Cyber Security Ultimately Is Military Security

Reporter: ZUO Xiaoyu

You Ji

Professor of Macau University, School of Social Sciences.
Research Area: national security.

With deepening development of cyber technology, in the future the Cyber Army and Outer-space Force will not only become new combat forces, but also will become standardized combat forces, in parallel with traditional navy and air force. The expansion of cyberspace security has a very close link to military transformation.

Reporter: "Strengthening the Army by Cyber Force" is the slogan that is often mentioned in today's world. Can the Cyber technology solve most present security problems that military faces?

You Ji: As it is well known, the development of cyber technologies began with the military needs. In the last century, the United States gradually expanded its military cyber-networking technologies to the civilian and the business through the market, evolving and resulting in a revolutionary force we see today. It has changed

fundamentally to people's daily life, and even becomes the most basic pattern of interpersonal relations. In this case, it is a military origin that turned cyber to be massively used in economy, society and culture. But we need to make clear that, although compared to cyber defense capabilities, the commercial and civil use is more extensive and with higher profile today, still, the core of cyber is of military. In fact, the core of the cyber security is military security. If there is no reliable defense cyber network as the first line of defense, the civilian cyber network will be very fragile. So, it is a strong military cyber-security that provides the Great Wall that is indispensable to the security of civil network.

Reporter: From the national cyber security strategy point of view, to win the "war without smoke", how long should China go to fill the gap to a military cyber power?

You Ji: Compared to developed countries, our military cyber technology still exists with a gap. In the last decade, China's cyber technology has developed very rapidly and fast, and is gradually narrowing the gap. The basis of a military cyber is the civilian electronic and information technology. The reason that China military cyber technology lagged behind in a period of time is because of overall weakness in basic electronics industry and Internet technology in the country, and that in turn is due to the fact that the cyber technology originally was born in the West. Now through substantial money and manpower input, the electronic technology in China now has come up to a leading position in the international community. Although still there is a large gap to the United States, in some key areas, these disparities are generally eroded to less a "generation gap".

If we can make it to less than a generation gap, then the US overwhelming military cyber capabilities against its adversaries can be undermined gradually to a comparative advantage, and major clashes between the great powers may not occur because of the relative balance of technologic powers that ensures mutual destruction. Because if there is no overwhelming advantage by a major power, to take a military action a country would have to take into account the cost of the action. In most cases, the US would think twice before taking actions. So for China in terms of national security, the shortcut is to rapidly develop our asymmetrical capabilities to confront adversary forces, not just we should have a new generation of aircrafts and submarines that are tangible combat platforms, but more importantly is to have an effective and intangible means, including cyber offensive and defensive system that are both military and civilian compatible. For the last five years, what makes Americans feel nervous and anxious is China has made a significant leap forward in its capability of both tangible and intangible weapons.

> **Reporter:** On April 27, China's first cyberspace Blue Book "China Cyberspace Development Report (2015)" was published. In consideration of China's establishment of a national network team, organizing the World Internet Conference, and proposal of double- seven (7 bottom lines for abiding by laws and national interests of domestic cyber networks, and 7 consensuses for Cyberspace to benefit mankind) strategic initiatives, what are your opinions on top-level design of the cyberspace governance?

You Ji: National top-level design and cyber capability are conflicting concepts to some

degree. As we just said, the rapid rise of China's military cyber capability is based on the capability enhancement of its civil electronics industry. Here, there is a dependent relationship: without strong basis of civil electronics industry, it will be impossible for development of military cyber technologies. In Chinese this phenomenon or relation is called “water without a source, or a tree without roots”. The dialectical unity of top-level design and civil technology development is that, the basic civil electronic industry and the IT industry serves as the main industry, but as it is market-oriented, it is impossible to achieve a perfect national top-level design. The horizontal market competitive pattern will drive agents to make revolutionary breakthroughs in innovation capability, thus it renders out a driving force for leapfrog development of the military cyber as a whole. IT industrial development will provide selectivity, reality and possibility for planning top-level military capacity. Vice versa, the top-down design of military cyber also sets up high technical standards and requirements for the civil industry, pushing a hand to promote the main industry to develop. So this is an interdependent relationship. On the one hand, we emphasize government’s appropriate input and intervention into the innovation or private areas, so to the best degree to play out private capital and innovative capabilities. On the other hand, we can turn private innovations into the practical capabilities - whether be it used for military or civilian- that is, in other words, to turn the power of knowledge into the achievements of high information technologies. No technical capability, no basis for national top-level design. Vice versa, no top-level design, it is difficult to get the cyber products into military capabilities. This is a complementary, independent relationship. National top-level design is very important, but it could not bring us with innovative designs, by the opposite, it could devise out imperfect or even

fault designs. So, it is a complex interaction that requires careful studies.

Reporter: How can civil technology powers communicate with the top-level designers?

You Ji: Shanghai forum as a platform facilitates very good communications. As scholars, we generally can sketch out some long-term trends in our speeches at the forum, particularly the keynote speech on big data by Professor Hui Zhibin which provides policy-makers a new way of thinking and brainstorming, and a new inspiration for design. Based on the international prospective forecasts, policy makers can make targeted planning, and this is the essence and significance of Shanghai Forum. Unfortunately, as a representative of the industry, Huawei's cyber security office didn't send a person to the Forum. Combining civil and academic forces is very important. My speech is a forward-looking forecast, and is relatively theory-based; while the Big Data research by Professor Hui Zhibin is more practical and operation-oriented that provides a richer, more detailed stuff for overall direction of the top level design. Russian scholars and American scholars present at the Forum made framework depictions from the perspectives of international scale and concepts. It could be used or implemented for the government policy making and management of the cyber networks, including governance of the government network system and governance of civil Internet interaction. Such speeches can be very good references. We hope we can make greater use of the platform--Shanghai forum, to communicate and exchange with the industry elites.

Reporter: Global cyberspace order has developed from the beginning of spontaneous presence to present stage's conscious adjustment. At the "turning point" of cyberspace governance, can you talk about your predictions on the future of global cyberspace order?

You Ji: This is a complex issue. The US has dominant advantages in cyberspace power in today's world. If the US is willing to use the technological advantage to benefit the mankind, then mankind will get benefited. But if it uses it to attack, repress or retaliate against other countries, it could lead to a further militarization of the Internet technology, resulting in increase tensions in inter-state relations, and resulting in higher possibility of confrontations between countries because of the US cyber hegemony. The relatively eased environment currently could therefore fall into a more violent conflict. For example, should the US insists to prosecute the six PLA armymen discussed in the forum, it obviously would not be conducive to a healthy development of bilateral relations between it and China. We hope that peaceful use of cyber technology can become a principle that can be widely accepted worldwide, allowing it to better serve to the mankind.