Speaking Out #164 October 30, 2012

Remote PC Control Case Exposes Cyber Security Flaws

Hiroshi Ito

Wrongful arrests involving viruses for remote control of computers have attracted attention in Japan. Someone took remote control of others' personal computers to commit the crime of sending threat messages. Police arrested innocent persons including those who reportedly confessed to their crime that they never committed.

E-mail statements from a person who claimed to be the culprit in the threat message cases indicate that the claimer took advantage of cyber technology to put police to shame. The reason the claimer could commit the crime while remaining anonymous is that any such culprit cannot be traced in the present cyberspace.

These cases, where police had failed to suspect anyone's remote control of others' personal computers, apparently indicate that Japan's cyber security arrangements are insufficient.

Cyber technology could be used to trigger war

What would happen when cyber technology is available for a wide range of people? For example, the Chinese Navy and the Japanese Maritime Self-Defense Force may face off against each other near the Senkaku Islands that are controlled by Japan and claimed by China and Taiwan. They may be unwilling to enter war. The Chinese Navy may be aware that it cannot defeat the MSDF, while the MSDF may remain bound by Japan's pacifism.

How will citizens act then? Japanese and Chinese citizens may offer their respective opinions and defame each other over the Internet. They may launch cyber attacks. (The Chinese government could be behind citizens' cyber attacks on Japan.) If such attacks lead to physical losses or human injuries, the military may lose self-restraint and open fire.

Given that cyber attackers are difficult to identify, we can suspect more complicated problems. Japan and China cannot benefit from their war.

But there could be a third country or a nongovernment party that would launch cyber attacks on Japan or China while spoofing itself as Japan or China in a bid to benefit from massive Japanese and Chinese spending and losses through their war. If China has an evil intention, it may launch cyber attacks on Japan while spoofing itself as a third country. Cyber attacks of this kind are very difficult to address.

What Japan should do

In order to prevent such developments, Japan should set up a technological mechanism against spoofing in the Internet, spearhead an international treaty banning cyber attacks on private sector infrastructure and have reliable allies or friendly countries. More importantly, Japan should have institutions and power to do so. To this end, Japan may have to transform itself. I believe that the time has come for us to seriously consider Japan's transformation.

(This report provides my personal views based on available media reports and does not represent any view of the company to which I belong.)

Hiroshi Ito is Corporate Officer, Cyber Security Laboratory, LAC Holdings, Inc.