INTERNATIONAL TELECOMMUNICATION UNION

ITU WORKSHOP ON CREATING TRUST IN CRITICAL NETWORK INFRASTRUCTURES

Document: CNI/10

22 May 2002

Seoul, Republic of Korea — 20 - 22 May 2002

CHAIRMAN'S REPORT

Introduction

1. At the invitation of the Administration of the Republic of Korea, and with the participation of Minister Dr Seungtaik Yang of the Ministry of Information and Communication of the Republic of Korea and the Secretary-General of the International Telecommunication Union (ITU), Mr Yoshio Utsumi, a workshop was held in Seoul, Korea, from 20 to 22 May 2002, to discuss the topic of "Creating Trust in Critical Network Infrastructures". The Workshop was organized as part of the Secretary-General's "New Initiatives" programme. Some 70 security experts participated in the meeting, representing a range of regulatory and policy-making agencies, public telecommunication operators, other private firms, academic institutions and others. Those present at the meeting participated in an individual capacity. Professor Deborah Hurley of the John F. Kennedy School of Government at Harvard University (US) chaired the meeting.

2. Three background issues documents had been prepared in advance of the Workshop and were presented and discussed at the Workshop. These dealt with:

- a general introduction to critical network infrastructures (by Professor Kijoon Chae, Ewha Women's University);
- a paper on international coordination to increase the security of critical network infrastructures (by Professor Seymour Goodman and colleagues from Georgia Institute of Technology);
- a "straw man" proposal on a collective security approach to protecting the global critical infrastructure (by Dr Stephen Bryen, Aurora Defense).

3. In addition, a number of country case studies had been commissioned, covering Brazil, Canada, the Republic of Korea and the Netherlands,[1] and were discussed along with the experiences of other countries and regional groups, notably India, Japan, Kenya, Malaysia and the ASEAN countries (notably the e-ASEAN initiative). This meeting complements a workshop held by the ITU-T Sector the previous week, at the same venue. Dr Hiroyuki Ohno (Japan) from ITU-T Study Group 17 provided a report on that meeting. While the ITU-T meeting focused on technical aspects of network security, this meeting was centred on the policy and regulatory implications of critical network infrastructures and on possible areas for international cooperation. It was agreed that the information provided and the discussion generated were extremely useful, especially to those currently involved in drafting national policies.

The nature of the problem

4. **Critical infrastructure protection** consists of providing for the confidentiality, integrity, availability and authentication of information and communication systems, including the data and information they transfer. Information and communication systems, including the global network of networks, are not static, but are dynamic and change over time. Similarly, the complete and total protection of critical infrastructures is never achieved. It is an ongoing, dynamic process. Moreover, critical infrastructure protection involves a learning adversary, i.e. other human beings. This is in contrast to other

[1] All of the meeting documents are available on the ITU website at: <http://www.itu.int/cni>.

areas of engineering, such as the civil engineering task of designing the physical structure of a bridge for example. Nevertheless, protection of physical assets is an important component of critical infrastructure protection and networks are only one part of the broader problem.

5. It is too narrow to take into consideration the Internet alone when planning for critical infrastructure protection. Instead, it is important to contemplate the **ubiquitous information environment**. There are numerous developments which are transforming current information and communication systems. These factors include the rapid convergence of information and communication technologies with biotechnology and nanotechnology. This will result in computation and communication occurring through all forms of media, which may be solid, liquid or gaseous, as well as within human beings and between human beings and the external world. The Internet will be rapidly surpassed and succeeded by the ubiquitous information environment, which will be characterized by the following features:

- embeddedness;
- ubiquity;
- unboundedness;
- decentralization.

This environment will require survivability and, if not sufficiently protected, will be vulnerable to cascading effects from security failures and system interdependencies, the magnitude and consequences of which are not at all well understood.

6. Most of the issues related to protecting critical infrastructures are non-technical. The most important of these issues is the **management of large, complex organizations**. Again, current understanding of this subject is limited. One issue that needs more consideration is that of the potential liability of software developers for bugs in their products and services, while taking into account the freeware and open source models.

7. Critical infrastructure protection, cyber-terrorism, and information warfare form a **continuum**. All relate to preserving the functioning of the critical infrastructure, so measures taken to protect critical infrastructure will assist in all these domains. They differ principally in terms of the actors involved and their intent. While cyber-terrorism and information warfare receive lots of publicity, it is essential to keep in mind that the vast majority of threats to, and breaches of, the critical infrastructure come, not from hackers, crackers, and terrorists, but from employees, who are negligent, fatigued, or insufficiently trained, and who unwittingly cause breaches or vulnerabilities.

8. A significant need is to raise **awareness** of the need for a systematic and consistent approach to security issues and to promote user education and training. A programme of education and training needs to be developed at all levels, including for schoolchildren, in order to reinforce an understanding of security issues, as well discouraging teenagers from becoming hackers. Security should also become a component of information system design courses, for example by ensuring the systematic inclusion of security considerations during design projects.

9. It is notable that the **performance criteria and quality of service requirements** for the Internet are shifting rapidly, as it becomes a mass medium used increasingly widely throughout society. The early Internet performance standard was “best effort.” It was apparent from discussions that this quality of service performance and guarantee is no longer sufficient, and that a standard similar to that applied to telephony services and emergency services – i.e. constant availability – is coming to be required. It is worth examining this question of performance criteria to decide on the standard? Is it to be similar to voice telephony, emergency telephone services, electricity provision, or some other standard?

10. In any event, human activity is increasingly entwined with the continued functioning of critical infrastructures. This, in turn, is increasingly dependent on the **goodwill of people all round the world**, including teenagers, for the continued functioning of the global networks of networks. Many policy issues arise from this fact, including jurisdiction, mutual assistance, evidence, and criminal prosecution.

11. Critical infrastructure protection includes not only the important issue of robust performance for daily business and personal activities, but also inevitably raises **issues of law enforcement and national security**. This is also true of other important resources, such as electricity, energy, and water resources. Similarly, while law enforcement and national security issues must be competently addressed, they must be

accomplished in the context of the use of these critical infrastructures in civil society. In this regard, privacy and security are compatible and can be mutually reinforcing. Protection of personal data will enhance the protection of critical infrastructures.

12. There is a need for much more study and an increased understanding of **risk tolerance**, risk assessment, and risk management in the area of critical infrastructure protection. It would be useful, in this context, to study analogous areas, such as the insurance industry, to import valuable lessons on risk into the critical infrastructure domain.

13. It was repeatedly noted that a lot is known about computer security, but that **implementation lags far behind**, with continued failure to implement security measures. There are a number of reasons for this deficit. Data on security vulnerabilities, threats, and breaches is insufficient. An incentive structure to encourage the private sector to improve critical infrastructure protection is absent. This is exacerbated by technology and competition cycles, which provide further disincentives for private sector attention to, and investment in, critical infrastructure protection. Better data will certainly help because it will demonstrate the case for improved critical infrastructure protection. This should be accompanied by the establishment of an incentive structure, which might include insurance requirements, liability, standards, and R&D and tax credits.

14. The fact remains that the **intrinsic security of the global network of networks is deteriorating** all the time. There are many factors that contribute to this increasing insecurity, including the continual addition of more computers, communication networks, data, information, and, most significantly, fallible human beings to the global network. In addition, there is an inverse relationship between the availability of hacking tools on the World Wide Web and the necessary sophistication of hackers.

15. A prime concern is the way in which companies, individuals and government organizations can be incouraged to take security measures. A number of participants indicated the need for an **incentive structure**, such as tax reductions, to enhance the willingness to improve security levels. Workshop participants agreed that the issue of security is not primarily a technological one. Secure protocols and technical responses to threats exist. However, the **political and financial will** to implement them is often lacking. At the present time, security is often regarded as a non-revenue producing activity and thus receives low priority, especially during times of economic recession.

The need for international collaboration

16. A recurring theme in the presentations and discussions during the workshop was the need for **international collaboration** in the protection of critical network infrastructures. It was quite clear to all participants that the current level of collaboration falls short in many respects.

17. Moreover, the amount of **national activity is insufficient** and patchy in almost all countries, as is sub-national activity. Improved attention and activity on critical infrastructure protection is urgently needed at all three levels: international, national, and sub-national.

18. Increased international effort and collaboration can provide an important and efficient resource for national and sub-national processes. **International consultation** will help to build consensus and provide more convergence in approach, which is important for providing protection of the global networks in a predictable, coherent, sustainable, and robust manner.

19. At the present time, collaboration between nations (at regional and international level as well as at sub-national level) and across sectors is limited and often relies on personal contacts. Greater levels of cooperation are restricted by the multitude of national laws and the limitations placed on the exchange of information. Better mechanisms, based on **procedures** and not friendships, need to be put in place. Agencies involved in the protection of critical network infrastructures need to possess a mandate enabling them to actively collaborate with foreign agencies in response to threats and attacks. To improve cooperation, laws and guidelines should be streamlined at international level, to provide agencies with comparable tools across borders.

What needs to be done

20. Having determined that greater international collaboration is certainly necessary, it is worth speculating what form this could take. As one example, in his paper (Doc CNI/04), Professor Goodman sets out a **fivefold framework for international collaboration**:

- International standards. International cooperation in developing standards is increasingly important, even in competitive markets. But just as important is cooperation in the *creation and implementation* of standards. For instance, the Wired Equivalent Privacy (WEP) encryption standard is successfully implemented on fewer than 15 per cent of IEEE 802.11 Wireless LANs in operation, and it is relatively easy to crack. As another example, there are at least 65 different proprietary firewall products, each of which has incompatible procedures and formats for maintaining activity logs due to a lack of standards.

- Information sharing. There is an understandable unwillingness to share information about cyber-attacks, if only for fear of exposing failings and undermining public confidence. There may be a role for a clearinghouse function that an international organization could play, as a trusted repository of current information. Such a clearinghouse could provide anonymity to the victims as well as coordinating information gathering and dissemination.

- Halting cyber-attacks in progress. One of the most useful steps that could be made would be to develop a standard methodology for the sharing of information across borders, especially *during* cyber-attacks, when time is of the essence. Dr Bryen proposed the creation of a Cyber Warning Centre, which could set common data reporting standards and could serve as an alert service. This could be combined with the clearinghouse function mentioned above.

- Coordinating legal systems. If defence against criminal or terrorist activities is to be active, rather than just passive, then there needs to be some coordination of legal systems so that hackers can not find safe havens. In the world of civil aviation, international cooperation was relatively successful in the 1970s in deterring hijackers. Existing treaty-level arrangements, such as the OECD *Guidelines for Security of Information Systems* or the Council of Europe *Convention on Cybe-crime*, are however relatively weak and non-inclusive.

- Providing assistance to developing nations. This will require collaboration between ITU Member States at different levels of economic and technological development. For example, the International Civil Aviation Organization (ICAO) has played a similar role in providing technical assistance to promote safety and security in civil aviation. Similar assistance is necessary to counter cyber-terrorism.

21. In developing such a framework for international collaboration, it is useful to consider **three dimensions of cooperation**, all of which form a spectrum of possible actions:

- Formal/informal, including the full spectrum of activities ranging, for instance, from a treaty-level formal arrangement to ad hoc cooperation between security experts and other stakeholders. It may be difficult to achieve such a treaty, but equally staying with ad hoc arrangements is likely to be unsustainable.

- Multilateral/bilateral, depending on the geographical scope of the level of cooperation.

- Active/passive forms of defence against unauthorised intrusion.

22. Of course, successful international cooperation must first be founded on **effective cooperation at the national and sub-national levels**. The country case studies and other country presentations revealed a range of problems in this area, ranging from turf wars, to overlapping mandates and unclear legal frameworks. Some countries have a proliferation of different organizations that are attempting to address network security issues, leading to a duplication of work and meaning that financial resources are thinly spread.

Future work

23. It was recommended that, where appropriate, governments, in consultation with the relevant industry sectors, begin a process of **risk assessment** of the vulnerabilities and risks to national networks, with a view to producing a follow-up action plan that address those risks. In addition, it would be useful to identify existing relevant mechanisms, activities, and institutions already at work on aspects of the issues of critical infrastructure protection.

24. Advanced info-communications networks, including the Internet, are highly dependent upon critical telecommunication infrastructure, e.g. for backbone and access networks. Similarly, Internet services may be substitutable for public telecommunication services. With convergence, there are clearly synergistic interests for both telecommunication and Internet providers in providing and operating secure networks. A **review of national policy and/or regulatory stances** may be appropriate, bearing in mind that asymmetric policies or regulation may potentially impede progress in information systems security and network infrastructure protection. As one example, national or regional security certification schemes covering both sectors might be envisioned.

25. Because of the many dimensions of the problems, it was considered unlikely that a **single international forum** would be able to resolve information systems security and achieve network infrastructure protection. Therefore, it would be most beneficial to work towards advancing specific areas in a number of international forums. Concrete examples of initiatives to be taken include information sharing, international technical standards and monitoring, halting attacks in progress, coordinating legal systems and providing assistance to developing countries. The appropriate forums, whether public or private sector-based, should be further identified, including intergovernmental and non-governmental organizations, such as the OECD, UNESCO, ETSI and others. At the time of the adoption of the *OECD Guidelines for the Security of Information Systems* by the OECD member nations, several countries supported the establishment of an Observatory for the Security of Information Systems. This proposal, timely when first proposed in 1992, is long overdue. It would provide a helpful umbrella capacity at international level for information exchange, awareness, education, promulgation of best practice, so as to benefit from ongoing technical, legal, policy, and management activities in other forums.

26. With respect to the **role of ITU**, the following suggestions were discussed:

- ITU should quickly review its current work programme activities vis-à-vis information systems security and network infrastructure protection and take action to reinforce its activities in this area. It was considered that ITU, as an organization made up of representatives of both governments and the private sector involved in coordinating global telecom networks (including IP-based networks) and services, represented a distinctive international forum for cooperative initiatives in this area.
- In particular, mention was made of the need for improved technical standards for both information and systems security and that there was a need for improved cooperation on Internet Protocol (IP related vulnerabilities and improved security standards between ITU and other relevant standards development organizations (e.g. IETF, W3C etc).
- Particular reference was made to ITU-T cooperation with experts in investigating possible vulnerabilities related to the implementation of Abstract Syntax Notation 1 (ASN.1), defined in ITU-T Recommendations. Because ASN.1 is widely deployed in protocols across both telecommunication networks and the Internet, it was considered that this risk be rapidly investigated. It has been suggested that the scale of the issues may be greater than for the Y2K preparation. Once the problems are validated, ITU-T should begin an action plan to cooperate with the appropriate organizations as well as manufacturers and vendors to widely disseminate information on how to address this possible vulnerability.
- It was suggested that the topic of information systems security and network infrastructure protection be included in the agenda of the World Summit for the Information Society (WSIS) as public trust in information and systems security is a cross-cutting issue, integral to the development of an Information Society.

- In order to take discussions initiated at this workshop forward, it is proposed that a bulletin board be created on the ITU website, in particular for discussion of the “straw man proposal” concerning a possible way forward.
- Where there are national or regional security certification standards that have been developed, consideration could be given to the development of an international mutual recognition scheme for security certification. ITU could assist, for instance, in elaborating common criteria for the designation of critical infrastructures.
- The ITU-D Sector should consider developing a programme of assistance to developing nations on awareness of critical infrastructure protection issues. ITU’s lead should encourage regional groups, for instance e-ASEAN, to work on this issue.
- ITU should widely disseminate the discussions and report from this workshop to its three Sectors and to its membership, in particular to developing countries, as well as to other international organizations, standards development organizations and other appropriate parties.