QUAD-PLUS Dialogue

The Heritage Foundation
ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
Vivekananda International Foundation India
The Tokyo Foundation

Tokyo Olympics and Cooperation for Cyber Terrorism

Lt. Gen. (Ret.) Noboru Yamaguchi
The Tokyo Foundation

Quad-Plus Dialogue
Washington, D.C.
February 28–March 2, 2017

CYBER THREATS

Japan in general has been safe in terms of global terrorism due to its geographic remoteness from the major sources of disturbance, the Middle East, and its relative neutrality in terms of religious confrontation between Abrahamic religions. The killing of 22 people including seven Japanese in Dhaka, Bangladesh, in July 2016 could be an evil omen for Japan. In fact, one of the seven identified terrorists used to be in Japan and left several months before the incident. In 2020, the Tokyo Olympic Games are scheduled that may provide terrorist groups with a golden opportunity to show up. Japan is no longer immune from global terrorism.

A serious challenge is confronting the ever-growing threat of mass destruction and murder by a range of methods. Public infrastructure such as transportation and electricity can be converted easily into highly destructive weapons. The accident at the Fukushima Daiichi Nuclear Power Station on March 11, 2011, underscored the dangers posed by our own infrastructure. The earthquake that hit the Tohoku region also triggered a secondary disaster of huge proportions when the resulting tsunami disabled the reactors' cooling system, leading to multiple meltdowns and the release of radioactive material over a large area. We cannot discount the possibility of an act of sabotage with similar consequences. Given the importance of computer control systems in today's nuclear power plants, it is conceivable that a cyberattack by a hostile group could disable a plant in much the same way that the tsunami did.

Computer networks play a critical role in virtually every aspect of our public infrastructure, and their role is expanding daily. Rapid advances in information and communications technology have brought artificial intelligence and the internet of things within reach. The diffusion of such technologies could leave us all the more vulnerable to cyberattacks that could cause widespread chaos and destruction by crippling public transportation or telecommunications networks, the water or power supply, or healthcare systems and facilities, not to mention industrial infrastructure like chemical plants and oil refineries. We must prepare and defend ourselves against this threat.

JAPAN’S PREPAREDNESS

On one hand, in terms of kinetic incidents that terrorists may bring, Japan’s law enforcement capability to deal with criminal acts including terrorist activities in particular is fairly robust due to its experience in fighting against ultra-left radicals such as the Red Army of Japan in the 1970s. On the other hand, Japan is seriously lagging behind in measures to deal with cyber threats in several areas such as legal bases that has caused weakness in implementing cybersecurity policies, developing cybersecurity technologies, and matching the necessity of human resources.

DEVELOPMENTS IN LEGAL ASPECTS

In the last fifteen years the government of Japan (GOJ) has been working hard to establish a sound domestic legal basis for national cybersecurity in order to catch up with the necessity to improve resiliency in cyberspace. In 2011, laws for implementation of the Budapest Convention on Cyber Crime were enacted and Japan became able to cooperate with the international community for preventing and dealing with criminal acts in cyberspace. As one of the rule makers on cybersecurity, Japan has continued its participation in discussions at the United Nations group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN/GGE). The UN/GGE report released in 2013 concluded that international law, the United Nations Charter in particular, “is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.” The group also concluded that the concept of state sovereignty and related norms and principles apply to the cyber domain.

There seems to be a general consensus among Western states that the existing law of armed conflict (LOAC) applies to cyberspace. In the meantime the International Institute for Strategic Studies Military Balance 2016 points out that there are open questions to answer raised by major non-Western countries such as Russia and China that include: “1) What constitutes an armed attack or the use of force in the cyber domain and what represents a legitimate response; 2) What constitutes a cyber weapon in a domain where most systems and capabilities are dual- or multi-use; 3) How proportionality and distinction—the requirement to minimize the impact of any military act on non-combatants—can be applied in an inherently dual-use domain; 4) How to deal with issues of state neutrality in the case of a cyberattack routed via third country."

While the international community has been working on legal aspects of issues related to cyberspace and made certain progress, the GOJ has been trying to catch up with such trends by establishing a domestic legal basis starting with the enactment of laws to implement the Budapest Convention as stated earlier. In 2014 the Cybersecurity Basic Act was enacted based on which the National Cybersecurity Strategy Headquarters along with its secretariat National Information Security Center (NISC) was established. Japan's first National Cybersecurity Strategy was developed based on the act as well.

There has been certain progress in policies related to cybersecurity including bilateral agreement with the U.S. on the issue. The Guidelines for Japan-U.S. Defense Cooperation agreed to in 2015 puts particular emphasis on bilateral cooperation in cyberspace by noting that the two governments will "share information on threats and vulnerabilities in cyberspace" and will "share information on the development of various capabilities in cyberspace, including the exchange of best practices on training and education," while the Self-Defense Forces (SDF) and United States Armed Forces "will contribute to whole government efforts to improve cybersecurity." This bilateral approach should be expanded to include cooperation with India and Australia as well as other like-minded friends and partners.

RESTRICTIONS FOR JAPAN TO DEAL WITH CYBER THREATS

While the GOJ has made progress in establishing a legal basis for cybersecurity, such efforts never satisfy the increasingly serious demands for better cybersecurity. There are a number of reasons why Japan's cybersecurity does not match the necessity resulting in serious restrictions. Firstly, because Japan is still at an early stage in cybersecurity as the basic act was recently enacted, it has a long way to go.

The second reason why there are shortcomings of effective policies to deal with the whole spectrum of cyber protection is lack of awareness on the extremely high level of cyber threats that are equivalent to an armed attack. For example, the National Cybersecurity Strategy does not seem to pay enough attention to such extremely serious cyber incidents. Accordingly, the strategy limits the mission of the SDF in cyberspace only to the protection of the SDF's own systems and private information and communications technology (ICT) infrastructure on which the SDF depend to accomplish their missions. In other words, while the U.S. and other militaries are tasked to defend the country including in cyberspace, the SDF are expected to defend themselves in terms of cybersecurity.

The third reason for shortcomings in cybersecurity is that Japan has not properly caught up with international discussions on legal aspects of cybersecurity. While Japan signed the Budapest Convention on Cyber Crime in 2001 and got approval of the Diet to ratify, it took ten years to establish a domestic legal basis to implement the agreement in 2004 and it was not until 2011 when the agreement became effective for Japan with a newly established legal basis. In terms of law on armed conflict, Japan’s comprehension of the issues is lagging behind as well. The international community has continued discussing applicability of existing international law to cyberspace and made a general consensus that international law applies to cyberspace to a certain extent, including the right of self-defense based on the UN Charter. There seems to be little sign that political discussions and decisions are being made within the government over the conditions and the procedures to take counter measures including use of force against a cyberattack that is regarded as serious as an armed attack. The question on cyber incidents during an armed conflict is another point to seriously discuss since we have witnessed various cases where cyber incidents occurred in support of use of conventional force such as massive cyberattacks during the armed conflict in Georgia in 2008.

The fourth reason for restrictions on Japan’s countermeasures against cyber threats is the highly rigid interpretation of the Constitution and other laws related to defense and security issues. Privacy of communications assured by the Constitution is rigidly interpreted and causing restrictions preventing Japan’s law enforcement authorities from widely monitoring communications in cyberspace. The fundamental idea of Japan’s so-called Peace Constitution often deters the government from taking offensive measures including those for collecting information necessary for national security.

CONCLUSION

The 2020 Tokyo Olympic Games will bring both bad and good news. For terrorist organizations like ISIL the Olympics may provide a golden opportunity to show up. Japan has to take immediate and decisive actions to drastically improve its cyber resiliency. In the meantime, serious threat perception related to such terrorism may improve awareness of public and policymakers on cyber threats posed by terrorists. Such threat perception shared within the private and public sectors will provide the government with stronger support for policies on cybersecurity while the private sector may have higher incentive to invest in cyber resiliency.

Japan, aiming at the 2020 Tokyo Olympics, should significantly improve its readiness to deal with cyber threats potentially caused by terrorist organizations through cooperation with the U.S., Australia, and India, as well as other ICT advanced countries. The U.S. is a superpower in terms of cybersecurity. Australia and India are among the most advanced countries in terms of ICT from which the international community increasingly enjoys the utility of cyberspace while facing new vulnerabilities. Areas of cooperation should include (1) sharing of threat information; (2) development and sharing of better practice in cyberspace; and (3) promotion of international and domestic public awareness on cyber threats by reaching out based on quadrilateral discussions like this.