sciendo

Land Forces Academy Review
Vol. XXX, No. 2(118), 2025

RISKS AND VULNERABILITIES ASSOCIATED WITH THE USE OF MOBILE PHONES BY ACTIVE PERSONNEL IN MILITARY STRUCTURES

Sorin TOPOR
National Institute for Research and Development in Informatics – ICI Bucharest, Romania,
sorin.topor@ici.ro

ABSTRACT

Military infrastructures are the fundamental pillars for ensuring the security and integrity of any military activity. Communication systems provide essential services, disruption of their functioning can introduce errors in the level of management and weapons systems, with serious effects on the safety, economy and stability of forces and assets. In this context, mobile phones, although they represent an indispensable tool for rapid communication and for maintaining effective coordination of actions, can introduce significant vulnerabilities that can be exploited for malicious purposes. This paper, based on the lessons learned from the Ukraine war, analyzes the risks associated with the use of mobile phones for effective communication and proposes a series of protective measures, of which educating personnel for the conscious use of these devices minimizes the value of electronic and cyber vulnerabilities, thus contributing to strengthening of military unit's security.

KEYWORDS: electromagnetic/cyber operation, information warfare, military education and training, mobile smartphone

1. Introduction

The use of mobile phones in current military activities has a significant impact on improving communication, with substantial effects on the efficiency and safety of carrying out any military activity, in an increasingly complex and dynamic operational environment. Current applications of massive data analysis and artificial intelligence (AI) ensure the interpretation and forecasting of enemy maneuvers, rapid decision-making in the planning and carry out of operations, control and coordination of weapons systems etc., which allow the use of robots in autonomous or controlled systems for missions of identification, surveillance and reconnaissance of targets, for the efficient execution of strikes etc., but also for maintaining social links of military and civilian personnel, within the structure of a military unit. All these technological innovations generate associated electromagnetic and cyber risks and vulnerabilities, with catastrophic effects in a complex conflict situation.

Modern warfare is characterized by unprecedented geopolitical complexity, the volatility of hybrid conflicts that combine tactics and techniques of conventional warfare with cyber-attacks, electronic attacks, disinformation, economic warfare

DOI: 10.2478/raft-2025-0034

tactics and other subversive measures. Currently, a ground offensive response must be supported not only by the effort of aviation and artillery but also by operations in cyberspace. Often, electronic and cyber-attacks carried out within the framework of operations carried out within the framework of the war in Ukraine were not limited only to the state borders of the belligerents, but had multiple implications at the level of neighboring states, international organizations, political-military alliances and other strategic partnerships involved in crisis management and in preventing the escalation of regional and international tensions.

Moreover, limiting the escalation of this war was achieved through permanent dialogue and diplomacy (Vevera, 2021), strategies that blocked a series of information manipulations by non-state actors (such as paramilitary groups, organized crime, hackers and cyber terrorists) who supported one side and encouraged violence, manipulated public opinion, used propaganda and other emotional techniques to the advantage of one of the actors involved and transformed them into unconventional adversaries of conventional armed forces.

The involvement of civilians in war is regulated by international conventions and treaties in the field of International Humanitarian Law, even if they have produced and used low-tech weapons (modified civilian drones, improvised explosive devices, improvised jamming devices etc.), with effects that amplify panic and fear among the military and the civilian population trapped in conflict areas, as well as with other serious psychological effects on global public opinion.

2. Research Method

The purpose of this paper is to highlight the importance of conscious education in the use of mobile phones, by applying technical measures of electronic and cyber defense, as well as by establishing protective measures for communication through these devices, managed by the personnel of military structures. Based on the lessons learned from the war in Ukraine, the present study examines how the lack of regulations, circumvention of technical measures or exaggeration of the application of protective measures generate risks and vulnerabilities with strategic and functional effects at the level of communication and weapons systems.

To this end, we conducted a comparative analysis of reports and other documents from open sources, tracking both events determined by proactive communication (on one's own initiative) and reactive communication (in response to the need for information), against the background of the intensification of actions specific to hostile propaganda and disinformation, with the aim of influencing public opinion, leaders and journalists.

3. Lessons Learned on the Impact of Mobile Phone Use on the Security of Digitalized Systems and Military Activities

The trend of training military forces to be effective in all dimensions of military operations follows two directions, one strategic and the other technological. Military leaders must be able to make decisions in real time, often from incomplete information, which implies great flexibility in thinking and a good ability to adapt to a complex environment. Through education, exercises and training based on essential strategies, they can develop their critical thinking to identify possible biases, to correctly evaluate evidence, to apply logical and rational solutions in order to develop a rigorous approach to problems. In most military

academies, study programs are augmented with disruptive educational technologies (AI/ML), the correct exploitation of which leads to the development of knowledge in an extremely short time.

It is observed that, at the level of active military units, a great vulnerability is represented by the unprepared and untrained human factor. Under this name we include mobilized soldiers, reservists, civilian contract personnel and even civilians, family members or close relatives who maintain contact with permanent soldiers and provide their emotional support. In situations of crisis and conflict, these human factors are much more vulnerable to manipulation, influence and disinformation. Among these individuals, the distortion of perceptions about a certain operational situation will influence the morale of deployed active personnel, decreasing their attention and concentration to accomplish a mission. Moreover, exaggerated fears, expressed within the community they belong to, can create currents of opinion that undermine local support for active military personnel, disrupt multicultural relations within civilian communities but also within military structures (military or contract personnel may come from different cultures and religions), damage or produce new tensions in relations between government institutions/agencies and international organizations, even in collaborative relations between states. All of these are resolved through permanent dialogue and diplomacy, which presuppose a language and conduct based on the sciences and art of communication (Ciupercă, Cîrnu, Stanciu & Cristescu, 2023).

On the other hand, an important factor affecting the morale and cohesion of the troops is the lack of regular communication with families, friends or even with hierarchical superiors. This state, at the individual level but also at the level of combat formations, develops feelings of abandonment and isolation. The lack of clear information about the purpose and progress of the conflict or any exercise in which the soldier is involved can generate confusion and discouragement, both at the individual and collective levels. Within small groups, the lack of communication can develop collective feelings of uselessness, frustration and non-recognition of their sacrifice, which, over time, will generalize to units and large units.

Hence the role and importance of maintaining communication between soldiers and their peers. And if they are deployed at great distances, they will certainly use mobile phones, even if, as the lessons learned from Ukraine show, the use of mobile phones will attract artillery fire or the attention of SIGINT structures.

In this conflict, during the organization and conduct of military maneuvers, both Ukrainian and Russian soldiers used mobile phones. Currently, any citizen, and even more so a soldier, is the owner of a smartphone, which is a pocket computer with which he can organize his daily routine. Having a computing power and an extremely large storage space, users store information such as: contact data, personal data, photos and videos, data and information useful in commercial transactions, other things that do not want to be forgotten. Hackers do not forget this aspect and are constantly looking for vulnerabilities to gain access to this sensitive data.

In military-specific activity, the use of mobile phones, especially smart phones, has revolutionized troop surveillance and artillery fire control. Ukraine has used smart applications to mitigate the effects of Russian drone attacks, especially in the area of civilian and strategic targets (Freese, 2023). Both forward structures and civilians have tracked and reported the evolution of

drones, geolocated the position of enemy troops, followed force maneuvers, located the position of artillery batteries by sound etc. Mobile phones are considered basic devices that have improved C4ISR capabilities. By including civilian communication technologies, kinetic effects have been optimized on a large scale throughout the battle space.

At the same time, the massive presence of electronic warfare systems and the tactic of keeping communication networks and infrastructures operational confirm the importance of collecting information from the calls and mobile devices of the adversary's military and civilians. For example, the Russian Leer-3 electronic warfare system, composed of two drones (Orlan-10) and a ground vehicle equipped with command-analysis-jamming equipment, can simultaneously receive more than 2000 signals, from a radius of 30 km, with the main mission of discovering concentrations of cellular subscribers located in difficult-to-reach areas, or with natural coverage such as forests, riverbeds, urban spaces and other unremarkable areas (Global Defense News, 2022).

Regarding the control of fire based on the geolocation of a mobile phone's emission, it is worth noting the Ukrainian attack with Himars missiles, from Makiivka (Southern Kherson Province) on 01.01.2023. Even though, in the Russian Army, procedures for the use of mobile devices were imposed, the negligence of their application, amid the celebration of the new year, resulted in 400 soldiers killed and another 300 injured (Krever, 2023).

Influencing public opinion through the Internet is another problem that has globalized information warfare, given that anyone can have a mobile phone. Even though video recordings and photos taken with smartphones can serve as evidence in international courts, the shaping of public perception has created, over time, controlled realities, polarized and radicalized the audience. Thus, images of massacres, mass graves, destruction, other horrors of human behavior, narrative stories of people involved in an event etc., were viralized and reposted. The main goal was to desensitize emotionally to the suffering of the enemy and to cultivate a sense of guilt, especially at the level of international public opinion. Even if it did not always work in Ukraine's favor, the speed of online updates, the takeover and dissemination of stories in the mainstream, the involvement of AI technologies in deep-fake propaganda and voice cloning etc., contributed to the development of pro-Russian emotions, with users becoming tired of the Ukrainian struggle for freedom, carried out on social networks, a situation that favored the development of anti-Western sentiments (Karalis, 2024) and the destabilization of Ukrainian society (Mysyshyn, 2024). The broadcasted images, possibly deep-fake, of the surrender of Ukrainian leaders (YouTube, 2024), have generated a significant threat to social cohesion and democracy, a decrease in the confidence of the military and the civilian population in the Ukrainian way of governance and the media's confidence in the success of the global effort to support Ukraine. Moreover, in order to understand the operational environment in Ukraine and to provide security assistance for the defense of Ukraine, the Americans have implemented adapted EUM (end-use-monitoring) regimes, which include, when circumstances allow, regular on-site visits. Thus, the US ensures that its assistance is effective and does not contribute to harm, instability and the amplification of conflicts, both from a political and practical point of view. The Biden Administration's suspicions were manifested in the organization and execution of controls regarding the distortion of support with weapons systems of Western countries

and their misuse. For rapid communication, they used barcode scanning applications included in the inspectors' mobile phones (Yosif & Stohl, 2024).

It is increasingly clear that in the areas where hostilities took place, having a smartphone guaranteed the provision of social assistance and allowed, by connecting to a DIIA web-portal (eSupport), services, protection and support for civilians whose health was affected by Russian aggression (Smusz-Kulesza et al., 2022).

Regarding telecommunications systems and their interconnection with critical infrastructure systems, the type of conflict highlighted their vulnerability to cyber-attacks carried out by non-traditional actors in support of the Russian invasion. In fact, both belligerents requested the support of people who wanted to join a cyber army, since the first days of hostilities (Duguin & Pavlova, 2023). The deactivation of Viasat Inc.'s KA-SAT satellite network on 24.02.2022 led to the interruption of internet service provision, impacting many Ukrainian government and military targets, the energy system, the Ukrainian civilian population, companies both in Ukraine and in many European countries, which propagated the effects of this attack outside the conflict zone (Viasat, 2022). The incident demonstrates that an operation against a specific communications and cyber system can have repercussions on other systems regardless of their location.

4. Results and Discussion

Mobile phones are key elements in ensuring the mobility of instant communication, in real-time location of correspondents and for quick access to critical information. Mobile phones can quickly transmit information (in voice or text messages), images (photos and video captures), as well as GPS coordinates, which constitute essential information for reconnaissance and surveillance missions, for coordinating activities in conflict areas, but also for other systematic activities of civilian life, such as:

– *Fast and secure communication*: Any mobile phone owner can transmit important messages and information within the military chain of command. Depending on the security of the network and the encryption of communications, the use of phones can become a quick method of transmitting orders or requesting support.

– *GPS and navigation*: Most modern phones have the GPS function, which becomes essential for navigating in unknown terrain or, by using a navigation application, to obtain essential data regarding an itinerary and choosing the optimal road.

– *Coordination and planning*: Applications can be installed on a mobile phone that allow the coordination and planning of activities. They can include interactive maps, propose routes, track the evolution of a behavior or the movement of an objective.

– *Facilitating monitoring and information*: Most mobile phones are equipped with video cameras that allow the taking of photos and videos. This allows for online video communications, barcode and QR code scans, document scans, direct translations from any language (via AI) etc.

– *Special applications for electronic support*: In some cases, mobile phones may include applications for interception and surveillance of electromagnetic emissions in a frequency band, as well as radio jamming applications, depending on the available technology.

– *Access to real-time information*: The owner of a mobile phone, through Wi-Fi connections and VPN solutions, can access strategic databases or news platforms, press reports, other information from live-stream platforms or social networking websites etc.

– *Telemedicine and medical support*: In case of injuries or medical emergencies, a mobile phone owner can request rapid medical help or provide information about the condition of victims resulting from an event to medical or paramedical teams.

These technological capabilities come with significant risks to physical or functional security, a situation that transforms them into targets of electronic and cyber warfare. The adversary will constantly seek to analyze data and fragments of personal information, information that generates a behavioral model of the target device owner etc., all of which information is obtained from both the analysis of the content of the communication and the electromagnetic emissions. In the context of modern warfare, this information is necessary in order to establish the current electronic situation and to understand the intentions of the opposing forces.

The main risks and vulnerabilities are:

– *Creating security breaches regarding unauthorized access to sensitive information*: Mobile phones can be easily lost, stolen or compromised. They can store or allow quick access to classified information, operational plans, the content of discussions between various military structures etc. A compromised mobile phone can also be used to intercept transmitted messages. Through "Man-in-the-Middle" attacks, some messages can be modified or destroyed, with effects on the performance of a specific activity;

– *They are vulnerable to cyber-attacks*: By allowing multiple connections, mobile phones become access points for attacks such as malware, phishing, DDoS etc. The exploitation of unauthorized applications by military personnel (for example, unauthorized communication applications or social networks) can generate vulnerabilities by discreetly installing programs that create back-doors, which will be exploited for espionage, data theft or user compromise.

– *They cannot fully ensure data confidentiality*: Multiple reports from technology and mobile phone service providers constantly draw attention to the risks related to confidentiality and the protection of personal and professional data. For example, geolocation functions can allow tracking the location of the user of a compromised phone, without the user knowing that the enemy is tracking and anticipating the movement of the structure to which it is part.

– *Using the mobile phone for multiple purposes also brings hardware and software vulnerabilities*: The race to develop these technologies by implementing new and new technological solutions and applications also produces new vulnerabilities regarding the exploitation of security breaches in operating systems or installed applications. Their remediation is carried out through successive updates, once a certain technological maturity is achieved.

Compromising a single mobile phone can have a devastating effect on a military structure of which we estimate:

– *Compromise of security missions (physical and strategic)*: If a mobile phone is compromised, a hypothetical enemy can gain access to tactical and strategic information, essential for the conduct of missions. For example, he can obtain attack coordinates, battle orders, force disposition, personnel morale etc., all of which endanger the lives of soldiers and the success of planned operations.

– *Endanger the safety of military personnel*: The use of mobile phones to communicate during an activity (firing or other training exercises, preparation or conduct of an attack etc.) can increase the

risk of interception which, in a conflict situation, endangers the lives of personnel deployed in combat positions.

– *Leakage of classified information*: A compromised phone can allow the extraction of classified information by enemy entities or by elements infiltrated into one's own device (special forces, radicalized individuals, organized crime groups, terrorists, spies etc.), the knowledge of which can change the course of a military activity.

Similar to protecting computers, mobile phones must be protected against electronic and cyber threats that can compromise personal data, communications and affect the lives of soldiers. The main protection and risk reduction measures are contained in a series of best practices, essential for a soldier to stay safe, including:

– *Use security features*: These include a passcode, strong passwords, fingerprints, facial recognition etc.;

– *Full Disk Encryption (FDE)*: It is a security measure that protects the data stored on the mobile device, transforming it into a form that is difficult to understand by someone who does not have the encryption key. Most modern smartphones contain the FDE function, which can be activated by default, without affecting other functions of the mobile phone.

– *Software update*: Both the operating system and installed applications have the possibility of updating to the latest versions. These security patches are made by manufacturers in order to eliminate security vulnerabilities. Applications should be installed only from official stores (Google Play or Apple App Store), with great care regarding the permissions granted for operation. Applications with broad permissions can collect a large amount of personal data, which, if the phone is compromised, can be manipulated by malicious actors.

– *Avoid sending sensitive information via text messages*: Even though text messages are encrypted as standard, they can be intercepted and read without sophisticated tools. Apps like Signal, WhatsApp and Telegram offer end-to-end encryption, which provides a good level of encryption when intercepting messages. Not even service providers can access the content of conversations. However, nothing prevents the interception of encrypted content itself. Metadata such as the identity of the participants in the conversations, timestamps, and frequency of communications can be extracted from it. Moreover, in the case of man-in-the-middle attacks, the attacker replaces a participant in the conversation and can establish new encryption keys, modify messages, use malware, or compromise the status of the person who legally owns the attacked phone through inappropriate language.

– *Avoid public Wi-Fi connections*: Public networks can be compromised by cybercriminals. If you must use such a connection, make sure there is a reliable VPN (Virtual Private Network) to encrypt your internet traffic.

– *Using the automatic data deletion function after a number of failed connection attempts*: This function can be useful in case of unauthorized access by a third party, in case of loss or theft of the device, being extremely useful for people who regularly handle sensitive information.

– *Implementing Mobile Dynamic Defense (MDD) technology in smartphones for the military*: This technology is the most secure current solution for using smartphones in secure communications. It allows the use of 4G/5G phone capacity together with voice and data encryption, in encrypted tunnels. Currently, this technology has some limitations, and may not be available in all conflict areas or outside cellular connectivity networks.

In addition, the mobile device's emission can be geolocated, which is why it is necessary to stop all connections when the device is effectively hidden, in tactical missions.

– Last but not least, *electronic and cyber protection procedures at the level of networks and military structures* must be based on user education and awareness of the technical risks and vulnerabilities that it can produce. At the level of each user, personal electronic and cyber security vulnerabilities include patterns of behavior in social networks, in online transactions of any kind and in the way of interpersonal communication. Many leaders do not know how their digital presence can be exploited until they are faced with consequences such as: tracking, fraud, theft of sensitive data and even being the victim of a physical attack. Most of the time, the information necessary to organize a cyber-attack is provided by the victims, through the uncontrolled publication of information related to personal life, family connections, images from vacations or from the work area etc.

5. Conclusions

Digitalization brings great opportunities but also specific threats. At the level of political-military alliances, of which Romania is a part, a series of electronic and cyber security strategies and programs have been established and applied. Especially for critical economic sectors, which are increasingly dependent on digital technologies, solutions and initiatives have been proposed to increase the resilience of critical infrastructures against electromagnetic and cyber threats, as well as other challenges facing Europe, NATO, the economy and global society.

Moreover, chip and mobile phone manufacturers allocate significant resources to identify and neutralize contemporary security vulnerabilities, such as "zero-day" vulnerabilities (i.e. security flaws unknown to hardware manufacturers), to prevent hacking and the installation of malicious software in mobile phone systems. In addition to technical aspects, a major dilemma is how to apply security measures to protect critical infrastructures and essential services in the context of protecting information and respecting individual rights. Commanders are obliged to implement strict measures to protect essential infrastructures and subordinate personnel.

On the other hand, these measures must be consistent with the protection of fundamental rights of the individual, in particular the right to privacy and the protection of personal data. In this context, a balance must be established between: the collection and processing of personal data without violating the right to privacy, electronic and cyber surveillance and control without the authorities intervening in the online activities of active personnel, the way to implement restrictive measures without affecting freedom of expression, the right to association or increasing self-censorship, the objectives and missions of the governing authorities and the transparency of decisions regarding the protection of data of active personnel, personnel in the army reserve or those in the general reserve.

The challenges are multiple and complex, and the solutions must be well-founded legally and technologically, in order to ensure both the essential protection of society, respect for the fundamental principles of the rule of law, and the security of military infrastructures. It is obvious that the use of mobile phones by the military brings huge benefits in terms of efficiency and rapid communication, with significant security risks. For effective protection, it is essential that, at the level of all military structures, advanced electronic

and cyber protection measures are adopted, and from a social aspect, personnel education for conscious assumption regarding exposure to specific risks.

We emphasize that interrupting the operation of mobile phones as a protective measure, in sensitive areas or for a period of time, is not as effective as desired and does not ensure effective protection. It is only a simple measure to prevent and eliminate vulnerable points of access to some sensitive information. Without adequate education of active personnel in order to form a culture of electronic and cyber security, only an increase in individual frustration and the creation of new vulnerabilities in the cyber defense of any activity is achieved.

By developing this analysis, we will seek to identify those benchmarks that establish the balance points between security and accessibility functions, in relation to measures to protect personnel confidentiality, a ratio that we consider essential for the management of electronic and cyber security at the level of military infrastructures.

REFERENCES

Ciupercă, E., Cîrnu, C., Stanciu, A., & Cristescu, I. (2023). *Leveraging socio-cultural dimension in cyber security training*. (pp. 5242-5248). DOI:10.21125/edulearn.2022.1239.

Duguin, S., & Pavlova, P. (2023). The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. *European Parliament, Directorate-General for External Policies, Policy Department, 10*. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf.

Freese, K. (2023). *Smart Phones Playing Proeminent Role In Russia-Ukraine War*. TRADOC G2. Available at: https://oe.tradoc.army.mil/2023/08/10/smart-phones-playing-prominent-role-in-russia-ukraine-war/.

Global Defense News. (2022). *Russian troops using Leer-3 able to jam Ukrainian army mobile phone signals within 30 km*. Army News. Available at: https://armyrecognition.com/news/army-news/2022/russian-troops-using-leer-3-able-to-jam-ukrainian-army-mobile-phone-signals-within-30-km.

Karalis, M. (2024). The Information War: Russia-Ukraine Conflict Through the Eyes of Social Media. *SFS Georgetown Journal of International Affairs*. Available at: https://gjia.georgetown.edu/2024/02/02/russia-ukraine-through-the-eyes-of-social-media/.

Krever, M., Voitovych, O., & Tarasova, D. (2023). *Ukraine claims hundreds of Russian troops killed in strike; Moscow says 63 died*. CNN World. Available at: https://edition.cnn.com/2023/01/02/europe/ukraine-makiivka-strike-intl/index.html.

Mysyshhyn, A. (2024). *Advanced Technologies in the War in Ukraine: Risks for Democracy and Human Rights*. German Marshall Fund, GMF ReThink report. Available at: https://www.gmfus.org/news/advanced-technologies-war-ukraine-risks-democracy-and-human-rights.

Smusz-Kulesza, M., Fedorova, A., & Moysa, B. (2022). *Social rights in Ukraine in time of war*. Report on the needs assessment, Council of Europe, p. 41. Available at: https://rm.coe.int/needs-assessment-eng-2/1680a9b407.

Vevera, V. (2021, October 20). Evaluation of Digital Diplomacy as a Form of Soft Power Projection in European Union CSDP Missions. *Bulletin of "Carol I" National Defence University*, 41-46. Available at: https://revista.unap.ro/index.php/bulletin/article/view/1225/1190, accessed on January 12, 2025.

Viasat. (2022). *KA-SAT Network cyber attack overview*. Corporate News. Available at: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

Yosif, E., & Stohl, R. (2024). *Ukraine Risks Revisited*. STIMSON Commentary, Conventional Defense Program. Available at: https://www.stimson.org/2024/ukraine-risks-revisited/.

YouTube. (2024). *Ukrainian Soldiers Surrender, Detail Zelensky's Explosive `Bleed Russia'Mission*. Watch. Available at: https://www.youtube.com/watch?v=Brg11Ov5lx8.