted in response. Expressing oneself is key to interests of people who use SoMe. It is, however, important to understand how a piece of information or an opinion posted online can affect your employer. One example of this behaviour is a case from Twitter, a SoMe giant. Its former CFO, Anthony Noto accidentally posted on Twitter what was supposed to be private information; a potential merger which was then in its early stages and not ready for the public to know. Anthony Noto quickly deleted his tweet, but several of his followers saved and shared it [21].

A similar case from our domestic part of the Internet concerned a Facebook post by the Chairman of the Free Trade Union of Postal Workers, claiming a potential bankruptcy of Polish Post. Unverified information like this is damaging to the goodwill of an organisation and may negatively affect its financial conditio [22].

3.2. Location disclosure risk

Another risk is disclosure of the location of sensitive military installations or military assets in operation. It is manifested first by sharing and tagging photos on SoMe, as well as using location services. When a photo is taken and uploaded to a SoMe, the photo medium may contain location data [23].

Many digital cameras and cellular phones available on the market today are capable of geotagging, or embedding geographical positioning data in image files. The geolocation data can still be extracted from photos uploaded to SoMe platforms.

Even when the image recorded in a digital photo contains no sensitive information, the geotagging embedded in the image file can explicitly identify the location, becoming a real threat to operational security. Many location services are already available on SoMe, such as Facebook, and include profile status, activity, and geographic coordinates. Many mobile applications, such as fitness apps, track the movement of their users. These location services are for smartphone users, prompting them to (willingly or unwillingly) publish their geographic location on the Internet.

Any tagging of technical equipment or seemingly irrelevant details may help hostile services to identify vehicles, their affiliation, or deployment locations. Photos and other media contain metadata, which is hidden information that can identify when, where (geotagging), and with what device a photo or other medium was made. While this information often has zero use to average users, they can help enemies identify military installations and their locations and ascertain if certain intelligence is still valid.

3.3. User anonymity risk

The SoMe systems today do not feature the sufficiently robust processes required to fully verify the authenticity of users' personal details. There are many users who exploit this by creating and maintaining anonymous or fake profiles. This mostly applies to stakeholders who use fake personalities to make friends with people of interest and access their private information. It makes sense at this point to refer to the Robin Sage experiment that was discussed during the Black Hat Security Conference in January 2011. The experiment demonstrated the ease with which classified information can be acquired using a fake user profile. For the experiment, a jarringly fake identity of a woman was created who claimed to be working for military intelligence [24]. The profile picture showed a girl that was actually 'borrowed' from an adult website, and the user's job title read 'Cyberthreat Analytics'. With the fake profile's activity, hundreds of links were established on different social networks. Throughout the entire experiment, the fake user profile received job offers from official authorities and private corporations; the profile was requested to attend and speak at various security conferences. Some of the information disclosed to the fake user profile was classified as sensitive. The results of the experiment are all the more embarrassing when one considers the many cautions from security experts about the hazards of SoMe.

3.4. System design risk

Social networks operate by exchanging and sharing user-generated content. The default settings of most SoMe platforms tend to maximise the visibility of users' personal data, minimising user privacy.

It often requires a lot of effort from the user to restrict the availability of the user profile and the information shared in their circle of 'friends'. Whenever SoMe implement new options for content sharing control, amend their policies, and the like, these activities are designed to increase the availability of SoMe user data by default. Facebook is a prime example; in December of 2009, the social network prompted its users to review their privacy settings [25].

For each of the setting areas 'Posts that I create', 'Status', 'Likes', 'Photos' and 'Notes', two availability options were provided: 'All' and 'Old settings', and all defaulted to 'All'. Facebook's prompt to review the privacy settings was mandatory, and the users were forced to choose one of the options before they could continue using the social network. Faced with the obligatory and troubling prompt, many users accepted the default setting without a second thought, which made most of their content more available than before the privacy settings update. The risk category discussed here is also present in hardware equipment design. Let us quote Maksymilian Dura's report posted on Defence 24, *Uboczne efekty postępu. Cyfrowe armie świecą jak choinka* (The Side Effects of Progress: Digital Armies are Lit Up Like Christmas Trees): 'Modern military units are chock-full of systems which generate their own electromagnetic signatures, by which they can be detected, tracked, and engaged by enemy EW (electronic warfare) systems. What is more, an attack based on electronic data acquired in prior can be performed with traditional weapons systems, such as missiles, artillery, or aircraft. It is a paradox that this predicament is most dire to the United States. By promoting the concept of "network-centric operations", every U.S. soldier is "lit up with electromagnetic signatures like a Christmas tree". Tactical calculators, CO's tablets, personal radio, WiFi cameras, rifle sights, GPS receivers, personal smartphones, smartwatches, night vision goggles, biometric sensors, or even LED torches – all this equipment can be detected by suitably designed and sensitive detectors'. Enemies undoubtedly take advantage of these solutions. Modern electronic warfare systems are capable of locating military units, determining their size, and sometimes even their plans.

3.5. Information aggregation risk

This risk type emerges from the opportunities the Internet provides for gathering SoMe data from social network users by collating various bits of personal data disclosed by the users, such as family members, friends, social circles, addresses, and contact networks. Data mining is very easy on SoMe.

A compilation of data from several SoMe user profiles or social networks provides access to information which would be very difficult or simply impossible to get in the real world. SoMe data mining can be potentially more prevalent than the general consensus would suggest. This applies equally to military information.

An enemy may collect different pieces of seemingly insignificant data for a length of time until the data can be understood and merged to get a 'bigger picture'. Such collection of aggregated information can expose sensitive data concerning a military organisation, its tactics, potential, and capabilities.

4. SECURITY MEASURES FOR SHARING SENSITIVE INFORMATION ON SOME

The experiences of military institutions around the globe vary in the method of tackling the challenges and threats of using SoMe with private user accounts. The initial efforts to counter the problem included a prohibition and denial of use of SoMe to armed forces personnel, especially on active duty in critical locations or on a tour of duty.

Russia passed an act of law which prohibits military personnel from having smartphones on them or communicating with the press. The Russian act also prohibits the operation of any means or devices that can post data, photographs, videos and geolocation online. In June of 2020, the government of India required the national military to ban 89 smartphone apps, of which 59 were Chinese and others included popular apps such as Facebook, Instagram and Snapchat. The U.S. Department of Defense allows the military to use SoMe services, albeit with controls and regulations in place. The U.S. DoD prohibits U.S. military personnel from using the Pentagon's Internet to access private websites and prevents posting of military information on private websites. Any military personnel member who posts information, photos or videos which are defamatory to ongoing military policy or military leadership, damaging to the goodwill of the military, or hazardous to the public peace will be punished for the offence. The British military applies procedures similar to those in the U.S.; the U.S. and UK military institutions have posted 'guidelines' on their official websites for military personnel using social media. The Israel Defense Forces passed a series of regulations for the functioning of users' SoMe; they include a strict prohibition on SoMe for intelligence and air force personnel. The German military also approved a number of acts of law relevant to information security on SoMe. Many countries have attempted to standardise their policies concerning SoMe and published guidelines to educate about the content that is inappropriate to post on the Internet.

Following the suit of other countries, Poland also features a number of online security activities. The General Staff of the Polish Armed Forces is running a threat awareness campaign hashtagged #*ŚwiadomiZagrożeń* (ThreatAware) to popularise the awareness of the dangers involved in users' presence and activities online [26].

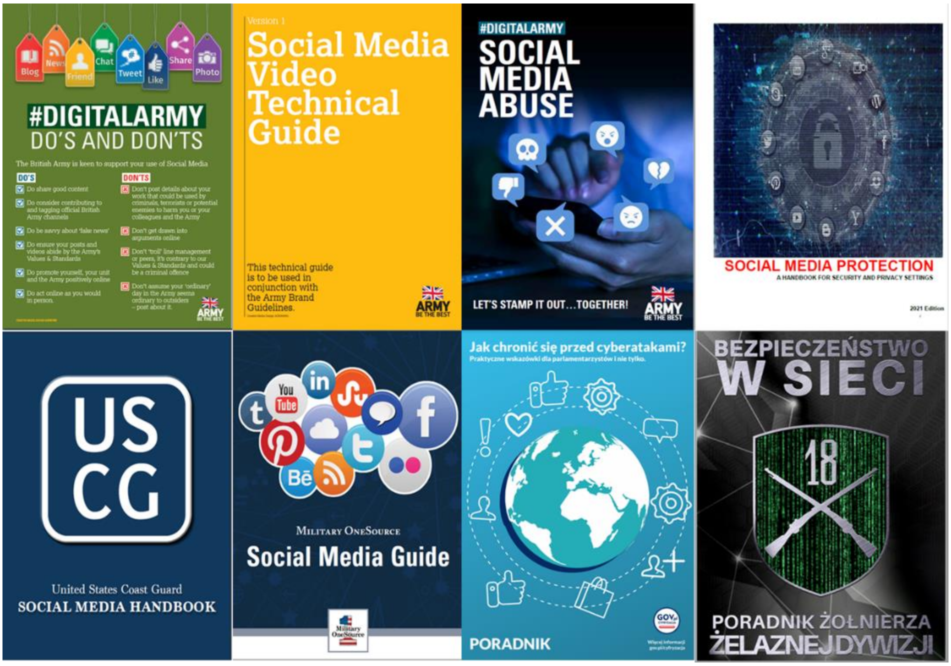

#DIGITALARMY
DO'S AND DON'TS
Social Media Video Technical Guide
#DIGITALARMY
SOCIAL MEDIA ABUSE
LET'S STAMP IT OUT…TOGETHER!
SOCIAL MEDIA PROTECTION
A HANDBOOK FOR SECURITY AND PRIVACY SETTINGS
US CG
United States Coast Guard
SOCIAL MEDIA HANDBOOK
Military OneSource
Social Media Guide
Jak chronić się przed cyberatakami?
PORADNIK
BEZPIECZEŃSTWO W SIECI
18
PORADNIK ŻOŁNIERZA ŻELAZNEJ DYWIZJI

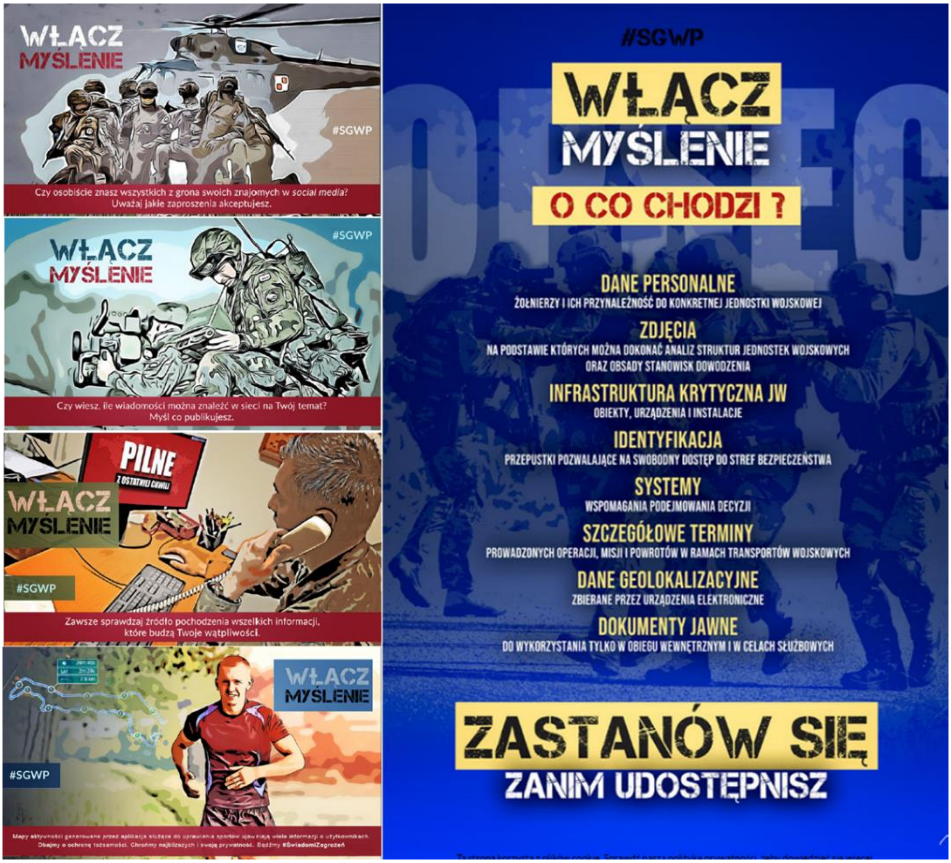
Fig. 4. Examples of military guides for education of SoMe users in different countries (Source: Proprietary research work)

To quote Col. Joanna Klejszmit, Spokeswoman of the General Staff of the Polish Armed Forces: 'The pace at which data flows and is distributed, and the human emotions involved have made it increasingly difficult to tell the true content from false. Education is a critical building block of immunity to disinformation. (…) The contents are largely addressed to military personnel, their families and loved ones. We also want to reach people outside the military community. We wish our audience to understand the meaning of the information they share. They need to understand that the information may be valuable to third parties. Making new relationships, sharing photos or data, or even circulating unverified information can be dangerous'.

The Polish Ministry of Defence issued Resolution No. 77/MON, a document of policy which regulates the operation of audio and video processing devices and the structuring of classified information protection during operations of the organisational units and teams reporting to or supervised by the Ministry of Defence.

The Resolution establishes the practice of operating devices that are prohibited in security areas and special operations facilities. To quote the Press Office of the Ministry of Defence Operations Centre: “The Ministry of Defence has issued guidance on the secure and advised operation of smartphones, cellular phones and other mobile devices for protection against security threats from unskilful use of these devices”.

A “Guide for The Iron Division Operatives: Online Security” was published to raise awareness about the hazards involved in the use of the most popular social media apps, networks and instant messaging services which are increasingly important in our lives. The Guide shows step by step how to safely use PC and smartphone apps.



Czy osobiście znasz wszystkich z grona swoich znajomych w *social media*?
Uważaj jakie zaproszenia akceptujesz.

Czy wiesz, ile wiadomości można znaleźć w sieci na Twój temat?
Myśl co publikujesz.

Zawsze sprawdzaj źródło pochodzenia wszelkich informacji,
które budzą Twoje wątpliwości.

Mapy aktywności generowane przez aplikacje służące do uprawiania sportów ujawniają wiele informacji o użytkownikach.
Dbajmy o ochronę tożsamości. Chrońmy najbliższych i swoją prywatność. Bądźmy #ŚwiadomiZagrożeń

DANE PERSONALNE
ŻOŁNIERZY I ICH PRZYNALEŻNOŚĆ DO KONKRETNEJ JEDNOSTKI WOJSKOWEJ

ZDJĘCIA
NA PODSTAWIE KTÓRYCH MOŻNA DOKONAĆ ANALIZ STRUKTUR JEDNOSTEK WOJSKOWYCH
ORAZ OBSADY STANOWISK DOWODZENIA

INFRASTRUKTURA KRYTYCZNA JW
OBIEKTY, URZĄDZENIA I INSTALACJE

IDENTYFIKACJA
PRZEPUSTKI POZWALAJĄCE NA SWOBODNY DOSTĘP DO STREF BEZPIECZEŃSTWA

SYSTEMY
WSPOMAGANIA PODEJMOWANIA DECYZJI

SZCZEGÓŁOWE TERMINY
PROWADZONYCH OPERACJI, MISJI I POWROTÓW W RAMACH TRANSPORTÓW WOJSKOWYCH

DANE GEOLOKALIZACYJNE
ZBIERANE PRZEZ URZĄDZENIA ELEKTRONICZNE

DOKUMENTY JAWNE
DO WYKORZYSTANIA TYLKO W OBIEGU WEWNĘTRZNYM I W CELACH SŁUŻBOWYCH

Fig. 5. The #*ŚwiadomiZagrożeń* (Threat Aware) campaign by the General Staff of the Polish Armed Forces. The main slogan: *Włącz myślenie* - Switch on Your Brain (Source: Proprietary research work)

Our users are routinely notified about the discovered system bugs and loopholes. There is also a twenty-four-seven hotline provided for reporting any deviations from the required practice of using electronic devices. It is important to know that the Ministry of Defence has security zones established where the use of cellular phones is restricted or strictly prohibited. These restrictions also apply during military exercise.

Note, however, that the Ministry of Defence prioritises education and raising awareness of online threats, the emerging fake news, hacking, and disinformation' [27].

5. CONCLUSIONS

The attempt at analysing the security of sensitive information on SoMe presented in this work leads to rather negative conclusions and demands continued education on the topic:

1. The defined risks are transient and tend to evolve as the digital technologies and cyberspace excellence become increasingly dynamic.
2. It is not feasible to formulate explicit tools and solutions that provide preventive controls against the risks of sensitive information disclosure. The risks specified in this work need to be managed by each military institution and reduced to acceptable levels, with regular revisions.
3. The ever-dynamic growth of the Internet, which includes SoMe, and the unending exchange of data by Internet users and military institution personnel requires continuing education, with top priority for practicing good conduct in virtual spaces that applies not only to military personnel.
4. The most effective tools in the pursuit of secure online activities are awareness raising, implementation of policies, guidance, and checklists, as well as regular training and support processes. This is especially important because of technological progress. Education should be regular, considering the influx of new online users and the pace of change in SoMe. New threats continue to emerge on the Internet. Online security should be supervised just like industrial health and safety.

Another problem that requires attention is strictly related to sensitive information disclosure on SoMe: the reception of SoMe published content. No media can ensure the right perception of content. The interpretation of information will always be subjective and vary between the audience members, but its understanding and proper effect largely depend on the care we take in selecting the contents to publish and the security of our actions as online users.

An interesting, well-edited website, a blog, or a piece of information can be highly interesting to the audience and may translate into many likes and shares.

It makes sense to make every effort so that the tools that SoMe are – and virtually available for free – an effective, secure, modern, and dynamic form of communication with the society in the domain of security.

Note that safe and aware activities in SoMe prevents disinformation first. By their presence on SoMe, military units strive to build their image by showing what they do and engaging in open communication. Continued work on fostering opinion and online awareness is an element of countering threats such as disinformation and fake news [28].

FUNDING

The authors received no financial support for the research, authorship, and/or publication of this article.

REFERENCES

[1] Wyporska-Frankiewicz, Joanna Beata, Ewa Cisowska-Sakrajda. 2022. „Dostęp do informacji publicznej a bezpieczeństwo państwa". *Wiedza Obronna* 278 (1) : 109-141.

[2] https://www.bbc.com/news/technology-13257940

[3] https://ubn.news/tiktok-s-short-video-led-to-the-bombing -of-a-shopping-mall-in-kyiv/

[4] https://edition.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html

[5] https://decorrespondent.nl/8480/this-fitness-app-lets-anyone-find-names-and-address-for-thousands-of-soldiers-and-secret-agents/260810800-cc840165

[6] https://www.huffingtonpost.co.uk/2015/07/06/hbsc-bankers-fired-after-filming-mock-isis-execution_n_7739528.html

[7] Sjp.pwn.pl (accessed: 08.07.2022).

[8] Łaski, Miłosz. 2020. *Uregulowania prawne dotyczące działalności portali społecznościowych.* Warszawa: Wydawnictwo Instytutu Wymiaru Sprawiedliwości.

[9] Konstytucja Rzeczpospolitej Polskiej z dnia 2.04.1997 r. (Dz. U. nr 78 poz. 483).

[10] https://tech.wp.pl/ grono-net-przestaje istnieć (dostęp 08.07.2022)

[11] Ok.ru (accessed: 08.07.2022).

[12] Aichner, Thomas, frank H. Jacob. 2015. „Measuring the Degree of Corporate Social Media Use". *International Journal of Market Research* 57 (2) : 257-275

[13] https://empemedia.pl/internet-i-social-media-w-polsce-2022-raport (accessed: 08.07.2022)

[14] https://www.newsweek.pl/polska/spoleczenstwo/facebook-dane-uzytkownikow (accessed: 08.07.2022).

[15] Twitter.com (accessed: 08.07.2022).

[16] https://instagram-press.com/ (accessed: 08.07.2022).

[17] https://step2health.pl/blog/aplikacje-zdrowotne-2019-b79.html (accessed: 08.07.2022).

[18] https://geekweek.interia.pl/systemy-operacyjne/news-ktore-aplikacje-wiedza-o-nas-najwiecej,nId,5112658 (accessed: 08.07.2022)

[19] Wei, Lee Hsiang. 2013. „Managing the Risks of Social Media in the SAF". *POINTER, Journal of the Singapore Armed Forces* 39 (2) : 13-22.

[20] Katz, Yaakov. 2010. "facebook details cancel idf raid*". Jerusalem Post*, 3 april 2010 (http://www. jpost.com/israel/article.aspx?id=170156).

[21] https://money.cnn.com/2014/11/25/technology/twitter-cfo-dm-fail/index.html

[22] https://pulshr.pl/prawo-pracy/poczta-zwolnila-pracownika-za-wpis-na-facebooku,68115.html

[23] Murphy, K. 2010. 'Web photos that reveal secrets, like where you live', *New York Times*, 12 Aug 2010 (http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html).

[24] Goodchild, J. 2010. 'The Robin Sage Experiment: Fake profile fooled military intelligence, IT security pros', *Veterans Today*, 11 July 2010 (http://www.veteranstoday.com/2010/07/11/the-robin-sage-experiment-fakeprofile-fooled-military-intelligence-it-security-pros).

[25] Boyd, Danah, and Eszter Hargittai. 2010. „Facebook privacy settings: Who cares?". *First Monday* 15, no. 8.

[26] *Cisza służy powodzeniu operacji'. Kampania Sztabu Generalnego WP dotycząca bezpieczeństwa w sieci*. (https://www.pap.pl/aktualnosci/news%2C1018850%2Ccisza-sluzy-powodzeniu-operacji-kampania-sztabu-generalnego-wp-dotyczaca-bezpieczenstwa-w-sieci).

[27] https://defence24.pl/sily-zbrojne/mon-zmienia-zasady-uzywania-smartfonow (accessed: 08.07.2022).

[28] https://cyberdefence24.pl/armia-i-sluzby/gen-gromadzinski-swiadomy-zolnierz-w-sieci-gwarantem-bezpieczeństwa-jednostki (accessed: 08.07.2022).

Zagrożenia dla instytutów wojskowych wynikające z funkcjonowania w środowisku mediów społecznościowych

Renata KOWALIK, Ewa ZAWÓŁ

Wojskowy Instytut Techniczny Uzbrojenia
ul. Prymasa Stefana Wyszyńskiego 7., 05-220 Zielonka

Streszczenie. Celem artykułu jest ukazanie skali zjawiska wpływu korzystania z internetu na potencjalne bezpieczeństwo kraju a także podniesienie świadomości w zakresie używania mediów społecznościowych. Brak bezpieczeństwa w sieci i uregulowań prawnych w w/w temacie musi nam uświadomić, jakiego rodzaju zagrożenia płyną z korzystania z aplikacji, mediów społecznościowych oraz komunikatorów, które odgrywają znaczącą rolę w naszym życiu. Bezpieczeństwo informacyjne – rozumiane jako ochrona informacji przed przypadkowym lub świadomym ujawnieniem, modyfikacją, umożliwieniem jej przetwarzania lub zniszczenia może być rozpatrywane w ujęciu technologicznym jak i kognitywnym. Fenomen mediów społecznościowych wykorzystuje potrzeby przynależności, szacunku i uznania. Szukamy akceptacji innych osób, nie do końca z naszego najbliższego otoczenia. To z kolei wyzwala w nas impuls dzielenia się w przestrzeni publicznej wszystkim co robimy. Nowoczesne urządzenia pozwalają na precyzyjną lokalizację ich użytkownika. Wpisy internetowe, które publikujemy nie mając wiedzy na temat tego, co można z nich wywnioskować, są czymś co może być wykorzystane przez potencjalnego adwersarza. Przy tak przedstawionej charakterystyce należy antycypować, że eksploatowanie mediów społecznościowych może być źródłem zagrożeń dla bezpieczeństwa państwa. Korzystając z atrybutów mediów społecznościowych zagrożenia te coraz częściej dotyczą bezpieczeństwa instytucji wojskowych. Zaprezentowana publikacja jest artykułem przeglądowym, a jej celem jest uporządkowanie i przedstawienie zebranej wiedzy a także szerzenie wiadomości w zakresie mediów społecznościowych w kontekście bezpieczeństwa państwa w ramach instytucji wojskowych. W artykule wykorzystano teoretyczne metody badawcze, takie jak: uogólnienie, analiza, synteza i wnioskowanie.

Słowa kluczowe: media społecznościowe, zagrożenie, źródła informacji, postęp technologiczny, bezpieczeństwo w sieci