The Trench Electronic Warfare – A New Threat to Critical Infrastructures

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

Abstract: The trench electronic warfare concept comes from the language of fighters on the Ukrainian front and became popular through its promotion by journalists and war correspondents. The paper is based on a semantic and content analysis of this new warfare concept and identifies possible directions of evolution applicable in various moments of modern war. At the same time, the paper highlights those aspects that, in peacetime, can become threats to critical infrastructures. Against these, some measures that can strengthen the strategies for the protection of critical infrastructures against unwanted events are proposed, such as unexpected effects or accidents caused by amateurs with minimal knowledge in the field of electronics, computing and IT. Furthermore, the risk of this concept being applied to combined attacks on critical infrastructure by criminal and terrorist organizations is growing. It is a danger anywhere in the world at this time of numerous social upheavals.
Keywords: electronic warfare, trench electronic warfare, critical infrastructure protection, cyber security.

INTRODUCTION

Electronic warfare is a form of military conflict in which electronic and cyber technology is used to gain tactical and strategic combat advantages in the electromagnetic environment (*Federation of American Scientists, 2000*). In general, armed forces use electronic warfare measures to identify the geographic location and characteristics of emissions from radars, weapons and munitions equipment and radio communication systems, but also emissions the IF frequency spectrum. The aim is to intercept adversary communications, to monitor force maneuvers, to attack computer systems and communications and radar networks in order to substantially contribute to the defense and security of its own systems that exploit the propagation of electromagnetic waves.

Electronic warfare can be used in many different ways such as jamming and disrupting enemy radio communications, intercepting enemy information and locating radio-emission stations, electronic disinformation and information manipulation etc., all of which are accomplished in a unique concept of

https://doi.org/10.54851/v5i2y202301

information operations. These are also used for ensuring the electronic protection of own forces against strikes with vector guidance through electronic systems. In addition, electronic disinformation can influence enemy's behavior by causing confusion regarding the control of information and catastrophic delays in enemy's own decision-making.

Therefore, electronic warfare includes symmetric actions with a force protection role or asymmetric actions executed, predominantly, for a smaller force aiming to compensate for combat power deficiencies and to create, in some directions or domains, tactical advantages in front of a more powerful force.

Even if electronic warfare has not undergone any spectacular transformations in recent years, with most modern armed forces limiting themselves to conceptual updates included in their own military strategies and doctrines, the study of the evolution of the conflict in Ukraine attests and confirms that electronic warfare is an essential component of any military operation (Beale, 2023). As it can be seen, military technology and electronic equipment have evolved a lot in recent times, conquering new fields such as cyberspace (Pomerleau, 2022). These, due to the specific nature of military operations with frequent maneuvers of the combatant forces, are dependent on electromagnetic waves in communication and sensors networks for the connection between the locations of combat positions. Therefore, the armed forces of the actors involved in a conflict are provided with a wide range of mobile electronic tools to detect, intercept and destroy the adversary's communication systems. Currently, in addition to traditional equipment deployed on land, naval, air and space platforms that require advanced technologies, radio jamming and cyber attack can be carried out with drones (Kaspersky, 2023).

Thus, electronic warfare has become more sophisticated and and has led to an insidious fostering of innovative skills and technologies even for force confrontation sequences. Even though some of these have a relatively short applicability duration, their effectiveness in the decisive moments of the war can help to surprise the opponent, increase his resource consumption, and finally achieve victory. In this context, in the background of the study of the war in Ukraine, the concept of trench electronic warfare emerged, which represents a form derived from the traditional lessons of electronic warfare to which cyber actions, drones and improvised devices are added. Why should it be studied? Because it is insidous, unpredictable and very difficult to control, it can always be added to the arsenal of weapons that a terrorist group or criminal organization can use against a critical infrastructure.

CRITICAL ANALYSIS OF THE TRENCH ELECTRONIC WARFARE CONCEPT

The trench electronic warfare is not yet a recognized term in any military regulations or doctrine. It began to be used in the publications of war correspondents being extracted from the jargon of both the Ukrainian and Russian militaries (Focus, 2023a). It probably originates from the summation of the notions of "trench warfare" and "electronic warfare". Even though specialized reports and analyses that use this notion have not yet been identified, it has been noticed that this concept has become popular among those who use the Russian language to analyze innovative aspects of the conflict in Ukraine, resulting from the launch of the so-called "Special Military Operation" of Russia on 24th of February, 2022.

Thus, on 14th of March 2023, on Facebook, a Ukrainian military man with the pseudonym Serghei Flesh described how created portable electronic warfare device to use against Russian drones in trench electronic warfare (Flash, 2023; Focus, 2023b), as it can be seen in Figure 1.

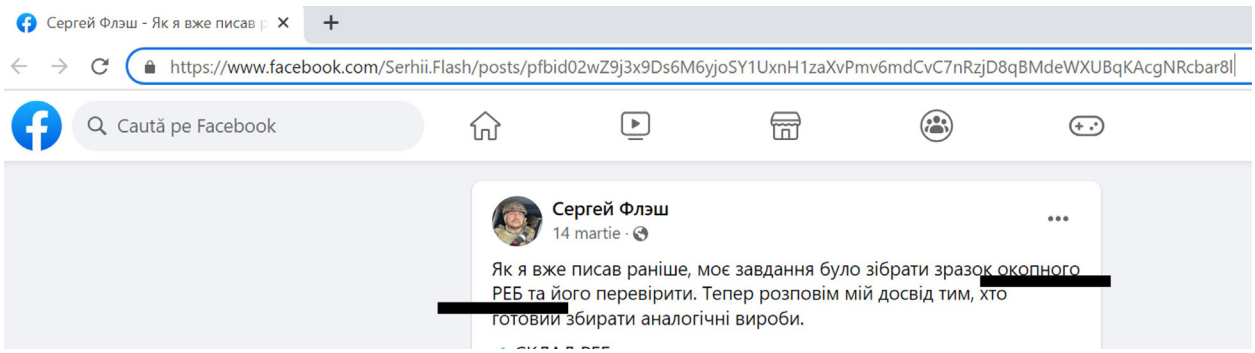

Figure 1. *Screenshot of the term trench electronic warfare (Flesh, 2023)*

In his post, he described how he accomplished the task of identifying, building, and testing an electronic device for trench warfare, and highlighted the experience gained for anyone interested in making such a device. He also answered questions and comments about how to purchase components and the manufacturing process of the device, providing photos and links to other sites. Of note is the accuracy of technical data and the indication of sources of purchase with information on price, reliability, robustness of components, as well as comparative analysis between sources of purchase and ways of buying to avoid the embargo, all against the background of promoting strong feelings of stimulating the fight against the Russians possessing far too advanced electronic warfare technology.

This post has a lot of shares and the level of credibility of the information is not in question. However, the popularity of the term "trench electronic warfare" has not gone unnoticed and, therefore, the identification of its content was sought.

Following the research conducted, the media concept of "trench electronic warfare" can be approached through two semantic directions, namely:

- Limitation of electronic warfare measures that can be used depending on the capabilities of the troops deployed in immovable or semi-mobile combat positions, on the contact line; or
- Depiction of electronic warfare being executed between military forces engaged in a weakening war.

In essence, the front line of the war in Ukraine was and is predominantly static, an observation resulting from the reduced mobility relative to the capabilities of the forces. In his article published following the war experience lived alongside Ukrainian soldiers, on the front in the Donetsk-Donbas region, during the fighting in 2017, Nolan Peterson concluded that this static war in the Donbas has effectively become a training ground for some of the newest combat technologies of Russia – especially small drones and electronic warfare assets (Peterson, 2021). After six years, this trend has remained unchanged.

From the point of view of mobility, an analogy with the First World War can be made, during which both sides engaged in static trench warfare, using artillery, machine guns and other attrition weapons, without making significant progress in gaining strategic advantage (Stănescu, 2022).

Currently, benefiting from modern weaponry, both actors engage in a trench electronic warfare in contact, a situation in which they start a battle for weakening the adversary over a long period of time, with advanced electronic technologies and with few decisive results in the electromagnetic environment, related to the spatial dimensions of conflict (on land, air and sea), and in cyberspace.

Even though it retains its known role, place, and destination, a trench electronic warfare may involve

innovative techniques and tactics driven by the use of electronic equipment and subassemblies that were not previously intended to be used as components of specialized combat equipment. The purpose of the actions is to gain an electronic advantage at a tactical-operational level. It can consist of the interception and surveillance of the adversary's radio communications, the disruption of some radio links of the troops, but also of the command and control systems of the drones or some strike vectors, the creation of confusion and misinformation of the troops and, last but not least, the influencing of public opinion.

Therefore, the trench electronic warfare is an asymmetric conflict in which the technology and capabilities of the adversary are very difficult to quantify and the equipment used can be very easily camouflaged among the civilian equipment of the non-combatant population. It can also be difficult to determine who controls the initiative and which side has the strategic advantage. In addition, trench electronic warfare can be difficult to manage because technology changes rapidly and requires constant adaptation to new tactics and technologies used by the enemy. From this point of view, this form of warfare can be more expensive for the force that does not exploit it, because it does not require significant investment in advanced electronic technologies and resources to avoid the effects of an array of improvised devices that can be abandoned, destroyed, or recovered and reused.

Generalizing, the model of trench electronic warfare can be identified in a wide range of conflicts, such as: wars between states or military alliances, operations executed by special forces, the fight against terrorism, etc. The results of this type of electromagnetic battle can decisively influence the way in which conflicts end.

Please note that not all electromagnetic interference represent an electronic warfare. If the concept of "trench electronic warfare" is considered a form of traditional electronic warfare, it must involve only specialized forces and means that belong to military structures and respect the conventions of war. Any type of activity in the electromagnetic environment that is carried out by civilian structures and does not fall under the specific laws of warfare, even if they have similar targets, is not electronic warfare. For example, the jamming executed on the broadcast of a radio station or any command-control system of a critical infrastructure is not electronic warfare if it is executed by radio broadcasts of a pirate radio or by non-compliance with the electromagnetic compatibility rules. It could be similar to terrorist activity not recognized as military warfare in the electromagnetic environment.

Moreover, the current convergence of electronic and cyber warfare actions, in addition to a multitude of beneficial effects, has also produced the opening of back doors for malicious applications. Against the background of conceptual confusions caused by misperceptions, under the effect of news to shock the audience, many military terms are distorted. Thus, a Wi-Fi hacktivism is assimilated to electronic warfare. There are people who, without any training in the domain, equated ATM thefts with electronic warfare, because they were carried out with electronic devices. Not every act of radio interception, electronic surveillance, jamming or protection of an electronic device can be an electronic warfare issue.

However, the lessons learned about electronic warfare must contribute to the development of technologies and capabilities for national security and defense of critical infrastructures.

THE INFLUENCE OF TRENCH ELECTRONIC WARFARE ON CRITICAL INFRASTRUCTURE SECURITY

One of the hallmarks of the war in Ukraine is the long-range strike of Ukrainian critical infrastructures to undermine the defenders' resistance, especially those located in urban areas. Artillery or missile fire strikes were executed concurrently with cyber, satellite and electronic warfare support. Against the backdrop of the poor provision of modern communications equipment and the low quality of radio operators, namely the mobilized

militaries who did not go through the full training period, electronic warfare generated some lessons learned that require careful study.

In the initial phase of the war, the equipment was identical, being manufactured in Russia, which caused multiple interferences due to the faulty management of the electromagnetic frequency resource concentrated in a relatively limited geographical space. Subsequently, the provision of NATO-compliant equipment to the Ukrainians increased the level of electronic protection of the communications of the Ukrainian battle groups. However, in areas with urban agglomerations still inhabited by civilians, the Ukrainian military used GSM services, making it very difficult to identify military phone emissions compared to the civilian ones. Even the Russian military was connecting to Ukrainian GSM networks. It is well known the moment when the Russian forces, trying to destroy the antennas of the cellular telephone systems in the Kharkiv region, disabled the services of their own military cryptophony network. Therefore, due to the use of the same type of technologies, the Russians could not completely disrupt the cyber infrastructure through cyber and kinetic strikes. Later, both actors used cellular telephony to locate and strike fighters using GSM mobile terminals (Devine, 2023). Any careless use of a mobile phone attracts a destructive strike with missiles and especially drones.

Similarly, the losses in drones, on both sides, attest to their intensive use and the diversity of missions. Both kinetic and electromagnetic measures are used to combat them. This is how anti-drone systems with laser-guided munitions, anti-drone drones, jamming equipment for the drone's sensors and GPS system, etc. appeared (Skove, 2023).

In addition, in order to achieve the objectives established within the combat missions, enormous amounts of military equipment were allocated to support the execution of maneuvers on the ground, in the air and in the electromagnetic environment in a difficult terrain that created great mobility problems.

Probably, the concept of trench electronic warfare arose to describe the use of improvised equipment made from components recovered from the electronic devices of destroyed systems or purchased from the electronics and hobbyist markets, for combating drones and confusing strike vectors. Although trench electronic warfare can be considered a less violent form of military conflict, it can have devastating effects on a country's critical infrastructure and economy.

If some conclusions about the manufacture and use of electronic jamming means are applied by a criminal or terrorist organization and used to execute a connective kinetic and electronic attack on a critical infrastructure, the effects can be devastating. It does not matter what name this new form of attack would take and whether or not it is executed by a military force. For example, an electronic attack measure executed in support of a cyber operation on a state's energy or financial networks can disrupt a country's economy and affect the lives of its citizens.

In addition, the trench electronic warfare can also have effects on international relations and diplomacy. The disclosure of sensitive information or the establishment of disruptive effects in the electromagnetic environment related to state border areas can damage diplomatic relations with neighbors and affect cooperation within the international community.

It can be seen that, with the increase of dependence on technology and the expansion of cyberspace, any amateur with minimal knowledge in the field of electronics, being assisted by artificial intelligence, can create an improvised device whose experimental use can produce effects within a radius of a few hundred meters. The question, therefore, arises as to what would happen if a critical infrastructure facility was in his vicinity and if that "researcher" was radicalized by a terrorist organization and ordered to carry out such an attack.

Not only critical infrastructures of national and international interest can be affected. The activity specific to this new concept, planned and carried out by a malicious non-military entity, can be directed at any private company

and public institution to obtain information on business plans, technological and industrial secrets, financial information, and personnel data including those of the top staff, etc. Such peacetime actions will complete the panoply of industrial and political espionage methods.

And all this is just a click away. As it could have been seen, information on how to make an improvised device for electronic protection is easy to find on the Internet. But what to protect as an individual and against whom? These are similar to tips for terrorists for IED (improvised explosive device) fabrication. For example, how hard would it be for an amateur researcher to set out to build a device in his garage, with an antenna, a modem, a tablet and open-source software, to finally emit a signal to protect himself against a nuclear attack? This hypothesis is surreal but who can guarantee that somewhere there would not be a person who thinks about this. And if, in his attempts, he emits signals that jam the radio systems of an airliner on an international flight route, the premises of an air catastrophe are easy to understand. Therefore, the concept of trench electronic warfare has deep ethical and moral implications and should be regulated by law, especially for the protection of critical infrastructures.

CONCLUSIONS AND PROPOSALS

The "trench electronic warfare" is a term that must remain only in the jargon of military specialists. It may represent a form of electronic warfare deployed in a military conflict in which advanced technologies are used to gain operational and strategic advantages and to control enemy radio and electronic sensor networks. Its content may include a series of measures to prevent and manage conflicts in the electromagnetic environment and in cyberspace in order to apply the best forms of defense and protection of own forces and means of combat.

The non-military variant of the content of this form of combat must not include the name of warfare in order to avoid confusion or misperceptions. Because they will be closely related to cyber attacks and cyber crises, these should be recognized as phases of strikes and be regulated through the effort of international diplomatic cooperation.

This form of warfare is very difficult to manage and can have devastating effects on a state's critical infrastructure and its economy. In order to reach and manage such conflicts, at the governmental level, at the level of companies, but also at that of individual users, a series of measures must be taken which may include:

- Investment in cyber security technologies, including the development of electronic and cyber defense capabilities, while training staff in managing a threat of this type;
- Development of policies and rules to prevent events created by the enthusiasm of individual researchers with improvised devices. These should not block the initiative but allow a control of the resources, while providing educational facilities to understand the correct ethical and moral aspects of the research carried out;
- International cooperation in order to establish norms and standards regarding cyber security;
- Prioritization of the education of individual users in order to correctly understand the strategies and policies adopted for the protection of systems and networks connected in the electromagnetic environment. These should include both basic aspects of cyber security (creating strong passwords, updating software, avoiding opening suspicious links or attachments, etc.) and basic electronic protection aspects to avoid electromagnetic interference;
- Raising awareness among all the users that a quick reporting of functional anomalies of cyber and electromagnetic security to the specialized services can help both in avoiding the occurrence of problems resulting from ignorance and in discouraging some criminals

from using this kind measures. A quick intervention will block the propagation of the unpleasant effects and prepare the specialists through a better understanding of the cyber and electromagnetic threats.

It is important to underline that electronic warfare is a very dynamic field and is continuously evolving. Specific risks and threats are changing rapidly. In convergence with the field of cyber attacks, the result must be carefully studied and security measures must be constantly updated to be able to deal with new threats.

Also, greater attention should be paid to aspects related to respect for human rights, privacy, and human health, in the context of the development of new cyber and electromagnetic technologies. Even if the monitoring and interception of communications can be justified in certain national security situations, they must be carried out in accordance with the fundamental norms and values of society, without restricting freedom of expression and the right to privacy.

It is essential that all members of a society act to prevent and manage specific threats. For achieving this goal, a series of measures that should be adopted at individual level, in order to deal more easily with a hypothetical event of this type, are proposed:

- Encryption of personal data – by using encryption algorithms, personal data can be protected against interception and unauthorized use;
- Authentication when using an electronic device – using two-step or biometric authentication can help protect user accounts and data;
- Installation of intrusion detection systems – the use of applications that continuously monitor traffic in WI-FI networks and for IoT devices used at home. They can identify and prevent possible cyber attacks carried out both remotely and from the border area;
- The use of backup and data recovery systems – such a system allows data recovery in the event of a cyber attack that leads to data loss or encryption, as well as deterring attackers by minimizing the effects of the attack;
- User awareness and education –today's users can be people without university degrees in computer science and IT. Through expansion of digitization, anyone can use a device connected to a network or an application on the Internet. Everyone must be aware of the importance of cyber security and respect the rules established by both the manufacturer of the respective electronic device and the network administrator, in order to avoid exposure to cyber and electromagnetic threats.
- Finally, governments must get involved in establishing a mass educational framework and not just in stimulating the training of specialists. A framework of information cooperation between the state, companies and individual users can raise both the educational level and the assurance of a higher level of cyber security. Moreover, by establishing international agreements and treaties that regulate behavior in cyberspace and the electromagnetic environment, traditional norms adapted to the new values of the digital society can also be promoted.

It is also important that there is continuous development of cyber security and electronic protection technologies through research and development to deal with the rapid evolution of cyber and electromagnetic threats. In the context of trench electronic warfare, it is essential that governments, through specialized structures, the academic environment of scientific research, as well as relevant companies assume responsibility for protecting their own information and activities against the background of identifying and developing appropriate security measures in the event of a specific threat. It is important to understand that fostering a cyber security culture among users also requires investing in mass educational programs, not only for specialists. Through educational and awareness campaigns by means of which citizens are systematically and

persistently taught the basics of cyber security, information about cyber risks and how to protect against them will be assimilated.

At the level of profile companies, there should be better cooperation with the academic environment for the development of cyber security technologies. Only the testing of cyber products, in an academic environment, by hundreds of students, can generate pertinent observations to improve and strengthen the performance of specific products.

Finally, it can be observed that only an integrated approach involving all actors in society can help find appropriate solutions to face the content of the concept of trench electronic warfare and any other specific non-military threat. Encouraging public-private partnerships in the cybersecurity industry can make an important contribution to protecting information and data in the electromagnetic environment and cyberspace. In addition, companies should be transparent about their cyber security policy and work with governments and other organizations to prevent cyber attacks and combat online criminal activities.

Therefore, the trench electronic warfare is a real threat to the cyber security of a state, against which preventive measures must be taken through proper collaboration and cooperation among all actors. On the other hand, trench electronic warfare can stimulate the emergence of solutions and the development of new technologies for the prevention and detection of specific pre-war parameters. For example, artificial intelligence, big data analytics, blockchain, cryptography and cyber-physical systems can be used to identify new attack patterns, identify vulnerabilities, and improve cyber security. It must be remembered that cyber security is a collective responsibility and that is why preparing to face such a threat becomes a national responsibility, where every individual must concern himself with his personal preparation. It also involves participation in theoretical, practical, and combined training and education programs to test the capabilities of organizations to respond to such threats. The ultimate goal is to protect critical infrastructure in any field, such as power grids, water systems, financial systems and other essential services.

If trench electronic warfare is a major challenge for states and organizations around the world, the protection of critical infrastructures that serve a society must be a priority objective for any citizen.

REFERENCE LIST

Beale, J. (2023) Ukraine war: How old tech is helping Ukraine avoid detection. *British Broadcasting Corporation - BBC*. https://www.bbc.com/news/world-europe-65458263 [Accessed 11th May 2023].

Devine, K. (2023) Ukraine war: Mobile networks being weaponised to target troops on both side of conflict. *Sky News*. https://news-sky-com.translate.goog/story/ukraine-war-mobile-networks-being-weaponised-to-target-troops-on-both-sides-of-conflict-12577595?_x_tr_sl=en&_x_tr_tl=ro&_x_tr_hl=ro&_x_tr_pto=sc [Accessed 12th May 2023].

Federation of American Scientists. (2000) JP 3-51. *Joint Doctrine for Electronic Warfare*. https://irp.fas.org/doddir/dod/jp3_51.pdf [Accessed:11th May 2023].

Flesh, S. (14 March 2023) *Facebook*. https://www.facebook.com/Serhii.Flash/posts/pfbid02wZ9j3x9Ds6M6yjoSY1UxnH1zaXvPmv6mdCvC7nRzjD8qBMdeWXUBqKAcgNRcbar8l [Accessed: 10th May 2023].

Focus. (2023a) *Ukrainian engineer assembles "trench EW" against drones of the RF Armed Forces: how it works (photo) [Украинский инженер собирает "окопный РЭБ" против дронов ВС РФ: как он работает (фото)]*. https://focus.ua/digital/551792-ukrainskiy-inzhener-sobiraet-okopnyy-reb-protiv-dronov-vs-rf-kak-on-rabotaet-foto?_x_tr_sl=ru&_x_%E2%80%A6 [Accessed 11 May 2023].

Focus. (2023b) *The Ukrainian "trench" EW will be able to protect the soldiers of the Armed Forces of Ukraine in the trenches on the front line: what is known. [Український "окопний" РЕБ зможе захищати солдатів ЗСУ в окопах на передовій: що відомо].* https://focus.ua/uk/digital/555214-ukrainskiy-okopnyy-reb-smozhet-zashchishchat-soldat-vsu-v-okopah-na-peredovoy-chto-izvestno [Accessed 11th May 2023].

Kaspersky (2023) *Security and drones – what you need to know*. https://www.kaspersky.com/resource-center/threats/can-drones-be-hacked [Accessed: 11th May 2023].

Peterson, N. (2021) Front-Line Report: Modern trench warfare in Eastern Ukraine. *Sandboxx, Coffe or Die blog*. https://www.sandboxx.us/blog/front-line-report-modern-trench-warfare-in-eastern-ukraine/ [Accessed: 11th May 2023].

Pomerleau, M. (2022) Services working to convergence EW, cyber warfare capabilities. *DefenseScoop*. https://defensescoop.com/2022/09/30/services-working-to-convergence-ew-cyber-warfare-capabilities/ [Accessed: 11th May 2023].

Skove, S. (2023) US Sending Experimental Anti-Drone Weapons to Ukraine. *Defense Systems*. https://www-defenseone-com.translate.goog/defense-systems/2023/04/us-sending-experimental-anti-drone-weapons-ukraine/384801/ [Accessed: 12 thMay 2023].

Stănescu, D. (2022) Daily life in the trenches, the perception of time, the imaginary of the Romanian front in the summer of 1917. [Viață cotidiană în tranșee, percepția timpului, imaginaru frontului românesc din vara lui 1917]. *Historia*. https://historia.ro/sectiune/general/viata-cotidiana-in-transee-perceptia-timpului-571181.html [Accessed: 12th May 2023].