Conference Paper

Information Warfare

Kozminyh S. I.

Financial University under the Government of Russian Federation, Doctor of Technical Sciences, Moscow, st. Shherbakovskaja, 38

Abstract

The article is devoted to the problem of information warfare in the modern world, the possible implications of cybercrime and cyberterrorism, the analysis of directions of the conflicts settlement in the area of information warfare between individual states. To improve the Proposals of the Russian Federation in the field of information warfare.

Keywords: information warfare, cybercrime, cyberterrorism, information confrontation, information technology, computer attacks, industrial espionage, propaganda, information calls.

Corresponding Author:
Kozminyh S. I.
SIKozminykh@fa.ru

Received: 11 December 2017
Accepted: 20 January 2018
Published: 13 February 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies Conference Committee.

1. Introduction

The rapid development of information technology and globalization at the end of twenty and the early twenty first century resulted in replacing the traditional force methods of warfare, information wars [5]. Every day we meet with a huge flow of news that various media serves at a certain angle, the facts are often distorted and it becomes harder and harder for a normal man to identify where the truth and a lie. Nowadays, only analysts can objectively assess where propaganda is, and where the facts are that are presented to the world editions, television and Internet news. Looking back at the experience of various countries information influence on an opponent during the various regional conflicts and civil wars, it is safe to say that at present it is information confrontation becomes the main weapon that largely determines the victory or defeat of one or other party.

2. The essence and content of information warfare

Technology of waging information wars appeared long before the emergence of modern conflicts. Obtaining and manipulating information to achieve political and military objectives have been used even when the first states appeared. Finding and obtaining the necessary, particularly important information was one of the main tasks.

Extracted information was effectively used by state and military leaders of Babylon, China, ancient Rome and Greece [4].

Today the secrets of silk production is already of little interest, more relevant secrets related to innovative technologies, databases, bank accounts and personal confidential information. As an example of modern espionage, it should be recalled, as a citizen of Ukraine, who was collecting for scientific and technical information on the activities of the Russian the machine-building enterprises, was arrested by the FSB of Russia in Sverdlovsk region in February 2015 year.

Another striking example of the information warfare is an operation developed by the United States and its allies against Iraq. The basis of this operation was a deployed propaganda about the presence of chemical weapons in Iraq, threatening the entire world. As a result of this propaganda in Iraq by the American coalition forces were brought into the country, the war was, the legitimate Government was brought down, the head of State was executed and the country was plunged into chaos. While chemical weapons were never found. Radical Islamists took control over the country, who currently rampage through Iraq, fight in Syria, as well as commit terrorist acts worldwide.

The unconstitutional coup in Ukraine also was preceded by long-term information processing (propaganda) both of its population and of the world community aimed at creating a negative image of Russia, allegedly guilty for all the troubles of Ukraine. As a result of this was the illegal seizure of power, the breakup of the country, the civil war, a profound economic crisis, the ruin of the Ukrainian people and breaking the ties with the Russian Federation [3].

Thus, at present, one can note an increase in the intensity of information warfare, primarily associated with various political conflicts. Strengthening of information warfare, on the one hand, is incited by the worsening political situation in the world, and, on the other hand, is associated with significant modernization of information global infrastructure that is used to achieve political, economic and other purposes.

As a result of the analysis of the scientific literature, it can be concluded that the information warfare includes classical methods such as: physical impact on lines of transmission information, direct removal of information and other previously known methods. As well as the new methods, such as: cybercrime and cyberterrorism, including computer attacks, hacking computer data, information repositories, and other methods. Some researchers believe that information warfare is entering an era of so-called bloodless conflict where confrontation occurs in "cyberspace" and

"cyberwars" or so-called hackers are much more important than individual weapons [1].

Along with the development and spreading of new information technologies, all the time newer and newer forms of attacks arise that are qualitatively different from previous attacks. Using such tools as computer hacking or the introduction of malicious computer programs can transfer the war from the real physical world in an intangible virtual world. The modern hacker knows no boundaries. Computer attacks can be implemented at a distance, by means of radio communication or via wired network of international communications, without physical intervention and outside the territorial borders of the enemy country. The damage caused to the enemy may be different, for example it can be physical harm to military or civilians, or malfunctions of computer systems, the failure of important military and Government communications systems in the time of dealing with the crisis in the country [2]. All this can lead to economic difficulties or simply breach the living conditions of the people that depend on various information systems.

As an example, an incident might be recalled when the Russians have blocked operations in foreign payment terminals with international plastic cards Visa and MasterCard. Russia had to quickly create their international payment system «Mir», which is protected from external threats.

Every second of the dozen people become victims of any cyber fraud. The most likely victims are young people who surf the Internet via mobile phones.

The Virus Wanna Cry made a lot of noise on May 12, 2017. This extortionist and encrypter literally paralyzed work of structures and offices in 73 countries around the world. Experts could not reach the database on their PC as on their screens there was onlyone highlighted message where and how many need to translate money into bitcoins.

The Bad Rabbit is a virus encrypter that is designed for operating systems Windows and discovered on October 24, 2017, attacked several Russian media, including the Interfax news agency and the Internet-newspaper «Fontanka», as well as the Kiev Metro and Odessa airport, demanding for unlocking one computer 0.05 bitcoins (about 16 thousand rubles) within 48 hours. Also, to a lesser extent, Germany and Turkey were subjected to this attack. The rrecovery of the site work and "Interfax" computers took more than a day.

It should be noted that such massive attacks, which were carried out using encrypters of these viruses, require considerable effort and money. But the aim of these attacks was not receiving any economic benefit, and an act of cyberterrorism for

the purpose of destabilizing the activities of individual media, transportation facilities and ultimately, political pressure on the State.

The examples give another confirmation that we have already entered into an era of cyberwars, which can cause damage to the waging parties no less than a traditional war.

Now the problem arises of interpretation and the definition of "information warfare". The closest international practice is the definition of "aggression", which is given in the resolution 3314 of the General Assembly and the Declaration of aggression. "Aggression" is defined as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations".

The extent of the damage on the consequences of the aggression can be compared with the impact of information warfare. Hence, in international practice conducting information warfare can be considered equal to aggression by one state against another or others.

The complexity in the treatment of some forms of information warfare as a "use of force" or "aggression" in the framework of international law does not mean that the international legal institutions cannot answer such questions. For example, Chapter VII of the UN Charter gives the Security Council authority to determine whether any "threats to the peace or acts of aggression, and the UN Security Council in such cases may recommend any countermeasures. Many information attacks, which cannot by definition represent a "use of force" or "aggression", of course, can be interpreted as a threat to peace and therefore, they are subjected to the consideration of the Security Council [6]. However, due to the complexity of the procedure for the adoption of UN Security Council resolutions, including those related to the right of veto, the response to such actions may not be as efficient as far as any specific situation requires this.

Certainly, information warfare occurred in history throughout the existence of mankind, and with every century they are becoming more sophisticated. Information confrontation at the present stage of human history is characterized by more complex methods of exposure of one state (community) to another. In the struggle for natural resources and territory the new methods of war were introduced, not physical but strategic and tactical, this is information warfare.

3. The main directions of activities of the Russian Federation in the field of information warfare

In the twenty first century the Russian Federation joined with a specific set of tools for ensuring the security of our country. But, due to the fact that the tools of waging information wars are now greatly improved, there is a need to improvement and protection mechanisms in response to information challenges [5]. As demonstrated by the conflict in South Ossetia, our country, unfortunately, has not been able to deal effectively with CIO Western media, with the result that for quite a long time in the world community there was a negative image of Russia. Mounted and retouched video news from leading tv channels of the world about "aggressive actions" of Russian troops in the zone of the Georgian-Ossetian conflict, "huge casualties among Georgian civilians formed some sympathy from the world community in relation to Georgia and on the other hand, a negative attitude towards Russian peacekeepers. At the moment a counterweight to Western media is the Russian TV channel Russia Today, which is constantly under attack by the West. However, because it is one, but there are a lot of them, it cannot effectively resist the Western media.

One of the main tasks for our state is currently a need for separation and inter-relation of the concepts such as "aggression" and "information attack", as well as other concepts in this area to make them recorded into the international law. The Russian Federation could be an initiator in this field in order to continue using the changes to resolve international disputes and use "right of self-defense" in response to information attacks.

The use of the term "information attack" in the international law can provide the basis for "maneuvering" in legal disputes and enhance the effectiveness of political and diplomatic actions against the above attacks. Aiming to the protection of civilian persons in time of information war, Russia could sign international treaties in advance, which will reduce not only the country, but the political damage and damage caused by certain types of attacks. Russia could influence the development of international law in the sphere of informational wars through the Declaration of the UN General Assembly [7]. Then an attack on the information system of the Russian Federation would fall under the legal jurisdiction of Russia, despite the fact that the perform-ers might be beyond the reach of public services in Russia. In the case of computer attacks against the Russian Federation could justify counter-moves aimed at stopping an attack or preventing attacks, using Article 51 of the Charter concerning the right of

self-defence. However, this ground may be controversial in the case of military action against another state, carried out the information attacks.

As mentioned above, the peaceful settlement of disputes is one of the basic principles of the Charter of the United Nations. The Charter prohibits the threat or the use of force by a state against the territorial integrity or against political independence of another State. The only legitimate use of force can take collective action to enforce peace under UN auspices, either individual or collective self-defense against an armed attack. An Internet attack on computers, or an attack using information warfare such as viruses, is a controversial definition of armed attacks, which certainly needs to be consolidated with the international law.

The second challenge is that the Russian Federation should promote international cooperation in the field of information confrontation. In this regard, Russia needs to strengthen international ties in this sphere by harmonizing laws and to cooperate in the investigation and prosecution of criminals committing crimes with the use of modern information technology. The decision of this task must include diplomatic engagement and consultations on criminal justice in the field of informational attacks, as well as assistance in consolidating the concepts "information attack" as illegal actions in those countries which still do not recognize such attacks as crimes. In addition, provision must be made for a procedure for the extradition of perpetrators of computer attacks, involving binding their extradition to a country against which the attack was made.

Equally important in ensuring the security of the Russian Federation should be the protection of mission-critical information systems not only from attacks, but also from terrorist threats, local and global wars and natural disasters. Some information systems can be so critical that most countries would be interested in cooperation with a view to their protection. The subject to such protection can be objects of atomic energy, electronic international financial markets, banks, stock exchanges, communication centres, information systems of railway transport flights and medical databases.

The Russia's policy in the field of countering information warfare should include two main lines, the first is to ensure reliable protection of all information resources of Russia, and the second is to be actively involved in the information counteraction hostile media, distorting facts and forming a negative image of our country in the eyes of the world community.

To meet the first challenge, you must determine what information resources Russia interest for potential adversaries, and the greatest value for law enforcement. It is necessary to determine the magnitude of risks for these resources based on probability of threats that may impact on them, the amount of damage that can be caused to these

resources and the effectiveness of protective measures. The more effective measures will be used to protect information resources, the less risk of losing them.

To solve the second problem it is necessary to intensify efforts to identify legal and not legal organizations working on hostile media, financed by foreign intelligence services and carrying out subversive information activity. The Elimination of such organizations, publicizing their subversive activities and bringing them to legal liability will significantly reduce the risks of information influence directed Prouty of the Russian Federation.

It is quite difficult to determine which bear damage from the period of information warfare. Often, society is unaware that influence on it with a specific intent. The result is "handled" society that rebels against the legally elected authorities.

4. Conclusion

In conclusion, it should be noted that the main instruments for the settlement of information warfare in the legal field already exists. These include: regulations of the International Telecommunication Union, international space law, regulations of international humanitarian law. In spite of the already existing legal framework it should be noted that, at the moment, it is not yet enough. Many countries are at risk of information warfare, including our country. Conflicts are moving from the real world into the virtual, but the damage might not be the only virtual, but also material. We must bear in mind the mistakes of the past, not to make them in the future.

References

[1] Andrianov V.V., Zefirov S.L., Golovanov V.B., Kolduev N.A. information security business/2-nd Edition revised. and extras. -M.: Alpina Pulishing House, 2011.

[2] Drums M.V., Denisencev S.A., Kashin V.B, etc. Naval radio-electronic warfare. From the experiments of the past before the decisive front in the future. -M: Centre for analysis of strategies and technologies, 2015.

[3] Kozminyh S. I. Organization of information protection in the Russian police. Manual.-m.: UNITI-Dana: law and right in 2016.

[4] Supplement A.S. Informational effects and organized prostupnost: a course of lectures. -M: INFA-m, 2007.

[5] Stepanov O.A., Baranov V.V., Klementyev A.S., Nekishev A.V., Shmonin A.V. topical problems of counteracting crimes in the sphere of high technologies. O. Stepanov.

Moscow: Academy of Ministry of Internal Affairs of Russia. 2013.

[6] Skiba V.Y., Kurbatov V.A. Guide for protection from internal threats to information security. Spb.: Piter, 2008.

[7] Winn Schwartau. On the threshold of world information war. Network World, United States. 09, 2007.