The Importance of U.S.-Japan Critical Infrastructure Protection Cooperation

Lincoln P. Bloomfield, Jr., Assistant Secretary of State for Political-Military Affairs
Remarks to the U.S.-Japan CIP Forum Hosted by the Vanderbilt Institute for Public Policy Studies
Washington, DC
November 30, 2004

Good afternoon. I'm pleased to be able to join my old friend Jim Auer, and to thank Jim for that kind introduction. I commend Jim and his colleagues from Vanderbilt University for organizing and hosting this forum. Additionally, let me congratulate all of you for coming together in this conference to focus attention on critical infrastructure protection (CIP) issues of concern to both our nations.

I want to say a few words today on creating a global culture of cyber security, and explain why ensuring the safety and security of networked information systems is a high priority for the United States.

Let me tell you why this matters. Five years ago most people had never heard of cyber security. But five years from now, the private sector here and in Japan will know which networks are best protected, because their communications, their operations, their business will depend on assured service. In the U.S., there is a need to know who is most reliable. So there is a strong and growing market for protection solutions. Other economies, Japan prominent among them, are destined to experience the same.

Our national critical infrastructures--power grids, water systems, and telecommunications networks--all depend on information networks. The smooth and reliable functioning of these systems is essential to the day-to-day well being of our citizens and to the ability of government to perform its duties. You could say this dependence on information systems is unhealthy--and it may seem that way once we realize the vulnerabilities being created. But the benefits we all derive from these technologies are so great that our economies will embrace them, risks and all.

I don't know if any of you saw yesterday's Financial Times of London, but they ran a feature on internet shopping. According to a research firm cited in the article, online retailing has gone up an estimated 25 percent in the U.S. in the past year, to an estimated $66 billion this year. The numbers for holiday season online purchases, in November and December--leaving out travel ticketing and online auction sites--have also risen 23 to 26 percent since last year, to an estimated $15 billion. This is serious business in the U.S. The Financial Times specifically cites Japan as well as the U.K. as the other markets where internet retailing is becoming an important factor in the economy.

The "information society" is also taking shape on a wider scale, all over the world. Each nation must face up to the need to protect its critical infrastructures if its people are to enjoy all the benefits that networked information systems can offer.

U.S.-Japan IT Relationship

Japan and the U.S. have a relationship that illustrates the vital information systems linkages of the two economies and the borderless nature of cyberspace. This interdependence is profound, and it is no longer voluntary, if it ever was.

U.S.-Japan annual two-way trade is in excess of $170 billion. U.S. foreign direct investment in Japan reached $65.6 billion in 2002, and was especially significant in financial services, Internet services, and software industries. Around two-thirds of Japan's 30 Gbps (giga-bytes per second) of Internet circuit capacity is used for the purpose of overseas transmission is directed to North America (including Canada). Two-way telephone calls between U.S. and Japan amounted to 21.5 million hours for 2002--27% of the total international calls for Japan.

Daily financial flows between the U.S. and Japan are in the billions of dollars. Information technology (IT) is

accelerating the market in currency swaps, derivatives, hedge funds, and other short-term capital flows. These connections also highlight that much if not most of the critical infrastructures are in the hands of the private sector.

It was only a few short years ago that the U.S. Government began to organize itself to deal with the problems of protecting the critical networked information systems. At that time, we recognized that our effort to protect our national interest would require a government partnership with the private sector. And, we knew that the effort could not simply be a national one. The simple fact is that what makes cyberspace unique and powerful and gives it great positive potential is its global reach. Of course, the very same quality makes it highly vulnerable to disruption. The threats are global and inevitably, the solutions must be global.

The United States and Japan can and should work together in shaping the global effort on which our economies will depend. I believe we all need to intensify our focus on the ways in which the reliability and availability of IT systems are being threatened. Every day brings another story of system vulnerabilities and criminal exploitations resulting in down time and economic losses. Over time, the size of economic losses from these interruptions gets larger. We need to recognize that the low cost of weaponizing IT and the likelihood of being able to carry out an attack with a reasonable expectation of impunity, makes networked systems a particularly attractive target for attackers, whether they be state or non-state actors.

And so my message today is that the U.S and Japan need to take steps to secure the interconnected critical information systems on which we rely, and we will get a better result if we do this together. I also wish to highlight the vital role of industry as the owner of critical infrastructures, a circumstance that clearly shows the need for partnership between government and industry to protect critical infrastructures.

Bilateral Discussions, Global Dimension

In June of 2002 the governments of Japan and the United States met for a first formal discussion of cyber security. Those talks brought together government experts and policy makers from a cross section of critical sectors to exchange ideas on our respective approaches to critical infrastructure protection. Industry also participated in those talks.

In February of this year, I called on Japanese officials in Tokyo, at the Cabinet Secretariat and in METI, to update our understanding of Japan's activities. In those meetings, I also explained changes in the U.S. Government's management of this issue, notably the reposing of significant responsibilities in the new Department of Homeland Security.

The governments of Japan and the United States plan to meet again in the spring of 2005 to follow up those discussions. Your meetings here this week are thus well timed to provide an important input from industry on progress to date and particularly areas you believe deserve more attention.

By now, the key government entities responsible for protecting our infrastructure in the U.S. and Japan have developed working relationships so that we are able to assist one another with early warning and other essential forms of cooperation. At this stage, both countries share a major interest in addressing our vulnerabilities from the rest of world. Therefore, the U.S. advocates efforts to shape the international environment in ways that reduce the risks to the global information infrastructures on which we depend. In adopting a resolution highlighting the OECD Guidelines for the Security of Information Systems and Networks, the UN General Assembly described this as the creation of a global Culture of Cyber Security.

When we are speaking about a global effort, we mean not just governments, but the full participation of the IT developers, vendors, data managers, and telecom providers that together form the vascular system of the global information network. The U.S. Government's experience has taught us that partnership is essential to the development of a *national* effort to promote cyber security among all participants in society. On the *global* scale, a solution to cyber security will require each nation to take systematic, coordinated actions to protect its own networked information systems. So we have our work cut out for us.

Reducing Risk

How do we reduce risk and advance our collective security? Risk reduction means preventing and protecting against incidents. It's not good enough simply to wait for networks to be disabled and to then manage the consequences. Risk reduction means continuous information sharing, within and across industries, between government and industry, across borders and between governments.

Risk reduction means active deterrence--that is, increasing our capacity, working among law enforcement authorities, to investigate, prosecute and punish those who attack information systems. What does this mean in practice? Let me

offer some observations based on the U.S. experience of the last several years.

First, each nation needs to survey its critical networked information systems, determine where the vulnerabilities lie, and establish programs to address them. Many countries with which we have held bilateral talks have done this. Security capabilities in computer products are crucial to overall network security and must be developed in a manner that allows them to be built into network architecture. Integrated, technology-based cyber security solutions should be designed around international standards developed in an open process.

Second, each nation should promote cyber security education and awareness, and foster this "Culture of Cyber Security" at every level of society. Doing so will require furnishing users and operators of the Internet with information that will help them secure their computers and networks and sensitize them to the vulnerabilities that exist in software and hardware.

Third, each nation needs to adopt cyber crime policies and legislation that will prevent and deter criminal misuse of computers and computer networks, consistent with respect for the privacy and individual rights of users. Each nation must also ensure that law enforcement has the capacity, some of it specialized, to investigate and prosecute cyber crime as well as the procedural rules in place to facilitate transborder investigation.

Fourth, nations can contribute to global cyber security by establishing a national capability for 24 hour-a-day, 7 day-a-week real time cyber incident warning and threat assessment in order to facilitate global information sharing on cyber threats. The U.S. is currently in the process of considering the appropriate framework for such exchanges, but is prepared today to begin preliminary exchanges with appropriate government entities.

Fifth, as I said at the outset, a public-private partnership is crucial to the success of any national program designed to promote cyber security, as the owners and operators of the information systems are the ones who must bear the greatest responsibility for implementing cyber security measures.

Lastly, the U.S. has found that the designation of a central coordinating entity for the nation--in our case, the Department of Homeland Security--is essential to be able to command the attention of the disparate sectors of the economy and independent government departments and coordinate a national cyber security effort. Strong CIP leadership properly located in the government is essential to mobilize the many entities with dominion over the information grid.

Multinational Efforts

These activities, taken together, are not as onerous as they may sound. Many countries, entire regions, and international bodies are now actively adopting similar cyber security measures, and provide useful models.

Important leadership roles are being played, particularly by multilateral organizations such as the OECD (Organization for Economic Cooperation and Development), the COE (Council of Europe), APEC (Asia Pacific Economic Cooperation Forum), the OAS (Organization of American States) and the G-8. Some of these organizations aid also in training and implementation.

The OECD pioneered ten key principles underlying its "Guidelines for the Security of Information Systems and Networks," from which the term "Global Culture of Cyber Security" was drawn. These principles describe the actions that users, developers or owners of networked systems should take in order to stay safe, in a way that is appropriate to their role. The organization is currently working on a clear and understandable action plan to aid in implementation.

The Council of Europe, which comprises 44 nations, built on pioneering work done by the G-8 on cyber crime and law enforcement cooperation, to develop the first international treaty instrument criminalizing the misuse of information technology. That treaty has now entered into force and is open to accession by additional countries. For those that might not choose to accede to the treaty, its provisions still provide a model template for updating domestic legislation in this area.

APEC’s Telecommunication Forum, also building on the G-8 cyber crime principles, has undertaken an ambitious program to train law enforcement and advise legislators to modernize national cyber crime laws. It has also provided the framework for establishing a region-wide Asia-Pacific Computer Incident Response Team (AP-CIRT), and is in the process of broadening its mandate to look at other issues related to critical information infrastructure protection.

Within our own hemisphere, the OAS is the first multilateral body to adopt a comprehensive cyber security strategy. Three independent committees of the OAS--the Inter-American Committee Against Terrorism, the Inter-American Telecommunication Commission, and the Group of Government Experts--teamed together to produce what they called an "Integral OAS Cyber Security Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cyber Security." The OAS General Assembly adopted this strategy only this past summer. It has three main

components: The Formation of an Inter-American Alert, Watch, and Warning Network to Rapidly Disseminate Cyber Security Information; The Identification and Adoption of Technical Standards for a Secure Internet Architecture; and Ensuring that OAS Members have the Legal Tools Necessary to Protect Internet Users and Information Networks. The three committees are busy planning for implementation of this initiative.

The G-8 High Tech Crime Group, which did the original seminal work in the area of cyber crime, has broadened its portfolio to encompass the full scope of critical information infrastructure protection (CIIP) and has developed new principles which can provide a guide for national action.

The UN is also playing a role, both through the General Assembly and through WSIS (World Summit on the Information Society). The U.S., as a participant in all these fora, takes care to ensure that these different regional efforts are compatible and provide the best possible foundation for successful international cooperation.

Since 1999, the U.S. has proposed four cyber security-related resolutions to the UNGA. Two of these built on the G-8 work on cyber crime, one adopted the OECD principles on the Creation of a Culture of Cyber Security, and one built on the later G-8 CIIP principles. These resolutions have raised awareness of the problem within the General Assembly and at the same time, provided a common sense road map for action. All four of these resolutions were unanimously passed, and we are grateful to Japan's Foreign Ministry for its stalwart support of these efforts at the UN.

Conclusion

I began my remarks by emphasizing that both government and the private sector have indispensable roles to play in any effort to protect networked information systems. The lesson that we in the U.S. Government have learned in our formative years on this issue is that government must lead by example. Once we in government adopted sound security practices on our systems and networks, U.S. industry began to take us more seriously.

As I hope I've made clear, for all that we have done in Washington, there's still a lot of important work for us to do at the official level, working with other capitals and within international fora. But the reality is that even if we in government are fully successful in carrying out all the official steps on our long agenda, we will still have failed to establish a credible condition of cyber security, at home or abroad.

It is you, in private industry, who design, build, own and operate the systems, and whose information is at risk of being lost or compromised. It is your networks that slow down and crash, and your systems that detect intruders. It is your systems that are at risk of being used by others to harm someone else's business and all who depend on them. The business case for robust investment in cyber security is becoming increasingly obvious through financial losses and potential loss of business. I predict we won't be debating this point much longer.

If there is a perspective that could be called "the American view" of cyber security, it is this: the protection of our critical networked information infrastructures has become as essential to the safety and well being of our citizens and economy as the physical protection of our buildings, monuments, and airports. Once you become aware of the scale and severity of threats to these infrastructures, you will never doubt this point.

So I commend you for taking the time to meet and focus attention on this very important challenge. My hope is that we are all setting a course for worldwide action, at the national level and at the level of companies and individual computer users, a course that will allow our citizens to gain the full measure of extraordinary benefits promised by information technology in the 21st century.

Thank you.