IJSRM
INTERNATIONAL JOURNAL OF SCIENCE AND RESEARCH METHODOLOGY
An Official Publication of Human Journals

Human Journals
Review Article
October 2017 Vol.:7, Issue:4

Information Threats: Types, Objectives and Methods

IJSRM
INTERNATIONAL JOURNAL OF SCIENCE AND RESEARCH METHODOLOGY
An Official Publication of Human Journals

Avazov Komil Hollyevich

[1] *Doctoral student of the Uzbek National University Named after Mirzo Ulugbek (Uzbekistan)***.**

Submission:	21 September 2017
Accepted:	30 September 2017
Published:	30 October 2017

HUMAN JOURNALS

www.ijsrm.humanjournals.com

Keywords: Information weapons, information warfare, Electronic field, electronic warfare, information society

ABSTRACT

Informational weapons will give the maximum effect only when it is applied to the most vulnerable parts of the ISS. The greatest information vulnerability is possessed by those subsystems that are most sensitive to input information - these are the systems of decision making, management. Based on what has been said, we can introduce the notion of an information target. The information target is a set of elements of the information system that belong or can belong to the sphere of management, and have potential resources for reprogramming to achieve goals that are alien to this system.

INTRODUCTION

Information-psychological warfare allows exerting an intensive influence on various processes at almost all levels of state and social order in any country or region. From time immemorial, mankind has faced the problem of information wars at all levels, and bow, arrows, swords, guns, and tanks, in the end, only completed the physical defeat of a community already defeated in the information war. The technological revolution led to the emergence of the term "information age" because information systems have become a part of our life and changed it radically. The information era also changed the way of conducting combat operations, providing commanders with an unprecedented quantity and quality of information. Now the commander can monitor the progress of combat operations, analyse events and bring information.

It is necessary to distinguish between the information age war and the information war. The war of the information age uses information technology as a means for the successful conduct of combat operations. On the contrary, information war considers information as a separate object or potential weapon and as an advantageous target. The technologies of the information era made possible a theoretical possibility, direct manipulation of enemy information. The information appears based on the events of the surrounding world. Events must be perceived in some way and interpreted to become information. Therefore, the information is the result of two things, the perceived events (data) and the commands required to interpret the data and associate the values with them.

Note that this definition is not related to technology. However, what we can do with information and how quickly we can do it depends on technology. Therefore, we introduce the concept of information function, it is any activity related to the receipt, transmission, storage, and transformation of information. The quality of information is an indicator of the difficulty of waging war. The more high-quality information the commander possesses, the greater his advantages in comparison with his enemy. Therefore, in the US Air Force, analysis of the results of reconnaissance and weather forecast is the basis for the development of the flight task. Accurate navigation increases the efficiency of the task. All together, they are types of military information functions that increase the effectiveness of combat operations. Therefore, we will give a definition of military information functions - these are any information functions that provide or improve the decision of the troops of their combat missions. At the conceptual level, it can be said that states seek to acquire information that ensures the fulfilment of their goals, take advantage of it and protect it. These uses and protection can be carried out in the economic, political and military spheres. Knowledge of the information that the enemy owns is a means to strengthen our power and reduce the power of the enemy or to resist it, and to protect our values, including our information.

Information weapons affect the information that the enemy owns and its information functions. At the same time, our information functions are protected, which allows us to reduce its will or the ability to fight. Therefore, let us define the information war - it is any action on the use, destruction, distortion of enemy information and its functions; protection of our information about such actions; and the use of our own military information functions. This definition is the basis for the following statements.

Information warfare is "the integrated joint use of the forces and means of information and armed struggle. Information warfare is a communicative technology for influencing information and information systems of the enemy with the aim of achieving information superiority in the interests of the national strategy while protecting its own information and its information systems.

Information warfare is only a means, not an end goal, in the same way, that bombing is a means, not a goal. Information warfare can be used as a means for conducting a strategic attack or counteraction.

The first to use the term "information war" was the American expert Thomas Rona in a report he prepared in 1976 for Boeing, and called "Weapon systems and information warfare." T. Rona pointed out that the information infrastructure is becoming a key component of the American economy. At the same time, it becomes a vulnerable target, both in the military and in peacetime. This report can be considered the first mention of the term "information war" [3]. The publication of the report of T. Ron served as the beginning of an active campaign in the mass media. The very formulation of the problem was very interesting to the US military, who tend to engage in "secret materials." The US Air Force began actively discussing this subject since 1980. From a military point of view, the term "information war" in our time was used in the mid-1980s. In connection with the new tasks of the US Armed Forces after the end of the Cold War. This was the result of the work of a group of American military theorists as part of GE. Eccles, G.G. Summers, and others. Later the term began to be actively used after the operation "Desert Storm" in 1991 in Iraq, where new information technologies were first used as a means of conducting military operations. Officially, this term was first introduced in the directive of the US Secretary of Defense DODD 3600 of Dec A few years later, in February 1996; the US Department of Defense launched the Doctrine of Control Systems Control. The publication defines the struggle with control and management systems as "the combined use of methods and methods of security, military deception, psychological operations, electronic warfare and physical destruction of control system objects supported by intelligence to prevent the collection of information, influence or destroy the opponent's ability to control and control over the battlefield, while simultaneously protecting their forces and allied forces, as well as preventing the enemy from doing the same "[3].

Most importantly, this publication defined the concept of war with control and management systems. In addition, this was the first time that the US Department of Defense identified the possibilities and doctrine of IW.

In late 1996, Robert Bunker, an expert at the Pentagon, presented a paper at a symposium on the new military doctrine of the US armed forces of the 21st century (the "Force XXI" concept). It was based on the division of the whole theatre of military operations into two components traditional space and cyberspace, the latter being even more important. R. Bunker proposed the doctrine of "cyber maneuver", which should be a natural complement to traditional military concepts aimed at neutralizing or suppressing the enemy's armed forces. Thus, the infosphere is now included in the number of spheres of combat operations besides land, sea, air, and space. ember 21, 1992. As military experts emphasize, the main objects of defeat in new wars will be the information infrastructure and the psyche of the enemy (even the term "human network" appeared). In October 1998, the US Department of Defense launched the "Unified Doctrine of Information Operations". Originally, this publication was called the "Unified Doctrine of Information Warfare." Later it was renamed the "Unified Doctrine of Information Operations." The reason for the change was to clarify the relationship between the concepts of information operations and information warfare. They were defined as follows:

Information operation: actions taken to impede the collection, processing, transfer, and storage of information by the enemy's information systems while protecting their own information and information systems;

Information warfare: a complex impact (a set of information operations) on the system of state and military management of the opposing side, on its military and political leadership, which already in peacetime would lead to the adoption of decisions favourable to the initiating party, and in the course of the conflict completely would paralyze the functioning of the enemy's control infrastructure.

Now there are quite a few different definitions of IW from the technical and technological point of view. In the corridors of the Pentagon, for example, this joking definition of "Information war is computer security plus money" [7]. Seriously, the military approaches the IW as it was formulated in Memorandum No. 30 (1993) of the Deputy Minister of Defense and the Joint Chiefs of Staff of the US Armed Forces [4].

The information war is understood here as the actions taken to achieve information superiority in supporting the national military strategy by influencing the information and information systems of the enemy while ensuring the security and protection of one's own information and information systems.

In the humanitarian sense, the "information war" is understood as one or other of the active methods of transforming the information space. In information wars of this type, it is a question of a certain system (concept) of imposing the world model, which is designed to provide the desired types of behaviour, about attacks on information generation structures, and reasoning processes.

The main forms of conducting technical IW are electronic warfare, war with the use of electronic reconnaissance and guidance, the deployment of remote point air strikes, psychotropic warfare, the fight against hackers, cyberwar. Before seriously analysing the various definitions of information war from a technical point of view, we note the inherent nature of it an important property.

The conduct of an information war is never accidental or detached but implies concerted efforts to use information as a weapon for conducting combat operations, whether on a real battlefield or in the economic, political, or social spheres. Therefore, as the basic and most general definition of IW, I propose the following.

Information warfare is a comprehensive holistic strategy, conditioned by the ever-increasing importance and value of information in command, control and policy matters "[4].

The field of action of information wars with this definition is quite wide and covers the following areas:

1) The infrastructure of life support systems of the state - telecommunications, transport networks, power plants, banking systems, etc.

2) Industrial espionage - theft of proprietary information, distortion or destruction of sensitive data, services; gathering information of intelligence about competitors, etc .;

3) Hacking and use of personal passwords of VIP-persons, identification numbers, bank accounts, confidential plan data, disinformation production;

4) Electronic interference in the processes of command and control of military installations and systems, "staff war," the disruption of military communications networks;

5) The worldwide computer network of the Internet, in which, according to some estimates, there are 150,000 military computers and 95% of the military lines of communication pass through open telephone lines. Whatever the meaning of the concept of "information war" was invested, it was born in the military environment and means, first, tough, decisive and dangerous activities comparable to real combat operations.

The military experts who formulate the doctrine of information war can clearly visualize certain of its facets: staff war, electronic warfare, psychotropic war, information-psychological warfare, cybernetic war, etc. Thus, information war is a form of conflict in which direct attacks take place on information systems to influence the knowledge or assumptions of the enemy. Information warfare can be conducted as part of a larger and more comprehensive set of military operations.

Thus, under the threat of information war, we mean the intention of certain forces to take advantage of the amazing opportunities hidden in computers, on the boundless cyberspace to conduct a "contactless" war in which the number of victims (in the direct meaning of the word) is minimized. We are approaching a stage of development when no one is a soldier, but all are participants in the fighting, said one Pentagon leader. The task now is not to destroy the manpower, but to undermine the people's goals, views, and outlook, in the destruction of society [7]. The civil information war can be unleashed by terrorists, drug cartels, clandestine dealers of weapons of mass destruction. The military has always tried to influence the information required by the enemy for effective control of his forces. Usually, this was done with the help of maneuvers and distractions. Since these strategies affected the information received by the enemy, indirectly through perception, they attacked the enemy's information indirectly. That is, in order for the trick to being effective, the enemy had to do three things.

Observe deceptive actions to deceive the truth by acting after deception in accordance with the goals of the deceiver. Nevertheless, modern means of performing information functions have made information vulnerable to direct access and manipulation with it.

Modern technologies allow the enemy to change or create information without first obtaining facts and interpreting them. Here is a short list of characteristics of modern information systems, leading to the appearance of such a vulnerability: concentrated storage of information, access speed, ubiquitous transfer of information, and large capabilities of information systems to perform their functions autonomously. Protection mechanisms can reduce this vulnerability, but not to zero.

Objectives of Information Warfare

There are three goals of information warfare: to control the information space so that we can use it while protecting our military information functions from enemy actions (counter information). Use information control to conduct information attacks on the enemy to increase the overall effectiveness of the armed forces through the widespread use of military information functions.

Here is an illustrative example of the use of an information attack when the Air Force carries out a strategic attack. Suppose that we want to limit the enemy's strategic capabilities to move troops by reducing fuel supplies. First, we need to identify refineries that will be the most appropriate targets for this attack. Then it is necessary to establish which factories produce the most fuel. For each plant, we need to identify the location of the distillation tanks. We organize an attack and, with a considerable economy of effort, we put the plants out of action, blowing up only the distillation tanks, and leaving all the rest of the equipment untouched. This is a classic example of a strategic attack. Now let us see how to achieve the same goal in the information war. All modern refineries have large automated control systems. These information functions are a potential goal in the information war. At an early stage of the conflict, we carried out a reconnaissance information operation to penetrate and analyse the control system of the refinery. In the course of the analysis, we found several vulnerable information dependencies that give us the means to influence the work of the refinery at the right time. Later, during the conflict, during one of the operations to block the enemy grouping, we used one of the vulnerabilities. We just stopped these plants. This, too, is a classic example of a strategic attack.

It is necessary to distinguish the information war from computer crime. Any computer crime is a violation of one or another law. It can be random, and can be specially planned; can be detached, or may be part of an extensive plan of attack. On the contrary, information warfare is never accidental or detached (and may not even be a violation of the law) but implies concerted efforts to use information as a weapon to conduct military operations - whether on a real battlefield or in the economic, political or social spheres. The theatre of information warfare extends from a secret cabinet to a home personal computer and is conducted on various fronts. An ever-growing arsenal of electronic weapons, mostly classified, represents the electronic battlefield. Speaking in military language, they are intended for combat operations in the field of command and control of troops, or "staff war." Recent conflicts have already demonstrated all the power and striking power of information warfare - the war in the Persian Gulf and the invasion of Haiti. During the war in the Persian Gulf, Allied forces on the information front conducted a range of operations ranging from the old-fashioned tactics of spreading propaganda leaflets to the disruption of Iraq's military communications network with the help of a computer virus. Infrastructure attacks inflict attacks on vital elements, such as telecommunications or transport systems. Geopolitical or economic opponents or terrorist groups can take such actions. An example is the disruption of the AT & T long-distance telephone exchange in 1990. Nowadays any bank, any power station, any transport network and any television studio is a potential target for impact from cyberspace.

Industrial espionage and other forms of intelligence threaten the great multitude of covert operations carried out by corporations or states against other corporations or states; for example, the collection of intelligence information about competitors, the theft of proprietary information and even acts of sabotage in the form of distortion or destruction of data. An illustration of this threat is the documented activities of French and Japanese agents throughout the eighties.

The collection of intelligence information also goes to new frontiers. The Lincoln Laboratory at the Massachusetts Institute of Technology is developing an air reconnaissance device the size of a pack of cigarettes. Another laboratory is working on chemicals that can be introduced into the provisions of enemy forces to allow sensors to track their movement through breathing or sweating. In addition, there are already satellite-tracking systems that have a resolution of several centimetres. Confidentiality is increasingly vulnerable as access to ever-increasing amounts of information becomes available in an ever-increasing number of subscriber sites. Important persons thus can become the object of blackmail or malicious slander, and no one is guaranteed against the spurious use of personal identification numbers. Nevertheless, the term "information war" owes its origin to the military and denotes cruel and dangerous activities associated with real, bloody and destructive military operations. The military experts who formulated the doctrine of information war clearly understand certain of its facets: headquarters war, electronic warfare, psychological operations and so on.

CONCLUSION

Public relations play an important role in the life of society. Initially created to inform the public about key events in the life of the country and power structures, they gradually began to perform another equally important function impact on the consciousness of their audience with the purpose of forming a certain attitude to the facts reported phenomena of reality. This impact was carried out with the help of methods of propaganda and agitation, developed over several thousand years. Soon public relations took an important place in the life of states, and with the development of technology and technology began to be actively used and at the international level in order to gain any advantages of the state controlled by it. Today, special attention should be given to the role of public relations in international conflicts, including geopolitical ones, since in recent years, along with classical weapons, the information and propaganda tool, which is based on work with various media, has been increasingly used.

REFERENCES

1. Afanasyev V. Social information and management of society. - M .: Knowledge, 2005, - 119 p.
2. Black S. Public Relations. What is it? Moscow: Nauka, 2007, 256 p.
3. MS Vershinin. Political communication in the information society. M .: Jaguar, 2006, - 256 p.
4. Zverintsev A.B. Communication management: A workbook of a PR manager: 2 nd ed., Rev. - St. Petersburg: Union, 2007, - 288p.
5. Kalandarov K.H. Management of public consciousness. The role of communication processes. M .: Science, 2006, - 154 with.
6. Krutskikh A., Fedorov A. About international information security. Moscow: The Word, 2008, - 234 p.
7. Malkova T.V. Masses. Elite. Leader. Moscow: Year, 2006, - 232 pp.
8. Mass information in the Soviet industrial city: The experience of a comprehensive Konnikova. - Moscow: 2006, - 347 p.

9. Pocheptsov G.G. Information war. M.: Garant Information Center, 2008, - 453 p.
10. Rastorguev S.P. Information war. M.: Science, 2008, - 235 with.
11. Rütinger R. Culture of Entrepreneurship. - Moscow: Leader, 2006, 672 p.