INTERNATIONAL TELECOMMUNICATION UNION

**ITU WORKSHOP ON
CREATING TRUST IN CRITICAL
NETWORK INFRASTRUCTURES**

**Document: CNI/03
20 May 2002**

Seoul, Republic of Korea — 20 - 22 May 2002

INTRODUCTION TO CRITICAL NETWORK INFRASTRUCTURES

This background paper was prepared by Professor Dr. Kijoon Chae of the Department of Computer Science and Engineering, Ewha Woman's University, Seoul, Republic of Korea, for the ITU New Initiatives Workshop on "Creating Trust in Critical Network Infrastructures", held in Seoul, 20-22 May 2002, hosted by the Government of the Republic of Korea. Thanks go to Sy Goodman, Andy Ozment, Davis King and Pamela Hassebroek for their contributions to the paper. Other papers prepared for the workshop are available on the ITU site at www.itu.int/cni. The paper has been edited by the ITU secretariat. The views expressed in this paper are those of the author alone and do not necessarily reflect the opinions of the ITU or its membership.

1. Introduction

1.1 It is hard to think of all the countless ways in which today's info-communications affect our lives. The phenomenal growth of the Internet and mobile communication, the WTO (World Trade Organization) basic telecommunications agreement on trade liberalization, rapid technological change, have all played a very important role, not only in forming a foundation for the information society, but also in influencing each individual's life. In particular, through the digitization of many different fields of society and economy, every nation has now established Internet communications in order to contend as an emerging leader in the new economy. Due to the phenomenal growth of the information-oriented society, today's world has become more dependent on the info-communication systems of organizations and companies. Also, as more information has been opened to public access, more people can share information on a global basis. Moreover, these trends are expected to intensify.

1.2 For these reasons, it is essential to guarantee the security of information that is considered of critical importance, from a political, economic, financial or social standpoint. In order to safeguard countries' critical information resources and to guarantee network security, the technical aspects of network security are the subject of much study. Although a network, or part of a network used to exchange information may have state-of-the-art security, in practice the level of security is only as strong as the weakest link in the entire network.

1.3 In the rush to move much of what we do in the real world onto info-communications networks, the implications of failure in our critical network infrastructures (CNI) are but poorly understood. This paper therefore aims to identify the explicit significance of CNIs, which are of crucial importance in politics, economy and society. Securing national CNIs against vulnerability, while ensuring their continued availability, will require creating trust among different parties. This will require collaboration and cooperation among countries.

1.4 This paper is structured as follows: Chapter two provides a definition and description of CNIs. In addition, it describes current trends in network design and their vulnerabilities. Chapter three explains current problems for CNIs and possible solutions to resolve these security problems. Chapter four describes cyber-terrorism and other areas impacting CNI. Finally, conclusions and areas for further study are presented in Chapter five.

2. What is critical network infrastructure (CNI)?

2.1 This chapter explains the significance of vulnerability in info-communications and distinguishes between physical and logical aspects of CNIs. In addition, it describes current trends in network design based on well-known and representative global networks.

2.1 Definition and description of CNI

2.2 The definition of CNI is dependent on the context in which it is used. A CNI can be identified as a public or private network that carries information relevant to national security and safety or information of high financial value.[2] CNI can also be defined physically as the whole network or a part of the network that exchanges information of high significance. For example, if the objective of the network itself is to exchange confidential information among nations, the whole network itself can be defined as a CNI. However, in the case of the Internet, it is appropriate to define pertinent parts as CNIs, because its objective is to simultaneously share information that is open to many anonymous users, and it has been increasingly used as a means to exchange important information for society and the economy.

2.3 The security of CNIs, which are a medium for the exchange of information, is crucially important in research, education, e-commerce, trade, etc. Previously, the important infrastructure of a country may have existed separately from that of other countries, both physically and logically, and there may have been only very limited contact between network designers and managers. However, network management functions are

[2] http://www.itu.int/osg/spu/ni/security/index.html

becoming increasingly automated and interdependent. Accordingly, vulnerability to "cyber attack", as well as to aspects of equipment failure or human error, etc., is rising, especially in the case of e-business. In this regard, because it is evident that CNIs will become a critical part of nationalcompetitiveness in the twenty-first century. While much policy attention has been focused on CNI security policies, there has been a lack of consistency owing to an absence of international standards and insufficient investment.

2.4 The most basic element for building the information society, in the pursuit of stability and prosperity, is to safeguard information. However, as data transfers grow in scale and as dependence on information becomes more intense, the security issue can only become more serious.

2.2 Network Trends and Vulnerabilities

2.5 This section outlines development trends of the Internet and the mobile Internet, and their potential vulnerabilities.

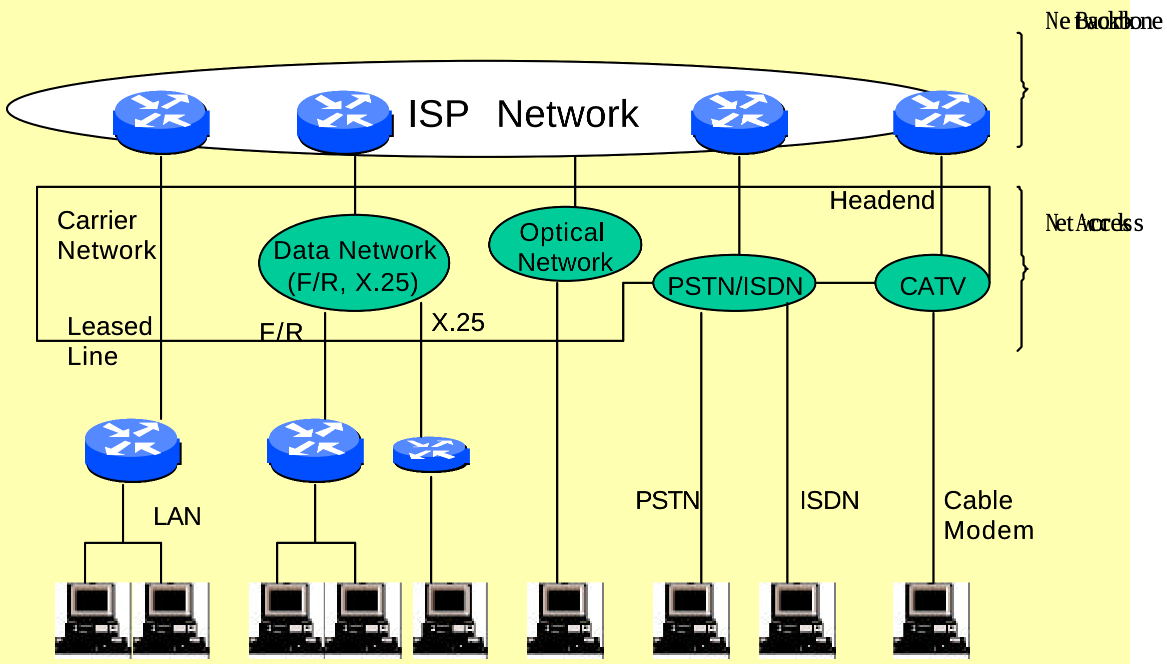
2.2.1 Internet

2.6 The twenty-first century is the era of the Internet. The Internet combines techniques of traditional industry and info-communication. However, it is still hard to provide a high quality of service due to various problems related to the Internet[3]. With respect to the infrastructure, there are such problems as inefficient communications, high costs and low transmission speeds to end-users, "bottleneck" impediments to the construction of high-speed networks, unfair network access policies, and inefficient network extension, etc. From a functional viewpoint, the Internet is sometimes associated with excessive waiting times and a service with no guarantees of the bandwidth available to end-users and quality of service (QoS) for real-time services. Moreover, security provision is often poor. In particular, the Internet is likely to be vulnerable to hacking, denial of service attacks, etc. Internet users cannot be sure that confidential information, for instance concerning their credit status, will not be leaked. For instance, Figure 21 shows the overall hierarchical architecture of the Internet, which may cause "bottlenecks", especially where many access networks are interconnected.

2.7 Accordingly, it is necessary to develop a next-generation Internet (NGI) in order to resolve today's Internet problems and to adjust to changes in demand as society becomes more information-oriented. In the short term, the NGI presents potential solutions to the problems of network congestion, service delay, lack of addresses, expensive charges, etc. Moreover, it supports multimedia and mobile services of a high speed and performance with guaranteed quality in the longer term. There are many countries and regions working on research and development (R&D) for the NGI, such as the United States, the European Union, Canada, Japan, and so forth.

[3] For a discussion of Internet security issues, see "A tangled world wide web of security issues" by Joris Claessens, Bert Preneel and Joos Wanderwalle, at http://www.firstmonday.org/issues/issue7_3/claessens/index.html

Figure 2.1: Hierarchical architecture of the Internet



Source : Electronics and Telecommunications Research Institute, KOREA (Aug 1999)

2.8 The United States has carried out an R&D project on high performance networks including trials running over high-speed testbed networks. This runs at speeds of between 100 to 1,000 times faster than the existing Internet. In addition, by linking more than 100 sites through a point-to-point access over a 100 Mbit/s circuit, it has been constructing the testbed that links government agency networks: vBNS[4] of NSF, DREN[5], NREN[6], ESnet[7], etc. It is also working to construct a special infra-network linking approximately ten or more NGI sites with point-to-point access at transmission speeds of more than 1 Gbit/s.

2.9 In Canada, many research groups, notably CANARIE[8], have made great efforts to establish NGI test networks promoting the CA*net2 project for a high speed transmission network based on ATM. Furthermore, it has been carrying out a CA*net3 project to study methods for optical routing, switching techniques, service applications, etc. The CA*net3 testbed utilizes DWDM (Dense Wavelength Division Multiplexing) and is the first fully optical Internet in the world. A possible architecture for the NGI is illustrated in Figure 2.2.

2.10 As depicted in Figure 2.2, there are NAPs (Network Access Points) linking networks and Giga-POP (Gigabit Point of Presence), etc. in the NGI. The access points link NSP (Network Service Provider) and ISP (Internet Service Provider) very efficiently, systematically, and reliably, thereby overcoming disadvantages inherent in the Internet structure. They manage routing efficiently, and combine high-speed networks and traffic into access points providing a variety of services. An Internet access point, such as the STAR-TAP[9] (Science Technology And Research Transit Access Point) shown in the figure, links international networks,

[4] Very high performance Backbone Network Service, http:// www.vbns.net

[5] Defense Research and Engineering Network, http:// www.hpcm.dren.net/Htdocs/DREN/

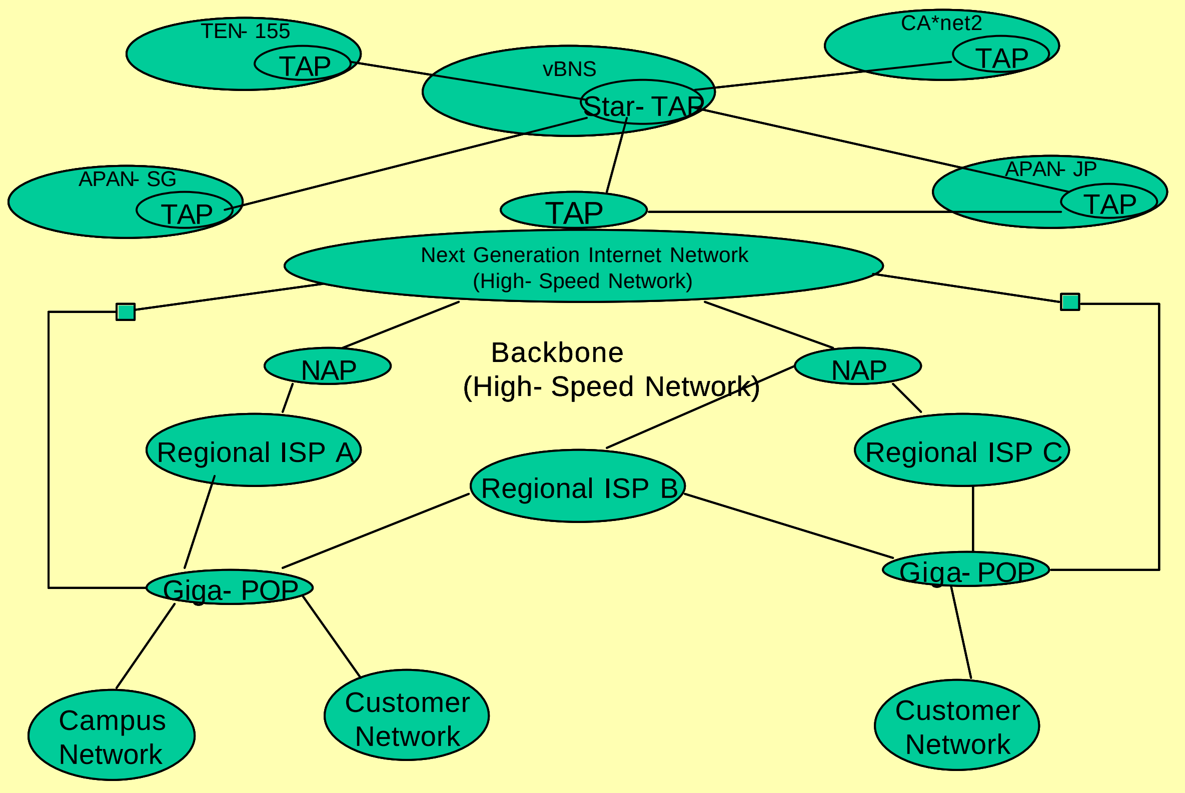
[6] NASA Research and Education Network, http:// www.nren.nasa.gov

[7] Energy Sciences Network, http:// www.es.net

[8] See http://www.canarie.ca

[9] http://www.startap.net

Figure 2.2: Hierarchical architecture of the Next Generation Internet



Source : Electronics and Telecommunications Research Institute, KOREA (Aug 1999)

through which confidential information could be transmitted. In view of this, it is necessary to apply a security system at the intermediate access point for ensuring secure communication among end-users.

2.11 Current information security services are applied to individual systems, and are generally limited to a particular nation rather than being applied to all nations or to international networks. Since the security system is located at the network access point, the overall network may show a drop in its performance, as it is vulnerable to hacking or cyber-terrorism. It is therefore imperative to have a security plan for the access point. In addition, interoperability among individual security systems should be provided and security nodes should be monitored and controlled. Furthermore, secure network techniques should be introduced providing information security services to meet users' various demands. This will result in improved protection of critical network infrastructures.

2.3 Mobile communication, mobile data

2.12 Over the last decade, the growth of the Internet and mobile phones has revolutionized our world. Today, their seamless combination promises anywhere, anytime, anyplace communication systems. Next-generation mobile systems foresee the convergence of mobile, fixed and Internet Protocol (IP) networks towards future high-speed services.

2.13 Cellular service has evolved from the carphone and the first-generation analogue system developed in the early 1980s to second-generation (2G) digital systems, providing better quality and higher capacity at a lower cost. ITU's IMT-2000[10] (or 3G) global standard has paved the way for innovative and integrated applications and services: multimedia messaging, infotainment, location-based services, to name but a few. The commercial rollout of 3G networks has been fraught with delays, due to high license fees and lack of market-ready mobile devices. The first 3G networks were deployed in Japan and Korea in 2001 and some

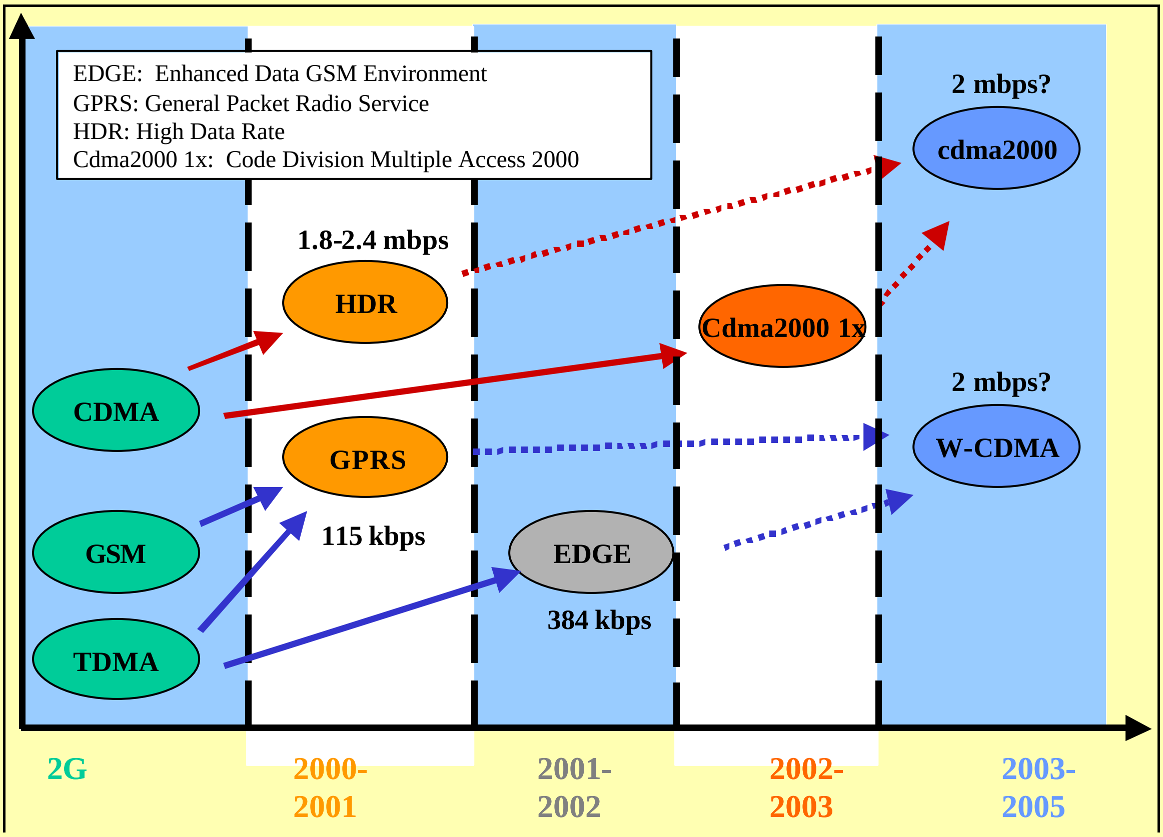
[10] See www.itu.int/imt

European countries are due to launch 3G in late 2002. Research and development on 4G systems has already begun.

2.14 The evolution of networks from 2G to 3G (in some cases, by way of 2.5G) will enhance the ability of users to send and receive data over a wireless platform. 2.5G solutions, such as GPRS (General Packet Radio Service) or EDGE (Enhanced Data rates for GSM Evolution) offer mobile data services at rates between 56 kbit/s and 144 kbit/s, the speed of conventional modems and ISDN lines, respectively. With 3G, full broadband applications will become available at transmission rates that will eventually reach 2Mbit/s. Figure 2.3 sets out the evolution of mobile systems and standards from 2G (CDMA, GSM, TDMA) to 2.5G (HDR, GPRS) to 3G (EDGE, Cdma2000 1x) and 3G (cdma2000, W-CDMA).

2.15 The dominance of multimedia traffic flows will be one of the key trends for future wireless networks. The ratio of data to voice traffic is set to change as we shift from circuit-switched to packet-based networks. It was with the deployment of second-generation systems that the vision of combining data and voice over mobile networks was first realized. One of the most widely used 2G data services is text messaging, particularly in regions where the GSM standard is prevalent. SMS allows users to send short text messages from one mobile phone to the other. The message text can be made up of words or numbers or an alphanumeric combination. It is believed that the first short message was sent in December 1992 from a personal computer (PC) to a mobile phone on the Vodafone GSM network in the UK. Each short message can be up to 160 characters in length when Latin alphabets are mainly used but non-Latin alphabets such as Arabic and Chinese are used, though this reduces the character set per message to around 70. This simple data application has proved to be extremely popular, with 30 billion messages being sent over GSM networks in December 2001, up from 14 million a year earlier[11]. Mobile Internet services over the GSM network have not fared as well as messaging services. Wireless Application Protocol (WAP) over GSM generally offers speeds of only 9.6 kbit/s over circuit-switched links. This translates into connection times

Figure 2.3: From 2G to 3G mobile systems



Source: ITU IMT-2000 and Beyond Study Group.

[11] Data from GSM Association (see http://www.gsmworld.com/news/statistics/index.shtml)

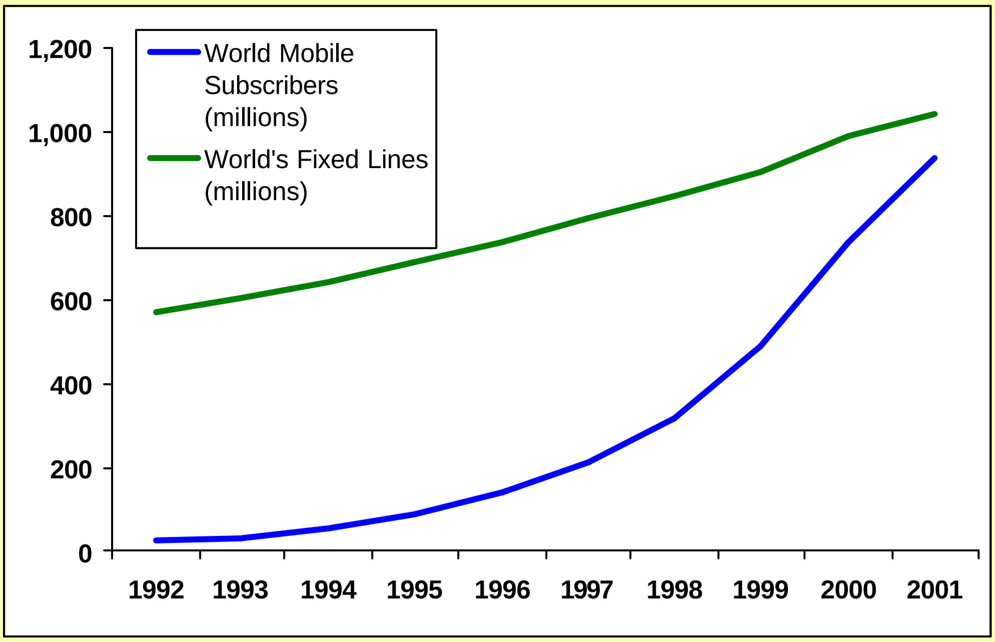
lasting up to 30 seconds, and extended delays for downloading. WAP's main competitor in the 2G space is Japan's i-mode (or information mode), a mobile Internet service first introduced by NTT DoCoMo in February 1999. Unlike WAP, i-mode has been one of the biggest success stories of the mobile world. In March 2002, DoCoMo boasted over 32 million i-mode subscribers. The advantage of i-mode lies first with its network technology, which is packet-based and 'always on'. In addition to a subscription fee, users are thus charged per packet for the service, rather than for the time they spend on-line. Content development policy has also played a significant role in i-mode's success: DoCoMo made it easy for content providers to create an open network of useful sites whereas the tendency in Europe has been to restrict "walled gardens" of content. A revenue-sharing scheme between operators and content providers has also provided incentives for content development in Japan.

2.16 It is expected that operators will eventually migrate their mobile traffic onto an all-IP network. This will translate into enhanced data transmission services for Internet-enabled devices. An all-IP wireless core network would stimulate the innovation of diversified services for consumers. As a core network, IP is scalable and can tolerate a variety of radio protocols. More flexible for application development than current networks, it can support a wide array of access technologies, such as 802.11b, W-CDMA, Bluetooth, HyperLAN as well as those that have yet to be developed.

2.17 At the end of 2001, the number of mobile subscribers worldwide was just short of one billion. At this rate, the mobile network is set to overtake the fixed network in 2002 in terms of the number of users. By the end of 2001, over 90 per cent of countries had a mobile network, almost one in every six of the world's inhabitants had a mobile phone and almost 100 countries had more mobile than fixed telephone subscribers. During 2002, mobile subscribers will overtake the number of fixed lines worldwide (Figure 2.4).

2.18 The deployment and increased use of wireless networks raises a number of security issues. While these networks allow increased freedom of movement, their proliferation means that security features such as corporate firewalls built around LANs and WANs no longer suffice. Data stores and data transmissions are becoming increasingly vulnerable to interception, hacking and viruses. In addition, with wireless becoming the network of choice, issues such as access to emergency services and the role of location-based services are being examined. The main vulnerabilities occur at the translation point between the wireless protocols and the wireline (fixed) protocols. Others exist once the transmission arrives at the wired Internet and become subject to the vulnerabilities of that network.

Figure 2.4: Mobile and fixed-line users worldwide, 1992-2001



Source: ITU World Telecommunication Indicators Database.

2.19 As more and more information of a private or sensitive nature is stored on mobile devices, strong authentication procedures are required to prevent security breaches. The new WAP (Wireless Application Protocol) 2.0 protocol has a security layer embedded into it known as WTLS or Wireless Transport Layer for Security. Authentication using Public Key Infrastructure (PKI) is also seen as essential in addressing the wireless security paradigm. It is clear that in order to encourage adoption, security measures must be transparent and user friendly. In relation to transaction security, the privacy firm Meconomy[12] makes the following recommendations:

1. The use of an open platform for devices, in order to enable users to apply their own privacy and security technologies.
2. Separation of personal identifiers from transactional data, to increase privacy and security
3. Use of data collected for a transaction should be limited to the specific transaction in question.

3. Current Security Issues and Ongoing Activities

3.1 Current Problems associated with CNI

3.1 An interconnected network may be used to save and transmit public or confidential data such as medical data, criminal records, etc. It may operate within a nation or as an international network with the complex interconnections. Accordingly, CNIs are vulnerable to many dangerous threats. The United States, the European Union and other governments have prepared strict legal policies concerning CNIs, in efforts to protect against such threats.

3.2 There are some examples of damage that may result from vulnerabilities or defects in today's CNIs. Services with high financial value, such as banking, e-commerce, trade, etc. have expanded internationally. Such networks exchange confidential data, not only within a nation, but also among nations. Thus, it is even more important to protect systems against network interruptions. However, according to some financial network operators, each component of the network (system, network, and customer access point) is vulnerable, if there is no technical security plan.

3.3 Other industries, such as aviation, space transport, mass transit, shipping, etc. also depend on CNI. Elements of a transportation system, such as vital communication, navigation or the information network, can be threatened in numerous ways. As networks become more global, more and more people have access to critical data. Abusers and intruders can take advantage of weak points in such networks. For instance, there are few technical security features for GPS (global positioning system), which is used as a navigation tool for aircraft, ships, automobiles, etc., and as a positioning tool during military operations.

3.4 Power can also affect the physical aspects of CNIs. Natural disasters can damage important data even if there are perfect back-up systems. In the event of a power failure, any critical data transmitted through the networks will be lost. Currently, Universal Power Supplies (UPS) can prevent unexpected damage like an internal power failure. The use of such facilities needs to be greatly extended if CNIs are to be protected from such damage.

3.5 Other examples of CNIs include energy infrastructures, such as oil and natural gas. Similarly, cyber disruptions or physical factors could result in damages on the structure stretching over a wide geographical range. A reliable international security system is necessary if such damage is to be prevented in advance.

3.6 These threats are in addition to other significant factors for CNI security: unauthorized access, network disruption, malicious software, environmental factors and accidental events, and so on.

3.7 Unauthorized access and intrusions may be motivated by intellectual challenge rather than financial profit. Generally, hacking can take advantage of weak points in information network systems being used for illegal acts or malign intentions. For example, hackers caused disruption of AOL, the world's largest Internet service provider, in June 2000. They intruded into service systems and accessed bank accounts of the

[12] See http://www.meconomy.com/solutions/index.html

company's members, revealing that even the world's largest Internet provider is vulnerable to hackers.[13] Such illegal intrusions can abuse confidential data such as passwords, credit statuses, etc. or violate individual privacy. Obviously, such threats are likely to undermine public confidence in e-commerce.

3.8 There are also many attacks through weak points in network components such as operating systems, routers, switches, name servers, etc. For instance, attacking name servers and damaging e-mail systems can cause websites to fold. Attacks can also intercept, block or modify traffic by attacking routing tables, or by overloading critical web servers, for instance by generating automated messages that flood critical network components. It is very difficult to protect against such attacks.

3.9 A software virus, such as "Trojan Horses", "worms", "I love you", "Melissa", "Kournikova", "Nimda", etc., is regarded as a factor with a high destructive power which can seriously threaten a critical system. For example, "Nimda" damaged some 8.3 million computers worldwide and caused about USD 590 million in losses, according to a computer security company.[14]

3.2 Possible solutions for security problems

3.2.1 Policies and technologies for CNI security

3.10 CNI security has become a more significant issue due to a variety of reasons, including data protection, economic dependency, national security and e-commerce. The rapid pace of technological development, competitive markets and globalization exacerbate the problem, as solutions rapidly become outdated. It may be that the full extent of security problems will only become apparent once experienced.

3.11 Despite the importance of network security, there has been relatively little research carried out on CNIs, perhaps because of the lack of willingness to share experiences and information. Resolving CNI security problems is an urgent priority that cannot wait until the market is fully developed: sufficient resources need to be invested earlier rather than later. Currently, grades of security capability vary greatly between different networks. There is no common policy or system to guarantee reliability. Furthermore, since IT industries evolve very fast, CNIs cannot be secured indefinitely using existing security tools.

3.12 This is one reason why international cooperation is needed. CNIs are present in almost every country in the world. It is important then, that nations cooperate with one another in developing CNI security systems and technologies. At present, there appear to be two major types of policy for increasing the reliability of CNI security:

- **Providing systematic legal solutions**. Currently, although each country applies legal restrictions for CNI security based on its own network situation, there is no international legal policy or system that applies. A systematic international legal solution for CNI security problems also needs to be developed.

- **Awareness-raising regarding the necessity of CNI security**. It is necessary to establish CNI organizations in different countries and to disseminate public information in order to raise awareness of its importance. One initiative of this kind is to be undertaken by the European Union, which intends to carry out "best practice" promotion campaigns and to encourage members to exchange data with one another.

3.13 The United States has conducted R&D on Federal Critical Infrastructure Protection. Several major efforts are under way to tackle the difficult issue of interdependency of CNIs. Those efforts are relevant to both of the policies listed above since their basic goals are similar. The policy efforts under way in the United States include:[15]

- Building a theoretical framework for understanding and predicting the nature of the CNI securities and their effects as a whole;

[13] CNN News http://www.cnn.com/2000/TECH/computing/06/17/aol.hacker.01/#r

[14] CNN News http://www.findarticles.com/cf_0/m5072/42_23/79562338/p1/article.jhtml?term=Nimda+%24590+million+of+losses

[15] Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities, Chapter V. Critical Infrastructure Protection R&D (January 2001).

- Developing the capability to model and simulate in real time the behaviour of the CNI by developing an architecture and related enabling technologies;
- Developing a set of quantitative metrics for measuring the scale of impacts of CNI disruptions;
- Developing new technologies and techniques to contain, mitigate, and defend against the effects of CNI disruptions;
- Developing capabilities to adequately and realistically test new methodologies, techniques, and technologies;
- Defining a set of tasks for further work on specific CNI policy issues that could be analysed using tools and methodologies. This could include, for example, characterizing the potential CNI implications, from national security and economic perspectives, of current trends within the private sector and their implications for national security identifying their vulnerabilities;
- Developing the ability to characterize and incorporate new critical infrastructures into models and methodologies, as such infrastructures develop.

3.2.2 Technologies to increase confidence in CNI security

3.14 No general concept of CNI has yet been clearly defined. Moreover, this is compounded by the general lack of public awareness. It is therefore difficult to suggest applicable technical elements in more than cursory detail.

3.15 However, it should at least be possible to suggest a starting point. The following security features are recognized in existing networks:

- **Availability.** The ability to access data on a network at any time, even when the network is operating under extreme circumstances.
- **Authentication.** The ability to identify a particular user, and to control access.
- **Integrity**. The requirement to check whether data are transmitted, received and stored without defect.
- **Confidentiality**. The requirement to protect specific data from unauthorized users and thereby to ensure users' privacy.
- **Non-repudiation.** The ability to confirm that a particular user has sent or received specific information, for instance, in relation to a transaction.

3.16 Currently, the most convenient and fundamental way to construct a systematic CNI security system is by applying a variety of security features including those listed above. For example, in regard to authentication, there has been intensive research work relating to the generation, distribution and management of a "key", which is shared by group members. This can be extended to the CNI level by consolidating each network component of the CNI into a representative group where a CA (certificate authority) is responsible for generating and managing the "key" for authentication purposes.

3.17 In order to apply fundamental network security features to CNI, it is a prior requirement to prepare an institution responsible for overall management and applications development. In addition, there is a need for international cooperation to develop innovative technologies for the establishment of relatively more systematic and reliable CNI security systems.

3.2.3 Cooperation mechanisms for CNIs

3.18 CNI concerns can be divided into those that are national and those that are international in scope. The former mostly concern the main security or government network in a particular nation. It is generally considered impossible to ensure the security of important data or strategic functions of a nation on the public Internet, which is vulnerable to many invasions, such as a hacking, terrorism or cyber war from a hostile country etc. So a separate network is generally required. For example, the United States Government has asked computer companies to establish a new safe communication network, Govnet[16], which is separate from the Internet, in order provide security against terrorists.

3.19 At the international level, CNI concerns mainly focus on trade and financial networks. Although these can exist at a national level, there is a drive to expand such networks internationally, for instance to facilitate global markets for e-commerce.. For example , SWIFT[17], a global data communication system, has been operating for the exchange financial information among international banks for many years. Similarly, in the trading world, electronic data interchange (EDI) networks allow the easy processing of customs documents.

3.20 It would take a very long time to recover modern networks without an efficient backup system. That delay would be enough to induce critical damage to national security or a national economy—the more significant the data, the more critical the damages can be. On 11 September 2001, when terrorists attacked the World Trade Centre in New York, it was possible to minimize damage with a remote backup system.

3.21 Currently, banks in most countries are equipped with counter measures against fire, flood, power failure, etc. that might cause unexpected outages. In other words, there is a reliable security system for public financial computer networks among the banks, such that a full backup system is available to store all financial transaction data for 24 hours. Also, bank members are often trained to prevent outages, and their networks are protected against hacking by many layers of security systems. However, they may not have established a remote place backup system against physical interruptions, like the one in New York. Since it is expensive to maintain a remote place backup system, a tape backup system is often employed instead. Nevertheless, in the wake of the events of 11 September, such systems have been reviewed.

3.22 It is necessary that there should be a security plan for network disruption, not only from intentional or accidental interruption in a network, but also natural disasters, etc. and this should operate if possible at an international level. As international network communication increases, so corresponding security problems increase. In other words, although a network of a particular nation may provide a high degree of reliability or security, the total network may still be vulnerable unless other interconnected networks are secured at the same level or above.

3.23 Accordingly, as an international cooperation for CNI security is now being regarded as a hot issue, detailed international cooperation mechanisms should be prepared to resolve security problems.

3.24 The OECD (Organization for Economic Co-operation and Development) security guidelines recommend a policy that limits its member from individual data distribution processes when a particular member is not equipped with a security system at the "same" level as that of other members. Similarly, the EU is cooperating with the United States in order to improve the security of critical infrastructures, and has made all possible research efforts on CERTs (Computer Emergency Response Teams) depending on CERT/CC[18], following a partial investment by the US government in October of 1997. The European Commission is also cooperating with international organizations, such as G8, OECD, UN, etc.

3.25 Organizations like the Global Business Dialogue on Electronic Commerce[19] and the Global Internet Project[20] have served as forums for discussion about security problems between private sector players, notably with regard to e-commerce. It is indispensable to exchange data continuously among such organizations in the interests of global security. Yet, in spite of the fact that cooperation for CNI security on the international level is regarded as essential, few of the existing international CNI security systems have been standardized. Therefore, international standard organizations, such as ITU, could play an important role in standardizing policies and technologies for CNI security.

[16] http://www.vnunet.com/News/1126080

[17] http://www.swift.com

[18] Network and Information Security: Proposal for a European Policy Approach. (Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of The regions)

[19] www.gbde.org

[20] www.gip.org

4. Cyber-terrorism and other areas impacting infrastructure

4.1 Cyber-terrorism

4.1 Spring, 2003: Emergency rooms receive hundreds of patients complaining of unexplained headaches, nausea and intestinal pain in a medium-sized city. Three elderly people die, triggering fears of a bio-terrorist attack. A hotel guest sees flames outside his door, calls 911, and hears nothing but obscene jokes in Swedish. On the coast, an oil tanker hits a reef two miles off its expected course, and a passenger plane strays onto a collision course with another jet.

4.2 These three incidents are examples of the results of possible "cyber-terrorist" attacks. The 911 call example is real—in 1997 hackers rerouted the 911 emergency telephone system in three Florida counties. The airplane and oil tanker incidents are plausible attacks that illustrate the damage terrorists could do by accessing critical systems like GPS navigation[21], air traffic control, and electric power grids. The sudden rash of illnesses is a possible result of a remote attack on the networks used to control dams and water treatment plants.[22]

4.3 What makes these potential attacks so dangerous is that they combine the ubiquity of computer networks with the asymmetric violence of terrorism. The 'asymmetry' of terrorism implies that a single terrorist can cause tens or hundreds of casualties. For non-cyber attacks like suicide bombings and mail bombs, however, the asymmetry is limited by the terrorist's ability to acquire weapons, recruits, and money and to transport them to targets. Nations can deploy border controls, bomb-sniffing dogs, and military forces to block these physical flows.

4.4 The pervasiveness of CNIs allows a cyber-terrorist to attempt equivalent damage from any country in the world, with little fear of being slowed or stopped by physical defences. The terrorist may be able to increase asymmetry by repeating attacks and discovering new vulnerabilities. The nation under attack may need international assistance both to plug security holes and to use new law enforcement mechanisms such as active defences. Any country whose laws or security technology are out of date is at risk of becoming an unwitting haven for cyber-attacks.

4.2 Defining cyber-terrorism

4.5 Achieving the international cooperation necessary to fight cyber-terrorism will require broad international agreement, both about what cyber-terrorism is, and about which means should be legally available to fight it.

4.6 "Terrorism" itself is notoriously difficult to define. One person's terrorist often is another person's freedom fighter; some nations have called other nations' military actions "terrorist"; and some call "terrorist" what others call protected speech. In cyberspace, it is clear that no international agreement will be able to fully resolve such political disagreements. One solution to this dilemma might be to follow the example of the International Civil Aviation Organization (ICAO). Just as ICAO criminalizes hijacking regardless of its political motives, an international agreement could define cyber-terrorism in terms of actions, regardless of their political content.

4.7 There are many other questions that are inevitably raised in attempting a definition of cyber-terrorism, due to the complexity of cyberspace and international law. Consider the following examples:

- Escalation – Does rhetoric about terrorism increase the risk of war?
  - ➢ In May 2001, after a Chinese fighter and a US reconnaissance plane collided, Chinese hackers launched a series of attacks on US computers.

[21] http://www.heritage.org/bookstore/2002/defense/HomelandDefenseweb.pdf

[22] http://online.securityfocus.com/news/319

- Since 1999, hackers in Pakistan and India have exchanged an increasing number of cyber-attacks, mainly attempting to deface websites, a few trying to steal sensitive data.[23,24]

Some media reports described these attacks as "cyber-terrorism" or "info-war". Equating them with terrorism, however, may exacerbate tensions between nuclear powers. Efforts to address them should defuse tension and avoid unenforceable promises.

- Are anti-terrorist measures appropriate for large-scale economic crimes?
  - In May 2000, Philippines investigators assisted by FBI computer experts arrested the creator of the "Love Bug" virus, which caused an estimated several US billion dollars of worldwide damage.[25]
  - In February 2002, controversy and legal challenges greeted the arrival of US Special Forces to assist Philippine forces against the Abu Sayyaf terrorist group.[26]

Defining a computer crime as terrorism may not always increase global cooperation, since many countries are happier to welcome civilian computer experts than to accept help perceived as a foreign military intervention. Any agreement defining viruses as terrorism needs to address these concerns.

- How do we avoid punishing bystanders?
  - In February, 2002, Mr. Lofti Raissi was freed after five months in a British prison. Once accused of helping in the attacks of 11 September 2001 against US interests, he now faces only minor charges.[27]
  - Several US universities have received complaints after student computers were penetrated by outside hackers and used to launch denial of service attacks.

The more broadly we define terrorism, the greater the risk of punishing uninvolved bystanders. Anti-terrorism investigations often use detentions without trial and unusual punishments for minor criminals caught in dragnets. For computer crimes, this risk is compounded by the difficulty of distinguishing perpetrators from people unaware that their systems or passwords had been compromised. Many nations would not want to extradite students for failing to secure their computers.

- How do we distinguish accidents from terrorism?
  - The USD 1billion Mars Observer was rendered useless by a single software bug.
  - Aum Shinryko, a Japanese cult that killed 12 people in a terrorist attack in 1995, developed software for over 80 Japanese firms.[28]

Anti-cyber-terrorism authorities must also address that unintentional programming errors might be confused with terrorist attempts.

- How do we reconcile different national definitions of human rights?

In the past, some nations have defined groups as terrorist whose primary activity was to report human rights violations, and some have prohibited forms of speech that are constitutionally protected in other

[23] "Cyber Attacks During the War on Terrorism: A Predictive Analysis", Institute for Security Technology Studies at Dartmouth College, September 21, 2001, http://www.globaldisaster.org/cyberattacks.pdf

[24] Dorothy Denning, "Activism, Hacktivism, and Cyber-terrorism: The Internet as a Tool for Influencing Foreign Policy," Information Technology and American Foreign Policy Decision making Workshop, February 04, 2000, http://www.infowar.com/class_2/00/class2_020400b_j.shtml

[25] Raju Chebium, "Love Bug virus raises spectre of cyber-terrorism", CNN.com, http://www.cnn.com/2000/LAW/05/08/love.bug/

[26] Rufi Viligar, "Legal Cloud over Philippine-U.S. War Games", CNN.com, http://www.cnn.com/2002/WORLD/asiapcf/southeast/02/20/ret.phil.us/index.html

[27] Alan Cowell, "Algerian Pilot Says Detention Has Made Him a Sept. 11 Victim," New York Times, February 16, 2002, http://www.nytimes.com/2002/02/16/international/16PILO.html

[28] Dorothy Denning, "Is Cyber Terror Next?" Social Science Research Council, November 1, 2002, http://www.ssrc.org/sept11/essays/denning.htm

nations. A global definition of cyber-terrorism must consider the need to protect human rights and the difficulty of getting nations to agree on what forms of speech should be tolerated.

4.3 What can be achieved through international cooperation?

4.8 Answering the above questions may seem difficult. The difficulty, however, only increases the importance of working towards an international agreement. As long as there are no international mechanisms for fighting cyber-attacks, a nation under attack will have to go beyond the international system to respond—either by tolerating attacks and doing nothing, or by acting unilaterally in way that might violate other nations' laws or that might escalate a cyber confrontation into physical warfare. International cooperation can reduce the risk of either of these undesirable outcomes. In addition to preventing attacks, cooperation can reduce tensions by proving a stable, diplomatic forum for nations to work out disagreements.

4.4 Other areas impacting infrastructure

4.9 Since CNIs deal with important information relating to national security and economies, there may be other network areas that also influence them. In order to prevent such networks from interfering with critical CNI data, and to ensure security, two possible constructive steps could be taken.

A. •Complete separation of the CNI from other network areas

4.10 The first method would involve ensuring complete separation of the critical network from other network areas. In other words, by separating networks that exchange less confidential information from the critical network, the net result will be heightened security. The US Govnet[29] is an example of such independent government administrative network that is planned to be a private voice and data network based on the Internet protocol (IP), but with no connectivity to commercial or public networks. One requirement for Govnet is that it must be able to perform functions with no risk of penetration or disruption from users on other networks, such as the Internet. To ensure security of critical data, organizations such as the CIA, the Pentagon or the Korean Ministry of National Defense are applying such separation methods to their network operations. The concept of constructing a CNI network that is entirely independent from the existing network maximizes the security of critical data. However, one downside of the concept is that it poses limitation to user access depending on the location and situation.

B. •Heightened security for other network areas related to the CNI

4.11 As stated previously, in order to ensure complete security of critical data such as information on national security, CNI networks are constructed separately, thus blocking all possible intrusions through other open networks. However, it would be virtually impossible to set up separate networks for every CNI. For most commercial or financial networks, CNI co-exists with the Internet, or even when built separately, it is usually interconnected with other networks for optimal data access. Although interconnected networks pose a threat to CNI security, they are realistically necessary to exchange information efficiently. Therefore, it is required to ensure further security by applying security policies and technologies at access point level or end-to-end level.

4.12 For this purpose, the CNI system must be able to provide high-level security for its critical information whenever there is a data access request from other network areas. Such methods include providing users who are allowed access to firewall, VPN (virtual private networks), and CNI with specific certification, or tightly applying security technologies, as discussed in Chapter four. For instance, an important system such as the EIS (executive information system) in a CNI could tighten security for specific data by managing data according to its level of confidentiality or by allowing differential data access according to users' level of authorization.

4.13 Whether to integrate or separate the network elements connected to CNI is also a very important issue. This can vary according to the network structure and the existing state of usage. If possible, the most effective method would be separating and providing high-level security for the CNI. However, if it is impossible to separate the CNI, or if such actions result in hampering user access, a more flexible form of action, such as expanded application of the CNI security area may be recommended.

[29] http://www.vnunet.com/News/1126080

5. Conclusion and areas for further study

5.1 Conclusion

5.1 It is very difficult to measure the extent to which IT (information technology) affects our lives today. Info-communication has played a significant role in societies and economies across the world and their interdependency is growing. In spite of the fact that the international networks transmit an enormous amount of important data with regard to national security or economic development, international infrastructures remain relatively vulnerable. Consequently, it is essential to modify and reinforce the security of those network systems that deal with confidential information, such as that having a high financial value or relevance for national security.

5.2 A CNI may be a public or private network. The distinguishing factor is that it carries information relevant to national security and safety or information of high financial value. Although the reliability of the CNI is significant for political, economical, and social systems, there is a lack of awareness of CNIs and no specific definition or scheme for ensuring their reliability. Intensive R&D activity and international cooperation regarding CNI security issues are therefore essential.

5.3 CNIs can be roughly classified into two categories: those that are completely independent and separate, those that are connected to other networks. The latter are becoming more common and therefore it is necessary to take a holistic approach to security issues.

5.4 As information technologies develop, networks become increasingly global and their degree of interconnection becomes more complex. Although many international organizations have prepared policies aimed at providing systematic legal protection, there is a lack of investment in CNI security and a lack of standardization. The necessary steps involve more research and greater standardization. At the same time, it is necessary to raise awareness over the indispensability of a CNI security system. Accordingly, it is urgent that common security issues be analysed, and solutions be developed through international support and cooperation.

5.2 Areas for further study

5.5 The following is a set of suggested principles for enhancing trust in CNIs:

- Establish detailed standards to distinguish between CNIs and non-CNIs.
- Classify CNI infrastructures, analysing those CNI systems in operation in order to understand their status and to assign them to a particular category.
- Analyse the vulnerable aspects in CNIs by category and prepare possible steps to enhance security for each category.
- Legislate an internationally certified warranty policy for CNI security and establish a specific standard for the security being applied for particular CNIs, in order to guarantee a certain level of service for users

5.6 Suggestions for the possible role to be played by ITU in this field are as follows:

- Establish security management standards at the international level in order to apply general security principles for CNI;
- Establish standards for security policies and technologies in order to guarantee the reliable and efficient operation of networks, both for independent and interconnected CNIs;
- Identify examples of CNI best practice.