Vojnotehnicki glasnik/Military Technical Courier

ISSN: 0042-8469

vojnotehnicki.glasnik@mod.gov.rs

University of Defence

Serbia

Damjanovi, Dragan Z.

TYPES OF INFORMATION WARFARE AND EXAMPLES OF MALICIOUS PROGRAMS OF INFORMATION WARFARE

Vojnotehnicki glasnik/Military Technical Courier, vol. 65, núm. 4, 2017, pp. 1044-1059

University of Defence

VOJNOTEHNIČKI GLASNIK / MILITARY TECHNICAL COURIER, 2017, Vol. 65, Issue 4

TYPES OF INFORMATION WARFARE AND EXAMPLES OF MALICIOUS PROGRAMS OF INFORMATION WARFARE

Dragan Z. Damjanović
Zrenjanin, Republic of Serbia,
e-mail: damjanovic1971@gmail.com,
ORCID iD: http://orcid.org/0000-0001-8169-4507

http://dx.doi.org/10.5937/vojtehg65-13590

FIELD: Informatics
ARTICLE TYPE: Professional Papers
ARTICLE LANGUAGE: English

Abstract:

The possibilities of the information management system are unimaginable. "Information warfare" (IW), defined as a targeted effort to undermine and neutralize hostile command and control systems for the purpose of protecting and coordinating the activities of command and control systems of friendly forces, is a frequently used term. Most of modern political and military systems of command and control are based on high speeds of computer-based communication. Hence, the information infrastructure is the "infomercial" arena in which information warfare is conducted. Every system or a person that forms part of this sphere is a potential target in IW. The form of information warfare is the way of its exposure and it is expressed through the structure of events and activities related to the processes that take place in it. This means that the form of information warfare is a special feature that distinguishes it qualitatively from other forms. It is evident that information warfare dramatically affects the mode of war, regardless of whether it is only an evolutionary period or represents a revolutionary development.

Key words: terrorism, systems, Internet, command and control systems, command and control.

Introduction

Every day we witness the incomprehensible capabilities of the information management system. For this reason, it is no wonder that in the daily conversation, "information warfare" (IW) is often mentioned. It is sometimes even regarded as a future cornerstone of the future military doctrines of some countries, even of those most developed ones.

Information warfare has enormous political, technical, operational, and legal implications for the military. Therefore, here we will try to define IW, identify potential military uses and applications, as well as the problems that are responsible for the implementation of this new doctrine.

What is information warfare?

Information Warfare (IW) is a targeted effort to undercut and neutralize the enemy's command and control system for the purpose of protecting and coordinating the activities of the command and control system of friendly forces (Blair, 2001).

Information warfare may include (Reisman & Antoniou, 1994):

- collecting tactical information,
- checking the accuracy of information,
- spreading propaganda and disinformation to demoralize or manipulate the opponent and the public,
- undermining the quality of opponent information,
- denying the opponent the opportunity to collect information.

Some governments spend billions of dollars to establish agencies that will collect and store information about potential threats to their security. Information is a strategic advantage (Campen, 2002).

This is a fact first understood by computer hackers, many of whom are currently serving long-term prison sentences, precisely because of attempts to alienate confidential information.

Types of information warfare

The form of information warfare is the way of its exposure and it is expressed through the structure of events and activities related to the processes that take place in it. This means that the form of information warfare is a special feature that distinguishes it qualitatively from other forms.

In the available literature dealing with information warfare, there are more views on the forms of its manifestation, the most widespread perceptions being those of eminent experts from that area Schwartau and Libbicky's.

Winn Schwartau classifies information warfare in three groups: 1) personal information warfare; 2) corporate information warfare; 3) global information warfare (Petrović, 2001).

According to Martin Libicki, information warfare occurs in the following forms: 1) warfare in the sphere of command and control; 2) intelligence

warfare; 3) electronic warfare; 4) psychological warfare; 5) hacker warfare; 6) economic-information warfare; 7) cyber warfare (Libicki, 1995). All of these forms are connected, especially hacker warfare and cyber warfare that are not completely disjunctive.

The official definition of the US Department of Defense on warfare in command and control is: ”Command and Control Warfare is a military strategy that applies information warfare on the battlefield in order to separate the command structure of the opponents’ from the units they command (the original English term is to be defeated) (Libicki, 1995). Defusing can be done by damaging the head (commander, command post) or door (communication), depending on different tactical and strategic purposes. Libicki believes it is much more important than finding the physical location of a commander finding a command post. Attacking the command positions, especially if it is timely adjusted, may have exceptional operational consequences and it is not necessary for the opponent to be ”beheaded”. In most situations, the command post is a knot in the entire structure of the opponent and its elimination is rarely missed if such a possibility is indicated.

It can be destroyed by classic bombs, but also by interrupting power supplies, electromagnetic interference, computer viruses, interrupting communications, etc. (Libicki, 1995). "Damage to the Door" means the intersection of communications by the enemy, which makes command and control incapacitated, which has a decisive influence on the final outcome of the conflict.

War in the sphere of command and control can be conducted offensively (C2 - attack) and defensively (C2 protect) (United States Department of the Army, 1993). Based on the above, it can be concluded that the aim of C2W is to degrade or destroy the opponents' potential for command and control while at the same time protecting their own C2 potentials from such activities.

Intelligence is an activity that aims at finding goals, evaluating combat actions, preventing surprises, etc. Primary intelligence sources can be classified into different categories: Human Intelligence (HUMINT), Signal Intelligence (SIGINT), Technical Intelligence (TECHINT) and others (Group of authors, 2000). In Brussels, on February 23, 2000, the European Parliament began a debate on a planetary spy network, called "Echelon". A network of 120 satellites covers the entire planet and makes a system that is able to control 2 billion messages daily, thanks to artificial intelligence and given key words. According to some western papers that are difficult to verify, the most commonly used keywords for automatic messaging devices in Echelon regional centers are: "kill the president", "anarchy", Glock-26 - a ceramic gun impossible to detect by metal detectors and other. The Echelon's satellite spy system, therefore, deals with the collection and analysis of various (political, security, economic,

technological, trade, etc.) data. The only control center in Gloucester (UK) employs 15,000 people who are involved in the analysis of collected data (Prvulović, 2002).

Electronic warfare is warfare in which electronic and other means directly affect the enemy's electronic means and systems as well as combat systems and weapons based on their use of electronics. Electronic warfare is also defined as a military activity that involves the use of electromagnetic and targeted energy in terms of dominating and managing events in the electromagnetic spectrum and in terms of an electronic attack on the enemy and its combat systems. Schlecher defines electronic warfare as ”a military action aimed at controlling the electromagnetic spectrum” (Schleher, 1999). According to a study by the Faculty of Electrical Engineering, University of Belgrade, electronic warfare is a set of military actions whose main goal is to control electromagnetic space, its domain. In the context of information and electronic war relation, electronic war is considered to be a subset of information warfare (Group of authors, 2000).

In FM-105 rule, electronic warfare is defined as ”any military action involving the use of electromagnetic and targeted energy to control the electromagnetic spectrum (EMS) or an attack on an opponent.” (United States Department of the Army, 1993). Electronic warfare is, in essence, the battle for the control of the electromagnetic spectrum.

In order to achieve the stated goal, activities that have an offensive character - Electronic Attack (EA) and defensive character - Electronic Protection (EP) are applied. In addition, Electronic Support (ES) represents activities aimed at collecting information for the needs of EA, EP, avoiding opponents’ actions, using their own combat resources (Group of authors, 2000).

An electronic attack is a part of electronic warfare involving the use of electromagnetic energy or targeted energy for an attack in order to degrade, neutralize or destroy the opponents’ combat potentials. Electronic jamming and deception are "soft kill" measures while "hard kill" measures are the effects of self-inflicted missiles on electromagnetic radiation (Anti-Radiation Missile – ARM) and action directed electromagnetic energy (Directed Electromagnetic Weapons - DEW). Electronic protection is a part of electronic warfare that encompasses activities aimed at protecting one's own people and means of the effects of electronic warfare by an opponent, and from unintentional emissions generated by own transmitters that can degrade, neutralize or destroy the combat potentials of their own forces.

Electronic support is a part of electronic warfare that includes activities of discovering, identifying, and location of sources of deliberate or unintentional radiation of electromagnetic energy to detect opponents'' actions, to discover the location of targets, to plan and implement support for electronic warfare and other tactical activities. Information about an opponent collected through electronic warfare has a significant intelligence dimension, and then electronic warfare can be viewed as intelligence warfare. However, intelligence warfare is in the function of planning and conducting electronic warfare and, in particular, the formation of an electronic picture of the battlefield. Therefore, the relation between electronic and intelligence warfare best describes the term coordination, which is also characteristic of some other forms of information warfare (Vuletić, 2005).

Szafranski under psychological warfare involves the use of information against the human mind (Szafranski, 1995). The United States considers psychological warfare an integral part of any armed conflict. Due to the great importance given to this form of IW, many professional and scientific institutions, faculties, research centers, institutes are engaged in the USA. A comprehensive system of military authorities and units for psychological warfare has been developed in this country. They are smaller in composition and narrow-specialized (10-15 members) so they can be combined for specific tasks. In the US military rule FM-106, the notion of psychological warfare is reduced and, at the operational level, it is talking about psychological operations. This document states that "psychological operations have the goal of transmitting selected information and indicators intended for foreign listeners and viewers in order to influence their emotions, motives and objective reasoning and, ultimately, the behavior of foreign governments, organizations, groups and individuals to achieve their own interests and goals. "The main goal of a psychological operation in protecting one's own command and control system is to minimize the effects of opponent's propaganda and activities in order to disinfect their own strengths and the population. The goal of PSYOP (psychological operations) is to influence the attitudes and behaviors of those they are pursuing (United States Department of the Army, 1996). According to the American philosopher and political scientist from the late twentieth century, Noam Chomsky, this method of conducting psychological warfare plays an important role and affects about 20% of the population, relatively educated, who takes part in making certain decisions. Media action on this structure of people and their acceptance of doctrine is crucial because they can take part in the creation and implementation of politics. The other part or 80% of the population is merely an observer of events, they should execute orders, messages and tasks and not interfere with the affairs of decision makers. This part of the population is just becoming a target of mass media, whose goal is that these people are

mere observers of events and perpetrators, who should not be tired of what is happening in the world (Stokić, 1995).

Hacker Warfare is one of the forms of information warfare that are most often performed by individuals. A hacker attack is usually aimed at congestion and changing the content of the attacked web site. Because of their functional and physical characteristics, computer systems represent an ideal target for attackers. In order to check the resilience of its computer networks against attacks by hackers, in 1994 the Defense Information Security Agency (DISA) tested and formed its own hacker team and ordered them to attack Pentagon computer networks over the Internet. After completing the testing, DISA's official position is that they are not prepared to defend themselves from the "electronic version of Perl Harbur" and that their computer structure is not safe (Munro, 1995). In October 1994, a Pentagon warned against a growing threat that goes beyond isolated, though irritating and increasingly frequent hacking attempts. It is about organized attacks on a wider, coordinated basis with strategic implications. Behind these threats can be terrorist groups or some countries and it is very difficult to detect them. The use of hacker warfare depends to a large extent on the number of computers in use and the number of Internet users. The degree of integration of computer networks is inversely proportional to the effects of hacker warfare. In contemporary conflicts and technologically inferior countries, they have the opportunity to successfully conduct hacker warfare.

The term "economic-information warfare" is still not fully defined, but it is clear that this form of information warfare is guided by information of economic significance for the conflicting parties. Information of economic importance can be information about various contracts, development strategy of the company, internal structure and organization, marketing and production plans, investments and more. It is obvious that, in a global context, the ”conflict” of the economic and intelligence services is constantly present, around confidential information that would be used against its competitors in the interests of its companies. This "conflict" essentially constitutes an economic (or an industrial) espionage. Former CIA director George Tenet pointed out that the economy was the primary area of intelligence work in the 1990s. Foreign espionage, and after so many years after the end of the Cold War, remains a major threat to Russian national interests, said Nikolai Kovalyov, the then head of the Federal Security Service (FSB) of Russia. The case of a spyware attack on IBM (International Business Machines), which was carried out by some twenty people who worked for Japanese Hitachi, is known to have stolen confidential information worth between 750 million and 2.5 billion dollars over the course of three years. The operation was cut in 1982 by the FBI in its famous sting operation. In 1997, General Motors made a loss of $ 100 million just because one side company developed a vehicle based on data

stolen from its premises (Munro, 1995). After analyzing all the methods and techniques (legal and illegal) of economic and information warfare on the world market, especially due to the fact that most countries do not have technologically equipped and efficient economic intelligence systems, an idea of special agencies that can provide such professional services emerged. The agency's job can be offensive (to help break a certain company or state into the global market by revealing confidential economic information about a particular market and rival companies or to expel a competitor from the game by various techniques) or defensive (to protect a country or company from the theft of industrial and business secrets, to disclose the use of corruption or other illegal means by a competitor in a particular business, thereby hindering that business, etc.).

The growing dependence of the society on information and communication technology creates numerous weak points. Because of these critical points, as well as due to the accentuated complexity and strong interdependence, national infrastructures that connect, run and serve computers have become extremely sensitive. The connectivity of network communications increases their vulnerability, due to the greater possibility of accessing the information structure from various parts of the world. Cyberspace is an area that provides new opportunities for warfare. Arkville and Ronfield defined cyber warfare as a series of actions that break or destroy the opponents' information and communication systems (Arquilla & Ronfeldt, 1995). Cyber warfare can be conducted offensively or defensively. The object of cyber attack can be everything that connects, launches and serves computers (military computer systems, state administration systems, air and rail traffic control systems, gas, water and electricity supply systems, and others). Given their importance, purpose and number, especially in the developed countries of the West, it is evident that the information environment offers cyber attackers the right wealth of choices of highly valued goals. Recognizing the growing problem, in order to protect the national information infrastructure, the United Task Force on Computer Network Defense (JTF-CND) was formed in 1998 in the United States. Its task is to monitor all existing and potential attacks on the information systems of the US Department of Defense, to link all federal agencies to the unique network and national infrastructure protection center and, in the event of an attack, to enable a quick network recovery and respond adequately. In February 2003, the National Strategy for the Security of Cyberspace, which provides the basis for the protection of vital national infrastructure (United States Department of Defense, 2015), was adopted in the USA. Cyber attacks are more extensive, more sophisticated, better coordinated than hacking attacks and directed towards the enemy's significant goals. The use of cyber warfare depends to a large extent on the number of computers in use and the number of Internet users. In an armed conflict, computer attacks may only be carried

out by members of the armed forces with a careful assessment of the potential damage to the attacked target.

Examples of malicious programs of information warfare

Most of the modern political and military systems of command and control are based on high speeds of computer-based communication. Hence, the information infrastructure is the "infomercial" arena in which information warfare is conducted. Every system or a person that is part of this sphere is a potential target in IW. Therefore, it is necessary to first identify, isolate and analyze each element of the enemy infosphere. They then deny, destroy, or make useless data that should reach the opponent. It is even more harmful if false information is inserted, and in this way the enemy starts to make wrong decisions (Toffler, 1993).

In addition, IW can influence political, economic or military goals through: conferences for journalists of important personalities, sabotage of the economy, sabotage of development facilities and scientific research, sabotage of satellite communications, destruction of the information network (Leonhard, 2008).

Information operations are planned for the transmission of selected information to a foreign population in order to influence their feelings and objective judgment, and therefore the behavior of foreign governments, organizations and society. The purpose of information operations is to encourage or reinforce foreign attitudes and behaviors suitable for achieving the political and military objectives of the information operations initiators. In these operations, propaganda methods from the field of psychological warfare are often used, and such operations are often referred to as information-propaganda activities. An example of such an operation can be found in the use of the term Palestinian state, which was used by the PLO around 1964, although it never officially existed, which meant a non-Jewish, non-Israeli country. In this operation it was important to release certain information into circulation. After that, it was first used by journalists, then by public opinion, and finally by politicians (de Arcangelis, 1999).

A person who has an unauthorized access to computer and telephone systems is called a hacker, and the friker term may also be heard (Sterling, 1992).

Since the 1970s when they first appeared, they have repeatedly shown their talent in overcoming computer security systems for accessing information. Not only that. They even approached the databases of various corporations and agencies, and thus caused damage in millions of dollars (Schwartau, 1994).

In order to achieve this, certain funds are needed, so-called Weapons. They can be divided into four categories: software, hardware, electromagnetic systems, and other means (Baker, 1998). The software consists of programs designed to collect, alter, deny information or even destroy the hostile infosphere. Examples of such software have even exotic names: demons, viruses, Trojan horses or Trojans, logic bombs, etc. (Trainor & Krasnewich, 2009).

A demon is a program which, when installed or introduced into the system, records all commands that are entered. It can detect access codes, encryption keys, or similar information. A similar program is a sniffer.

Virus is a program that after attacking files files on the computer or those on the network. It extends to other files without any real damage or can make them unusable, causing deletion of files.

”Virus is a program or code that replicates itself in other files that it contacts. Any program, a boot sector, a document that supports macros can be infected and infected by changing the contents of that file and copying its code in it.

A computer virus usually consists of two parts.

– The first part is a self-copying code that allows the propagation of the virus
– The second part is useful information that can be harmless or dangerous.

Some consist only of a self-copying code. Sometimes a virus requires the interaction of a person to propagate such as launching a program that contains a virus or opening an infected file.The first true ancestor of today's virus was the Prevading animal that was able to access other programs on the UNIVAC 1108 computer system. The first confirmed finding of a computer virus was in 1981 and it was called Elk Cloner. This virus infected the BOOT diskette sector for Apple II computers. In 1988, it was the Jerusalem virus that erased all running programs, and in 1989 Datacrime was able to execute the low-lewel format of the zero path on the disk. In the same year, a real virus firm was activated in Bulgaria. At least 50 viruses including New Zealand and Michelangelo have been created so far.

A biological virus cannot reproduce itself, but it can capture the cells of another organism and use the reproductive mechanism of each host cell to make its own copy. New copies leave the host and look for new hosts to repeat the process. The software virus works the same way. It extends from a program to a program, or from a disk to a disk, and uses every infected program, file, or disk to make as many of its copies as possible. Virus software is usually hidden in the operating system of the computer or in application programs. Some viruses do nothing but playback, others

display messages on the computer screen while others destroy data or delete discs.

One of the most famous email viruses was the Melissa virus. Melissa spread like a fire among Windows systems, infecting 90000 systems in just a few days. Melissa was not designed to damage the systems, but suddenly a message burst out some email servers. The 30-year-old author of the Melissa virus, a resident of New Jersey,attracted by a Melissa player, was discovered and prosecuted (Milosavljević et al, 2013, p.281).

Viruses can be transmitted in many ways, and nowadays virtually all viruses are transmitted over the Internet, and can also be transmitted by diskettes, interchangeable hard disks, compact discs and other removable media.

Trojan horses in computer jargon are malicious programs that are ”masked” as useful or expanding ”attached” to other useful programs. ”Trojans” usually do unwanted actions in a computer, hidden in the "background". The most common of these unwanted actions is the disclosure of user passwords, bank information and other confidential information by ”eavesdropping” the data exchange or simply by reading those files, and reporting them to the ”owner” of theTrojan horse.

There are also Trojan horses in the police service dealing with the collection of information for the purpose of detecting a criminal offense (Remote Forensic Software). This form of citizen spying is enforceable in some countries and is carried out under a court order, in some, despite the conflict with the Constitution, in the preparation phase, while in some cases it has been rejected. Such Trojans are spread by installing or updating commercial operating systems and other software and hardware components of computers, as well as through Internet providers by infiltrating into existing data transfer mechanisms, which must, in their products and services, be provided at the request of the country concerned.

Famous Trojan horses

– Back Orifice
– Netbus
– SubSeven.

”Trojan horse is a program that can do something useful while simultaneously carrying out some secretly destructive work. As in the old story of a wooden horse that brought Greek soldiers through the gates of Troy, a software trojan horse hides the real enemy. These programs often have game-like names or user programs. When an inexperienced individual takes over and launches such a program, he can erase files, alter data, or cause another type of damage. Some network saboteurs use Trojan horses to pass secret information to other unauthorized users. One type of Trojan horse - a logic bomb is programmed to attack as a

reaction to a particular event or sequence of events. For example, a programmer can install a logic bomb designed to destroy data files if a programmer ever appears on a list released in the company's personal service file. A logic bomb can be activated when a particular user logs in, when he enters a special code into the database field, or when the user performs a certain order of actions. If a logic bomb is triggered by an event associated with a timer, it is called a timed bomb. There is a well-known virus with a logic bomb, programmed to destroy computer files with data on Michelangelo's birthday (Milosavljević et al, 2013, p.281).

Spyware is a broad category of malware created to partially intercept or take control of the computer without the knowledge or permission of the user. Although the name suggests that it is about programs that monitor the work of users, this name today denotes a wide range of programs that exploit the computer to gain benefits for a third party. The spy is different from virus and worm in that it usually does not reproduce itself. Like many new viruses, a spy is designed to exploit infected computers for commercial gain. Typical tactics are displaying pop-up ads, stealing personal data (including financial information such as credit card numbers and passwords), tracking online activities for marketing purposes, or redirecting HTTP requests to advertisement pages. In some cases, the spy is used to check compliance with the license terms for using the program.

Infection in most cases occurs when opening pages with illegal or pornographic content.

Computer worms are computer programs that multiply themselves. They use computer networks to copy to other computers, often without the influence of the man. Unlike viruses, they do not have to infect other programs by their actions. They can also be accessed as a file in the e-mail, and their access to the computer allows for gaps in operating systems and applications. Worms make the network more difficult, and can damage data and reduce computer security. Internet worms and viruses create problems for infected computers, but worms can do more damage due to network traffic that they generate when expanding the Internet. For example, SQL Slammer worm doubled in January 2003 the number of infected computers every 8.5 seconds.

The first known worm was made by a Kornel University student during an experiment in 1988. The worm was accidentally released onto the Internet and blocked 6000 computers across the United States. In the summer of 2001, a worm called Code Red appeared. Its target was Internet services that run under Microsoft servers. The US government and Microsoft have sent warnings about worms and made free software patches to protect the server (Miles et al, 2017).

Security and reliability issues are the most critical in military applications. For the successful implementation of the mission, the army must make sure that its systems are safe from spying and enemy attacks.

At the same time, many modern military applications are pushing the boundaries of information technology beyond what they have ever been. Huge assets are invested in the development of smart weapons - missiles that use a computerized guidance system to locate the target. Command guidance system allows the operator to control the missile path.

Self-powered self-propelled projectiles can monitor moving targets without human assistance, using infrared thermal self-leveling devices or ”visual pattern recognition” technology. Weapons using ”smart” guidance systems can be extremely precise in determining the exact position of enemy targets in many cases. One problem with high-tech weapons is that they reduce the time that people have to make a decision between life or death. As the time for making a decision decreases, the possibility of error increases.

An even more controversial possibility is for people to be completely excluded from the decision-making process. The trend in military research is clear about weapons that require almost immediate reactions - what only computers can do. An autonomous system is a complex system that can assume almost complete responsibility for the task without human data entry, verification or decision making. The automated defense system from the projectiles has been stirring up public hearings on false alarms. But for many who understand the limitations of the computer, the biggest question is the reliability of the software. Tavi systems require tens of millions of program code lines. The system cannot be fully tested in advance because there is no way to precisely simulate unpredictable global war conditions. In order to operate efficiently, the system should be absolutely reliable. A small mistake can lead to a major disaster. Many military experts suggest that future wars may not be conducted in the air, on land or in the sea. The front line of the future can be in the cyber space. Attacking connected computer networks, the enemy can damage telecommunications systems, power lines, banking and financial systems, hospitals and medical systems, water and gas supplies, oil pipelines and emergency government services without the use of conventional weapons (Milosavljević & Mišković, 2011).

Conclusion

The doctrine of IW has significant implications for modern military theories. Now an enemy soldier is no longer a big target. The effort is aimed at preventing communication between the command and the soldiers, in order to prevent the coordinated actions of the enemy. This can be achieved by breaking into the command and control system of the enemy and its infantry by using computer systems of weapons and

software attacks. Goals can be of military, political or economic significance. Still, many questions remain unresolved. Intelligence agencies need to evaluate the benefits of coordinated hacking and tampering and obtaining important information.

The nineties of the twentieth and the beginning of the twenty-first century will be recorded in the world history as a period of expansion of the applications of various forms of information warfare. Based on the above facts, it can be concluded that the application of a particular IW form depends on a number of circumstances (eg funds available) and is determined by the goals to be achieved. An analysis of the application of information warfare in contemporary conflicts provides an answer to the question of which the form of information warfare is permanent and which is a temporary companion of armed conflicts. Permanent forms of information warfare are C2W, EW and psychological warfare. Hacking, economic-information and cyber warfare are occasional and very often used forms of information warfare in contemporary conflicts. First of all, it takes a lot of studies and discussions to make the theory of information warfare a practical doctrine. It is evident that information warfare will dramatically affect the mode of war, regardless of whether it is only an evolutionary period or represents a revolutionary development. All in all, there are great efforts by individuals and groups of researchers that information warfare become a part of the military service in the 21st century.

References

Arquilla, J. & Ronfeldt, D., 1995. *Network war and cyberwar*, a copy of the study publication in "Comparative Strategy". RAND Corporation. Volume 12.

Baker, D., 1998. *The Shape of Wars to Come*. New York, Stein and Day, Publishers.

Blair, B.G., 2001. *Strategic Command and Control*. Washington, D.C., The Brookings Institution.

Campen, A.D., 2002. *The First Information War*. Fairfax, VA, AFCEA International Press.

de Arcangelis, M., 1999. Electronic Warfare from the Battle of Tsushima to the Falklands and Lebanon Conflicts. Poole, Dorset, Blandford Press.

Group of authors, 2000. *Elektronski rat - stanje i perspektive.* Beograd, Elektrotehnički fakultet Univerziteta u Beogradu (in Serbian).

Leonhard, R., 2008. The Art of Maneuver: *Maneuver Warfare and AirLandBattle*. Novato, CA, Presidio Press.

Libicki, M.,1995. *What Is Information Warfare?* [e-book]. Washington, National Defense University. Available at: http://www.dtic.mil/get-tr doc/pdf?AD=ADA367662. Accessed: 2017 Apr 19.

Miles, T., Wayne, J., Karen, S. & Jason, B., 2017. *Guidelines on Electronic Mail Security*, [e-book]. Gaithersburg, National Institute of Standards and Technology. Available at: http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800 45v2.pdf. Accessed: 2017 Apr 19.

Milosavljević, M. & Mišković, V., 2011. *Elektronska trgovina*. Beograd, Univerzitet Singidunum (in Serbian).

Milosavljević, M., Veinović, M. & Grubor, G., 2013. *Informatika* . Beograd, Univerzitet Singidunum, p.281 (in Serbian).

Munro, N., 1995. The Pentagon's New Nightmare: An Electronic Pearl Harbor. *Washington Post*.

Petrović, S., 2001. *Kompjuterski kriminal*. Beograd, Ministarstvo unutrašnjih poslova Republike Srbije (in Serbian).

Prvulović, V., 2002. *Ekonomska diplomatija*. Beograd, Megatrend univerzitet primenjenih nauka (in Serbian).

Reisman, W.M. & Antoniou, C.T., 1994. The Laws of War: A Comprehensive Collection of Primary Documents on International Laws Governing Armed Conflict. New York, Vintage Books (Random House).

Schleher, C., 1999. Electronic Warfare in the information age. Artech House.

Schwartau, W., 1994. Information Warfare: Chaos on the Electronic Superhighway. New York, Thunder's Mouth Press.

Sterling, B., 1992. The Hacker Crackdown: Law and Disorder on the Electronic Frontier. New York, Bantam Books.

Stokić, L.J., 1995. *Novi svetski poredak i YU drama*. Beograd, Zenit (in Serbian).

Szafranski, R., 1995. When waves collide, Essay contest on the Revolution in Military Affairs. *Joint Force Quarterly* .

Toffler, A.H., 1993. War and Anti-War: Survival at the Dawn of the 21st Century. Boston, Little, Brown and Company.

Trainor, N.T. & Krasnewich, D., 2009. *Computers, 2nd ed*. Santa Cruz, CA, Mitchell Publishing, Inc.

- United States Department of the Army, 1993. FM 105 Information Operations- Washington, D.C., Headquarters Department of the Army.

- United States Department of the Army, 1996. FM 106 Information Operations- Washington, D.C., Headquarters Department of the Army.

- United States Department of Defense, 2015. The Department of Defense Cyber Strategy. [Internet]. Available at: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. Accessed: 2017 Apr 19.

Vuletić, D., 2005. *Informaciono ratovanje u savremenom sukobu*. Beograd: Vojna akademija. Magistarska teza (in Serbian).

ФОРМЫ ИНФОРМАЦИОННЫХ ВОЙН И ПРИМЕРЫ ВРЕДОНОСНЫХ ПРОГРАММ В КИБЕРВОЙНЕ

Драган З. Дамянович
г. Зренянин, Республика Сербия

ОБЛАСТЬ: информатика
ВИД СТАТЬИ: профессиональная статья
ЯЗЫК СТАТЬИ: английский

Резюме:

Неисчерпаемые возможности системы информационного управления с каждым днем становятся все более очевидны. Очевидно и их применение в так называемой «информационной войне» (ИВ), которая представляет собой целенаправленные действия, предпринятые для достижения информационного превосходства, путём нанесения ущерба , и противника при одновременной защите и управлении информацией, информационными процессами и информационными системами как своих собственных, так и дружественных сил. Большинство современных политических и военных систем управления и командования используют высокороскоростную связь при помощи компьютера. Таким образом, информационная инфраструктура или «инфосфера» стала ареной для кибервойны. Любая система или человек, находящиеся в зоне «инфосферы» являются потенциальной мишенью в информационной войне. Форма информационной войны проявляется в способах воздействия, включающих представление структуры событий и действий, связанных с процессами, которые происходят в ее рамках. Кибервойна по своей неординарной форме существенно отличается от других видов войн. Ее появление, безусловно, влияет на методы военного дела внося как эволюционной, так и революционной характер в развитие военной стратегии.

Ключевые слова: терроризам, системы, интернет, системы командования и управления, управление и контроль.

ОБЛИЦИ ИНФОРМАЦИОНОГ РАТОВАЊА И ПРИМЕРИ ЗЛОНАМЕРНИХ ПРОГРАМА КОМПЈУТЕРСКОГ РАТОВАЊА

Драган З. Дамјановић
Зрењанин, Република Србија

ОБЛАСТ: информатика
ВРСТА ЧЛАНКА: стручни чланак
ЈЕЗИК ЧЛАНКА: српски

Сажетак:

Могућности система за управљање информацијама су несагледиве. Све чешће се помиње „информационо ратовање" (ИР) које се дефинише као усмерени напор да се изврши подривање и неутралише непријатељски систем команде и контроле ради заштите и координације активности система команде и контроле пријатељских снага. Већина модерних политичких и војних система команде и контроле заснива се на високим брзинама комуникације помоћу компјутера. Отуда је информациона инфраструктура, односно „инфосфера", арена у којој се води информационо ратовање. Сваки систем или лице који су део ове сфере представља потенцијалну мету у ИР. Облик информационог ратовања је начин његовог експонирања и исказује се кроз структуру догађаја и активности везаних за процесе који се у њему одвијају. То значи да је облик информационог ратовања посебна карактеристика која га квалитативно разликује од других облика. Евидентно је да информационо ратовање драматично утиче на начин ратовања без обзира на то да ли је оно само еволуитивни период или представља револуционарни развој.

Кључне речи: тероризам, системи, интернет, командни и контролни системи, команде и контроле.

Paper received on / Дата получения работы / Датум пријема чланка: 31.03.2017.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 23.06.2017.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 25.06.2017.