Dorel DANCIU
Babeș-Bolyai University of Cluj-Napoca, Romania

SOCIAL MEDIA AND THE SECURITY OF MILITARY OPERATIONS

Abstract:	*In the last decade, social media and Social Network Sites have decisively changed how internal and external communication takes place in the military. One of the most important advantages of social media is the facilitation of new forms of social interaction and communication. The integration of text, images, and sounds in the same interactive communication system, accessible at any chosen moment, within a global network, fundamentally changes the character of military communication. In the context of the new types of military operations, having predominantly the characteristics of the hybrid war, the security of the operations (OPSEC) remains a critical requirement.* *The increasing number of military social media users from deployed areas of operations could compromise information security and missions. Building a security culture in the field of SNS use through education is an easy and almost cost-free action, for information disclosure prevention.*
Keywords:	**Social media; social network sites; Info Ops; cyber security; OPSEC**
Contact details of the authors:	E-mail: dorel.danciu@ubbcluj.ro
Institutional affiliation of the authors:	**Babeș-Bolyai University/Doctoral School of Sociology**
Institutions address:	21 Dec.1989 Bd.,128, Cluj-Napoca, 400604, 0040.264419958, socasis.ubbcluj.ro, secretariat.socasis@ubbcluj.ro

Introduction

We are living in the era of the digital revolution that increasingly influences every aspect of our lives. The presence of digital communications and devices, the internet, the World Wide Web, social media, smartphones, robotics, artificial intelligence, big data analysis, and much more are reshaping the world we are living in[922]. Communication technology is fundamental to society; each technology leaves its mark on media form and content. The use of communication technology influences social transformation and communication revolutions determine social revolutions[923].

The traditional public sphere has witnessed changes. We can refer, without any mistake, to a public space of virtual communities generated by the Social Network Sites (SNS) and the multitude of forms of communication that use the internet as a media support, associated with the traditional public space.

Encyclopedia Britannica defines social media as a form of mass media communications on the Internet (such as on websites for social networking and microblogging) through which users share information, ideas, personal messages, and other content (such as videos)[924]. One of the most important advantages of social media is the facilitation of new forms of social interaction and communication. The integration of text, images, and sounds in the same interactive communication system, accessible at any chosen moment, within a global network, fundamentally changes the character of communication. We intend to briefly analyze the theoretical approaches regarding social media influence on military activities, using the NATO perspective. Then, the theoretical approach will be complemented by a practical example in the form of a case study.

[922] Antony Giddens, Philip W. Sutton, *Sociology*, the 9th Edition, Polity Press, Cambridge, 2021, p. XI
[923] Denis McQuail, *Mass Communication Theory*, the 6th Edition, Sage Publications, London, 2010, p. 92
[924]https://www.britannica.com/topic/social-media (21.11.2023)

Social Media and the Trend Toward Mobility and Accessibility

Social media has decisively changed how internal and external communication takes place in the military. Social Network Sites (SNS) as platforms that enable social media, generate the multiplier effect for the diffusion of content. Social networks have given each user the right to an opinion related to the subjects on the public agenda. Social media and SNS allow access to a greater variety of information, as well as the possibility to follow the dynamics of an event in real-time. It is important to observe the trends in terms of accessing social networks, from which devices SNS are accessed, and the preferences of users according to age. Since members of the armed forces are largely subject to societal trends, the statistics are also valid for the military field.

To achieve a more accurate profile of those who access social networks, depending on location, age, network type, and access mode, we use some up-to-date statistics. According to Statista, in 2022, the current number of smartphone users in the world today is 6.92 billion, meaning 85.82% of the world's population owns a smartphone. 93.4% of internet users access the internet using a mobile phone and 99% or 4.95 billion social media users access networks using a mobile device[925]. Accessing the Internet from mobile devices has registered a significant increase in recent years, showing user preferences, especially for smartphones. Worldwide, in 2023, approximately 61% of Internet users accessed from such devices, almost double compared to 2016, when 31% accessed the Internet in this way[926].

In 2023, the most used worldwide social network platform is Facebook, with approximately 2.9 million users per month. It is followed in the ranking by YouTube, WhatsApp, Instagram, WeChat, and TikTok, as seen in Figure 1[927].

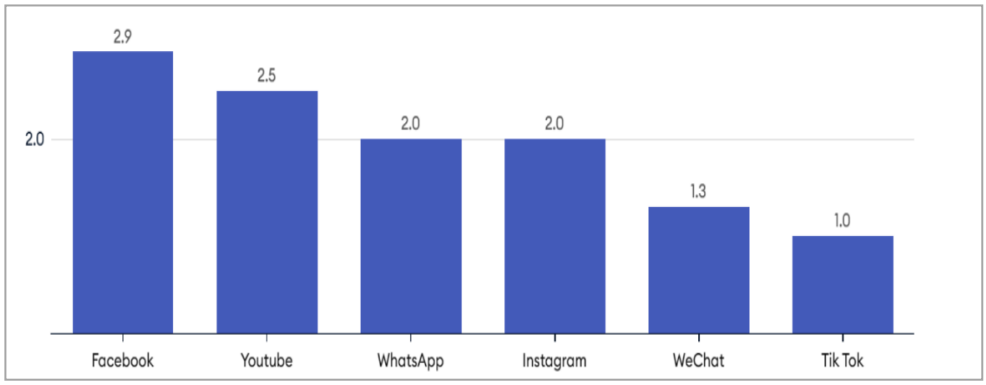

Figure 1. Monthly Active Users by Social Media Platform (in millions)[928]

Recent statistics, which analyze accessibility for the entire year 2022, related to user demographics show that young people are the most interested in using social networks, more specifically those aged between 18 and 29 who have accessed at least 84% of social media. Access to social networks decreases with the growth of the analyzed age segment, as we can see in Figure 2[929].

[925] Ani Petrosyan, *Internet usage worldwide-Statistics&Factsm*, https://www.statista.com/topics/1145/internet-usage-worldwide/ (10.09.2023)
[926]Josh Howarth, *Internet Traffic from Mobile Device (Nov 2023)*, on https://explodingtopics.com/blog/mobile-internet-traffic (10.11.2023)
[927]J.D. Belle Wong, Cassie Bottorff, *Top Social Media Statistics And Trends Of 2023*, https://www.forbes.com/advisor/business/social-media-statistics/ (15.09.2023)
[928] *Biggest social media platforms 2023* | Statista (15.09.2023)
[929]*Idem*

Figure 2. Percentage of Each Age Group that Uses at Least One Social Media Site[930]

Social Media Usage. Challenges And Opportunities for The Military

First, it is important to identify the professional soldier in the current social context. Almost 50 years ago, Charles Moskos studied how the US military made the transition from the institutional to the occupational model and observed that although the army enjoys certain autonomy, it remains a social organization. Any societal trend of change will have echoes within the military as well. Moreover, the army has gone through a process of transition from the institutional model to that of an organization with an occupational model, a tendency to adapt military structures to civilian structures and trends[931]. Morris Janovits also analyzed this concept, considering the professional soldier a "citizen-soldier", the result of the integration of the military into civilian society, because of the shared democratic values[932].

Social media is part of the communication strategy of military organizations, integrated into other public affairs activities. Thanks to the informal way of addressing, it can easily reach the target audience, thus contributing to the fulfillment of the communication objectives. At the same time, social media can also be a tool to combat rumors and misinformation[933]. The communication process based on social media platforms, especially WhatsApp and Facebook Groups, has led to a significant increase in the interaction between soldiers, sharing best practices, and learning from each other's experiences[934].

Once the public image of the military institution is consolidated, social media can become a very good tool used by military institutions for the selection and recruitment of new members of the armed forces. For the military's audience of potential recruits, social media is very important. The age category of potential candidates for military enlistment is characterized by the widespread use of social networks[935].

Social Media is an Information Operations (Info Ops) force multiplier so that it can be used as a tool for transmitting messages to the target audience, to influence and change attitudes, opinions, and perceptions, using specific tactics of disinformation, deception, and propaganda[936]. In their book "LikeWar: The Weaponization of Social Media", authors Peter Singer and Emerson Brooking explain how social media

---

930 *Social Media Use in 2021* | Pew Research Center

931 Charles Moskos, *Armata, mai mult decât o ocupație?,* Ziua, București, 2005, pp. 15-21

932 Holly Giroux, *Social Media's Impact on Civil-Military Relations: Balancing the Good with the Bad*, "Wild Blue Yonder Online Journal", 2021, https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2871481/social-medias-impact-on-civil-military-relations-balancing-the-good-with-the-bad/ (20.10.2023)

933 *Idem*

934 *Idem*

935 Jennie W. Wenger, Heather Krull, Elizabeth Bodine-Baron, Eric V. Larson, Joshua Mendelsohn, Tepring Piquado, Christine Anne Vaughan, *Social Media and the Army: Implications for Outreach and Recruiting*. RAND Corporation, 2019, https://www.rand.org/pubs/research_reports/RR2686.html (28.09.2023)

936 Kyle Deem, *Social Media and the Military: How the Field Grade Leader Should Understand, Approach, and Control Social Media Warfare*, 2020, p. 10, https://apps.dtic.mil/sti/pdfs/AD1124619.pdf (25.09.2023)

became a powerful weapon of warfare and call this ”weaponization” of social media, a sort of new asset in modern warfare[937].

Limitations, Constraints, And Risks of Using Social Media in the Military. Social Media and OPSEC

By using social media, military personnel are exposed to the risk of engaging in political activities, contrary to military codes of conduct[938]. The increasing number of military social media users from deployed areas of operations could compromise information security and missions. SNSs allow the collection and automated processing of information related to military personnel and own units that can later be used by the adversary in the targeting process[939].

The widespread use of mobile devices with extensive technical possibilities for information sharing has led to a significant increase in the risk of breaching the security of military activities and missions by military personnel.

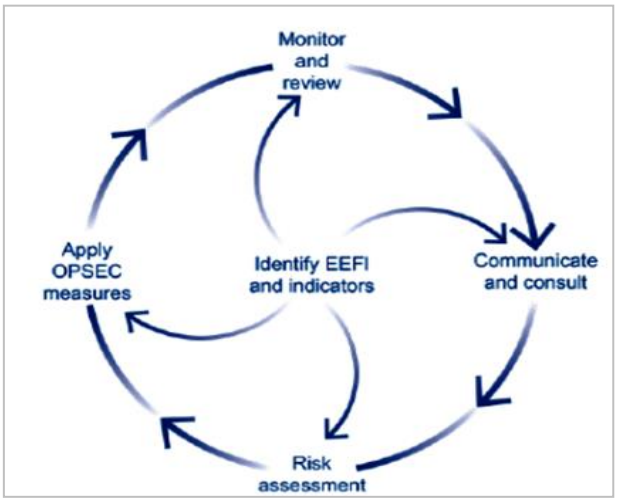

Figure 3. The five-step OPSEC model[940]

Sensitive information on troop location, military force structure, areas of operations, and troop movements can be used by adversaries during open intelligence-gathering activities[941]. Allied Joint Publication-3.10.2 presents NATO’s perspective on Operations Security or OPSEC: a process that gives a military operation or exercise appropriate security, using passive or active means, to deny the enemy knowledge of the dispositions, capabilities, and intentions of friendly forces. OPSEC aims to deny critical information and indicators to adversaries[942]. According to the same document, OPSEC is a cyclic capability, it consists of five steps that cover all operation phases, even the post-conflict period. The first step refers to sensitive data identification (essential elements of friendly information - EEFI) and understanding what kind of data is stored on its systems and is of interest to the enemy. With sensitive data identified, the military structure

---

937 Peter Singer, Emerson Brooking, *Likewar: The Weaponization of social media*, 2018, https://www.perlego.com/book/3184265/likewar-the-weaponization-of-social-media-pdf (30.09.2023)

938 Holly Giroux, *Social Media’s Impact on Civil-Military Relations: Balancing the Good with the Bad, ”*Wild Blue Yonder Online Journal”, 2021 https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2871481/social-medias-impact-on-civil-military-relations-balancing-the-good-with-the-bad/, (21.10.2023)

939 Kyle Deem, *Social Media and the Military: How the Field Grade Leader Should Understand, Approach, and Control Social Media Warfare*, 2020, p. 11, https://apps.dtic.mil/sti/pdfs/AD1124619.pdf, (27.09.2023)

940 North Atlantic Treaty Organization, *Allied Joint Publication-3.10.2. Allied Joint Doctrine for Operations Security and Deception,* p. 12, AJP-3.10.2, publishing.service.gov.uk (10.12.2023)

941 Eva Moehlecke de Baseggio, Olivia Schneider, Tibor Szvircsev Tresch, *Social Media and the Armed, Forces* , Springer, p.194, https://doi.org/10.1007/978-3-030-47511-6 (15.10.2023)

942AJP-3.10.2, *Allied Joint Doctrine for Operations Security and Deception*, March 2020, p.3 https://www.gov.uk/government/publications/allied-joint-doctrine-for-operations-security-and-deception-ajp-3102a (10.10.2023)

needs to determine the potential threats to this data. This step is called risk assessment and consists of risk identification, risk analysis, and risk evaluation. Applying OPSEC measures is the most important step, Monitoring and reviewing the effectiveness of OPSEC measures and communicating and consulting will complete the cycle. The identification of sensitive data begins with the analysis of the informational flows of the military organization, carried out officially through the structures of public affairs and public information. For military leaders and commanders, balancing OPSEC rules and legal obligations with public opinion and mass media on free access to information is a real challenge[943].

During the use of social media for the benefit of current military activities, *security at the source* is the practice most suitable for military activities, an extension of practices in the field of protection of classified information. While at the strategic and operational level, the doctrines, directives, and other operational planning tools represent useful working tools for commanders and decision-makers, at the level of military personnel, standard operating procedures (SOPs), the tactics, techniques, and procedures (TTPs) transposed in the form of guides or even documents of the type do's/don'ts lists are effective means of education in the realm of social media use during military activities.

Cyberspace operations are divided into defensive cyberspace operations and offensive cyberspace operations, associated with Info Ops[944]. Defensive cyberspace operations or cyber security are generally aimed at preventing and/or terminating and mitigating ongoing malicious activities in cyberspace and recovering from their effects, thus preserving mission assurance. These operations protect networks and systems, and the information therein, for which NATO has been granted authorized access[945]. Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from the enemy's attacks.

Geo-tagging is one of the biggest threats to the security of military operations, and the use of social media during missions of a high degree of risk, and complexity and carried out in secret could compromise the security of the personnel involved in the respective military actions[946]. Most of the mobile devices used by deployed soldiers have built-in GPS cameras. As a result, each photo taken, or video recorded and potentially disseminated could include an accurate description of the location of the recording by displaying geographic coordinates, altitude, and longitude coordinates.

Building a Security Culture in The Field of SNS Use Through Education

OPSEC is very important during all peacetime and wartime military activities but is a critical requirement during deployments and operations. The training of military personnel and the effective use of technical means specific to cyber security can lead to the achievement of communication objectives through social media. It is much easier and almost cost-free to prevent information disclosure than to mitigate the effect of unintended information dissemination.

The security-first model is the concept that effectively incorporates the security requirements of military operations and the technical security requirements that lead to the safe operation of IT systems and technologies[947]. This security model involves permanent vigilance, surveillance, and the reduction or elimination of security risks and threats, including technical means and IT technologies. This model also requires the military organization to monitor threats in real-time. Also, in the security-first model people have a major and proactive role to counter threats, and engaging employees in security awareness training is a good way to achieve this goal[948].

To improve cyberculture, military organizations must take concrete steps to communicate the importance of cyber security to employees and provide them with tools, skills, and knowledge for success. Security

[943]ACO/ACT *Public Affairs Handbook*, May 2020, p. 71, https://www.act.nato.int/wp-content/uploads/2023/06/nato-pao-handbook-2020.pdf (15.10.2023)
[944]AJP 3.20, *Allied Joint Doctrine for Cyberspace Operations*, January 2020, p. 16 https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320 (12.10.2023)
[945]*Idem*
[946] *U.S.Army Social Media Guide*, https://www.army.mil/socialmedia/ (25.10.2023)
[947] Art Gilliland, *Building A Security-First Culture: the Key To Cyber Success*, https://www.forbes.com/sites/forbestechcouncil/2023/01/03/building-a-security-first-culture-the-key-to-cyber-success/?sh=53ad195fa10f (22.09.2023)
[948] *Idem*

awareness training should be a top priority for all military organizations, and the implementation of the concept starts from the leadership's example[949]. The same concept of changing mindsets applies to engaging soldiers in security awareness training. Military personnel are the first line of defense, but often they're busy with pressing work responsibilities and view these exercises as a chore[950].

Guidance on Maintaining Security Online

NATO guidance on online security recommends several categories of information that could represent a risk when using social media[951]: personal information, account details, details about work/unit, and operational information. The standards of personal conduct in the digital environment contain a detailed list of recommendations designed to ensure personal and mission security, which start from the premise that social media can pose a threat when not used appropriately. The basic principle is to analyze operationally any information posted in the form of text or image[952]. U.S. Army Social Media Guide proposes the "Think, Type, Post" strategy while using social media, an effective way to analyze in detail the possible adverse effects of personal behavior in the online environment[953].

In addition, according to the directive presented above, there are several measures to protect military personnel: understanding and applying security settings, avoiding unnecessary share of information during the registration process, safekeeping of accounts and passwords, and thorough verification of posted images, to avoid the transmission of sensitive information[954].

Starting from the approach that OPSEC is a permanent responsibility of each military, the NATO guide recommends proactive conduct in situations where the dissemination of sensitive information is observed by others, which consists of immediate reporting up the chain of command to the person responsible or the structure that responsible for information security[955].

Case Study: Example of Russian OPSEC Failure in Ukraine

The online publication "Task & Purpose" recently presented a conclusive case of violation of OPSEC using data provided by social media-enabled geolocation tools[956]. The protagonist of this case is a Russian soldier from the 10th Spetsnaz Brigade who posted on the VKontakte network, a widely used SNS in Russia, pictures and short videos of him and his colleagues while they were stationed in an accommodation area.

Some of the images posted had geolocation tools activated, so it was easy to link them to the highly precise attack launched by the Ukrainians that destroyed the place where the troops were stationed. Moreover, the same soldier also provided the Ukrainians with evidence that they managed to hit the target, publishing pictures of the destroyed buildings shortly after the attack. These last pictures helped the opposing side to make an effective battle damage assessment.

Shortly after the incident described above, the Ukrainian side executed several strikes on a compound in Makiivka, on New Year's Day, based on the triangulation of the GSM signal from the Russian soldiers' phones. It is estimated that several dozen Russian soldiers lost their lives in that incident. Along with the use of social networks, the use of mobile phones as an alternative to encrypted communications appears to be a major weakness of Russian military actions on the Ukraine front.

---

[949] *Idem*

[950] Manoj Srivastava, *How to create a security-first culture, https://www.securitymagazine.com/articles/97287-how-to-create-a-security-first-culture* (23.10.2023)

[951] ACO/ACT *Public Affairs Handbook*, May 2020, pp 161-163, https://www.act.nato.int/wp-content/uploads/2023/06/nato-pao-handbook-2020.pdf, (15.10.2023)

[952]ACO *Digital Media Engagement Guide*, 2020, p. 38, https://www.act.nato.int/wp-content/uploads/2023/06/nato-dmmg.pdf (01.10.2023)

[953] *U.S.Army Social Media Guide,* https://www.army.mil/socialmedia/ (20.09.2023)

[954]ACO *Digital Media Engagement Guide*, 2020, p. 39 https://www.act.nato.int/wp-content/uploads/2023/06/nato-dmmg.pdf (01.10.2023)

[955] *Idem*

[956] Jeff Shogol, *Russian soldier gave away his position with geotagged social media posts*, 2023 https://taskandpurpose.com/news/russian-military-opsec-failure-ukraine/, (15.10.2023)

Conclusions

Nowadays, social media and SNSs are part of new types of wars and are actively used to create effects in battlespace. We refer to the "weaponization" of social media. Social media is a double-edged sword. It is very important to constantly evaluate the advantages and disadvantages of using social media in the military environment and balance the need for openness with the requirements of mission security.

It is almost impossible to control the phenomenon of using social networks during military activities. However military decision-makers can create the necessary framework for educating military personnel about the operational risks of using social media while on missions without considering the OPSEC rules.

OPSEC is very important during all peacetime and wartime military activities but is a critical requirement during deployments and operations. Building a security culture in the field of SNS use through education is an easy and almost cost-free action, to prevent information disclosure prevention. It is much easier and almost cost-free to prevent information disclosure than to mitigate the effect of unintended information dissemination.

Bibliography

Books

1. Giddens, Antony; Sutton, Philip W., *Sociology*, Polity Press, Cambridge, 2021
2. Moehlecke de Baseggio, Eva; Schneider, Olivia; Szvircsev, Tresch, Tibor, *Social Media and the Armed Forces*, Springer, 2020
3. Moskos, Charles, *Armata, mai mult decât o ocupație?,* Ziua, București, 2005
4. Singer, Peter; Brooking, Emerson; *Likewar: The Weaponization* of Social Media, Eamon Dolan/Houghton Mifflin Harcourt, New York, 2018

Studies and Articles

1. Belle, Wong, J.D.; Bottorff, Cassie, *Top Social Media Statistics and Trends of 2023*, "Forbes Advisor", May, 2018, https://www.forbes.com/advisor/business/social-media-statistics/
2. Deem, Kyle, *Social media and the Military: How the Field Grade Leader Should Understand, Approach, and Control Social Media Warfare*, Fort Leavenworth, Kansas, Social Media and The Military: How the Field Grade Leader Should Understand, Approach, and Control Social Media Warfare (dtic.mil)
3. Giroux, Holly, *Social Media's Impact on Civil-Military Relations: Balancing the Good with the Bad*, "Wild Blue Yonder Online Journal", 2021, https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2871481/social-medias-impact-on-civil-military-relations-balancing-the-good-with-the-bad/
4. Shogol, Jeff, *Russian soldier gave away his position with geotagged social media posts,* "Task&Purpose", 2023, https://taskandpurpose.com/news/russian-military-opsec-failure-ukraine/
5. Srivastava, Manoj, *How to create a security-first culture, https://www.securitymagazine.com/articles/97287-how-to-create-a-security-first-culture*
6. Wenger, Jennie W.; Krull, Heather; Bodine-Baron, Elizabeth; Larson, Eric; Mendelsohn, Joshua; Piquado, Tepring; Vaughan, Christine Anne, *Social Media and the Army: Implications for Outreach and Recruiting*, RandCorporation, 2019, https://www.rand.org/pubs/research_reports/RR2686.html

Documents

1. ACO/ACT *Public Affairs Handbook*, May 2020, https://www.act.nato.int/wp-content/uploads/2023/06/nato-pao-handbook-2020.pdf
2. ACO *Digital Media Engagement Guide*, 2020, https://www.act.nato.int/wp-content/uploads/2023/06/nato-dmmg.pdf
3. AJP-3.10.2, *Allied Joint Doctrine for Operations Security and Deception*, March 2020, https://www.gov.uk/government/publications/allied-joint-doctrine-for-operations-security-and-deception-ajp-3102a
4. AJP-3.20, *Allied Joint Doctrine for Cyberspace Operations*, January 2020, https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320

Websites

1. https://www.army.mil
2. http://www.britannica.com/
3. https://www.gov.uk/
4. https://www.statista.com/