

AJISS-Commentary

The Association of Japanese Institutes of Strategic Studies

IIPS

Institute for International
Policy Studies

JIIA

The Japan Institute of
International Affairs

RIPS

Research Institute for
Peace and Security

Editor:

Akio Watanabe

Editorial Board:

Hideki Asari
Masashi Nishihara
Taizo Yakushiji

Online Publisher:

Yoshiji Nogami
President, JIIA

No.143. 17 February 2012

PATRIOTIC GEEKS WANTED TO COUNTER A CYBER MILITIA

Motohiro Tsuchiya

Cyber-attacks are hitting the headlines almost every day. Crackers, or black hat hackers, are trying to access sensitive defense industry information and stealing e-mail passwords from Diet members, threatening to disrupt key communications infrastructure. The “attacks,” however, have killed no one, at least here in Japan. Probably few have died directly from them around the globe either. Very few who have planned and executed the attacks have been arrested so far.

The views expressed in this piece are the author's own and should not be attributed to The Association of Japanese Institutes of Strategic Studies.

China and Russia often appear on the usual suspect list. However, there is no evidence showing that the attacks are state-sponsored. The two countries claim that they are also victims. Given the current state of technology, it is extremely difficult to pin down the attackers.

Of course, this does not mean that there are no state-run or state-sponsored cyber-attacks, let alone that such attacks can be ruled out in future. However, the truth is that the overwhelming majority of cyber-attacks are currently planned and executed by private militias and mercenaries. Although the United States and other countries have started to create special cyber-units within their military forces, militaries and governments on the whole have only a limited number of experts who are familiar with the technologies used in cyber-attacks and security holes. Because such advanced technology and skills bring good prices in the private sector, no one but ardent patriots would choose to work for the government.

The actors executing cyber-attacks can be divided into three categories. The first is young people with plenty of idle time on their hands. They join in attacks for fun by utilizing tools at such places like Internet cafes. The second is those who engage in espionage seeking intelligence for profit. The third is experts in the military sector who conduct test attacks in preparation for future cyber war and try to find security holes. They may carry out attacks themselves but may additionally hire attackers from outside.

Japan was one of the first countries to introduce cyber security measures, having set up the National Information Security Center (NISC) under the Cabinet Secretariat in 2005. The initial concerns were primarily technical issues, exhibiting little awareness that cyber security has to do with national security and crisis management. However, since major cyber-attacks were carried out against the US and South Korea in July 2009, Japan has been making preparations on the assumption that it could be the next target. The government drew up a special national plan titled "Information Security Strategy to Protect Japanese Nationals" in May 2010.

The real challenge of such a strategy is whether the government can secure good experts to counter militias and mercenaries. The rewards that the

government can offer would be too small for competent geeks. Even if the government succeeds in employing them, it would be vulnerable unless it keeps them committed long enough – think about the risk of them being hired by adversary forces after their stint in the government! Success hinges on whether the government can secure patriotic geeks.

The attacker has the upper hand in cyber war. The defender must be prepared for an attack that could come from anywhere, at any moment. There are even cases in which defenders are not aware that they are under attack. Unless the government secures experts who can detect a cyber-attack at an early stage and take effective measures, national defense will be rendered fragile. In an era of increasingly high-tech weapons, damage to communication facilities can be fatal to defense operations. Fostering and securing cyber-experts to defend the national nerve system is urgently needed. 

Motohiro Tsuchiya is a professor at the Graduate School of Media and Governance and Deputy Director of the Global Security Research Institute (G-SEC) at Keio University.