Transition of rivalry between USA and China to new Internet-space

Petukhov Alexander Yur’evich, Komarov Igor Dmitrievich, Starkin Sergey Valer’evich, Markova Alexandra Veniaminovna

NI Lobachevsky Nizhny Novgorod State University, Russia, Nizhniy Novgorod, Gagarin Avenue, 23, 603950

ARTICLE INFO

Article history:
Received 25 June 2014
Received in revised form 8 July 2014
Accepted 10 August May 2014
Available online 30 August 2014

Keywords:
Information wars, China, US, Internet.
Cybersecurity, NSA, PLA

ABSTRACT

The current article is devoted to the analysis of the transition of rivalry between USA and China in the information networks. The authors determine the basic institutions, which are dealing with development and investigation of information wars and psychological operations. The state of China’s cybersecurity and its basic mechanisms of manipulative techniques are also examined.

INTRODUCTION

The modern condition of the international system is undergoing serious changes, which correspond to the realities of the existing order. However there is a deterrent factor in the framework of this “evolution”. Taking into attention the transition of center of international military activity in the Asia-Pacific region and technical development of the Asian countries, it remains acute to consider the cybercrimes through the prism of China-US foreign policy activity, which are the major actors of the Asia-Pacific region.

The agenda is defined as information security and deterrence of cyberattacks and cybercrimes. Technological development contributes to the vulnerability increase of the majority of countries.

People's Liberation Army of China technically inferior to US, but its growth and modernization rates are increasing, despite the exciting internal economic development and social reforms in China. The governmentally supported projects of cyberattacks and testing of possible scenarios of hacking into the infrastructure systems, energy supply, headquarters of large companies, corporations, scientific-research centers of Taiwan Republic of China are the basic elements in the framework of the international system cyber and information war (subsequently, methods, which have been tested on the Taiwanese companies, are used for hacking American institutions and organizations).

Hackers - the soldiers of the new wars:

In accordance with the Taiwan's National Security Bureau data, China is constantly increasing strength of its cyberarmy. It currently employs 100,000 people. According to unconfirmed reports, Beijing spends approximately $ 2.7 million (€ 2 million) per year to finance the needs of hackers and various types of cyberoperations [1].

Taiwan government and Washington are seriously concerned about the growing cyberthreats from the PRC. According to May 2013 report of the US Ministry of Defense, “In 2012, a large number of computer systems around the world, including those owned by the U.S. government, became targets of attacks, some of which are directly related to the Chinese government and the army” [1].

Taiwan's Ministry of State Security stated that China deliberately infects sites of government agencies, military departments, as well as major corporations in Taiwan with different viruses and malware. The ministry assured that actions of this kind are usually significantly activated in periods of rising tensions between Taiwan and China [7].

Use of cyberspace as an additional leverage in modern political processes is an essential element. Considering the implementation of information technologies in military units, ensuring cyber security becomes
an integral part of security in general. Thus, the Air Force Taiwan ready to use unmanned aircraft to gather intelligence on the Chinese army (32 UAVs have been already put into service) [9] that will allow controlling the PLA activity in the Taiwan Strait. This intelligence can be used by the United States, given their experience with drones in the Afghanistan-Pakistan border. Application of such methods by the opponent army stimulates government funding into the development of cybersecurity against cyber attacks.

U.S. drone intelligence operations are kept secret but it is known that strategic UAVs Global Hawk fly over the territory of China for this purpose, capable of rising to a height of 18 kilometers, which makes them inaccessible to the majority of air defense assets.

In its turn, Chinese military produce a number of alternative measures to combat drones. Among them are the following: the use of electronic protection for mute onboard electronics and signals between the UAVs and military communications satellites; cyber attacks with the aim of breaking Global Hawk control systems; usual smokescreens that hide objects from the enemy observation [3].

Protection of national interests with the use of cyberspace is not the main focus of Chinese hackers. Beijing aspirations are the stimulation of scientific and technological progress, which in turn forces scientific and technical intelligence to work actively, using a wide range of possibilities, such as the traditional and / or non-traditional (introduction, bribery, provocation) and new. Thus the infrastructure acquisition of a military nature is of fundamental importance for China, but exclusively for peaceful purposes. That is displayed in the accompanying documents. However, Beijing uses different channels in order to master technical information revealing military capability development (from legitimate, through diplomatic channels, to illegal).

Information and psychological warfare:

Another level of confrontation on the Internet is information-psychological one.

Information begins to bear both creative and destructive force, but to a much greater degree than it was previously. If previously the goal was to adjust object views and create short-term emotions, today the information field can make a significant change in the pattern of attitude and philosophies of man, changing his cognitive installation.

Apparently, the events of the last days, weeks and years lead us to conclusion that the arms race has been accompanied by information and psychological race. War of ideologies and cultures took global form and does not hesitate to use any ways. In this regard, methods and schemes are improved, for example, entire institutions in USA study and develop new ways to conduct psychological operations (procedures) and methods of protection against them. Moreover, National Cryptologic School NSA (National Security Agency) trains 19 000 people per year (13.5 thousand - civilian personnel NSA, 2.5 thousands - military personnel, 3000 - from other departments) [6]. Training of specialists in the "information war" is also conducted by some other U.S. institutions.

In the People's Republic planning and implementation of measures for employment of information technology to disrupt information objects and telecommunication infrastructure of foreign countries is carried out by the ministries and agencies, which are responsible for the enforcement of state and military security of the country as a whole: the Ministry of Defence (MoD) and the Ministry of State Security (MSS) of the PRC.

Speaking about the People's Liberation Army (PLA), the Main Political Department of the PLA is responsible for execution of information warfare operations and assurance of information and psychological defense of the military forces. Thus, the use of information technology to disrupt information objects and telecommunication infrastructure is regarded in China solely as an integral part of information warfare at the state level. Its main content is "the fight against control systems", which is understood as a set of measures for the comprehensive effects on the troops control systems and enemy weapons, with the use of program methods, electronic warfare and fire damage.

The General Staff of the PLA coordinates the organization of information warfare in computer networks by the electronic warfare. This body holds control over specialized centers, which research the possibility to access information networks and protect control networks. Analysis of the opportunities of information warfare is also conducted in parts of psychological operations, electronic warfare and communications central and district command.

It should be noted that currently organizational structure units designated to conduct information warfare are developed in the PLA. According to the views of Chinese experts, they should include those of computer intelligence and counterintelligence, electronic virus attacks, virus protection and protection from other weapons’ exposure to electronic computers [2]. Particularly important role plays dealing with the issue of Taiwan [5] and the growing Chinese nuclear potential [8].

Mechanisms of information warfare:

The basic mechanism of such units operation in the information war is the organization of manipulative psychological operations of various sizes. The classic method of such manipulations is evoking different forms
of neurosis in the individual. Speaking about a group of people, neurosis is transmitted as a disease passing from one individual to another. Then, the “infected” group is treated as if all of the member were neurotics [5].

Provoking on the psyche of the individual symptoms of borderline psychopathology is based on significant effect of manipulative techniques. For example, the individual psyche can be encoded by the information transmitted through social networks. Such coding mentality is based on the laws, according to which any information first enters the subconscious mind, and from there has an impact on the consciousness.

Disease (neurosis, for example), as well as any form of mental instability as a result of any other kind of disease (ARD, for example, or the flu, or any other form of sickness), as well as increased fatigue, drunkenness, and so on, are a kind of example of the so-called altered states of consciousness, when the mind (consciousness) of the individual can no longer stand barriers on the way of new information, in order to evaluate different kinds of information. We must note that such an assessment is required, and it characterizes the psyche of a healthy person. Brain of an individual is generally arranged so that it is not able to remember all the information coming into it from the outside world, so all the information after the censorship of the psyche, when only part of the information falls into the consciousness and is used in the near future, is deposited in the subconscious. Only there, in the subconscious, such information stays for the lifetime of the individual, and is able to move into the consciousness of even a few decades later.

Obviously, in the moment the modern media, especially online media, has a huge number of different technologies of impact on society that could potentially carry a significant risk. It lies in the fact that an individual is particularly unprepared and ignorant of those manipulations and easily gets into the net and becomes paddle toy. Apparently, manipulated individuals are confident that they act as they wish, are free and ready to defend “their” interests [10].

Conclusion:
Thus, USA and China are gradually increasing their ability to conduct cyber warfare and information warfare. The number of corresponding structures is constantly growing and receiving equipment and investment; new types of equipment and devices are developed, dozens of scientific departments operate in the interests of such organizations.

All this leads to the new inevitable round of competition, especially brightly it will manifest itself in the Asia-Pacific region, where China has almost no comparable opponents in military and economic power. No wonder why Japan is radically revising its own military doctrine; additionally, China still has complex relations with Vietnam.

Close economic cooperation between the U.S. and China and their mutual dependence deter the opportunity of the military conflict and open rupture of economic relations, sanctions etc. However, it expands the possibilities for information warfare and increases the value of the effectiveness of such operations.

This work was supported by grants from the Board President of the Russian Federation (Project MK-259.2013.6).

The research is supported (partly supported) by the grant (the agreement of August 27, 2013 № 02.B.49.21.0003 between The Ministry of education and science of the Russian Federation and Lobachevsky State University of Nizhni Novgorod)

REFERENCES
