Mini Review

BIOMEDICAL
Journal of Scientific & Technical Research

ISSN: 2574 -1241

DOI: 10.26717/BJSTR.2021.33.005362

# The Information and PSY Wars of the Future: Chinese Cyber Troops

**Andrey Molyakov***

*Institute of information technologies and cybersecurity, Russian State University for the Humanities, Russia*

***Corresponding author:** Andrey Molyakov, Institute of information technologies and cybersecurity, Russian State University for the Humanities, Russia

**ARTICLE INFO**

**Received:** January 06, 2021

**Published:** January 15, 2021

**Citation:** Andrey Molyakov. The Information and PSY Wars of the Future: Chinese Cyber Troops. Biomed J Sci & Tech Res 33(2)-2021. BJSTR. MS.ID.005362.

**Keywords**: Cyber Troops; Red Dragon Hacker Group; concept of “Three Wars”; Electronic-Viral Weapons, PSY wars; Electronic-Viral Weapons; Red Dragon

## ABSTRACT

Modern information and communication technologies make it possible to reprogram a person faster and cheaper than to kill. Cyberwar is becoming the dominant type of information warfare and its strategic goal is to achieve spiritual, political and economic power. Network-centric technologies are most effective here. A special place on cyber warfare is occupied by psychotropic weapons, which provide an impact on the ethnic, religious and collective psychology of citizens of the “enemy” territory. External forces form a model of behavior through the manipulation of major power and other social groups. The battle for dominance in cyberspace has begun, primarily between the United States and China. Despite the absolute leadership of the USA in the field of Internet technologies, Communist China began to prepare for network wars. The Chinese army, technically losing to the Americans in conventional and nuclear weapons, began to invest in the latest technology. At the same time, the Chinese have relied on an offensive war in cyberspace. Realizing that China’s path to a superpower will continue to be a weak spot for military power compared with the United States, China has made asymmetric deterrence a key element of its military strategy by creating cyber divisions. The Chinese cyber strategy “kick from the corner” is the most predicted scenario for the future blitzkrieg.

## Introduction

Cyber war is not only hacking other people’s information resources to obtain information of interest or making them unusable at least for a while. Cyber warfare is a special method of fighting countries, complementing the previously existing methods of delivering physical attacks, but this time in cyberspace [1]. This is especially important in our century of a sharp separation of the USA in military power from other countries, which determined the search in these countries for different options for asymmetric answers. In this regard, China is no exception, although the power of its Armed Forces is large enough, but not enough to reach a direct traditional confrontation. To understand the options for asymmetric answers, in this case Chinese, let us first consider the general situation characteristic of cyberspace. The number of Internet users over the next decade has exceeded 1.5 billion, which is approximately 25% of the world’s population. At the same time, the share of the United States is declining due to the growth of users mainly in the Asia-Pacific region.

As a result of the information revolution, a global network society has emerged. Washington was convinced that in the World Wide Web, owning information, he would “forever” rule the world. But at the beginning of the twenty-first century, the dependence of the world community on the United States - “information imperialism” - was undermined by the triumphant spread of the Internet and especially social networks. The global Internet system has become a factor in political and economic reality and is turning into geopolitical communication, where the mobility of information becomes a strategic resource that does not have a territorial state organization. For the first time in the history of mankind, a decline in the status of the state has occurred. The information revolution has hit the state monopoly on information. She transformed ideas about national security, which for centuries proceeded from the premises of the creation of the military and economic power of the state. The main priorities of national security are changing. Along with material goals, values that can be protected with a sense of dignity, national pride and civilizational affiliation become targets of defeat in Information and PSY Wars and conflicts.

## The philosophy of Information and PSY Wars of the People's Republic of China (PRC)

In a clash with the Soviet Union in the late 1960s, the PRC leadership learned that in the fight against an enemy equipped with modern technology, the direct path of confrontation is not the best. Since the late 1990s, the Chinese strategic doctrine has seen the rise of the theory of unilateral warfare, using several multidirectional attacks of a non-military direction to achieve military results, for example, damage to communications or the financial infrastructure of the state. Cyber war is the central element of a one-way combat strategy. The Chinese military developed many theories about modern war a decade ago, and now you can see how events are "played out" and cyber war plays a key role in them. The Chinese textbook on military science and military strategy notes that "war is not only armed struggle, but also all-round competition on the fronts of politics, economics, diplomacy and law". The concept of "Three Wars" calls for the use of "psychological warfare", which means propaganda, deceit, threats and coercion, "media war", influencing public opinion and gathering public support at home and abroad, and a "legal warfare" that uses international and domestic judicial instruments to promote Chinese national interests.

In the People's Republic of China, the planning and implementation of measures to use information technology to disrupt the functioning of the information and telecommunication infrastructure of foreign countries is carried out through the ministries and departments responsible for ensuring the state and military security of the country as a whole, namely the Ministry of Defense and the Ministry of State Security. In the People's Liberation Army of China (PLA), the Main Political Directorate is responsible for conducting information war operations and providing information and psychological protection for troops. At the same time, activities to use information technology to disrupt the functioning of information and telecommunication infrastructure facilities are considered in the PRC exclusively as an integral part of the information war at the state level. Its main content is "the fight against control systems," which is understood as the totality of measures for the integrated impact on the control systems of enemy troops and weapons, carried out by software methods, electronic warfare and by means of fire destruction.

## Types of Information Weapons of China

The most promising types of information weapons in China include electronic-viral weapons (EVW), radio interference generating devices, disposable and reusable generators of various types of electromagnetic energy (explosive, explosive magneto-hydrodynamic, beam-plasma and others). As the processes of informatization strengthen in the areas of state and military administration of the leading countries of the world in the military scientific circles of China, more and more importance is given to the study of issues of program-electronic impact on information resources stored or circulating in the computer information-control systems data arrays. At the same time, the effective use of electronic-virus tools, often referred to as electronic-virus weapons, is highlighted in the information warfare. The main features of the EVW are the relative cheapness of its production with high impact efficiency, secrecy of use, autonomy, duration of operation, the possibility of transformation, a variety of implementation methods (via radio channels, through computer networks, undercover), as well as the ability to disable almost all modern control systems troops and weapons.

The EVW is entrusted with the solution of the following main tasks: obtaining information constituting state or military secrets of the opposing side, misleading it, paralyzing command systems, and intervening in the process of controlling enemy troops and weapons. To realize the capabilities of electronic-viral weapons, it is proposed to create a theory of electronic-viral warfare, form special units and units, and develop appropriate tools. To conduct electronic-virus warfare, electronic-virus attacks and anti-virus protection are being developed. All means of emulsion explosives are divided into software (all types of viruses) and hardware (means of influencing both the electronic equipment as a whole and its individual elements). The work of elite hacker groups in the 15th zone of the NUDT [2], engaged in the development of microelectronic products, in particular microprocessors, including CT-2, is a significant threat.

The general idea of these works is to integrate hardware-controlled software agents into high-performance microprocessors and graphic accelerators, whose work against the background of the general high performance of the microprocessor or accelerator will be invisible. This bookmarking work in equipment is led by Qin Bo Wu, Kylin's chief developer, who also leads the China's military intelligence hacker community. The line for introducing hardware bookmarks will be implemented, in particular, at the Taiwanese TSMC factory. On this occasion, the order of the military leadership of the PRC was given. Den Lu, deputy director of innovation at TSMC (Taiwan), a lieutenant colonel of Chinese military intelligence, is responsible for this work, previously actively participated in the creation of the hacker group "Red Dragon", which is now connected to the work of specialists from the 15th zone of NUDT. We should remember that the TSMC factory is 60% owned by China [3,4].

## The Structure of China's Cyber Military Forces

In the PRC, the main structures responsible for ensuring information security, depending on the tasks to be solved, are following:

**a)** Ministry of Communications and Information Technology;

**b)** Ministry of the Interior;

**c)** Ministry of Defence.

Structurally, the PRC's cyber military (3rd PLA Department of Military Intelligence is closely related to intelligence structures, so a description will be given as a whole, including the structure of Main Intelligence Directorate. General information about the Armed Forces of the PRC will also seem to be interesting and useful. The location of the main centers for the preparation of cyber military forces in the PRC is shown in Figure 1. The People's Liberation Army of China (PLA) is the armed forces of the PRC, the largest army in the world. The legislation provides for military service for men from 18 years old, and volunteers are accepted up to 49 years old. Due to the large population of the country and the sufficient number of volunteers, the call has never been made. In wartime, up to 300 million people could theoretically be mobilized. The PLA is subordinate to the Central Military Commissariat of the Political Bureau of the PRC. The post of the chairman of the Central Exhibition Complex is the key for the whole state. It belongs to the President of the PRC. China established 7 military districts. The task of the troops of the PLA active service includes defensive military operations and, if necessary, according to the law, assistance in maintaining internal public order (Figure 1).

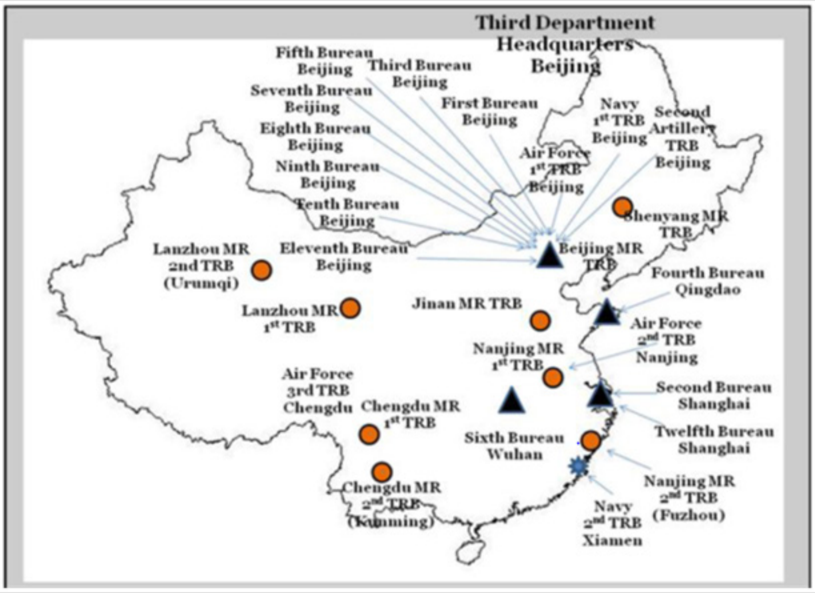

**Figure 1:** Location of the main cyber military training centers of the PRC.

Their centers are indicated by yellow circles (MR - military region):

**a)** Shenyang Military District (Shenyang MR)

**b)** Beijing Military District (BeiJing MR)

**c)** Lanzhou Military District (Lanzhou MR)

**d)** Jinan Military District (Jinan MR)

**e)** Nanjing Military District (Nanjing MR)

**f)** Guangzhou Military District (GuanZhou MR)

**g)** Chengdu Military District (Chengdu MR)

The reserve troops participate in regular military exercises, if necessary, provide assistance in restoring public order, which is provided for by Chinese laws, in the event of a war after state mobilization they turn into regular active troops. The Central Military Council, through the General Staff, the Main Political Directorate, the Main Directorate of Rear Services and the Main Directorate of Military Equipment, exercises combat command and also directs military development. Main Intelligence Directorate of the General Staff of the PLA is the central organ of military intelligence of the PRC. General management and control over the activities of the PLA is carried out by the Central Military Council of the PRC, subordinate to the Central Committee of the CPC. The operational management is carried out by the chief of the PLA General Staff. The head of the Main Intelligence Directorate is appointed by decree of the Chairman of the PRC.

The structure of the Main Intelligence Directorate is currently as follows (Figure 1):

**a)** The First Bureau (First Bureau, Beijing) - intelligence intelligence in China.

**b)** The Second Bureau (Second Bureau, Shanghai) - foreign operations.

**c)** The Third Bureau (Third Bureau, Guangzhou) - cybersecurity and the conduct of information and psychological wars.

**d)** The Fourth Bureau (Fourth Bureau, Qingdao) - operational and technical support.

**e)** Fifth Bureau (Fifth Bureau, Beijing) - coordination of regional departments.

**f)** Sixth Bureau (Sixth Bureau, Wuhan) - military counterintelligence.

**g)** Seventh Bureau (Seventh Bureau, Beijing) - processing and analysis of incoming intelligence.

**h)** Eighth Bureau (Eighth Bureau, Beijing) - Institute of Contemporary International Relations.

**i)** Ninth Bureau (Ninth Bureau, Beijing) - department of its own security, coordination of special departments in the army.

**j)** Tenth Bureau (10th Bureau, Beijing) - collection of scientific and technical information; Eleventh Bureau (11th Bureau, Beijing) - electronic intelligence and computer security (similar to the NSA).

**k)** The Twelfth Bureau (12th Bureau, Shanghai) - military-space intelligence (analogue in Russia 4 Central Research Institute of the Ministry of Defense of the Russian Federation).

Let us give further enlarged comments on the training centers of the cyber military forces of the PRC, which are given in small print in Figure 1.

**1)** AirForce 1st TRB is the main training center for specialists in the field of radio intelligence, electronic warfare for the needs of the Air Force of China. Located in Beijing.

**2)** AirForce 2nd TRB is the main training center for specialists in the field of creating secure telecommunication systems, experts in the field of computer security for the needs of the Air Force of China. Located in Nanjing.

**3)** AirForce 3d TRB is the main training center for hacking specialists. Here is created a “training cyber training ground” for training officers in the field of introducing information wars. Located in Chengdu.

**4)** Navy 1st TRB is the main training center for specialists in the field of radio reconnaissance, electronic warfare for the needs of the Navy of China. Located in Beijing.

**5)** Navy 2nd TRB is the main training center for specialists in the field of creating secure telecommunication systems, experts in the field of computer security for the needs of the Chinese Navy. Located in Xiamen.

Second Artillery TRB is the main center for training specialists in the field of engineering intelligence and technical protection of information for the needs of artillery and missile forces. Located in Beijing. Chengdu MR First TRB - 57 research institute of the Ministry of Defense of the People’s Republic of China, also known as the Southwest Institute of Electronics and Telecommunications Technology (西南 电子 电信 技术 研究所). Here officers undergo training in the specialty of “Comprehensive protection of automated control systems (ACS) for the needs of the PRC Air Defense Forces.” Located in Chengdu. Chengdu MR Second TRB - here officers undergo training in the specialty “Cryptography and Cryptanalysis” for the needs of the Air Defense Forces of China. Located in Kunming. Lanzhou MR First TRB is the main training center for specialists in the field of creating secure telecommunication systems, experts in the field of computer security for the needs of the PRC. Located in Urumqi (Uyghur Autonomous Region of China).

Lanzhou MR Second TRB is the main center for training specialists in the field of specific (satellite) intelligence for the needs of the PRC. Located in I-Zhou (Uyghur Autonomous Region of China). Nanjing MR First TRB - here is the National Research Center for Information Security Technology (国家技术 安全 研究 中心), Nanjing. Nanjing MR Second TRB - located here are the Information Security Research Institute 3d Bureau (信息 安全 研究所), Nanjing. Jinan MR TRB - there is 56 research institute of the Ministry of Defense of China, also known as the Jinan Institute of Computer Technology - Jiangnan Computer Technology Research Institute (江南 电脑 科技 研究所), the National Crypto Center 11th Bereau, Jinan.Last year the Office of Information Technology of the Joint Defense Headquarters of the Armed Forces of the People’s Republic of China put into effect instructions on how to conduct an independent assessment of the vulnerability of computer networks used and implemented in the national Navy.

In accordance with this document, quarterly inspections will be carried out at headquarters, formations and units with the involvement of civilian specialists, during which, in particular, it is ordered to solve the following tasks: - remote (hidden and non-destructive) analysis of the presence of deficiencies in hardware, software and administrative support of computer networks of the Navy;

**a)** Hacking of password protection systems for restricting access to information and the implementation of cyber-attacks of the types DDoS (Distributed Denial of Service), DOS (Denial of Service) and others;

**b)** Search for other “windows of vulnerability” in browsers, mail agents, server and gateway software.

In order to increase the effectiveness of interaction with scientific organizations and industrial companies of the PRC of various structures that can solve the problems of preventing the disruption of the functioning of information and communication infrastructure facilities, of the authorized executive authorities from foreign countries, the National Cyber Cop Committee has been created in the PRC. It includes representatives of the government, industry, the Ministry of the Interior, as well as computer security experts. The priority tasks of this committee are: development of standards for the safe use of networks; informing users about possible cyber threats; preparation of recommendations for the development and production of specialized software for protecting information flows. In the Chinese Armed Forces, in order to coordinate the activities of the armed forces and interact with other security forces in the field of information warfare, the Defense Information Warfare Agency has been created as part of the joint defense headquarters.

The main functions of this structure are: the development of forms and methods of conducting information warfare; control over ensuring information security of troops; coordination of the activities of bodies of information warfare of the armed forces of the PRC, organization of their joint operations; conducting, together with the Ministry of Internal Affairs, psychological operations in the country. The directions of activity of the agency suggest the possibility of its participation in the future in solving problems associated with the disruption of the functioning of the information and communication infrastructure of foreign countries.

## Conclusion

Cyber-attacks allow you to penetrate into secure communication systems and exercise control over databases. Satellite communications, combat command and control of troops, banking operations, energy facilities, including nuclear power plants, are already under attack. Hacker attacks are especially dangerous for modern infrastructure, nuclear power plants and chemical plants. In this war it is extremely difficult to ensure cyber security. Since the "kick from around the corner" strategy is applied when you don't know the enemy "in the face" and the geographical coordinates of his location in order to retaliate. In contrast to the use of weapons of mass destruction in a nuclear war, megacities remain in place in a cyber war, but the state's multidimensional communication space is paralyzed. Cyber warfare is much cheaper and more effective than classical military conflicts, a real asymmetric weapon. So, cyberspace is becoming a global battlefield - the virtual space of the World Information Network, in which there are no customs, tax and other restrictions for the transportation of an intellectual product.

Cyberspace is becoming the same strategic battlefield as land, sea and airspace. But unlike them, in cyber war the factors of space and time lose their significance. The military command and cyber units for waging high-tech warfare are available in the armies of China, the USA, and Germany. In total, about 30 countries have online cyber armies, including Israel, France, Russia, India, Iran, Pakistan, South and North Korea. The creation of a network of collective cyber defense of the North Atlantic military bloc under the auspices of the United States. The main conclusions, taking into account the development of modern supercomputer technologies, are as follows:

**a)** A high-performance elemental base of supercomputers is used, there are a huge number of components, which increases the likelihood of bookmarks and makes it difficult to deal with them.

**b)** Supercomputers have the highest performance, a large number of simultaneously executed processes (hundreds of thousands - up to a million), and this determines the difficulty of tracking the events occurring in them in order to detect intrusions.

**c)** Information processed using supercomputers is usually associated with solving national security issues and solving critical scientific and technical problems, managing critical infrastructures, etc., this is a serious motivation for organizing attacks.

**d)** Users of supercomputers are highly qualified and there are usually a lot of them, which increases the risks of internal attacks.

**e)** Highly qualified are those who are interested in attacks on supercomputing resources of people who usually represent organized communities supported at the state level.

**f)** An attacking supercomputer can quickly assess the state of an attacked object, find vulnerabilities, plan and conduct a mass attack, quickly adapt according to the results of its conduct and conduct a series of subsequent attacks.

## References

1. Grinyaev SN (2006) The battlefield is cyberspace. Theory, techniques, means, methods and systems of information warfare. Based on materials from a foreign press. Moscow pp. 442

2. Molyakov AS, Eisymont LK (2017) Technological Methods Analysis in the Field of Exaflops Supercomputers Development Approaching. Global Journal of Computer Science and Technology: Information & Technology 17: 37-44.

3. Amarasinghe S (2009) ExaScale Software Study: Software Challenges in Extreme Scale Systems. DARPA IPTO, US Air Force Research Laboratory pp. 153.

4. James Dally, William BlackSchaffer, David Parikh, Vishal Park (2008) An Energy-Efficient Processor Architecture for Embedded Systems. Computer Architecture Letters 7: 29-32.

**ISSN: 2574-1241**

DOI: 10.26717/BJSTR.2021.33.005362

**Andrey Molyakov.** Biomed J Sci & Tech Res