The 15th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 12th-13th 2020

INFORMATIONAL RESOURCES UNDER THE THREAT OF CYBER WARFARE

OANCEA Constantin-Bogdan, M.A. student

Regional Department of Defense Resources Management Studies, Brasov, Romania

Abstract:
This paper wants to show the vulnerabilities to which, the information resources of today's society are subjected. As technology has progressed at an alarming rate and technology dependence has become increasingly acute, today's society is at increased risk of informational regress. The main threat is cyber warfare, which has spread since the beginning of the 21st century. Cyber warfare can affect all branches of information resource management, from espionage and stealing personal data for use in illegal activities to damaging the critical infrastructure of a state. An unstoppable cyber-attack in time can bring the destruction of the information resources but also can bring the world back to the stage of the Middle Ages.

1. Introduction

The huge scientific and technological leap known to mankind in the last century continues to exert obvious influences on the military phenomenon in all its forms of manifestation. The emergence and development of computer networks have irreversibly marked the way in which military operations are planned and conducted, especially the way in which information operations are carried out. State-of-the-art technology immediately became a component part of all modern combat systems, which led to a change in strategies, techniques and methods of waging war in all areas of its development.

Due to the transformations in the nature of war itself, as well as the transition from economies based on the production of goods by brute force, to speculative economies based on maximizing the exploitation of intellectual potential, war so devastating in the past has now become a war waged by the "force of the brain", in which strategy is directly influenced by available technology. The war changed its physiognomy, typology, conception regarding the use of weapons and technique, as well as the forms and procedures of combat, leadership of actions and training of troops. The current operational environment includes, in addition to the "classic factors" - terrestrial, air, maritime and outer space and the information environment, which also includes the cyber environment.

Identified and quantified in the mid-1970s, information warfare was officially recognized by politico-military thinkers as a distinct type of warfare, as important as land, sea, air, and space warfare.

Information warfare could be defined as an act of denying, exploiting, distorting or destroying the information and means of command, control and processing of the enemy, protecting their own, while exploiting the functions of military intelligence.

Although apparently respecting the principles of a classical war, information warfare differs greatly from it, involving the use of a less conventional weapon, information, which, by using or not using it, can be a danger to the security of the other side. This type of war aims especially at influencing the public opinion, the personnel of the opposing army, representing more a technique of weakening their power by using some means of psychological influence.

Depending on the specifics of the actions carried out by these structures, on their orientation, we can speak of an offensive form, respectively a defensive one of the information war and, depending on the mission and the activities carried out.

2. Informational resources versus physical resources

Even though, at first site, those two types of resources have nothing in common, in our cybernetic era, they are more linked to each other more than ever. Nowadays, every job has, more or less, a digital component.

As the economies of developed countries exploit the benefits of the Internet, the infrastructure and secrets of these countries become increasingly vulnerable to cyber-attacks. If in the last century wars took place on the battlefield, today obtaining the resources of opponents involves more and more often a battle in the virtual territory. Theorists consider cyberspace to be the 5th field in which a war can take place, after soil, sea, air and space.

The development of the information infrastructure, in the process of globalization, which includes media and online advertising structures, electronic services, social platforms and blogging platforms, generates more and more sophisticated interconnection possibilities. But the information society also means critical infrastructure, that is, those information services and systems that are so vital to a state that decommissioning or destroying them can cause destabilization of national security, the economy, or the state of affairs, population health, or blocking the efficient functioning of state structures and institutions.

From stealing confidential personal data to economic fraud, blackmail and terrorism, a whole range of serious criminal offenses have been transposed into cyber. The most worrying, of course, are those targeting critical infrastructure. The biggest problem is that the world's governments, even if they have faced cyber-attacks, have continued to invest in the development of technology without investing in security measures in order to protect these technologies.

3. Informational attacks in the real world

The first large-scale cyber-attack took place in 1982 when the United States planted a "logic bomb" in gas flow control systems in a Trans-Siberian pipeline in the USSR. A powerful explosion took place and it seems that the "computer-contaminated" equipment that the Soviets had buy from a Canadian company, was to blame, without suspecting that there would be problems. The logic bomb refers to a code inserted in a way intentionally in software; the malicious function will be triggered at a certain moment when a series of conditions are met.

However, the 1982 incident is disputed by many and the "logic bomb" theory has been categorized by many specialists as a farce. The cyber-attacks that there is evidence of are much more recent.

In 2007 and 2008 a number of administrative sites in Estonia were attacked in the DdoS style and the source was clear: the Russian Federation. The attack was then considered serious and was seen by many as a revelation, but analyzing from the perspective of what has happened since then, the attacks in Estonia were technologically commonplace. An important role for them was that governments and international institutions realized that the cyber part must be taken as seriously as possible and security divisions were set up. Cyber-attacks were no longer a niche, but were seen as an area where serious things could happen if no defense was taken.

Another resounding episode was the brief war between Russia and Georgia for the South Ossetia region in the summer of 2008. Hackers in Russia launched attacks on Georgian sites, but one cannot speak of a cyber-war because the Georgian side had a very weak response. In addition, the Russian Federation entered Georgia with tanks, and computer attacks led to the opening of the actual military attacks. What has the international community learned from this conflict? That there is a

need for cooperation between countries in the field and those specialists from various countries must share their experience.

Another "manual" chapter for the evolution of cyber-attacks was the Stuxnet "worm" discovered in 2010. It was at that time the most advanced cyber weapon and, attacking the command and control systems of power plants, could lead to serious delays in the program of Iranian nuclear power plant, especially at the Natanz plant.

Reports from then on noted that Stuxnet could act on centrifuges in Iranian nuclear power plants, altering their angle of inclination, so that they disintegrated at high speeds because they were no longer perfectly straight. Then came evidence that Stuxnet was developed by the United States and Israel. Stuxnet had descendants and came up with an important lesson: well-aimed cyber weapons can be created that can affect gigantic industrial installations from a distance. Cyber-attacks become extremely sophisticated and have clear purposes.

Stuxnet was the beginning and from it derived more and more sophisticated computer "worms", in 2012 Flame was discovered which was created for cyber espionage and had the ability to steal confidential data, take screenshots, gather information about attacked systems, stored files and contact details. It could even record audio conversations if that computer has a microphone attached (including from the webcam). He could even record phone conversations if he could connect to the phone's Bluetooth device. Complexity had increased to special levels.

In less than a generation, the information revolution and the introduction of virtual space in every aspect of society have changed the world, with the advantages, but also with the related security challenges.

3.1 Informational resources used by Russia

Lately, the Russian Federation has most often and most obviously resorted to the use of the information resources in support of its efforts to regain global power status. In a glossary of terms developed by the Russian Military Academy, information warfare (informatsionnaya voyna) is not limited to wartime, while the Western meaning refers to limited operations carried out during hostilities. But the Russian approach is much broader, using history, culture, language, nationalism and more to run cybernetically-supported disinformation campaigns with diverse goals. In this regard, the most eloquent examples are the conflict in eastern Ukraine and the annexation of the Crimean peninsula.

The success of Russia's information domination during the annexation of the Crimea in 2014 is well known. In addition to the fact that Russia then gained control of the print and television media, it also successfully controlled telecommunications, including internet, thus isolating Crimea from external information flows. The result was a degree of control over public perception in Crimea, which later helped legitimize the annexation of the peninsula. The way this was done was by simply taking physical control of the internet communications infrastructure and then by selectively interrupting cable communications.

4. Conclusion

Information and communication technology has evolved a lot and now offers solutions for many of humanity's concerns, and, implicitly, for the military. It is also obvious that it is not technology that is the focal point of a system, but organizational culture and operational structure. For this reason, it should be emphasized once again that, in terms of information operations, technology offers solutions to all the theoretical challenges posed by the initiators of the concept or by military officials, but cannot replace human resource issues.

At the same time, it should be mentioned that the globalization and digitalization of society may lead in the near future to a much more intense use of the contemporary information weapon during the war.

References

[1] Dumitru Cristea, Roceanu Ion, *Războiul bazat pe reţea, provocare a erei informaţionale în spaţiul de luptă*, Bucureşti, Editura Universităţii Naţionale de Apărare „Carol I", 2005;
[2] Hentea Călin, *Arme care nu ucid*, Bucureşti, Editura Nemira, 2004;
[3] Petrescu Stan, *Războiul Informaţional*, Editura Militară, Bucureşti, 1999;
[4] Dughin Alexandr *Bazele geopoliticii si viitorul geopolitic al Rusiei*, Editura Eurasiatica, Bucureşti 2011.
[5] https://en.wikipedia.org/wiki/Logic_bomb.
[6] https://www.bbc.com/news/39655415
[7]https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html