NIDS 防衛研究所
The National Institute for Defense Studies

China's Basic Awareness of Cybersecurity

Masaaki Yatsuzuka (Research Fellow, Asia and Africa Division, Regional Studies Department)

NIDSコメンタリー

Introduction

At the 36th Collective Study Session of the Communist Party of China Politburo held in October 2016 on the theme of implementing the country's strategic plans to emerge as a cyber superpower, General Secretary Xi Jinping emphasized, "China must work toward its goal of becoming a cyber power by accelerating reinforcement of security and defense capabilities in cyberspace, accelerating the promotion of social governance using IT, and accelerating the advancement of China's right to speak internationally and right to set rules governing cyberspace."[i] Later, the Chinese government adopted the Cybersecurity Law in November 2016 (which took effect in June 2017), which was followed by the announcement of *the National Cybersecurity Strategy* at the end of December 2016 and *the International Strategy of Cooperation on Cyberspace* in March 2017. These documents show China's active involvement in cybersecurity.[ii]

Cybersecurity initiatives differ between major countries and the formation of international rules on cyberspace is still in the stage of development. Amidst this, it is worth noting that China is reinforcing its cybersecurity initiatives. This is because China's actions will have a major impact on Japan's cybersecurity as well. The key is developing an understanding of China's basic awareness of cybersecurity, which serves as an impetus behind its initiatives.

This paper examines the background behind China's efforts to strengthen its cybersecurity initiatives, and after analyzing the basic awareness gleaned from statements made by China's leadership and policy documents, examines potential issues facing Japan's security.

Cybersecurity itself can be categorized into governance in cyberspace and military use including cyber warfare. The scope of this paper includes analysis of China's awareness of cybersecurity in a broad sense including both. As will be discussed below, this is because China considers these aspects to be closely interrelated, and examining both will be beneficial in considering Japan's security as well.

China strengthening its cybersecurity initiatives

China's cybersecurity efforts began before the Xi Jinping administration. During the Hu Jintao administration, China released the *"Opinions of the Leading Group for Strengthening Information Security Assurance Work"* in 2003 and the *"Some Opinions concerning Forcefully Moving Informatization Development Forward and Realistically Guaranteeing Information Security"* in 2012. The efforts of the Xi Jinping administration are based upon this foundation. On the other hand, policy documents from the Hu Jintao administration focus on expectations of the information economy and the government's measures for increasing governance in cyberspace. In contrast, during the Xi Jinping administration, the viewpoint of "national security" has been incorporated more, leaving the impression that the administration is emphasizing active involvement in the formation of international rules.

There are three factors behind the stance of the Xi

Jinping administration. First, China's economy relies more and more on cyberspace, which is viewed as an engine of economic growth, and at the same time, the government wants to control cyberspace in a more secure manner. China's Internet users already exceed 700 million as of 2015, while the information economy accounts for 26% of the country's GDP. Without a doubt, this trend will continue in the future.[iii] On the other hand, economic crimes in cyberspace and cyber attacks from overseas have become rampant, which poses a threat to the sustained development of China's economy. For the Communist Party of China (CPC), economic growth justifies its governance, and so security in cyberspace is a problem directly related to social stability and the CPC maintaining its grip on power.

Second, international competition in cyberspace is becoming fierce. Thus, it can be pointed out that China's leadership recognizes that it must quickly gain the initiative in cyberspace. General Secretary Xi stated during a speech in April 2016, "Today, the competition for cybersecurity by major powers is found not only in technology, but also in idea and influence."[iv] China's *National Cybersecurity Strategy* states "International competition for control of cybersecurity resources, the right to set rules, occupation of strategic high positions, and the pursuit of strategic hegemony, will continue to intensify," indicating China's clear sense of impending danger. For China's leadership, now is an important time for tightening its grip on initiative in the formation of international rules on cybersecurity.

Third, the Xi Jinping administration is aware of the central importance that cyberspace plays in modern warfare. China's leadership has built up military power citing the goal of victory in "localized war under informatized conditions (信息化条件下局部战争)" from the early days of the Hu Jintao administration. This military doctrine aims to efficiently protect the interests of the nation without conflicting with the overarching goal of economic development, by keeping down the cost of conflict through limited political, military and economic goals. To end fighting in a short period of time and in a limited arena, it is important to have joint operation capabilities crossing over different military branches and military information systems connected through a network; and therefore, cybersecurity has been given an extremely important position within the context of China's modern warfare. The Xi Jinping administration is ushering in large-scale reforms of the People's Liberation Army (PLA) in order to create a military force that can implement this doctrine, while changing the tune to "winning informatized local war (信息化局部战争)."[v] The Strategic Support Force, established at the end of 2015 as part of these reforms, is an organization of critical importance to information warfare in charge of space, cyberspace and electronic warfare. This force is a direct embodiment of the Xi Jinping administration's point of emphasis.

Based on the above, the Xi Jinping administration has expanded its interest into the formation of international rules related to cybersecurity, from its original focus on economic activities and domestic governance in cyberspace. Every year since 2014, China has held the World Internet Conference, which plays host to political leaders, cyber experts and cyber companies from around the world. General Secretary Xi delivered a keynote speech at the second World Internet Conference held in December 2015 when he presented the "four principles and five propositions" (The four principles of 1. Respect cyber-sovereignty; 2. Protect peace and security; 3. Promote open cooperation; and 4. Establish sound cyberspace order, and the five propositions of 1. Accelerate construction of global cyber-infrastructure and promote Internet-based communications; 2. Create online cultural exchange and sharing platform to promote mutual exchange; 3. Promote new development in the cyber-economy and encourage co-prosperity; 4. Ensure cybersecurity and develop order in cyberspace; and 5. Build e-governance system and promote fairness and

justice.)[vi].

As seen with General Secretary Xi's recommendations, the international community should welcome China's aim for international order in cyberspace that is secure and fair. On the other hand, the direction of China's cybersecurity initiatives differ from other developed countries including Japan, which is a fact that cannot be ignored, as China could threaten the security of other countries. In such cases, understanding the characteristics of China's cybersecurity awareness will be essential.

China aims to establish "Information Dominance"

The sense of national sovereignty in cyberspace can be cited as a characteristic of China's cybersecurity. *The National Cybersecurity Strategy* states, "Cyberspace is already a new and important domain of human activities similar to land, sea, air and space. Cyberspace sovereignty is an important aspect of national sovereignty." Western countries, including Japan, acknowledge sovereignty in cyberspace, but they consider it to be an extension of territorial sovereignty and emphasize at the same time avoidance of government intervention from the standpoint of maintaining freedom of expression.[vii] In contrast, it is important to note that there is a major difference in government intervention with Western countries, as the national sovereignty advocated by the Chinese government includes the right to regulate contents in domestic cyberspace. Even *the International Strategy of Cooperation on Cyberspace* emphasizes the need for control, "While there is a need to advocate for freedoms similar to real world society, cyberspace must maintain order and not become a 'lawless area'." Also, China's Cybersecurity Law, prohibits infringement of national security, honor and interests through cyberspace, incitement of the overthrow of the government or socialist system, and the spread of misinformation that could disturb the economic and social order (Article 12). It also contains provisions for the Chinese authorities to pursue the legal liability of overseas institutions, organizations and people, including freezing their assets or imposing other sanctions (Article 75).[viii] In other words, the Chinese government aims to build a cyberspace where it rigorously censors and interrupts information, regulates freedom of speech, and cracks down on the activities of companies, NGOs, and individuals in domestic cyberspace, as well as it can refute and ignore international criticism about these actions.

China's emphasis of the sovereignty of cyberspace can be traced to its sense of caution that international cyberspace can threaten domestic politics and in particular the legitimacy of the CPC. *The International Strategy of Cooperation on Cyberspace* states, "China will firmly maintain its stance of protector of cyberspace. China is a victim of hacker attacks." The same can be heard from China's national defense officials.[ix] The supreme mission of security for the CPC is its own stable governance. Consequently, the CPC considers the spread of government criticism on social networking services (SNS), such as that seen during the Arab Spring, as correlating to social instability and a security issue that could shake its rule. *The 2015 Science of Military Strategy* published by the National Defense University Press states, "Since the start of the 21st century, cyberspace has already been used by several countries to incite a color revolution in other countries," indicating China's sense of caution.[x] The Chinese government possibly equates cyber attacks from overseas seeking to overthrow the CPC as the same as the spread of misinformation criticizing the government or the CPC through SNS.

Based on this awareness, the Chinese government believes it must lead the formation of new international rules on cybersecurity. Furthermore, it believes that new conventions, rather than existing international laws, should be applied because cyberspace is a new and unique domain. *The International Strategy of Cooperation on Cyberspace* asserts, "Cyberspace is a new domain that requires the prompt establishment of relevant regulations

and principles of conduct." This is believed to be based on the awareness that applying conventional international laws to cyberspace will require human rights, such as freedom of speech and secrecy of communications, to be obeyed in cyberspace, too, making China's censorship and eavesdropping difficult[xi]. Therefore, China aims to form rules through its own leadership while essentially toeing the line with other Shanghai Cooperation Organization (SCO) countries including Russia, instead of Western powers that call for freedom of speech. *The International Strategy of Cooperation on Cyberspace* states, "China will secure tolerance and openness in related international processes to strengthen developing countries' representation and the right to speak."

That is, the above suggests that China's leadership is aiming to create a situation where the Chinese government can control the flow of information inside and outside the country wherever possible, by taking the lead in forming international rules on cyberspace; rather than simply stepping up its own control, from the standpoint of sustained economic growth and the stable governance of the CPC. Dean Cheng of the Heritage Foundation refers to China's information activities as establishing "Information Dominance."[xii] This involves being able to gather, transmit, analyze, assess, and exploit information more quickly and more accurately than one's adversary. It includes the conduct of political warfare, which shapes and influences friendly, adversary, and third-party views and assessments. The establishment of Information Dominance by China has implications not only on cyberspace governance but also information warfare, and it will have a serious effect on Japan's security as well.

Points at issue about China's cybersecurity

The following three points should be considered in terms of future trends in China's cybersecurity. First, cybersecurity in terms of China's military includes not only intelligence activities during an emergency, but also political warfare during peacetime. The Chinese government considers political warfare during peacetime to comprise the 'three warfare (三战)' of public opinion, psychology, and law. The problem is that China's approach to traditional political warfare and this manoeuvring has developed on the back of the country's vast economic might and new technologies. For example, the perpetrators of theft of confidential information and alteration of information in cyberspace and cyber attacks inciting public opinion through false rumors are difficult to identify, and in the case of smaller scale cyber attacks, it is difficult to even notice them. On a more strategic level, through cyber attacks, China attempts to incite public opinion and cause wavering of decision making by leaders of countries that are locked in disputes with China. At the same time, it is believed that China isolates opposition internationally, legitimizes its own responses, and deals with the conflict in an advantageous matter without resorting to armed conflict. This type of political warfare in cyberspace could cause various grey zone situations that blur the lines between peacetime and wartime. Further examination is needed concerning this point going forward.

Second, also relating to the above is the standards and thresholds for military attacks in cyberspace. *The 2013 Science of Military Strategy*, published by the PLA Academy of Military Science states, "Cyber warfare is low cost and highly effective, so cyber warfare is easier to occur than other types of war." Conversely speaking, the psychological hurdle to cyber warfare even in China may be lower than conventional war.[xiii] For example, with regard to soft skills, such as cyber attacks (on information) that do not cause physical damage to command systems of enemies, known as C4ISR, there are some point out the possibility that China considers these as defensive measures to avoid escalation to war.[xiv] However, assuming a target country deemed this as a military attack, there is a risk that the situation could escalate to warfare, including the use of

conventional weapons.

Third is the difference between awareness of deterrent in cyberspace. During a speech in April 2016, General Secretary Xi stated "China will reinforce its cybersecurity defense capabilities and coercive (威慑) capabilities. The fundamental essence of cybersecurity is antagonism and the essence of antagonism is the competition between offensive and defensive capabilities." China's coercive (威慑) capability is a concept close in meaning to deterrence. According to *the 2015 Science of Military Strategy*, Cyber deterrence can be categorized into (1) strategic level deterrence where cyber attack capabilities against another military's C41SR system or core transportation and communications infrastructure deters the other party's cyber attacks, and (2) tactical level deterrence that can hold in check dispersed, small scale cyber attacks and cyber penetrations.[xv] With regards to cyber deterrence, the basic conditions for forming a deterrent relationship of (1) intention, (2) capability and (3) mutual understanding represent a fundamental problem because they are extremely vague in cyberspace. In other words, costs are required to identify cyber attackers, and in addition to the difficulty of assessing China's attack and response capabilities, there is the problem of what exactly China considers to be a military attack in cyberspace. For example, in terms of government criticism and the spread of misinformation using SNS as discussed above, the Chinese government may determine this to be a cyber attack depending on the scale and situation. In such an instance, it is not clear how China would retaliate and against who. While keeping such difficulties in mind, if China seeks to reinforce its deterrence capabilities in cyberspace in the future, the international community must deepen its understanding of China's intentions and capabilities as well as promote mutual understanding through communication.

Conclusion

Taking into account the above, when considering Japan's cybersecurity, one must pay attention to both competing and cooperative aspects. As for the former, Japan's own initiatives and establishment of deterrence capabilities under the Japan-US Alliance can be cited. For example, technological R&D related to cyber-defense, reinforcement of survivability of important cyber infrastructure, and development of highly advanced cyber-personnel such as that currently being examined mainly by the National center of Incident readiness and Strategy for Cybersecurity (NISC) will contribute to Japan's deterrence by denial. With an eye on expanding deterrent through the Japan-US Alliance, deterrence capabilities through punitive measures in cyberspace will also need to be examined. Therefore, Japan will need to closely discuss with the US side about approaches to cybersecurity cooperation including sharing of China's cyber attack risk and capability assessment information, and retaliatory measures for various situations from peacetime to emergencies.

In terms of collaborative responses, establishing a mechanism for bilateral dialogue with China concerning cybersecurity can be cited. Already, the US and China agreed to establish a dialogue mechanism on cyberspace at the summit meeting held in September 2015, and already several ministerial level talks and working group discussions have taken place. These dialogues appear to be limited to cyber crimes and preventing theft of intellectual properties, but it also appears they have had a certain effect.[xvi] The Chinese government considers itself a victim of cyber attacks and at the same time it is actively cracking down on cyber crimes that could inhibit the country's economic growth. Consequently, from this point at issue, through establishing information exchanges and dialogue mechanism, it is possible to reduce the number of unnecessary cyber attacks and business espionage, and

foster trust in the process. Already, cyber discussions have taken place between the diplomatic authorities of Japan, China and the Republic of Korea on three occasions. While utilizing such mechanisms, higher level bilateral frameworks and cyber discussions between defense authorities can be examined.

Also, from the standpoint of cooperation with the international community, it will be important to actively involve China in the formation of international rules on cybersecurity. Joseph S. Nye of Harvard University points out as one element for deterring cyber attacks the formation of international rules for sharing taboos on the scope of cyber attacks, and toward this end the fostering of trust between countries.[xvii] While it may take a long period of time to conclude a new international treaty related to cybersecurity that China seeks, for example, the results of strongly policy-inclined discussions, such as the Tallinn Manual led by the *NATO* Cooperative *Cyber Defence Centre* of Excellence (CCDCOE), represent a relatively low political cost, while not legally binding, and contribute to fostering international rules for deterring cyber attacks.

(Completed on May 12, 2017)

---

[i] "Xi Jinping: Accelerate the indigenous innovation using IT; making continuous efforts toward the goal of a cyber superpower," *CPC News* (October 10, 2016) (http://cpc.people.com.cn/n1/2016/1010/c64094-28763907.html) Hereafter, final access for all sites occurred on May 11, 2017 for all sites.

[ii] National Cybersecurity Strategy, *Xinhuanet* (http://news.xinhuanet.com/politics/2016-12/27/c_1120196479.htm); International Strategy of Cooperation on Cyberspace, *Xinhuanet* (http://news.xinhuanet.com/politics/2017-03/01/c_1120552767.htm).

[iii] Zheng Bijian, "The Networking Trend Contribute to China's Peaceful Rise," *China Information Security* (February 2017).

[iv] Xi Jingping, "Remarks at the Cybersecurity and Informatization Conference," *Xinhuanet*, April 25, 2016 (http://news.xinhuanet.com/politics/2016-04/25/c_1118731175.htm).

[v] China's Military Strategy White Paper (May 2015) (http://www.scio.gov.cn/zfbps/gfbps/Document/1435341/1435341.htm)

[vi] Xi Jinping, "Xi Jinping's remarks at the 2nd World Internet Conference," *Xinhuanet*, December 16, 2015 (http://news.xinhuanet.com/politics/2015-12/16/c_1117481089.htm).

[vii] Keiko Kono, *Observations on International Law concerning Cybersecurity – Focus on the Tallinn Manual*, The Japan Society of Strategic Studies (January 2015), pp25-45, and Yu Harada, *Disputes concerning Cyberspace Governance* (NIDS Commentary No. 43, March 2015) (http://www.nids.mod.go.jp/publication/commentary/pdf/commentary043.pdf)

[viii] "Cybersecurity Law of the People's Republic of China"

[ix] A *Chinese defense ministry spokesman provided a detailed number of attacks in March 2012. People's Daily Online* (http://military.people.com.cn/GB/17534712.html)

[x] Xiao Tianliang ed. "The Science of Military Strategy" (National Defense University Press, 2015), p.143.

[xi] Motohiro Tsuchiya, *Cyber Security and International Politics*, (Chikura Publishing, 2015), pp. 157-158

[xii] Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger: California, 2017, pp. 15-16.

[xiii] The Strategic Research Department of the Chinese Academy of Military Sciences, "The Science of Military Strategy" (Military Science Publishing House, 2013), p. 191.

[xiv] Joe Mcreynolds, *China's Evolving Military Strategy*, The Jamestown Foundation: Washington DC, 2017, pp183-184.

[xv] Xiao Tianliang, "The Science of Military Strategy," p. 147.

[xvi] Gary Brown and Christopher D. Yung, "Evaluating the US-China Cybersecurity Agreement Part3," *Diplomat*, January, 2017, (http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/).

[xvii] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (Winter 2016/17), pp. 60-62.

プロフィール profile

Masaaki Yatsuzuka

Research Fellow, Asia and Africa Division, Regional Studies Department

Areas of Expertise: Political/Foreign Affairs in China, International Security Studies in East Asia

Planning and Coordination Office,
The National Institute for Defense Studies
Telephone (direct): 03-3260-3011
Telephone (general): 03-3268-3111 (ext. 29171)
FAX: 03-3260-3034
* Website: http://www.nids.mod.go.jp/