



IIPS

Institute for
International Policy Studies

▪ Tokyo ▪

IIPS International Conference

“The IT Revolution and Security Challenges”

Tokyo

December 10-11, 2002

THE IT REVOLUTION AND SECURITY CHALLENGES



On 10-11 December 2002, the Institute for International Policy Studies (IIPS) hosted an international conference and symposium entitled “The IT Revolution and Security Challenges” (co-sponsored by the Nippon Foundation) at the ANA Hotel Tokyo. The conference followed on from the IIPS conference entitled “The IT revolution: Challenges from innovation in information and communication technology and the role of government,” which had been held the previous year.

As the IT revolution continues to advance and as our societies and economies become increasingly reliant on information technology, risks to security posed by the use of this technology have begun to appear. Numerous issues have arisen in this connection; for example, there are growing concerns about whether the right balance is being struck between insuring the security of society and the individual’s right to privacy, and about the danger of hackers breaching financial IT systems, such as those used in e-commerce. In addition, for the sake of national security there is now a clear necessity for a unified response to cyber-terrorism from government and the private sector. In recognition of these risks, and in the knowledge that insuring the security of society is an even greater priority in a post-9/11 world, this year’s conference and symposium consisted of comprehensive discussion from an international perspective on the IT revolution and attendant security issues.



The first session, entitled “IT and Security of Society” and moderated by Taizo Yakushiji (research director of IIPS), saw reports from four panelists. First, Professor Shigeo Tsujii of the Chuo University Faculty of Science and Engineering, explained the role of encryption in security, in the context of the growing freedom and convenience offered by information technology. Professor Doug Tygar of the University of California, Berkeley, discussed the importance of an architecture for handling personal information and the best methods

for disclosing information, as well as various other technologies that could resolve the conflict of interests between privacy and national security. Dieter Gollmann of Microsoft

Research in the UK described problems with end-user systems related to the IT revolution and the importance of user education and new policies. Finally, Mr Kim Hong-Sun, CEO of SecureSoft in Korea, examined the evolution of information security technology and the conflict between this technology and national security, as well as the importance of building an IT culture, citing examples drawn from Korea's rapid integration of IT into society and the accompanying business developments.

In the discussions that followed, it was noted that a distinction needs to be made between national security and information security. It was also suggested that Japan invest more in research on information ownership and the separation of supervisory functions so as to prevent privacy violations. Further to the issue of privacy, it was pointed out that, if countries are to be able to work together despite the fact that the cultural differences between them suggest radically different responses to the issue, approaches that take account of these differences must be formulated.



The second session, “The Transformation of National Security and Cyber Terrorism” (moderated by Ryukichi Imai, distinguished research fellow of IIPS), featured presentations from three panelists. Raisuke Miyawaki, first cabinet media spokesperson, commented on the quantifiably increased menace that marks a new phase in cyber-terror, and the emergence of virulent computer viruses. Olivia Bosch, visiting fellow at the International Institute for Strategic Studies in the UK, noted that responses to cyber-risk are being

developed around the world, and explained the importance of appropriate government and corporate responses to potential cyber-war. Finally, James Lewis, director for technology policy at the Center Strategic and International Studies in the US, described cyber-terrorism as a national security issue, and explained the differences between critical infrastructure systems and computer networks in terms of their levels of vulnerability.

The subsequent discussion was lively, and suggestions included leveraging experience gained in dealing with the Millennium Bug and the importance of international cooperation, as well as a proposal to establish a cyber-defense



alliance (CDA) of democratic countries, styled along the lines of NATO. Regarding Japan's preparedness, comments ranged from the importance of a system able to interact with a putative CDA, to a possible change from a perception of cyber-security as a technology issue to something more akin to the United States' view of the problem, as one of national security. Other suggestions included the development of technology to counter cyber-terrorism.



The third and final session (moderated by Shinzo Kobori, distinguished research fellow at IIPS) was entitled “e-Commerce and Stability of Financial and Economic Systems” and saw comment from three panelists. Mitsuru Iwamura, professor at the Graduate School of Asia-Pacific Studies, Waseda University, pointed out the risks inherent in a situation where one operating system holds a monopoly of the market, and the difficulties in regulating cross-border e-commerce. Antoin O Lachtnain, founder of Digital Messenger in Ireland, explained the

various ways to attack information systems, as well as actions to counter these. While there is no perfect defense, the presenter noted that it was important to develop technological responses that took care to balance privacy, convenience, and cost concerns. The final panelist, Michael Yap, CEO of Commerce Exchange in Singapore, commented on the new risks to e-commerce systems posed by technological innovation and increased accessibility, and the necessity for management to take a proactive stance on this issue and to balance the risk of hacking with the cost of security. He went on to recommend coordinated action between government, management, and technicians.



Delegates then discussed, from various perspectives, their concerns about a single operating system occupying such a large share of



the market. It was also noted that, as risk grows with the use of new technology, there are problems with endeavoring to control this through technological and systemic means, and that there are also trade-offs between security and convenience, and between security and privacy.

In the symposium following these discussions, moderator Yoshio Okawara, President of IIPS, led Professor Doug Tygar, Mr Raisuke Miyawaki and Professor Mitsuru Iwamura in reporting the proceedings of each of the preceding sessions.



The discussion was then opened to the other panelists and the floor. In the ensuing discussion, participants pointed out that a distinction should be made between national security and computer security, and that a global network is being laid on top of various systems, cultures, and histories. As such, government policies should take into consideration the differences found in approaches to security and privacy. As key national infrastructure is increasingly operated by the private sector, it becomes that much

more necessary to formulate policy aimed at building a system to insure that this infrastructure is run effectively. Other views expressed were: that by providing infrastructure for electronic government, governments strengthen their own role as players; that there is a need to secure personnel and funding, and to make organizational improvements in order to increase information security; and that education is important in heightening awareness of security as a cultural issue.