Japan Faces New Cyberwar Era

By Jun Osawa
Senior Research Fellow

In 2011, it became clear that successive, targeted cyberattacks had been launched against Japanese government ministries and agencies. In addition to the revelation in January that the Ministry of Economy, Trade and Industry had been targeted by a cyberattack, it was reported in September that there had been cyberattacks on defense-related companies such as Mitsubishi Heavy Industries. Then, in October, there had been an attack on the computer network of the House of Representatives, and it was confirmed that several dozen servers had been infected. In consequence, some representatives' IDs and passwords may have stolen. It appears that government institutions have been the object of these kinds of targeted cyberattacks since around 2007. However, it was not until 2011 that the nature of the damage was reported and became public knowledge. The year 2011 could even be termed the "first year of cyberwar" for Japan in that it was the year in which the current reality of cyberattacks became widely known.

It is apparent that there have recently been two changes in the nature of cyberattacks: a transition from nontargeted to targeted attacks designed to steal classified information, and the commencement of concerted cyberattacks targeting control systems of infrastructure providers.

Targeted attacks designed to steal classified information

Since around 2007, cyberattacks have switched from prank attacks aimed at infecting an unspecified, large number of hosts to targeted attacks with the objective of stealing top-secret information from specific organizations and individuals.

A succession of attacks directed at Japan's parliament, government ministries and agencies, governmental organizations, and defense industry have been detected, and there is now an urgent need for an all-out national effort to devise countermeasures.

Cyberattacks targeting control systems of infrastructure providers

In addition to targeted attacks, the telltale signs of attacks designed to paralyze the control systems of vital social infrastructure have begun to appear in recent years. Since attacks on control systems would have an adverse impact on people's actual lives, this has become the top-priority cyberspace defense issue in the USA and other countries.

As a matter of urgency, Japan must make an all-out national effort in every industry—including the nation's vital core infrastructure, such as electric power and gas—to protect control systems from cyberattack.

In this regard, the attention of information security experts was drawn in particular in 2010 to the Stuxnet worm, which targeted control machinery in Iranian nuclear facilities. Officials at the major security company Symantec, which conducted detailed analysis of Stuxnet, characterized Stuxnet as the most significant phenomenon in computer security of the past 20 years and as the first instance of malware that actually attacks physical facilities. Analysis revealed that, in operation, Stuxnet consists of 15 different modules and that it must have taken not a few engineers a period of time ranging from a few months to a few years to develop. That it was sophisticated enough to hijack control of high-frequency converters which regulate centrifugal separators

used for uranium enrichment over a period of at least two years indicates that these cyberattack modules must have been developed with nation-state support.

Since the year 2000, the telltale signs of attacks designed to paralyze control of vital social infrastructure such as electric power, gas, and water supplies have been evident in the USA and other countries. The industrial control systems for vital infrastructure providers consist of field control equipment, such as PLCs (programmable logic controllers), actuators, and valve control devices, and a whole plethora of information technology devices, such as server and client PCs, which are used in the observation and measurement of conditions. It is claimed that, normally, control systems are not too susceptible to cyberattack, since as a security measure they are either not ordinarily connected to networks or are connected to them through a firewall. It has also been thought that since each system is customized for the particular enterprise using it and is thus unique to that enterprise, it would be difficult to attack without thorough knowledge of the inner workings of the system, and that such systems are also immune to ordinary computer viruses. In fact, however, it has recently become clear that these control systems are highly susceptible to cyberattack since, in most cases, they are running the same operating system as a PC and are periodically receiving data input or update modules.

Richard Clarke, the former US Special Advisor to the US President on Cyber Security and Cyber Terrorism, has written that "cyber war is real"[1] and that "cyber war has begun,"[2] stating that there is "the potential to change the world military balance and thereby fundamentally alter political and economic relations."[3] In fact, preparations for cyberwar are already underway in several nations. As early as 1999, China advanced the doctrine of "unrestricted warfare" in reference to cyberwar, and, since around 2002, it has been establishing information-war militia and forming combined teams comprised of private-sector IT companies, universities, and People's Liberation Army computer network task forces within the military forces under the control of each military district. Even North Korea is believed to have a several-thousand-strong cyberunit consisting of cybercombat personnel who have been selected as early as elementary school and trained from then onwards. In the USA, an increasing sense of the danger of cyberwar has seen the establishment of the United States Cyber Command and the formation within four armed-services branches (the US Army, Navy, Air Force, and Marine Corps) of the Army Cyber Command, the Twenty-Fourth Air Force, the Tenth Fleet, and the Marine Corps Forces Cyberspace Command. It cannot be denied that Japan's efforts to protect its cyberspace are lagging behind.

If Japan is to protect its cyberspace, it is essential that it first detect attacks without delay and widely publicize early warnings, which will require Japan to establish an organization to collect and analyze information about cyberattacks. This organization must encompass the public and private sectors and all branches of government. Second, Japan must form a task force to record and analyze attack patterns, deal with attacks, and protect vital infrastructure. Third, it will be essential for Japan to foster talented personnel who can win a cyberwar.

[1] Richard Clarke, *Cyber War: The Next Threat to National Security and What to Do About IT* (New York: Harper Collins Publishers, 2010), P.30.
[2] Ibid., p. 31.
[3] Ibid., p. 32.

It will be impossible to defend against cyberattack through defensive measures alone. It will also be necessary to invade attackers' networks in return and to accept the idea of "cybercounterattacks in self-defense" for purposes of identifying adversaries and striking back at them.