Theoretical and Legal Aspects of Cyber Warfare

Prof. Dr. Alexander A. Galushkin

[1]Department of Humanitarian, Social, Economic and Information-Legal Disciplines, Stolypin International Institute of Informatization and Public Administration, Moscow Region, Russian Federation
[2]Department of Municipal Law, Peoples' Friendship University of Russia, Moscow, Russian Federation
Email: alexander.galushkin@yandex.ru

Doi:10.5901/mjss.2016.v7n1p570

Abstract

In the given article author studies the theoretical basis of the 'cyber warfare' phenomenon and analyzes its different definitions. In his analysis the author compares different definitions and their wording. The author gives definitions to some interrelated terms and phrases. According to him, apart from goals and objectives, a proper full definition should also mention possible parties to the conflict, suggest a list of possible targets, suggest a list of the "weapons" used in cyber warfare. The author points out that without a detailed definition that takes into consideration all aspects of cyber warfare, it is highly problematic, if possible at all, to come up with proper legal tools against cyber wars. At the end of the article the author concludes that recently cyber wars have affected business corporations and non-governmental organizations far more often than public or local institutions. Cyber warfare has become a real threat that must be taken into consideration. Given its novelty we must ensure that the concept of the phenomenon as well as new possible threats are well studied.

Keywords: *Internat, space, information, war, warfare, threat, security.*

1. Introduction

The aim and objectives of the research is the research of some basic theoretical and legal aspects of cyber warfare, including study of theoretical basis of the 'cyber warfare' phenomenon and analyzes its different definitions.

The process of Internet expansion is different and not geographically even – a lot depends on the population size and density, per capita income, the median age, education level, and how developed the information and telecommunication structure in the region is. 48.4 per cent of the users today are located in Asia, 21.8 percent – in North and South America, 19 per cent are in Europe, 9.8 per cent – in Africa, and 0.6 per cent are located in Oceania (Galushkin, 2015).

Cyber warfare is a new phenomenon that hasn't been studied well yet, so there is no commonly accepted definition. Cyber wars are completely different in their nature compared to traditional armed wars. Another term used to describe cyber wars in literature and the mass media is "computer wars".

According to the famous Ukrainian scientist A. Merezhko, "cyber warfare is the use of the Internet and other information technology tools related to it by a government in order to damage another country's military, economic, political and information security as well as its sovereignty" (Merezhko, 2014).

According to the Defense Technical Information Center of the US Department of Defense, "cyber warfare is politically motivated computer hacking aimed at sabotaging and espionage. It is a type of information war that is sometimes considered analogous to traditional armed conflict" (DOD – Cyberspace, 2011).

According to Legal Advisor at International Committee of the Red Cross Laurent Gisel, "cyber warfare is means and methods of warfare that consist of cyber operations carried out by or against a computer or computer network, amounting to or conducted in the context of an armed conflict, within the meaning of international humanitarian law (IHL)» (Gisel, 2014).

The definition of cyber warfare given by the weekly American magazine "Secret" is very simple: "cyber warfare is warfare in cyberspace" (Tomorrow there was cyber war, 2011).

According to the SecurityLab.ru information resource, "cyber warfare is a war in the Internet aimed at putting government computer systems out of order" (Latest news for cyber warfare, 2014).

The US specialists R.A. Clarke and R.K. Knake define cyber war as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke, Knake, 2010).

All the definitions mentioned above are totally truthful but neither of them embraces all the aspects.

2. Research Methods

It the present article a wide range of research methods are used, including qualitative quantitative. Data analyses play an important role, giving author and opportunity for the correlation

3. Discussion

Thus, professor A. Merezhko's definition says that one of the parties in cyber war is a sovereign state, although it might as well be a corporation, association and other organizations (especially international ones).

The Defense Technical Information Center of the US Department of Defense points out that cyber wars involve politically motivated hacking, thus ignoring the fact that hacking is not necessarily a tool of cyber warfare and the actions are sometimes not politically motivated at all.

Cyber wars can often be caused by economic, social and other numerous reasons, including political ones but those will only be a factor among others.

The statement about cyber war being a type of information war is questionable as well because the attacking party may not aim for informational influence on the civil population or the military.

Psychological warfare is close in its nature to the information warfare notion.

According to one of the definitions, "information war is a type of conflict the key target of which is information stored in government, intelligence, military and other systems of the enemy. The concept of the modern information war has been developed quite recently. The US specialists suppose that cyber revolution that caused proliferation of all sorts of information systems across-the-board became grounds for the information war development» (Electronic Warfare >> Information Warfare, 2014).

As professor V. Krysko put it, "psychological warfare is a complex of different tools and methods of influence aimed at changing people's psychological properties (views, opinions, values, attitudes, motives, stereotypes, behavior), as well as group standards, public spirit and awareness in general» (Krysko, 2003).

It is safe to say that cyber warfare is just one of the information war forms with a whole lot of special features and characteristics.

Legal Advisor at International Committee of the Red Cross Laurent Gisel views cyber wars strictly within an armed conflict and international humanitarian law, thus not taking into consideration a lot of special aspects of cyber warfare.

According to one of the definitions, "international conflict is either direct or implicit clash of interests of two or more parties (countries, group of countries, peoples, political movements) caused by a subjective or objective disagreement between them".

These disagreements can be of territorial, national, religious, economic, military and strategic, scientific and technical character, etc.

However, at the end of the day such conflicts always turn out to be political because the disagreements are solved within the existing domestic, foreign and military policies of the countries involved, through their implementation mechanisms» (Achkasova, Gutorova, 2010).

Another view is that "international conflict is defined based on its types ("international law has always been related to resolving the wars, disagreements and conflicts between countries as well as other situations referred to as "international conflict" these days" (Legal Conflictology, 2015), based on being viewed as sociological (escalation of disagreements between the parties or political "a conflict is relations of political character between two or more parties in which the existing disagreements are expressed acutely" (International conflicts, 1972).

4. Summary

The reason why it is so hard to come up with a unified definition of conflict in international law is that the term is used differently and the phenomenon is studied by various disciplines» (Chernoudova, 2005).

The American magazine "Secret" gives the shortest, still probably the most accurate definition. However, they only define "the battlefield", skipping giving any characteristics to cyber warfare as such. Moreover, it's not completely clear what is meant by cyberspace.

The famous SecurityLab.ru information source describes cyber warfare as clashes in the Internet. However, cyber wars are not always carried out within the Internet only.

R. Clarke and R. Knake view cyber warfare as actions of one country against another, not mentioning other possible participants.

As V. Artyukhin points out, the phenomenon of cyber warfare is relatively new, and all of the given definitions are either too broad, or too specific.

There are a lot of other definitions apart from the ones mentioned above, but all of them are quite similar and are only different in the choice of words and phrases.

According to the author, apart from goals and objectives a proper full definition should also include possible parties to the conflict, suggest a list of possible targets, suggest a list of the "weapons" used in cyber warfare.

The author points out that without a detailed definition that takes into consideration all aspects of cyber warfare, it is highly problematic, if possible at all, to come up with proper legal tools against cyber wars.

From the military point of view, "doctrinal study of the information warfare issues in the USA began straight after the Persian Gulf war (1991) in which state-of-the-art information technology was applied by the US armed forces for the first time.

An instruction of the Department of Defense TS3600. 1 that came into force on December 21, 1992 contained a basic strategy on the fight against information warfare. This paper defined it as a complex informational impact on the enemy's government and military systems, and included five key elements: psychological operations, counterintelligence operations and ensuring the operations carried out by the forces are safe, deception, electronic warfare, annihilations of the enemy's control centers and communication systems» (Korsakov, 2012).

In most developed countries today information services are present in all possible areas of people's lives. So there are a lot of legal tasks to fulfill yet (Bachilo, 2001). Information services can be divided into public, local, commercial and others – all provided by different public or local institutions, for-profit or non-profit organizations, different associations, etc.

Success of a lot of companies depends on how well they are represented in the Internet by their websites to quite a large extent. Given the advanced development level of the information technology nowadays, apart from some basic operations like reading and browsing, websites can offer a range of advanced services including legal formalities.

If during cyber war the resources attacked are government-protected or belong directly to the government, then in some ways we can say that the attack has been carried out against the country.

However, recently cyber wars have affected business corporations and non-governmental organizations far more often than public or local institutions. Cyber warfare has become a real threat that must be taken into consideration. Given its novelty we must ensure that the concept of the phenomenon as well as new possible threats are well studied.

Unfortunately, so far such work has been unsystematic and sketchy. According to the author, it can only be efficient at the international level and should entail development of the relevant international legal framework.

5. Conclusion

It is important to understand that with the development of information technologies and shift of trade and services to the Internet space meaning of 'cyber warfare' is changing constantly. New forms and methods of 'cyber warfare' appear.

For example, currently, "according to public opinion polls 44% of men and 29% of women are interested in politics. 54% of the "first sex" and 61% of the "second sex" are not engaged in social activities, 79 and 91% respectively don't participate in political forms of civil activity"(Tarusina, Isaeva, 2014). However often such interest is not going too much beyond the activity in the Internet.

Internet became recently subject to active political and information wars. Based on personal opinions persons form own opinion and choose sides. Many forget that "duty of proving existence of circumstances which may be the basis for the review of the court decision lie on the shoulders of the person (side) that makes the appeal " (Sangadzhiev, Marchuk, Galushkin, 2013).

Such actions are also becoming part of modern cyber warfare and are to be studied thoroughly. Appropriate legislation is required.

6. Acknowledgments

Research is conducted with the financial aid of the grant of the President of the Russian Federation MK-4283.2015.6

References

Achkasova V., Gutorova V. (2010). Study guide for higher education institutions. Moscow.
Bachilo, I. (2001). Law and the information society. Information Society, 4, 25-32.

Chernoudova, M.S. (2005). Concept of Conflict in International Law. Moscow Journal of International Law, 2.
Clarke, R., Knake, R. (2010). Cyber War: The Next Threat to National Security and What to Do About It. HarperCollinsPublishers.
DOD – Cyberspace (2011). Dtic.mil. [Online] Available: http://www.dtic.mil/doctrine/jel/doddict/data/c/01473.html (June 6, 2015)
Electronic Warfare >> Information Warfare (2014). Modern Army. [Online] Available: http://www.modernarmy.ru/article/282/informacionnaya-voina (June 6, 2015)
Galushkin, A. (2015). Internet in modern Russia: History of development, place and role. Asian Social Science, 11 (18), 306. DOI: 10.5539/ass.v11n18p305
Gisel, L. (2014). War in Cyberspace. Independent Newspaper. [Online] Available: http://nvo.ng.ru/armament/2014-02-14/9_cyberwar.html (June 6, 2015)
International conflicts (1972). Moscow, International relations, 41.
Korsakov, G. B. (2012). Information weapon of the superpower. Ways to the peace and safety, 1 (42), 34-59.
Krysko, V. (2003). Dictionary and reference book on social psychology, 230.
Latest news for cyber warfare (2014). SecurityLab.ru. [Online] Available: http://www.securitylab.ru/news/tags/%EA%E8%E1%E5%F0%E2%EE%E9%ED%E0/ (June 6, 2015)
Legal Conflictology (2015). Moscow, 176.
Merezhko, A. A. (2014). Draft Convention on prohibition of the use of cyber warfare in the global information and computer network (the Internet). Center for Policy Studies in Ukraine. [Online] Available: http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57 (June 6, 2015)
Sangadzhiev, B. V., Marchuk, N. N., Galushkin, A. A. (2013). Questions of fair justice and judicial authority functioning in Russian Federation. World Applied Sciences Journal, 28 (7), 920. DOI: 10.5829/idosi.wasj.2013.28.07.2046
Tarusina, N. N., Isaeva, E. A. (2014). Gender tendency of Russian political activity from the perspective of jurisprudence. American Journal of Applied Sciences, 11 (12), 1978. DOI: 10.3844/ajassp.2014.1976.1979
Tomorrow there was cyber war (2011). The Secret magazine, 29.
Vgl.: Handbuch Ve,reinte Nationen (1991). hrsg. von Rüdiger Wolfrum. 2., völlig neu bearb. Aufl. München: Beck, 418.