Chinese Information and Cyber Warfare

https://www.e-ir.info/2010/04/13/chinese-information-and-cyber-warfare/

DANIEL VENTRE, APR 13 2010

More and more frequently, accusations emerge from industrialized and developing countries, pointing towards China (the PLA, “Beijing”, the “government”, or its hackers), accusing it of being the source of major cyber attacks. These have reached sensitive targets, such as critical information infrastructures, the servers of big international firms and government agencies. The methods which are used in such “attacks” (not a clearly defined concept) are usually those of cyber criminals: intrusion, data theft, interception of data and communications, the spreading malwares and viruses, use of Botnets and web defacement. If cybercriminals are motivated by financial gains however, several of these attacks are not money-oriented operations. Some of them probably try to serve other goals, such as intelligence or the dissemination of ideologies.

But since current network-analysis technologies do not enable us to attribute the cyber attacks to one or another actor, it is difficult (or even impossible) to assert that the Chinese government and/or Chinese army are involved in the incidents assigned to them.

Nonetheless, China has demonstrated its intention to become an internationally leading player in the fields of Information Warfare and Cyber Warfare: more than 20 years ago, the country began to publish its theories, doctrines, policies or strategies concerning both defensive and aggressive use of cyberspace. Recently, a student from the Institute of Systems Engineering of Dalian University of Technology (China) published a research paper titled “Cascade-Based Attack Vulnerability on the U.S. Power Grid”[1]. Several American experts and journalists analysed this publication as being a new demonstration of China’s offensive motivations against American infrastructures (and then against the security and sovereignty of the USA), and also as the proof of China’s involvement in a new arms’ race in cyberspace.

Let’s remind ourselves here of the main characteristics of this Chinese approach to Information Warfare[2] and Cyber Warfare, which has two main dimensions, military and civilian, both developed through theoretical and practical considerations.

The military dimension

The dazzling success of the USA in the first Gulf War was interpreted by several armies in the world as the victory of new technologies. According to this model, information and information technologies’ dominance were supposed to provide total control over the battlefield and was the key to military success, victory and power. This conclusion called for a radical transformation within the armed forces. The RMA (Revolution in Military Affairs) concept and the following Transformation, guided the new strategies of evolution in Chinese military affairs, as it did in several industrialized countries worldwide. In this context, the concept of Information Warfare acquired greater consideration among military experts in China. Since the mid 1990’s, the Chinese army has implemented its modernization, guided by the concept of “informationization” (that means the acquisition of dominance over information technologies and cyberspace). A great number of publications have defined the concept and strategies of Information Warfare in China.

In 1995 the General Wang Pufeng, considered as the “father” of Chinese doctrine of Information Warfare, said that:
– The goal of Information Warfare is no longer the conquest of territories or the destruction of enemy troops, but the destruction of the enemy’s will to resist.

– Information Warfare is a war in which the ability to see, to know and to strike more accurately and before the adversary, is as important as firepower.

In 1997, Colonel Baocun Wang added that:
– Information Warfare can be conducted in times of peace, crisis and war
– Information Warfare consists of offensive and defensive operations;
-The main components of Information Warfare are C2 (Command and Control), Intelligence, Electronic Warfare, Psychological Warfare, Hackers Warfare and Economic warfare.

In 1999, Colonels Qiao Liang and Wang Xiangsui in their famous "Unrestricted Warfare"[3] , a book concerning the art of asymmetric warfare between terrorism and globalization, emphasized that *"technological progress has given us the means to strike at the enemy's nerve centre directly without harming other things, giving us numerous new options for achieving victory, and all these make people believe that the best way to achieve victory is to control, not to kill*". That form of modern warfare, called "unrestricted", means that the weapons, techniques are now multiple, that the battlefield is everywhere, that there will be no longer borders between War time and Peace time. *"The battlefield is next to you and the enemy is on the network* ", and the information war is the war where the computer is used to obtain or destroy information.

Finally, let's mention the review "Liberation Army Daily, which in 2006 defined information warfare as:
– a process to take advantage over the enemy in a war under conditions of informationization
– a process which finds its strongest expression in our ability or inability to use several means to obtain and ensure an efficient flow of information; our ability or inability to make full use of the permeability of information space to share and connect information and information systems, to merge materials, energy, and information and create a combined fighting force; and in our ability or inability to weaken the information superiority of the enemy and operational effectiveness of the enemy's computer equipments.

With these theoretical approaches, the Chinese military modernization is guided by the concept of "informationization" which means developing a network architecture allowing the coordination of military operations in all dimensions. The strategy of information warfare is contained in the Chinese concept of iNEW (Integrated Network Electronic Warfare), defined by General Dai Qingmin in the early 2000's. iNews is the integration of electronic warfare (EW), computer network attacks (CNA) in the offensive side, and in the defensive role in protecting networks (CND – Computer Networks Defence), and intelligence operations (CNE – Computer Networks Exploitation). The joint action of CNA and EW against C4ISR and logistic systems networks of the adversary constitutes the basis of offensive Chinese Information Warfare.

In 2003, the Central Military Commission Committee of the Chinese Communist Party endorsed the concept of "3 Warfares"[4] within the concept of military Infomation warfare:psychological warfare, media warfare (influencing public opinion both nationally and internationally), and legal warfare (which is to use the tools of national and international law to gain the support of the international community

Several military training centres (in Zhengzhou, Wuhan, Changsha…) have delivered training programs to military staff since the mid 1990s. Since 1997 international media have reported a lot of Information Warfare exercises, conducted by military forces. The exercises are evidence of the transition from theory into practice.

The actual Information Warfare and Cyber Warfare capabilities of China remain unknown. But whatever these capabilities are, gaining power and superiority of cyber dimension has become a major issue in China: the global level of military development is measured through the level of Information Warfare capabilities. The objective is to be able to win wars conditioned by information (information warfare, cyber war) before 2050.

Without any ambiguity, China is committed in this way: Cyber war is no longer a matter of science fiction, declared Colonel Dai Qingmin in 2009, adding that "*the Internet will become the place of an inevitable arms race*".

The civilian dimension

In 1995 General Wang Pufeng evoked the revival of the "people's war" concept, made possible by the integration of civilian and military experts in the same struggle: the traditional battlefield no longer exists, the war may be everywhere and becomes everybody's matter.

Concretely, the involvement of the civil sector is reflected in many ways:
– China develops its military capabilities in close relationship with private industry and academia, putting into practice the policies promoting the connection between private and public sectors, civilian and military sectors. This phenomenon can be observed in a great number of industrialized nations.
– At the frontier of civil and military dimensions, militia units established by the Army in various military provinces, involve citizens from the industry or academia. Units have been set up that have expertise in Information Warfare, Electronic Warfare, Psychological Warfare, Information Operations, Network Warfare, etc.
– Some sources suggest the existence of links between some suppliers of the PLA and the hacker community, but one might question whether the Chinese army has any power over this community.
– The "Annual Report on the Military Power of the People's Republic of China", reminded us in 2003 of the dangers inherent in nationalist hacking (hacktivism) during times of crisis. Many actions are credited to Chinese hackers: waves of cyber-attacks following the bombing of the Chinese Embassy by NATO forces in Belgrade in 1999, attacks against the interests of Taiwan; attacks against the U.S. official websites in protest against the collision between a Chinese fighter jet and a U.S. spy plane in 2001, attacks against Tibetan websites and, in 2008, attacks against the website of the Embassy of France in China following a meeting between the Dalai Lama and the Head of the French President Nicolas Sarkozy. The list of hacktivists' attacks is a long one.

Chinese Information Warfare is mainly devoted to managing power relations with the outside (to ensure the position of China on the world stage), but this may also be applied within the framework of its borders: information and cyberspace superiority are a matter of power in China.

But in recent years, technological progress has played the spoilsport. Social networks (Twitter, Facebook…) have become new actors and tools on the national and international political scenes. In August 2009 an article published on Cenews Site (Central European News in Chinese) described Twitter and the social networks as a new weapon, a tool of subversion, of cultural and political infiltration of a country, a tool for spreading rumors, a powerful political and destabilization tool.

Cyberspace is a vulnerable weaponized system. China knows how to play with it. But it is the victim of this vulnerability too.

—

Daniel Ventre is a researcher, and expert on Information Warfare and Cyber Warfare, Conflict in Cyberspace theories and doctrines analysis with a geopolitical approach. He has published several articles about Information Warfare in China, Russia, India, Japan, Singapore, and is the author of *Information Warfare*. He blogs at http://infowar.romandie.com.

[1] www.thenewnewinternet.com/2010/03/22/chinese-publish-research-paper-envisioning-cyber-attack-on-u-s/

[2] According to U.S., *Military Intelligence* magazine, 1997, Jan-Mar issue, Douglas Dearth, *"Implications, Characteristics, and Impact of Information Warfare*", the term "Information Warfare" has been used for the first time by Tom Luona in 1976.

[3] http://cryptome.org/cuw.htm

[4] http://www.c4ads.org/files/Three%20Warfare%202010.pdf *Treble Spyglass, Treble Spear: China's "Three Warfares"*. By Timothy Walton.

Daniel Ventre is a researcher, expert on Information Warfare and Cyber Warfare, Conflict in Cyberspace theories and

doctrines analysis, with a geopolitical approach. He has published several articles about Information Warfare in China, Russia, India, Japan, Singapore, and books. http://infowar.romandie.com.