U.S.-Japan Symposium
150 Years of Amity & 50Years of Alliance
June 18-19, 2010, Washington, D.C.

The Danger of Cyber Illiteracy in the National Security Arena

Raisuke Miyawaki
Chairman, Ochanomizu Associates
Former Advisor to the Prime Minister for Public Relations

This is the "Age of Asymmetric Warfare." After the Cold War – with its reliance on nuclear deterrence – we've seen astonishing advances in conventional weapons development – particularly in targeting and delivery capabilities – in countries such as the US. It is almost impossible for an enemy to successfully challenge an advanced country such as the United States in conventional combat. This has led to the development of 'asymmetric strategies.'

Asymmetric actors include not only terrorist groups; emerging nation states that already have powerful militaries are also aiming to make full use of newly developed asymmetric attack capabilities. China is a prime example of this. Upon learning of the 9/11 terrorist attacks in 2001, China's President Jian Zhu Ming reportedly highly praised two Chinese Air Force generals for their foresight in co-authoring the book, "Beyond Limited Warfare," published in 1999. In this book, they specifically focused on cyber and other 'asymmetric' attacks carried out invisibly and without forewarning – as occurred on 9/11.

In general, offence is easier than defense. It is much more difficult for a conventional force to defeat asymmetric guerrilla and terrorist attacks. Isolation strategy and intelligence activities are the only effective ways to win against them. The same concept applies when facing cyber and other asymmetric attacks – particularly when 'on defense.' A comprehensive protective strategy is now needed, one that can be constructed within the framework of a "national security infrastructure" – that involves politicians, scholars, researchers, bureaucrats, business executives, intelligence agencies, the military, and others.

However, the current 'cyber defense' situation in many democratic countries is weak. This is not surprising given a general lack of cyber literacy among the people responsible for national security. They are too often averse to studying cyber related issues because the technology is simply too difficult. Thus, they are apt to hand-off the issues to their subordinate IT technicians, or, as in the case of Japan, to do almost nothing at all. I consider this an abandonment of their

responsibility. In asymmetric warfare, national security officials too often focus only on 'conventional' terrorist attacks, not on "asymmetric" cyber attacks and related matters – despite these also being crucial "national security" issues.

To effectively intercept asymmetric attacks from 'Cyber Rogue' countries, I would like to emphasize the aforementioned lack of cyber literacy in the national security arena of democratic countries in particular. I appeal for close collaboration between Japanese and United States' national security experts (not just their cyber-security experts) in order to fight – both defensively and offensively – against asymmetric enemies.

A new international scheme must be created to combat cyber misdeeds by 'Cyber Rogue' countries. From an attacker's perspective, it is much easier to deal with targets that do not coordinate and talk with each other. Thus, from a defensive standpoint, an international cooperative scheme between certain countries is potentially of great value, as the conventional Japan-US relationship is important for deterring more conventional threats.

The scheme would require starting from two fundamental points – drafting rules of permissible and prohibited 'cyber' behavior for member countries, and laying out sanctions for violators – both members and non-members. This can be called a "Cyber Defense Alliance."

Noting the Japan-US Alliance's 50th anniversary and their capabilities as the top two cyber countries in the democratic world, Japan and the United States should now take the initiative in establishing a new world order in the cyber arena. This will take time and hard work, though given the current circumstances we can afford to do no less.