10.53477/2668-2028-21-39

DIGITALIZATION OF THE MODERN FIGHTING FIELD UNDER CYBER SECURITY

Ovidiu-Dumitru RUSU, PhD candidate
Lieutenent-colonel, Doctoral School, "Carol I" National Defense University,
rusuodumitru@yahoo.com

Sorin TOPOR, PhD
Captain (N), Professor, "Carol I" National Defense University
sorin_topor@yahoo.com

Abstract: *The digitalization of the modern battlefield is a product of technological development in the field of communications and information technology. With the digitalization of modern communication systems and information technology, malicious programs/applications have been developed that can destabilize the cyberspace infrastructure. The complexity and diversity of cyber-attacks have generated fierce competition among states to ensure supremacy of cybersecurity in cyberspace. Most cybersecurity experts appreciate that research in this relatively new field is only at the pioneering level. The future and technological evolution in the field of cybersecurity will show us that, at the moment, very little is known about how cyberspace will look and develop. Although the civilian environment has the supremacy in terms of the technological development of cyberspace, it is certain that the military environment will import new technologies and adapt them to its own requirements.*

Keywords*: digital revolution; digitization; communications and information technology; cyber security; cyber warfare.*

Introduction

The digital revolution, considered the fourth industrial revolution is a phenomenon that was officially discussed for the first time at the International Conference in Davos, SWITZERLAND, held on January 23-26, 2016[1].

The use of the new concept was based on the human-technology binomial and refers mainly to the interaction of technologies in the real world, the biological world and the digital world.

If the time horizon in which the Digital Revolution appeared is not clearly delimited (it is estimated that this stage of technological evolution is outlined after the year 2000), the other three industrial revolutions being quantified much more accurately.

The first Industrial Revolution begins in 1784 when the power of water, coal and steam is used to mechanize the production process.

The second Industrial Revolution appeared about a century later, more precisely in 1880, with the use of electric power in the production process.

The Third Industrial Revolution has been showing its qualities since 1969, when electronic equipment and information technology were used to automate production[2].

We notice that one of the main goals that led to the realization of the industrial revolutions was the growth and modernization of the production process.

Also, analysing the time gaps in which industrial or digital revolutions have made their presence felt in society we can say that they have a characteristic that can be quantified, namely, the time frame at which they occur is permanently reduced. If the time gaps between the occurrences of the first industrial revolutions are about a century, between the third Industrial Revolution and the fourth Digital Revolution, the time period is about 50 years, half of the previous intervals.

[1] https://www.cnbc.com/2016/01/19/davos-2016-whos-attending-the-world-economic-forum-and-whos-not.html, accessed on 31.12.2020, at 08.05.

[2] Dorel Banabic, *The evolution of technology and technologies from the first to the fourth industrial revolution and their social impact,* Romanian Academy, 2018.

In this regard, there are three pertinent questions to which the scientific world does not yet have the complete answers:

a) At what time interval will the fifth revolution be recorded?

b) To which field of activity will the fifth revolution correspond?

c) What will be the official name of the fifth revolution?

If the time horizon and the name of the fifth revolution are more difficult to anticipate, it is estimated that the field of activity will be represented by artificial intelligence, by achieving a symbiosis between man and artificial intelligence.

Digitalization of the modern battle

The emergence of the Digital Revolution has generated a number of changes and even paradigm shifts in terms of planning, organizing, conducting and evaluating military operations.

After the end of the Second World War, the victorious states, and not only them, generated fierce competition in the field of armament and technological supremacy in the production of weapons systems.

This global competition recognized in history as the "Cold War", whose main actors were the USSR and the US, has led some states to develop hitherto unknown military capabilities (especially nuclear ones) in order to discourage initiation of any major conflict.

Despite all these attempts, military conflicts did not cease to exist, but their intensity and duration were not similar to those of the Second World War. The aims of triggering the new military conflicts were multiple and complex: the resizing of certain spheres of influence at regional and global level, the fight against terrorism, different ideologies, resources, the annexation of certain territories, etc.

The digitization of military platforms and military equipment operating in the tactical, operational and strategic field will ultimately generate a complex digital map that will allow on the one hand the real-time display of all equipment and military operating in the area of responsibility, and on the other on the other hand, corroboration with other information from other credible sources will significantly contribute to the exercise of command and control by military leaders over subordinate forces.

Basically, by digitizing the battlefield, the commanders have at their disposal an augmented reality consisting of the physical reality existing in the field over which are superimposed a series of digital contents that do nothing but improve the real situation from an informative point of view.

The final decision belongs to the commander who through his staff will analyze the augmented reality on the ground, will corroborate it with other information from other sources and will establish the mission of subordinate forces after conducting an analysis of optimal courses of action.

Connecting combat equipment/combat platforms and the military to communications systems and information technology will generate a huge amount of data that will give rise to the following problems:

- Is there enough storage space for the data generated?

- How will the false or non-valuable data be separated from the important data in the decision making?

- Are there algorithms/applications for a correct data analysis?

- How will data (from a cybernetic point of view) be protected in communication systems and information technology?

- How will the communications infrastructure and information technology be physically protected?

All these problems mentioned above, and certainly others that will be identified, must be solved in a professional manner by the military specialists by adopting specific and timely measures for each problem.

The digitization of combat equipment/platforms (smart weapons and ammunition, combat robots, unmanned aircraft, driverless vehicles) ensures better efficiency in the tactical field, but the vulnerabilities identified are increasingly numerous and complex generating a series of major risks.

Lately, there is more and more talk that robots with artificial intelligence capabilities will gradually replace the professional military human resource. It is a point of view that raises a number of issues to which military decision-makers do not yet have the appropriate answers. But one thing is certain: the human dimension will long have control over military decisions on the modern battlefield.

Digital field cyber security

The development of military communication systems and information technology, the digitization of combat equipment/platforms, the implementation of artificial intelligence capabilities in certain structures of the armed forces have obviously led to an increase in vulnerabilities and associated risks in cyberspace.

Many states with modern armies have set out to invest substantial funds in research to ensure cyber security, but also in the training and education of specialists in this complex and unpredictable field.

Every modern army wants to have at its disposal well-trained force structures capable of guaranteeing cyber security.

Ideally, each organizational entity that manages/uses communication systems and information technology should have the necessary resources (financial, technical and human) to enable it to combat hostile cyber actions.

The training of cybersecurity specialists is a complex and long-term process that must be carried out continuously in optimal conditions.

The participation of Romanian military specialists in the exercises organized at national level (under the leadership of SRI - Romanian Intelligence Service) or at NATO level (under the leadership of the Center of Excellence for Cooperation in Cyber Defense) is absolutely necessary, first of all, to acquire new skills. The exercises organized by the Romanian Intelligence Service and the Center of Excellence for Cooperation in the Field of Cyber Defense are activities in which various scenarios close to the realities of the cyberspace are simulated[3].

Also, the entities responsible for cyber security organize a series of courses structured on modules that offer participants the opportunity to train theoretically and practically on levels.

Knowledge of cybersecurity legislation is another important aspect that communications, information technology and cybersecurity specialists need to acquire and propose amendments to improve/modify it.

Reality reveals to us every day that there is a legislative gap in the field of cybersecurity which must be eliminated by constantly updating the current legislation with concrete amendments.

Another problem identified in cybersecurity is that some countries in the world refuse to align (only partially accept) to international law on rules regarding navigation or copyright in virtual space. In most cases, such state entities motivate their own actions by stating that complying with such rules would seriously harm national security.

The digital components of the modern battlefield can be affected to a greater or lesser extent by hostile cyber actions. The operation of digital combat equipment/platforms at optimal

[3] https://www.sri.ro/articole/exercitiul-national-de-securitate-cibernetica-cydex-editia-iv, accessed on 31.12.2020, at 08.45.

parameters depends on the existence and application of cyber measures in time, on the reaction-response principle.

The desire of military leaders to ensure the success of their military operations leads them to use a wide range of available capabilities. In this sense, the development of cyber warfare capabilities (offensive and defensive) is a priority for all states with modern armies.

Achieving information superiority in armed confrontations is a key requirement that must be ensured through all available means. An essential role in achieving information superiority is played by communications systems, information technology and cyber security of digitized combat equipment/platforms.

However, for the proper functioning of digitized combat equipment/platforms, it is mandatory to ensure their cyber security by implementing appropriate security policies that generate prompt and effective responses.

In principle, the main threats in cyberspace can arise from three directions:

a) a direction is represented by the physical part where direct attacks (missiles, artillery, sabotage, etc.) can be executed against the infrastructure elements of communication systems and information technology, digital combat equipment/platforms or social engineering actions;

b) the second direction consists of programs/applications through which the opponent can execute cyber-attacks by introducing malicious programs/applications that can infect the hardware or software part of the systems;

c) the last direction could be represented by the hostile actions executed by the members of their own organization.

We appreciate that state or non-state actors operating in cyberspace are in most cases invisible and difficult to identify. It must always be borne in mind that cyber actions carried out by a single person can put even state-level entities in major difficulty.

Conclusions

As ROMANIA is a member of prestigious international organizations, the EU, NATO and the UN, it provides a major advantage in the development of cyber security.

Although many states do not officially recognize that they have offensive capabilities in the field of cyber warfare, they certainly exist and are used primarily in certain situations of crisis, conflict or war.

There is more and more talk in the media about cyber warfare as a component of information warfare along with command-control warfare, information-based warfare, electronic warfare, psychological warfare, economic warfare, cultural warfare, ideological warfare, etc. The components of information warfare are not constant in number or delimitation, varying from one author to another depending on his experience and professional training.

Starting from the premise that defensive and offensive actions are the main forms of basic combat of armed struggle, and the absence of one cannot ensure the success of military operations, we can state that any army with specialized structures in cybernetics must develop offensive capabilities and defensive ones that guarantee the security of cyberspace.

The digitization of the modern battlefield in conditions of maximum cyber security is an essential and mandatory requirement for the planning, organization and conduct of military conflicts specific to the 21st century.

In order to have control of military equipment/platforms that are dependent on the functioning of the virtual space, the armed forces are forced to build their own integrated cybersecurity architectures that ensure the functioning of the cyberspace under normal conditions.

The dependence of all military structures within the armed forces on the normal functioning of cyberspace is an obvious reality today that determines a rethinking of the way in which military conflicts will unfold at a tactical, operational and strategic level.

If a few decades ago confrontations in cyberspace were seen as phenomena of the science-fiction field, now they have become a reality of the modern battlefield. The complexity of confrontations in cyberspace is a feature determined primarily by the evolution of cyber threats and vulnerabilities.

The military cyberspace must be seen as a component of the national/international cyberspace which, in order to function at optimal parameters, needs modern technologies, human and financial resources.

The planning and organization of modern military communications infrastructures and secure information technology can be achieved by implementing the following measures:

- creating a common legislative framework at EU, NATO and at international level;
- permanent technologization of military communications infrastructures and information technology;
- building integrated cyber security architectures with modern equipment and programs/applications;
- permanent training of military specialists in the field of cyber security by participating in specific national and international exercises;
- permanent adaptation of cyber security measures to the evolution of cyber threats and vulnerabilities existing in the virtual space.

BIBLIOGRAPHY

1. *Romania's national defense strategy for the period 2020-2024*, Bucharest, 2020.
2. *White Paper on Defense*, Ministry of National Defense, Bucharest, 2020.
3. BANABIC Dorel, *The evolution of technology and technologies from the first to the fourth industrial revolution and their social impact*, Romanian Academy, 2018.
4. *Strategy on the digitalization of education in Romania*, Ministry of Education and Research, 2020.
5. *Threat Landscape for 5G Networks Report*, ENISA, 2020.
6. *Railway Cybersecurity*, ENISA, 2020.
7. https://www.defense.ro.
8. https://intelligence.sri.ro
9. https://certmil.ro