



IIPS

Institute for
International Policy Studies

▪ Tokyo ▪

IIPS International Conference

“The IT Revolution and Security Challenges”

Tokyo

December 10-11, 2002

**“Changes and Challenges
in the Cyber-Terrorism Environment”**

by

Raisuke Miyawaki

Former Adviser

to the Prime Minister for Public Affairs

Changes and Challenges in the Cyber-Terrorism Environment

Raisuke Miyawaki

10 December 2002

There is presently great upheaval surrounding cyber-terrorism, which is seemingly on the verge of entering a new stage of development.

During the year 2001, three highly symbolic events took place that involved hackers and virus writers. In addition, there is a noticeable trend towards collaboration between terrorist groups, nations that realize the military value of cyber-attacks, and politically motivated hacker groups.

The first of these three events took place on 21 May 2001, when the Attrition website, which mirrors website defacement activities, was closed. This site was a forum where hackers could boast about the websites that they had defaced. Attrition's owner Brian Martin noted that: "we were receiving more traffic in one day than we had in the first two years of operation. We couldn't process it all." In fact, defacing websites has now become so commonplace that it is hardly worth bragging about anymore.

The second event was the crash of the CERT Coordination Center site at Carnegie Mellon University, which was taken down by a DDoS attack. The CERT group represents the foremost authority on hacker attacks, and the ease with which their site was crippled illustrates just how powerful such attacks have become.

The third event was the appearance of powerful and highly virulent worms and viruses, such as Sircom, Code Red, and Nimda.

In addition, concern has increased over the activities of cyber-rogue nations and terrorist groups with a high interest in cyber-activities, who are actively targeting important infrastructure in the US and Japan. After the attacks of 9/11, Chinese president Jiang Zemin lauded the foresight of the two senior air force colonels from the Chinese People's Liberation Army who authored *Unrestricted Warfare*, a paper predicting the future of war and "anything goes" attacks, including cyber-terrorism. Patriotic Chinese hacker groups, such as the Hacker Union of China and the China Eagle Union, have mounted concentrated attacks as a form of protest, for example against the content of Japanese textbooks and the emergency landing of a US spy plane on Hainan Island.

During the Kosovo conflict, a global consortium of volunteer hackers mounted a cyber-attack against government institutions in the US and the UK, the two countries that took the lead in NATO's bombing of Yugoslavia. This heralded the arrival of politically motivated cyber-NGOs or "hacktivists," and such groups are becoming even more politically active in the arena of anti-globalization protest. It would be a natural development if these movements developed links with terrorist groups that were targeting the US and other developed nations.

Hence, on the brink of this new era of cyber-terrorism, we are confronted with the following: an advanced, sophisticated level of technology for hacking and virus creation (one that has become commonplace); certain countries that have become cyber-rogue or cyber-terrorist nations; patriotic hacker groups and cyber-NGOs who are ready to team up with these nations; and various other potential cyber-terrorists who are ripe for recruitment. In

other words, the pranksters have grown up and now represent a more politicized and more professional threat with which we must contend.

What we must be mindful of is the fact that the objective of the individuals and nations who are engaging in cyber-terrorism is not terrorism itself, but rather to strike at enemy nations by paralyzing their critical infrastructure and inspiring fear in their citizens. In other words, unless cyber-terrorism is properly regarded as a means of attacking important infrastructure, the countermeasures that are developed may prove ineffective.

From this perspective, I would like to emphasize three facets of international cooperation in the struggle against cyber-terrorism, and discuss how they relate to Japan.

The first of these is the personal ability of those in the leadership strata in those countries that are cooperating internationally. In particular, Japan's leadership stratum (that is, those in leadership roles in politics, business, and the media) suffers from a lack of leadership brought about by an inability to properly understand the IT revolution and the lack of a national security perspective.

On 31 March 2001, six websites—including those of the Liberal Democratic Party (LDP) headquarters and the Sankei Shimbun—were attacked five times over the course of the day, in what warnings which had appeared several days earlier on a Korean government website termed a “cyber-demonstration.” The LDP site was shut down completely, and the Sankei Shimbun experienced interruptions to some of its operations. Yet, other than a few minor references in the Sankei Shimbun and other newspapers, there was no widespread acknowledgement of the fact that Korean hackers had brought down the website of the LDP headquarters—the official site for LDP members of the Diet. In contrast, reports of—and opinions on—the attack and the damage that it had caused were circulated widely on the Internet. Thus, it appears that if one were to rely solely on the traditional news media, one might well remain uninformed about this kind of critically important event.

In contrast to China's leadership stratum, which is comprised predominantly of individuals with a background in the hard sciences, Japan's leadership stratum—including its leaders in the manufacturing industry—consists predominantly of people with a background in the social sciences; this has been the case for many years. After the Meiji Restoration, efforts were made to foster potential leaders who had a background in law with a view to building a modern nation. The effects of those efforts are still with us today. The resulting absence of scientific and technological savvy renders cyberspace and the like an invisible hazard, and—worst of all—engenders a kind of rejection. In the business sector, the non-technical owner tends to leave everything in the hands of his technically oriented executives; within companies, responsibility is further delegated to network specialists.

In addition, Japan's leadership stratum lacks a national security perspective. This is the legacy of Japan's total reliance on the US in military and intelligence matters during the Cold War era. Japan's peculiar linguistic environment reflects this by regarding the terms “military” and “intelligence” as taboo. Military and intelligence activities hinge on cutting-edge science and technology; hence, the clueless leadership stratum falls behind in the IT revolution and has a hard time understanding cyber-terrorism.

What will be the result? There is an obvious gap between Japanese and US countermeasures for cyber-terrorism.

First of all, both countries approach the problem from different angles—the US from the perspective of national security, and Japan from the perspective of technology. Thus, at the core of investigations, research, and countermeasures in the US are to be found ex-

intelligence agents, ex-military personnel, and specialists on organized crime and terrorism; in Japan, however, one finds network specialists, and cryptographers are made to run the show. The difference can also be seen in the policies themselves—the US is focusing closely on critical infrastructure, while Japan’s “security policy” is little more than a manual of technological solutions for businesses. This policy talks of viruses and Trojan horses but never leaves the technological plane and never broaches the key questions: “which targets will be attacked by whom, using which methods, and for what purpose?”

Before we talk of “international cooperation,” we must first address the questions surrounding the ability of those in the leadership stratum to discuss international cooperation on cyber-terrorism.

The second issue relates to the type of organization which is required for dealing with cyber-terrorism. This problem can be seen in all countries, not just in Japan. In most countries cyber-terrorism constitutes a criminal act in violation of existing laws—that is, a cyber-crime. However, cyber-terrorism might also represent one stage in a cyber-war and be based on the national strategy of a state. Thus, it is vital that the threat of cyber-attacks—whether posed by cyber-crime, cyber-terrorism, or cyber-war—against critical infrastructure (as distinct from on-going, more general crimes, such as Internet fraud or pornography) be addressed rapidly and effectively.

Yet, in all countries law enforcement institutions’ levels of awareness, ways of assigning duties, and organizational methods remain largely unchanged, clearly indicating that the problem is still regarded as one simply of criminality. The Council of Europe’s Convention on Cyber-Crime was drafted with child pornography in mind, and the core concept of international cooperation which it embodies amounts in practice to nothing more than extradition. Even the final communiqué of the G7 Lyon Summit employed the term “hi-tech crime,” thereby endowing a criminal activity with a rather prestigious-sounding title—somewhat surprising given that the context of the debate was law enforcement! The Japanese police too continue to use the term “hi-tech crime.”

Cyber-terrorism is a trans-national security issue. The US Department of Homeland Security will doubtless be perceived as a powerful model. Japan’s cyber-terrorism policy—an initiative of the prime minister—is on the right track, and, given its momentum, there is hope that it will become a model for an organizational reshuffle and redistribution of authority that can enable a smooth transition to international cooperation.

The third and final point is the creation of an international scheme for deterring and controlling cyber-terrorism and cyber-war.

A cyber-war could start in tandem with conventional weapons as part of a conventional war with a clear national strategy, but would be more likely to start in the form of cyber-terrorism, with a concealed national strategy. Yet, before the hostilities began there would probably be sufficiently thorough cyber-surveillance. However, if the proposal for an international scheme proceeds to the discussion stage, there are three prohibitions that will probably be imposed. The first is “weaponization.” This should be prohibited as an act that would disrupt the grand new world order which has been constructed as a tool for comfortable life and abundant prosperity. Thus, as acts of hostility, cyber-first strikes must be banned; however, cyber-attack could be recognized as a legitimate form of counter-attack.

The second prohibition is “attacks on civilians,” just as in the conventional rules of war.

The other prohibition is the “support of volunteer hackers.” In the heat of international friction over national interests, patriotic hackers will want to conduct cyber-attacks against

government institutions, critical infrastructure, and public websites in the opposing country. This is only natural; yet, these people are viewed under the existing world order as up-and-coming cyber-terrorists, and all countries must be obligated to put a stop to such activities. A country that failed to do so would be treated as a cyber-rogue or cyber-terrorist nation.

Countries that violate these three prohibitions would have appropriate sanctions imposed on them by an international organization, and this arrangement would constitute the framework of the scheme.

In contrast, there is a military need for a Cyber-Defense Alliance. The CDA would function rather like NATO and would have two absolute requirements: a shared sense of values (in other words, democracy); and an adherence to absolute secrecy. It is regrettable that Japan does not meet this latter requirement for participation in a CDA.

In addition, it is extremely important that each country protect its critical infrastructure by providing and sharing with other nations advanced and sophisticated methods and technology for conducting cyber-attacks, tracking down the sources of such attacks, and defending against them. It may be assumed that this is already occurring; however, nations that already possess advanced technology should insist on confidentiality agreements that prevent other countries from acquiring the technology. Yet, even though Japan is developing highly advanced technology, the fact that this could be leaked without warning—even without any action on the part of foreign intelligence agencies—renders Japan ineligible for participation in any international cooperative effort based on advanced technology. Politicians and the representatives of the media would do well to keep this in mind.