A2005:015

IT Security in the USA, Japan and China

Martin Ahlgren,
Magnus Breidne,
Anders Hektor

itps SWEDISH INSTITUTE FOR GROWTH POLICY STUDIES

IT Security in the USA, Japan and China

- A Study of Initiatives and Trends within Policy, R&D, Industry and Technology

Martin Ahlgren
Magnus Breidne
Anders Hektor

SWEDISH INSTITUTE FOR GROWTH POLICY STUDIES

ITPS, Swedish Institute For Growth Policy Studies
Studentplan 3, SE-831 40 Östersund, Sweden
Telephone: +46 (0)63 16 66 00
Fax: +46 (0)63 16 66 01
E-mail info@itps.se
www.itps.se
ISSN 1652-0483
Elanders Gotab, Stockholm 2005

For further information, please contact Martin Ahlgren
Telephone + 46 70 304 37 56
E-mail martin.ahlgren@itps.se

Foreword

The Information Society is becoming a more and more important part of society in general, and reliable information technology infrastructures and applications are becoming important for sustainable economic growth. Several critical infrastructures in society are also interlinked with the cyber infrastructure. Computing, communications, and storage resources worldwide have continued to grow but unfortunately computer security incidents have also continued to show parallel growth patterns. Current approaches to IT security are also considered insufficient and policy formulation includes several different possibilities and challenges.

The following report gives an overview of information technology (IT) security in the USA, Japan and China, with the primary focus on the USA. The report includes an analysis of IT security in a broad context including policy, research and development initiatives, industrial trends, the impact of information security, organizational processes, security threats and technology segments. However the main focus is on the implications for technology, research and development. A short overview of IT security initiatives in Sweden is also included.

The aim of this study is to provide input to VINNOVA (The Swedish Agency of Innovation Systems) regarding different trends of importance for the funding of IT security R&D and to the Swedish formulation of IT and innovation policy. The report has mainly been written by Martin Ahlgren. Anders Hektor has written all the content about Japan, and Magnus Breidne about China.

Östersund, October 2005

Sture Öberg
Director General

Table of Content

Summary

Improving information and IT security is important because dependence on different information systems and IT networks is increasing within the whole of society and the cost of IT-related incidents is significant. A broad top-down approach regarding IT security including regulation, R&D, standardization & certification, organizational processes and threats is used in this report so as to identify factors of importance for growth in the IT security industry and for the improvement of IT security in Sweden. Several different policy options exist and an appropriate balance between short-term administrative and organizational initiatives and long-term initiatives such as R&D is necessary in order to create improved IT security.

One fundamental characteristic of IT security is the international dimension, which increases the importance of international perspectives such as those covered in this study. The need for further international initiatives is also expressed in the Swedish IT Policy Government Act of 2005[1]. This study of IT security in the USA, Japan and China focuses on policy and R&D perspectives adding additional dimensions to the Swedish policy formulation not covered by other reports[2].

This report concludes that cyber security in the USA is considered to be an area of low priority compared to other Homeland Security issues. However the investment in safety and security applications based on IT is significant and the integration of IT security and physical security is an important trend. The annual federal budget in the USA for cyber security R&D is about 200 million USD and the annual budget for IT related Homeland Security projects is approximately 10 billion USD.

Japan has given IT security policy high priority including a specific office in the cabinet office. The policy and R&D of relevance to IT security in the USA is divided between cyber security, information security and critical infrastructure protection and their Critical Infrastructure initiatives are ahead of several other countries. In China too great dependence on foreign IT security suppliers is considered a threat to national security and one of the most important issues in China is to develop their own basic software.

It is important to recognize that legislation with an impact on information security is one of the most important reasons for increased investment in IT security in both USA and Japan. In the USA initiatives for risk and cost-benefit analysis for the prioritization of initiatives are important. Certification initiatives such as Common Criteria are getting more requested for Critical Infrastructure systems but China has several national standardization initiatives for IT security.

To facilitate R&D IT security test beds are considered an important initiative, and security as a service is one direction for development in the future. New methods

[1] *The Swedish Government: Från IT-politik för samhället till politik för IT-samhället, proposition 2004/05:175*

[2] *SOU 2005:71; Swedish National Post and Telecom Agency: PTS-ER-2005:7; Swedish Emergency Management Agency: Samhällets informationssäkerhet, lägesbedömning , 2005; VINNOVA: Förslag till en nationell strategi för säkerhetsforskning, 2005*

for designing and engineering secure systems including R&D areas such as Vulnerability Analysis and Code Scanning tools are also important. In the USA new secure networks have been created because the Internet does not provide sufficient security. However, the priority of IPv6 especially in China could be of benefit to the country in the future.

Swedish work on the formulation of an IT security base level could learn from the initiatives in the USA based on the Federal Information Security Management Act (FISMA) of 2002. Instruments to consider for the evaluation and tracking of progress are e.g. IT security guidelines, reporting requirements on agency compliance, best practice and IT security metrics.

Initiatives for IT security awareness is considered important in Sweden, however, learning from the initiatives in other countries should be an integral part of on-going work in Sweden. In the US awareness certification programs for organizations have been launched, cyber security training for school children is increasing in a larger number of schools and the National Science Foundation is funding R&D within human computer interface for security. Japan too has prioritized initiatives such as IT security training for young people.

Administrative and legal initiatives for improved IT security in Sweden need to be combined with appropriate R&D initiatives. New approaches are considered necessary to protect computer systems and networks. The available technology is considered not to provide sufficient protection. The US National Science Foundation established a Cyber Trust R&D programme in 2004. Different initiatives relating to IT security at Swedish agencies need to consider the importance of fundamental IT security R&D.

Several sources indicate that a more systems-based approach to IT security, including a holistic end-to-end architecture, is important. Today’s specialized products are considered not to provide sufficient integration and there is a broad consensus among computer scientists that the approach of patching up in order to add security is not suitable in the long run. R&D issues include e.g. distribution and definition of security policies in the network. Swedish telecom system knowledge could be an advantage for the creation of a systems approach for secure cyber infrastructures. A systems-based approach to IT security is a possible Swedish focus area.

Sammanfattning

(Summary in Swedish)

Förbättringar av informations- och IT säkerhet är viktigt därför att beroendet av olika informationssystem och IT-nätverk ökar inom många samhällssektorer. Dessutom ökar kostnaderna för IT relaterade incidenter. I denna rapport används en bred ansats för studien av IT-säkerhet omfattande faktorer som reglering, FoU, standardisering & certifiering, organisatoriska processer och hot för att kunna identifiera olika faktorer som påverkar och kommer att påverka tillväxten inom området IT-säkerhet samt förbättringen av IT-säkerheten i Sverige. Flera olika policyalternativ finns för att skapa en förbättrad IT-säkerhet men det krävs en lämplig balans mellan administrativa samt organisatoriska åtgärder och långsiktiga initiativ som FoU-satsningar för att åstadkomma en varaktig förbättring av säkerheten.

En viktig egenskap för området IT-säkerhet är den internationella dimensionen vilken ökar behovet av internationella perspektiv av vilka ett antal belyses i denna studie. Behovet av bland annat ytterligare internationell samverkan uttrycks också i IT-propositionen från 2005[3]. Denna studie av IT-säkerhet i USA, Japan och Kina är inriktad på satsningar inom politik och FoU och kan bidra med underlag till den svenska politikutformningen samt komplettera andra studier inom området[4].

I denna rapport konstateras att cybersäkerhet i USA är ett område med låg prioritet jämfört med andra delar av den inhemska säkerheten (Homeland Security). Satsningarna på säkerhetslösningar baserade på IT är emellertid omfattande i USA och integrationen mellan IT-säkerhet och fysisk säkerhet är en viktig trend. Den årliga federala budgeten i USA för FoU inom IT-säkerhet är cirka 200 miljoner USD vilket kan jämföras med den årliga budgeten för IT-relaterade projekt med inriktning på Homeland Security på cirka 10 miljarder USD.

I Japan prioriteras området IT-säkerhet vilket visar sig bland annat genom att IT-säkerhetsfrågorna hanteras av en egen enhet inom regeringskansliet. Politikutformningen av relevans för området IT-säkerhet är i USA uppdelad i områdena cybersäkerhet, informationssäkerhet samt skydd för kritiska infrastrukturer. Inom området skydd av kritiska infrastrukturer ligger USA före flera andra länder. I Kina anses det alltför stora beroendet av utländska leverantörer av IT-säkerhet vara ett hot mot den nationella säkerheten och en av de mest centrala frågorna i Kina är utvecklingen av egen grundläggande mjukvaruteknik.

Lagstiftning som påverkar området informationssäkerhet är en av de viktigaste anledningarna till de ökade investeringarna i IT-säkerhet i både USA och Japan. I USA är initiativ för prioritering av insatser baserat på risk- och cost-benefit-analys

[3] *The Swedish Government: Från IT-politik för samhället till politik för IT-samhället, proposition 2004/05:175*

[4] *SOU 2005:71; Swedish National Post and Telecom Agency: PTS-ER-2005:7; Swedish Emergency Management Agency: Samhällets informationssäkerhet, lägesbedömning , 2005; VINNOVA: Förslag till en nationell strategi för säkerhetsforskning, 2005*

viktiga. Certifieringsinitiativ såsom Common Criteria efterfrågas för system som används i kritiska infrastrukturer. Kina har dock ett flertal nationella initiativ inom både standardisering och certifiering av IT-säkerhetsteknik.

För att underlätta FoU anses testbäddar för IT-säkerhet vara ett viktigt initiativ. En utvecklingsinriktning framöver är tjänster inom området IT-säkerhet. Ett viktigt FoU område är också nya metoder för design och utveckling av säkra system omfattande t ex. sårbarhetsanalys och verktyg för kontroll av mjukvarukod. I USA skapas nya säkra nätverk på grund av att Internet inte erbjuder tillräcklig säkerhet men prioriteringen av IPv6 i speciellt Kina kan bli en fördel för landet framöver.

Det svenska arbetet med att formulera en basnivå för IT-säkerhet skulle kunna lära av initiativ i USA baserade på lagen Federal Information Security Act från 2002. Initiativ som borde beaktas för utvärdering och uppföljning av införandet av lösningar för IT-säkerhet är t ex. krav på rapportering av nivån för IT-säkerheten hos myndigheter, guider för IT-säkerhet, mätetal för IT-säkerhet samt exempel på bra införande.

Initiativ för att öka medvetandet om IT-säkerhet anses vara viktiga i Sverige, men ett kontinuerligt lärande av erfarenheterna från andra länder borde vare en integrerad del i arbetet. I USA har program för certifiering av medvetandet om IT-säkerhet lanserats, initiativ för utbildning av skolelever sprider sig och National Science Foundation finansierar FoU inom området användargränssnitt för IT-säkerhet. Även Japan prioriterar initiativ som t ex. utbildning av ungdomar inom IT-säkerhet.

Administrativa och legala initiativ för förbättrad IT-säkerhet i Sverige måste kombineras med lämpliga FoU satsningar. Nya ansatser för att skydda datorsystem och nätverk anses i USA vara nödvändiga att utveckla. Tillgänglig teknologi erbjuder inte tillräckligt skydd. National Science Foundation i USA etablerade FoU-programmet Cyber Trust år 2004 för att driva på utvecklingen. Svenska initiativ inom området IT-säkerhet bör beakta vikten av grundläggande FoU inom IT-säkerhet för att skapa långsiktig IT-säkerhet.

Ett flertal källor pekar på behovet av en mer systembaserad ansats till IT-säkerhet omfattande en arkitektur för helheten inkluderande användare, nät och applikationer. Dagen specialiserade produkter anses erbjuda otillräcklig integration och det finns en konsensus bland datorforskare att dagens ansats baserade på så kallad Patchning för att åstadkomma IT-säkerhet är långsiktigt otillräcklig. FoU-problemen omfattar bland annat distribution och definition av IT-säkerhetspolicy i näten. Svenskt systemkunnande inom telekom skulle kunna vara en fördel för skapandet av en systembaserad ansats för en säker Internetinfrastruktur. En systembaserad ansats till IT-säkerhet är ett möjligt svenskt fokusområde.

1 Introduction

1.1 Growth Policy Perspectives

The Information Society is becoming a more and more important part of society in general. The functioning of cyberspace is essential to the economy and national security (White House 2003A). Because of the productivity gains of information technology (IT) almost every sector in society is dependent on its IT infrastructure. A reliable information technology infrastructure is important for sustainable economic growth. Information Technology (IT) is a main driver of economic growth according to several studies[5], and full utilization of the productivity potential of IT requires organizational and user confidence in information technology services and solutions. Because of today's security vulnerabilities the full potential of IT is not always utilized by organizations. The purpose of IT security products and services is to manage risks associated with use of information technology. Creating user confidence and trust in IT is a complex issue which includes several different challenges. Strengthening information security, network security, privacy and consumer protection is considered important for the further development of the Information Society.

Risks associated with technological development are of importance for society and risk is a core policy issue. The number of risk-related motions before the Swedish parliament increased three times during the period 1964 to 1994 (Ekonomisk Debatt 2003A). Money is invested in solutions for risk reduction including safety and security solutions, and it is important to understand the risks related to information technology and possible action to manage the risk. The risk perception of information technology[6] and the risk compared to other technologies are policy issues that have an impact on the need for regulation and other policy actions (HHS 2002A). The risks relating to information technology can also be managed in other ways such as portfolio management (MIT 2004A). Interest in assessing and managing risks associated with technologies has also increased over recent years because of incidents such as terrorist attacks (RAND 2004A).

A large part of the cyber infrastructures in several countries is controlled by private entities, which makes the policy process complex and public-private partnerships very important. The global nature of the Internet and the potential to launch attacks from other countries makes law enforcement particularly complicated, and increases the need for international cooperation. Several critical infrastructures are also interlinked with cyber infrastructure. Computer networks control physical objects such as electrical transformers, trains, pipeline pumps, radar and the stock markets. Developments over recent years show that criminality will move into the digital society if the law enforcement capabilities not are in place (ISPC 2005A, White House 2003A). Policy for IT security can be seen as one part of the policy

[5] *Such as Brynjolfsson, E., Information Technology and Productivity: A review of the Literature, Massachusetts Institute of Technology.*

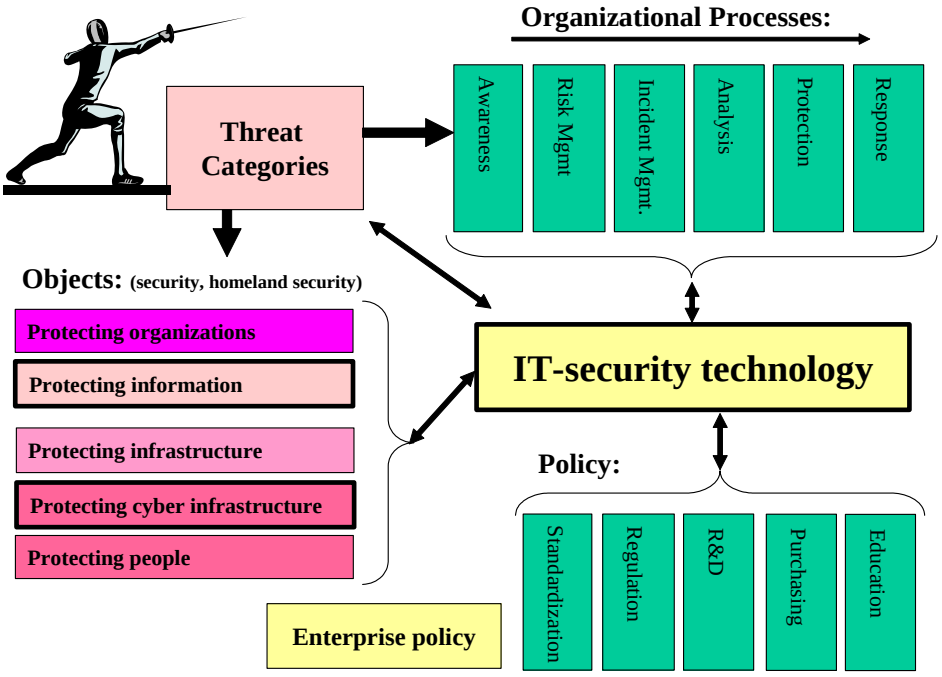
[6] *Sjöberg, Lennart, Perceived information technology risks and attitudes, Center for Risk Research, Stockholm School of Economics, SSE/EFI Working Paper No 2002:5.*

framework for crisis management which is becoming more and more important on the policy agenda also in Sweden, because of different incidents in Sweden and other countries in recent years. The number of IT incidents and the amount of industrial espionage is also increasing. Several different policy instruments for IT security do exist such as regulation to increase the requirements on companies, investment in R&D for long term improvements of the information infrastructure, and a market-based approach which includes instruments such as product liability and cyber security insurance policies.

1.2 Dependence on Information Systems

Information is one of the most important and valuable resources any organization controls, and a majority of the information is managed by information systems. The number of knowledge-based organizations is also increasing, and intellectual property is often an organization's most valuable asset. The business of several organizations is based on information. Information security is also evolving from a firewall activity into a broader IT risk management role. The purpose is to reduce the organization's risk exposure. Information security is of importance for several different organizational processes and can be an integral part of all processes. Information security is not an engineering discipline: only about 10 percent is about technology, the rest is about policy and processes (ISPC 2005A). Over recent years new federal regulation in the USA and other countries has been a very important driver for the implementation of new IT security solutions to protect digital information. Information security is becoming a more important management priority and has become a top priority for several public and private sector organizations.

Figure 1 A Conceptual Overview to IT Security – Threats, Objects, Processes, Policy and Technology.



Source: ITPS

Computing, communications, and worldwide storage resources continued to grow. The global information technology infrastructure has undergone a dramatic transformation during the last decade. Unfortunately, computer security incidents and threats continued to show parallel growth patterns. The frequency, impact and cost of cyber security incidents are continuously increasing. The total number of attacks is increasing by over 20 percent annually (PITAC 2005A). IT infrastructure is to a large extent based on the Internet with attributes such as openness, inventiveness and an assumption of good will. However, the attributes of the Internet have made it a target for criminals. The "ubiquitous interconnectivity results in widespread vulnerability" (ISPC 2005A). As the use of the Internet for commercial purposes continues to grow, so do the opportunities for its abuse by criminals. Organizations need help to protect against the increasing risk of incidents such as identity theft, corporate espionage, data pirating, information security breaches and cyber terrorism. The data can be stolen or corrupted and criminals can destroy business value. Today's computer systems are often so complex that functionality and security cannot easily be guaranteed. The operating systems, the applications and networks can all be attacked by using known bugs, design approaches, weaknesses in platforms, unsecured communications paths and poor programming techniques. The current technology approaches are also considered inadequate.

Security can be considered a cost or an investment with an expected return on investment. But security constraints are often a short-term bottleneck for the user or the operation, which is a reason for the traditionally low priority assigned to information security. The motivation for usage and investment in security can be low if the probability of threats is not high enough, and if regulation does not force investment. It is also often difficult to estimate the probability of different incidents and the potential cost which makes investment decisions even more difficult.

1.3 Definitions

Trust is a broad concept including several different factors such as information systems security. According to US National Security Telecommunications and Information Systems Security Instruction (NSTISSI) information systems security is defined as "the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats". IT security is one area that is necessary for the securing of information systems. In this report IT security is defined as technology, solutions and services for the purpose of securing the digital infrastructures and different nodes connected to the networks. The nodes can be e.g. computer systems, power grid control systems, a car, a weapon system, a wireless phone, information databases, or other devices. IT security is more of a systems engineering segment than a specific technological area. Secure IT systems are created by combining several different technological components such as intrusion detection systems, firewalls and authentication solutions. The term cyber security, including different aspects of protecting Internet and Internet traffic, is very common particularly in the US and is consid-

ered an important part of IT security. IT security is used in this report with the same meaning as information and communication technology (ICT) security.

Table 1 Concepts and Terms, an overview

Concepts	Comments
Trust in IT	Including e.g. education, policy, usability, technology
Information Security	Protecting the information
IT security	Protecting e.g. networks, information systems
Cyber Security	Protecting the cyber infrastructure and nodes
Homeland Security	A broad concept complementing National Defense
Critical Infrastructure (CI) Protection	Protection of e.g. roads, railways, power grids
Security & Safety prod. based on ICT	Border protection, container trackning, pipeline monitoring
Sensor Networks	Generic technology for productivity improvements

Source: ITPS

Technology used for protection against physical intrusion such as security and safety products based on ICT is not a primary part of this study. Security and safety applications based on ICT include e.g. sensor networks for border protection, RFID for container screening and tracking, long range radar for aircraft detection and sensors for pipeline monitoring systems. It is important to recognize the difference between IT security and IT used in security and safety solutions. The general security market is using more and more ICT solutions to facilitate the protection of different objects. However, safety and security applications based on sensor networks are just one of several different application areas for sensor networks. Sensor networks can be classified as a generic technology for productivity improvements. However, issues such as the convergence of digital and physical protection are of interest for this study. Information systems security as a major driving force for IT security is also very important. New regulations have transformed IT security into an issue of corporate governance. The report covers both legal, administrative and technology aspects of IT security. However, the main focus is on the implications for technology. A common objective is that security should be designed in from the beginning. IT security could also be seen as part of an overall quality framework.

1.4 Purpose

This report includes an analysis of IT security in a broad context including policy initiatives, R&D programmes, industrial trends, the development of standard, organizational security processes as a major driver for IT security, threat categories and some technological segments. All the different aspects are important for the development of IT security policy and the funding of IT security R&D. A previous ITPS report Homeland Security and R&D in the United States[7] gives an overview of US initiatives within Homeland Security. The geographical focus of this study is primarily USA, but initiatives in Japan and China are also included. Different Swedish initiatives are also covered in order to be able to draw appropriate conclusions. The aim of this study is to provide input to VINNOVA (The Swedish Agency of Innovation Systems) regarding different aspects of importance for the

[7] *ITPS report A 2003:014*

funding of IT security R&D. The development of relevance to the Swedish formulation of IT and innovation policy are also covered. A good understanding of the international initiatives and trends within IT security facilitates the formulation of a Swedish funding strategy for IT security R&D, and functions as an input to the formulation and implementation of IT policy. The objective is to identify those trends and initiatives such as particular R&D- and technology areas within IT security that are expected to be important for the improvement of IT security and growth of the Swedish IT security industry. This study is based on different kinds of reports, conferences and interviews with members of academia, industry and policy. The report has mainly been written by Martin Ahlgren. Anders Hektor[8] has written all the content about Japan and Magnus Breidne about China.

[8] *Shigeyuki Naito and Naoko Sekiguchi at ITPS in Japan have provided support to Anders Hektor.*

2 IT Security in Sweden

This chapter includes a brief overview of some different Swedish and European initiatives within policy, academia and industry to promote information- and IT security research, development and usage.

Several different policy issues relating to IT security exist in Sweden, such as organizational responsibility (SOU 2005:71), Internet security (Regeringen 2005A), the funding of security R&D (VINNOVA 2005A) and information security at Swedish government agencies (KBM 2005A).

Policy Initiatives

- **ITPS evaluation of the Swedish IT policy**. The Swedish Institute for Growth Policy Studies (ITPS) published a report about IT and trust in 2003 (ITPS 2003A), the report was a part of an evaluation of the Swedish IT policy. The report concludes that it is difficult to define trust in IT and that it is usually interpreted as IT security. The report proposes the use of the IT policy instrument reliability. The study also proposes that a study regarding the use of reliability labelling for different solutions be enacted in Sweden. The possibility of having an IT Ombudsman to manage different issues relating to trust is also discussed in the report. R&D and technology aspects of trust are not covered by the report.
- **A study about trust in IT by the Swedish IT Policy Strategy Group.** The Swedish IT Policy Strategy Group at the Ministry of Industry, Employment and Communications published a report about trust in IT and the Internet in 2004. The report covers issues such as the importance of trust for IT policy, different interpretations of trust and possible policy implications. The report concludes that general initiatives are not the most important component for the government to increase trust. The proposals discussed in the report include e.g. information about IT security for the public, requirements for public procurement, the creation of an Internet Ombudsman and more focus on IT crime. The report does not include any major international benchmark studies and research, and development implications are not considered in the report (CEPRO 2004A).
- **The Ministry of Defence study of Information Security.** The Ministry of Defence initiated its Information Security Investigation (InfoSäkutredningen) in 2002. The purpose of the assignment was to create a proposal for the development of a national strategy for information security; the assignment included different aspects of signal defence. A sub report titled Secure Information (Säker information, SOU 2005:42) was published in May 2005; a previous sub report was SOU 2004:32. The final report (SOU 2005:71) was published in September 2005. There is a need for a coordinated policy and responsibility within information security according to the investigation. The investigation proposes that responsibility for coordination of policy and administrative information security should be assigned to the agency KBM. Responsibility for co-ordinating technical information security should be assigned to a new gov-

ernment agency (Institutet för signalunderrättelsetjänst och teknisk informationssäkerhet) based on competence at FRA according to the study SOU 2005:71. The study also proposes that responsibility regarding Common Criteria be transferred from Swedac to KBM, and that an R&D programme for information security including annual funding of SEK 10-15 be developed at KBM.

- **EU policy recommendations about ICT.** The report *Rethinking the European ICT Agenda – Ten ICT-breakthroughs for reaching Lisbon goals* (PWC 2004A) was published in 2004 by the Ministry of Economic Affairs in the Netherlands. The report concludes that: "A crucial condition for a broad deployment and use of ICT by business and consumers is user confidence". The EU needs to create liabilities, give priority to cyber crime, and ensure the availability of critical infrastructures. According to the report "improvements of user confidence is of high relevance for realising the Lisbon goals". ICT is considered to be an important driver for growth.
- **The Swedish IP policy Act of 2005.** A new Swedish IT Policy Government Act was published in July 2005 (Regeringen 2005A). Availability and security is one of three objectives defined in the Act. A strategy for a more secure Internet based on physical and logical infrastructure, information, further knowledge and international co-operation needs to be developed according to the document. A new law for Swedish Internet top domains is proposed, and is considered important for Internet security. The aim of the law is to establish secure and efficient administration of the national top domains and to enable government control of the administration.
- **Gender aspects.** Gender aspects of trust in IT also have policy implications. According to a study published by the Swedish Internet Infrastructure foundation (II-Stiftelsen), men have a greater trust in the Internet than women. Thus, according to the study here is a significant gender difference. Of women 60 percent are afraid to use the Internet for security reasons compared to 47 percent of men (IIS 2005A).
- **Other policy initiatives.** Regulatory requirements on suppliers of communication services to register and store Internet traffic have been discussed in different EU member states. The aim is to facilitate different kind of criminal investigations, but the privacy concerns are also on the policy agenda.

Government Agency Responsibilities

- PTS, the Swedish National Post and Telecom Agency, has a responsibility for electronic communications. The department for network security at PTS includes the Swedish IT Incident Centre (SITIC) with the responsibility for incident management and reporting. The staff at SITIC includes about 18 employees. PTS also works on initiatives such as the project Safe Surfing including outreach to the public. In February 2005 PTS published a report proposing different ways to secure the Internet infrastructure (Strategi för att säkra Internets infrastruktur) (PTS 2005A). The report proposes e.g. regulation of the

Internet infrastructure leading to increased government control, outreach activities to increase security awareness, national and international co-operation on IT incidents and co-ordinated research into different aspects of Internet security with the focus on information security aspects of the Internet.

- KBM, the Swedish Emergency Management Agency, is co-ordinating the development of crisis management for Swedish society. KBM has a special unit working with IT security which provide services such as training. Different newsletters and reports about IT security are also published. The agency provides a recommendation, not mandatory, for a basic level for IT security (BITS – Basnivå för IT-säkerhet) to be used by federal, regional and local government. KBM is also required to publish an annual study of information security. KBM has also published a report about IT- and Information Security and Malicious Code at some Swedish government agencies (KBM 2005A). The report proposes that there is a need for more co-ordinated governance for IT security at the agencies. Too many agencies today have responsibility for different tasks within IT – and information security - and there is a lack of co-ordination, the study proposes consolidation of responsibility. The implementation of a mandatory standard for information security at the agencies also needs to be considered according to the study. KBM is also funding R&D with an annual budget of about SEK 58 million.
- FMV, the Defence Materiel Administration, has an assignment to establish a certification procedure for Common Criteria, a standard for IT security certification. Advanced certification based on Common Criteria is today mostly an issue for National Security Systems.
- FRA, the National Defence Radio Establishment, has responsibility for provide technical competence and support within information security to assist initiatives in case of national IT incidents. The agency is also involved in different kinds of technical support, performance of IT security penetration tests and other tasks.
- The Swedish Consumer Agency is also involved in different initiatives to improve cyber security. The agency has required increased responsibility by industry to protect the consumers; the agency is considering further regulation as an alternative.
- The Swedish Government Act 2001/02:10 defines a need for an evaluation and certification system for products. In 2002 Swedac signed the Common Criteria Recognition Arrangement for the recognition of Common Criteria certified products.
- The status for the usage of different IT security solutions in Sweden is studied by the government agency Statistics Sweden (SCB – Statistiska Centralbyrån). In Sweden programs for virus control were used by 92 percent of companies with more than ten employees in 2004 compared with 85 percent in 2003. Firewalls were used by 69 percent of companies, data storage outside the premises by 59 percent and data encryption by 22 percent of companies according to SCB (SCB 2004A).

Research & Development Funding

- The European Commission has identified the need for further security R&D. "Political, societal and technological developments have created a fluid security environment where risks and vulnerabilities are more diverse and less viable" (EU 2004A). The European Commission launched the three-year R&D program Preparatory Action for Security Research (PASR) in 2003 including about EURO 65 million for funding during the period 2004 to 2006. The programme is a first step towards a new security R&D programme from 2007. The European Commission adopted a communication (Security Research: The Next Step) (EU 2004A) concerning the new European Security Research Programme (ESRP) in 2004. The communication was based on the proposal *Research for a Secure Europe a report of the Group of Personalities in the field of Security Research*. ESRP will form part of the 7th EU Research Framework Programme for 2007 to 2010. The European Security Research Advisory Board has advised the EU on the possible content and implementation of the ESRP in 2005.
- VINNOVA (Swedish Agency for Innovation Systems) in co-operation with e.g. FOI and FMV published a proposal for a Swedish security research and development programme (VINNOVA 2005A) in February 2005. The proposal includes R&D funding of SEK 150-200 million to be co-ordinated by KBM, resources for participation in US security R&D programmes and increasing initiatives to strengthen the competence of government acquisition of security solutions including the development of e.g. technical requirements. VINNOVA does not have any particular R&D programme for IT security today or a strategy for funding of IT security R&D.
- The Knowledge Foundation (KK-Stiftelsen) has founded a research project at Karlstad University with SEK 6.5 million concerning secure telephony on the Internet with particular focus on SS7 signalling over the Internet. The Swedish IT Security Network for PhD Students (SWITS) is also funded by the foundation.

Some Research & Development Activities

- SecLab at Stockholm University is a laboratory for research into computer security and security informatics. SecLab includes about ten employees and PhD students. Research areas are e.g. management of information security, intrusion detection systems and Common Criteria application research. Other major Swedish R&D centres for IT security are e.g. SICS.
- The conference IEEE 6th International Workshop on Policies for Distributed Systems and Networks was held in Stockholm at the beginning of June 2005. The aim of the conference was to bring leading researchers and industry experts together to discuss problems, solutions and experiences in developing policy-based systems.
- The German Fraunhofer-Institut für Sichere Informationstechnologie is an example of a large European research centre with the focus on IT security. Over

one hundred employees are active in all relevant fields of IT security and form a broad base of competence for cross-technology development.

- The Swedish firms Appgate and Columbitech are two examples of firms that provide solutions for secure wireless access. Fingerprint Cards and Precise Biometrics are examples of Swedish firms providing biometric solutions, but even if biometrics is a priority segment for the US Department of Homeland Security it was difficult for Fingerprint Cards to find finance for the company in 2005.

3 Policy

3.1 International Cooperation

Spam, network security, cyber crime and Internet governance are on the agenda of the third meeting of the United Nations World Summit on the Information Society (WSIS) in November 2005, Tunisia (UN 2005A). The issues include administration of the domain name system and Internet Protocol (IP) addresses, as well as issues which are relevant to the Internet but have a much wider impact, such as competition policy, liberalization, privatization and regulations, and intellectual property rights and dispute resolution.

Many IT security measures take place on the international arena and Japan made an agreement with USA on September 9, 2003 that the two countries should embrace their roles as global leaders to create a "culture of security". They also agreed to work together and in compliance with the Council of Europe Convention on Cyber crime, and in multilateral organizations such as APEC, the G8 and OECD, to implement cyber security and cyber crime recommendations and action plans that are adopted in these organizations. Japan has also had an agreement with the European Union since 2004, which includes initiatives to make the internet more secure by sharing perspectives, policy thinking and to cooperate, bi- and multilaterally to fight against spam. Besides cooperating with the USA and recognizing mainly western agreements, Japan is playing leading role in common Asian initiatives in connection with IT security partly in the ASEAN+3 but also, and perhaps more closely, with China and South Korea.

With the ambitious goal of building an advanced IT society originating in Asia, a special mechanism has been set up for collaboration between China, Japan and Korea in several areas. Those that relate to IT security are: joint experimental trials and the international standardization of advanced high-speed networks, IPv6-related devices, next generation mobile networks, electronic tags, digital broadcasting, information network security and Open Source Software. The three countries are exchanging information in these and other areas , in order, among other reasons, to promote technical co-operation in the investigation and the exchange of information on cyber crime.

The largest number of organized cyber threats to money has originated in Russia, which makes the fight against cyber crime more complicated. One of the leading European countries in terms of information security is the Netherlands, and Israel is leading in the integration of physical and information security according to the global information security benchmark Mapping Security Index (MS 2005A). Mapping Security provides details about the best practice, regulations and security trends of different countries.

3.2 IT Security Policy in the USA

Cyber security is in the US is considered an area of low priority compared to other homeland security issues and this is not particularly surprising because IT incidents do not usually cause any casualties. However things could be different in the fu-

ture. The Department of Homeland Security was created after the September 11th terrorist attacks and the focus is on protecting people. The National Cyber Security Division (NCSD) at DHS, responsible for cyber security, is within the Information Analysis and Infrastructure Protection Directorate (IAIP). The 2006 budget for NCSD is about 73 million USD, only 0.2 percent of the total DHS funding. By way of comparison the programme for bio-terrorism threats at Department of Health and Human Services has an annual budget of about 4 billion USD and the project BioShield a funding of 56 billion USD. The Department of Homeland Security is also a large organization with 180,000 employees and several different organizational challenges (WP 2005A). The total DHS budget has increased by more than 200 percent between 2002 and 2006. However, the total federal funding for IT security is significant and has increased from 2.7 billion USD in 2002 to 4.2 billion USD in 2003 or about 6.5 percent of the total federal IT budget (OMB 2004A). The IT security budget for each agency is allocated to different projects depending on the agency mission and projects defined by regulation such as the Federal Information Security Management Act.

The federal IT budget, as a part of the total budget, is in line with IT spending by the industry. The total federal budget for information technology is about 60 billion USD, about 27 billion is for Department of Defense and about 10 billion for homeland security projects. The President's IT budget for 2006 includes an increase of IT spending at DHS by 35 percent to strengthen e.g. prevention programmes and screening initiatives (OMB 2005A). IT is a federal priority and particular security applications based on information and communication technology such as the DHS projects. An important fact it that there is resistance in the US by several large companies within the IT industry to any kind of major government cyber security initiatives which have an impact on policy formulation. Regulation could be a threat to the development of the IT industry according to some industry representatives. The IT industry prefers in general market-based approaches. Increased cyber security could be managed by industrial initiatives or by increased government regulation. A lot of private investment in IT security has been driven by non IT-specific regulation such as the Sarbanes-Oxley Act, further described in the chapter on information security.

Table 2 Federal Cyber Security Funding

Military Cyber Security	**R&D 2004**	**Other 2004**
National Security Agency	50	---
Advanced Research And Development Activity	17	---
Defense Advanced Research Projects Agency	---	---
Civilian Cyber Security		
National Science Foundation	76	29
Department of Homeland Security	18	73
National Institute of Standards & Technology	10	37
Department of Justice	7	---
Total (million USD)	**178**	**139**

Source: NSF 2004A, DHS 2005A

One part of the strategy for Homeland Security is The National Strategy to Secure Cyberspace (White House 2003A) published in February 2003. The federal strategy was developed in collaboration with state and local governments, universities and organizations. Private-public partnerships are an important part of the strategy process because the majority of cyber resources are controlled by private organizations. The strategy states that “the private sector has the most important role to play in cyber security”. The strategy has been the basis for the federal administration's work with the Congress to secure federal security budgets. The Department of Homeland Security (DHS) has the main implementation responsibility for the strategy. DHS responsibilities include securing key resources, providing crisis assistance, coordination with other agencies and R&D funding. The strategy for cyberspace is complemented by the National Strategy for the Physical Protection of Critical Infrastructures. The strategy for cyberspace is an initial framework for organizing and prioritizing initiatives. The defined strategic objectives are the prevention of cyber attacks, the reduction of vulnerability to cyber attacks and minimizing the recovery time from attacks. Enhanced cyber threat analysis is also necessary to address long-term trends for threats and vulnerabilities. The five critical priorities for cyberspace security defined in the report are (White House 2003A):

- A National Cyberspace Security Response System focusing on improving the response to cyber incidents and reducing the potential damage. Rapid identification, information exchange and remediation are important. National public-private partnerships for analysis, warnings and response are necessary. Public-private architecture for responding to incidents is proposed.
- A National Cyberspace Security Threat and Vulnerability Reduction Programme for issues such as weaknesses in technology and the implementation of solutions. Defined actions are enhancing law enforcements capabilities, creating a process for national vulnerability assessments, improving Internet protocols and routing and reduce software vulnerabilities.
- A National Cyberspace Security Awareness and Training Programme are important to reduce vulnerabilities. There is a lack of accepted multi-level certification programmes for cyber security. Proposed actions are a national awareness programme and create training and education programmes.
- Securing Governments Cyberspace. Government can lead by example in cyberspace security, including creating a marketplace for more secure products through procurement.
- National Security and International Cyberspace Security Cooperation focusing on improving the international management of attacks impacting national assets. International cooperation to facilitate information sharing needs to be established.

The Department of Homeland Security has created several different organizational entities to manage cyber security issues. NCSD was established in 2003 to identify, analyze and reduce cyber threats and vulnerabilities, coordinate incident response and provide technical assistance. NCSD is also working with the private sector to improve security of the US information infrastructure. NCSD has also established

the US Computer Emergency Response Team (US CERT) for tracking incidents, ranking severity and generating real-time alerts.

A report published in March 2005 by the Congressional Research Service concludes that several challenges are associated with the definition of public policy for cyberspace security (CRS 2005B). The report was requested by the House Homeland Security Committee's Economic Security, Infrastructure Protection and Cyber Security Subcommittee. The report defines four particular issues. According to the report "computer networks have many of the characteristics of a public commons which makes it more difficult for market mechanisms to improve cyber security". The global nature of cyberspace makes it difficult to obtain co-operation and co-ordination and little agreement on the best approaches to securing cyberspace exists. The regulatory initiatives are also often not in line with the fast pace of technological development. The report describes two possible models for improved government involvement. One approach is to require companies to report on security preparedness and have liability protection for companies that comply with the rules. The other approach is to define regulations and use inspectors to monitor compliance. The report also defines other legislative options such as:

- "Encouraging the adoption of cyber security standards and best practice."
- "Using procurement practice to make cyber security a priority."
- "Requiring mandatory reporting of certain kinds of security breaches."
- "Providing mechanisms for product liability actions."
- "Helping the insurance industry develop cyber security insurance policies."

A study by Illinois State University (ISU 2003A) states that "the poor state of security on the Internet is the direct result of a market failure". Software companies have distributed products without having liability for faulty products. The time-to-market pressure has also contributed to the number of faulty products. However, recent federal legislation requires mandatory public disclosure of the security position of organizations in the financial and healthcare industries. According to the study cyber insurance policies are an attractive market solution to the software security problem. Some companies have also begun to issue cyber insurance policies to cover against e.g. hacker intrusion damage and virus infections.

The National Cyber Security Partnership published a National Cyber Security Progress Report in February 2005 (NCSP 2005A). The report concludes that achievements within cyber security have been made in areas such as capabilities for large-scale network intrusion detection and for communicating cyber threats, structures for intra-industry information sharing of security related information, creation of programmes for cyber security assessments and certification and development of best practice guides.

3.3 IT Security Policy in Japan

Japan has a history of successful and proactive IT-policies. The Cabinet of Prime Minister Jonichiro Koizumi has taken measures to promote Japan as an IT-nation by taking initiative to the IT Strategic headquarter in the cabinet office. The head-

quarters are led by Koizumi himself and consist of all ministers and eight additional non-government experts. The purpose of the headquarters is to promote an advanced Japanese information and telecommunications network society.

Starting with the e-Japan Strategy in 2001, outlined in IT Basic Law of 2000, concrete measures to safeguard IT security have been a prioritized area. Detailed and revised measures have been included for annual policy programmes since then (See timeline in Appendix). In the Policy programme of 2004, the "security and reliability of advanced information and communication networks" is one of five prioritized policy areas, detailing 49 measures involving all ministries and many agencies. While several measures from 2004 have been concluded, several still remain. In the "IT policy package 2005", the following measures relating to IT security have been put forward:[9]

- Overcoming social issues such as forgery and phishing: Collecting and sharing information within and outside Japan to seek measures to address these problems. Designing a framework to give warning to citizens. Submitting a bill for partial amendment as a measure against spam.
- The setting up of a National IT Security Center and an IT Security Policy Conference.
- Promoting public awareness on the personal information protection act; promote efficient handling of complaints; sorting out penalties associated with information misappropriation within the government.
- Assessing the level of information security maintained by local public agencies; enacting an ordinance by all local public agencies relating to personal information protection and formulating an information security policy.
- Providing advanced IT training based on open source software and hands-on information security training for young people under the age of 20; Promoting hands-on training and demonstrations to nurture IT security experts; provide seminars for individuals involved in IT security initiatives.
- Establishing guidelines and an information security report to be used by corporations to share information and benchmark information security measures.
- Upgrading and enhancing the necessary equipment, supplies and devices to ensure a further advancement of the Internet observation system.

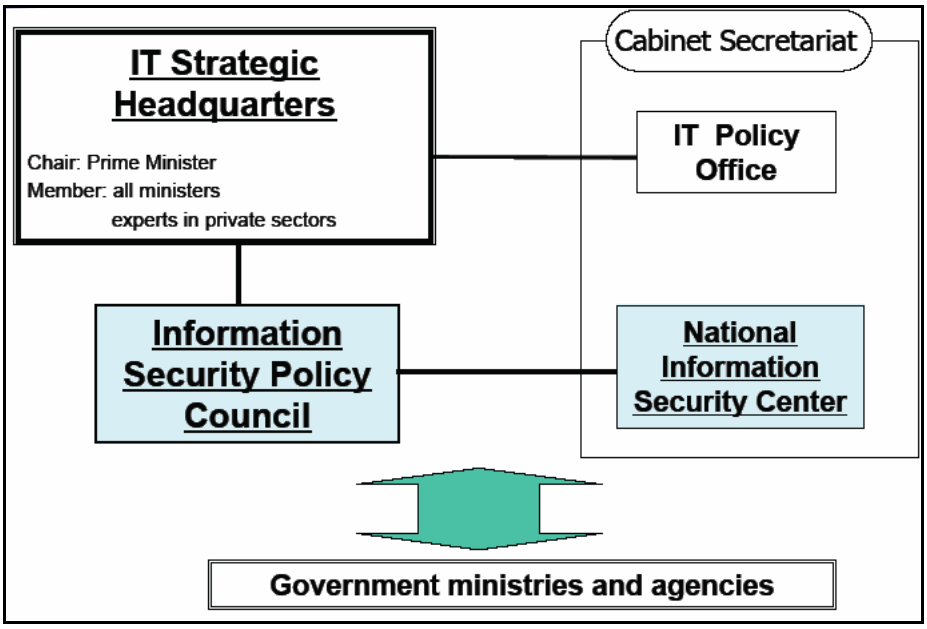
The cabinet office previously had two bodies to work on IT-strategy: an IT policy office and an IT Security office. Placing the IT Security office right alongside the general IT policy issues shows how high a priority it is given in Japanese society. The office is, however, in a process of reorganization. In order to address the rising

[9] *Several measures are directed to using IT in order to increase safety and security e.g. implementation of IC-passport and immigration control, activities for disaster prevention, Intelligent Transportation Systems, food product information, etc. Included here are only such as relate to the safety and security of IT-systems; an advanced food safety and security system utilizing u-technology: R&D for creating food product information to consumers in the framework of ongoing initiatives based on food traceability.*

importance of IT security issues, a Committee for Essential Issues on Information Security with members from the IT security office has been given a mandate to formulate a National Strategy on Information Security by collecting opinions of experts and to place its recommendations before the IT strategy headquarters. They began their work in July 2004 and made their first recommendations in November 2004, to 1) establish basic strategies on information security policy and enforcement authority, and 2) establish more effective co-ordination within the government to compile and enforce measures to ensure security in government networks.

In effect, this meant a reorganization of the IT Security office and its working relation to the IT-Strategic headquarters which had been in operation since 2000. Starting in April 2005, the IT Security Office was exchanged for the National Information Security Center, NISC. The path of communication to the IT-Strategic headquarters is through the Information Security Policy Council, which substitutes the previous IT Security Expert Meeting and the IT Security Promotion Committee (see picture below).

Figure 2 IT Security in the Cabinet Office.



Source: MIC 2005A

The *National Information Security Center, NISC*, brings about a strengthening of the IT Security government staff from 18 to 35 and a total of about 60 planned for 2006. The Mission of NISC is to 1) plan a basic strategy for information security policy, 2) promote comprehensive measures for information security concerning government organizations, 3) support such government organizations in cases of information security incidents, and 4) strengthen the information security of critical infrastructures.

The Information Security Policy Council exchanges the IT Security Expert Meeting and the IT Security Promotion Committee. The latter consisted of the Director Generals of all ministries and agencies (roughly comparable to the Swedish

Toppledarforum). Its missions are to 1) develop basic strategy through annual, mid-, and long-term plans, for information security policy. 2) assess information security policy based on the basic strategy. 3) undertake ex-post facto assessment of information security policy and its publication. 4) develop safety guidelines for information security, uniform throughout the government. 5) recommend information security policies for each ministry based on the government-wide safety guideline. 6) to cope with and respond to emergencies and incidents.

In the light of the recommendations of the Committee for Essential Issues on Information Security, the Ministry of internal affairs and communication (MIC) presented in 2004 five initiatives for safe and secure network foundations. MIC mainly supports application-oriented research by industry-academia and national laboratories collaborations. The initiatives are:

1. Support for Telecom-ISAC activities; guidelines and standards for safety and security measures in telecom networks; certification of ISPs by the Safe Secure ISP Mark, preferential tax treatment for telecom carriers that obtain facilities which contribute to improved reliability.
2. R&D for secure technologies which include the establishment of the Information Security Center at the National Institute of Information and Communication Technology and initiatives to secure telecom infrastructure and capabilities to analyze viruses etc on networks.
3. Establishment of a mechanism to secure collaboration and the distribution of information on threats, SPREAD (Security Promotion Realizing Security Measures Distribution), the purpose of which is to provide the general Internet user with easy-to-understand information and advice on threats.
4. Strengthening user-side security measures by the previously mentioned tax levy, information initiatives and virus alerts, and enacting regulations on illegal access, digital signatures and the ratification of the European Council cyber crimes treaty.
5. Creating easy access to safe and secure network services by supporting international standardization and promoting R&D initiatives for a user-centered development of networks (e.g. network authentication infrastructure and timestamp platform technologies).

3.4 IT Security Policy in China

The management of risk is, generally speaking, a very important issue for the Chinese leadership. IT Security is, of course, only one aspect of this, but nowadays an aspect that is receiving more and more attention from the Chinese government - as well as from local Chinese companies. Although more and more perceived as a major threat during the 1990s, it was not until 2003 that “Preliminary Suggestions on the Strengthening of IT Security” (*kuan yu jia qiang xin xin an quan bao zhang gong zuo de jian yi*) was published by the State Council Informatization Office (SCITO). This document has now been renamed “Document 27 of the State Council” (*er shi qi hao wen jian*). The increasing awareness of the importance of IT

security was further underlined in the year 2004 by the fact that the fourth section of the 16th National Congress of the Chinese Communist Party decided to regard IT Security as just as important as political stability, economic safety and national defence (PD 2004).

It is obvious that China started comprehensive work on IT security very late, but it now has, in "Document 27 of the State Council" (Document 27), a framework for future work as well as a first document describing the division of responsibilities between different governmental organizations. Document 27 is not an open document because it also includes aspects of national security. Despite the fact that Document 27 is partly confidential, the general guidelines are well known. IT security is considered as needing both organizational and technological measures. Protection should have a high degree of credibility, although the measures used should be in proportion to the 'value' of what is protected. Awareness and training, along with R&D, are important issues. In Document 27 of the State Council the goal is described as building for China a national IT Security protection system according to the principles of "active defending" (*jiji fangyu*) and "all direction prevention" (*zonghe fangfan*) by implementing a good combination of managerial work rules and advanced technology. The time frame considered is approximately five years, i.e. the period from 2005 to 2010. This period is said to be a critical one for China when it comes to implementing IT security. By 2010 a multi-faceted IT security system should exist in the majority of government agencies and larger and medium sized companies. The meaning of "active defending" is that security should be achieved through the constant active development of processes and technology, while "all direction prevention" means that IT security is the common responsibility of the government, enterprises and private persons, i.e. of everyone who benefits from IT development. The idea is that the whole of society should understand that IT security is the responsibility of everyone in society. It also means that multiple methods such as legal, technical and administrative should be adopted in solving problems of IT security. IT security is regarded as a "systematic engineering mission" (*xitong gongcheng / tixi jianshe*).

An outline of China's IT security-strategic policies and measures could be summarized as follows:

- Strengthening the leading role of the government at different levels of IT security work and fully applying the strategic policies of the central government to IT security
- Strengthening the basic work of IT security, so as to increase the capability of sustainable development on IT security (including setting up a complete IT security law system, IT security-related standards, IT security information and training systems)
- Speeding up the industrialization of IT security-related products, especially products manufactured by Chinese companies
- Actively participating in international co-operation, especially in legal action against cross border crime on the Internet

- Adopting effective measures to improve the protection ability of the basic net infrastructure and important information systems (including regulations on the level of protection of IT security, the differentiation of responsibilities of authorities, system builders, operators, setting up IT security direct report channel and emergency systems)

The initiatives now taken by the government to strengthen IT-systems in order to implement the strategies can be subsumed under one of four categories: administrative, legal, standards/certification, and R&D. In March 2005, Mr. Gu Jianguo, Deputy Director General of Public Information Net Security Inspection Bureau of the Ministry of Public Security, presented the following list of weaknesses of the Chinese IT infrastructure (NS 2005C):

- IT security management system cannot cope with the IT development.
- The fundamental backup capability and infrastructure of IT security is weak
- The existing laws, rules and regulations cannot meet the needs of the IT security work development
- IT security research and development and industrialization of related products are being developed too slowly
- Some of the core technologies are still not totally controlled by China
- A system that can meet the work load and need for informing and training personnel of IT security has not yet been set up
- The protection capability of China's basic net and important information system is not strong enough to resist serious IT security incidents
- Lack of effective measures and means to fight net crimes, unhealthy culture shock and threats of IT war

China's Internet regulations and legislation are guided by the principle of "guarded openness" – seeking to preserve the economic benefits of openness to global information, while guarding against foreign economic domination and the use of the Internet by domestic or foreign groups to co-ordinate anti-regime activity. From the first linking of China to the global Internet in 1994, central authorities have consistently sought to control China's Internet connections. Heavily restricting international connectivity has been a key principle in China's nascent Internet security strategy. International connections for all five of China's major networks still pass through proxy servers at official international "gateways." Filtering and monitoring of network traffic is still focused at this level. Derisively termed "The Great Firewall" by hackers and journalists worldwide, this strategy has enjoyed varying degrees of success (Cherry 2005). Originally, there were many reasons for constructing the Chinese network along the lines of this "Great Firewall" model. The gateways would modulate the pace of China's opening up to the world through electronic interaction. The gateways were to serve as the first line of defence against anti-government network intrusions. They would serve as a firewall, restricting the amount of information about internal networks available to foreign intruders. The

gateways were designed to prevent Chinese citizens from using the Internet to access forbidden sites and anti-government information from abroad.

A recent study by the Open Net Initiative (ONI), in conjunction with Harvard's Berkman Center for Internet and Society, reveals an increasingly sophisticated set of mechanisms through which Chinese internet users are prevented from accessing material deemed off-limits by the Chinese government (ONI Report 2005). Though government statements emphasize anti-pornography crackdowns, ONI found the primary focus of China's filtering system to be on political content. Public security organs and internet service providers employ thousands of people – nationwide, at multiple levels – as monitors and censors. Their job is to monitor everything posted online by ordinary Chinese people and to delete objectionable content. The key to the filtering system, however, is automated technology – equipment and software coming from outside China (mostly the US) – enabling China's service providers to enter hundreds of thousands of banned keywords and web addresses for automatic blocking. In the network now taking shape in China, CN2, many of the existing constraints will be largely eliminated, making censorship more a matter of politics than of technology. The more state-of-the art the router, the more "granular" its filtering mechanisms become. Thus, experts predict the new network will enable the Chinese government to control and monitor online speech even more tightly.

In addition to the technological controls of the Great Firewall, the Chinese authorities also require all Internet businesses, including Internet service providers and cyber cafés, to obtain operating licences. In the first of a number of periodic crackdowns, more than 17,000 cafés were shut down in 2001 for failing to block Web sites that were considered to be subversive or pornographic. As recently as March 2005, more than 2100 café licences were revoked for not blocking porn. Internet service providers also have to record every message that crosses their networks. Messages that seem to violate a law must be forwarded to the Ministry of Public Security and two other state agencies and then deleted. Cyber cafés are not required to run so-called censor ware — software that inspects data packets for banned keywords. But many do so of their own accord (Cherry 2005).

There is not yet any general IT-law for the whole of China. A major and slowly progressing work is in progress to formulate a national law applicable to all the different provinces in China. Presently, urgent issues are being treated on an *ad-hoc* basis. Because the Chinese Telecommunication Law has not yet been worked out, the Administration Permission Law and Telecommunication Rules and Regulations are being applied in regulating the management activity of net connections and licences. Moreover, Net Information Security Regulations are also being drafted. Some of the existing laws, rules and regulations governing IT security are:

1994	Computer Information System Security Protection Regulations, MPS
1995	People’s Police Law, the regulations for the police as to how they should protect the security of computer systems, MPS
1997	New Punishment Law, (for crimes committed via computer), NPC

1997	Security Protection Management Regulations on Protection of Computer Information Net Connection with Internet, MPS
2000	Management Regulations on the Prevention of Computer Viruses, MPS
2000	Business Secret Code Management Regulations, SCITO
2000	Internet Connection Encryption Regulations, MPS
2004	Electronic Signature Law, National People's Congress

The year of 2000 was the most active year for many of China's governments' agencies to make different kinds of rules and regulations in regulating Internet activities. More than 17 were produced that year. By reading them, one can find that they only stressed the role that the government should play, but not the role of the IT security industry (NS 2005D).

3.5 Information Security Policy

Regulation for different industrial sectors is today one of the major forces driving technology investment in information- and IT security in the US. The situation is similar in Europe, the European regulation Basel II is considered to be one of the major force driving investments in information security. Companies in the US will spend about 15 billion USD in 2005 on compliance-related activities. The major regulations with an impact on private companies are Sarbanes Oxley Act of 2002 with a total compliance cost of 6,1 billion USD, HIPAA of 1996 with a cost of 3,7 billion USD, Gramm-Leach-Bliley Act of 1999 SEC at a cost of 1.3 billion USD and other regulations at a cost of 4.4 billion (IW 2005E). The cost of regulatory compliance over the next five years is estimated at 80 billion USD. About ten years ago almost no regulation existed in the US that had an impact on information security (ISPC 2005A). Compliance-related investments are so far in many ways more important for the IT security industry than the federal initiatives within homeland security.

The Federal Information Security Management Act (FISMA) of 2002, which is a part of the Electronic Government Act of 2002, replaced the Government Information Security Reform Act (GISRA) of 2001. GISRA introduced annual review and reporting requirements about IT security on federal agencies. FISMA aimed at further strengthening information and system security and US federal government agencies need to comply with the regulation (OMB 2004A). FISMA requires the National Institute of Standards and Technology to develop IT security guidelines in a number of areas such as minimum security standards. FISMA also includes requirements on system configuration management, system continuity and information system inventory management. FISMA defines that the Office of Management and Budget is required to submit a report to Congress on the agency's compliance with IT security requirements. OMB has also issued guidance for the agencies on how to report IT security including quantitative performance measures. In early 2004 OMB reported e.g. that the number of federal IT-systems that had been certified and accredited had increased to 62 percent from 47 percent a year earlier. The

number of systems with an up-to-date IT security plan had increased from 62 percent to 73 percent, progress for several other parameters was also reported (OMB 2004A). Beginning in January 2006, agencies must according to FISMA requirements set up 17 minimum security controls on all major applications and general support systems. The security controls are described in the NIST document *Special Publication 800-53: Recommended Security Controls for Federal Information Systems*.

The Sarbanes-Oxley Act (SOX) of 2002 requires information security to be employed to ensure the effectiveness of internal controls over financial reporting. Especially Section 404 has implications for information security. Companies listed in the US have had to comply with SOX since early 2005. SOX was created because of financial fraud relating to companies such as Enron and WorldCom. The Congress adopted the Sarbanes-Oxley Act to protect investors and shareholders by ensuring the integrity of financial reporting and forcing corporate officials to take full responsibility for public disclosures required under the law. Companies need to strengthen their corporate governance and expand internal accountability. The law creates greater pressure on IT organizations to provide reliable information. Companies need to implement information security to the extent necessary to ensure the effectiveness of internal controls over financial reporting. SOX is considered to be a burden on companies, the total cost in 2005 for US companies to comply with SOX being estimated at 6.1 billion USD including technology costs of 1.7 billion USD (IW 2005E). All Swedish companies listed in USA also need to comply with SOX but not until the end of 2006.

The Gramm-Leach-Billey Act (GLBA) requires financial institutions to ensure the confidentiality, integrity and security of customer information such as name, social security number, income and credit card history. GLBA has a broad impact on organizations, and companies need to comply from 2002. Federal agencies perform compliance audits. The Health Insurance Portability and Accountability Act (HIPAA) governs privacy, security and electronic transactions for healthcare providers. Privacy regulation is connected in the US to different technology areas which makes the situation rather complex in several cases. A privacy debate is related to each emerging technology segment such as RFID and nanotechnology. The Identity Information Protection Act of 2005 is one of several proposed pieces of legislation in 10 states that deal with emerging uses of RFID. Californian companies also need to notify customers if personal information may have been accessed according to the Californian Data Privacy Act.

On April 1st, 2005, the Personal Information Protection Act came into force in private companies in Japan. The law was approved in 2003 and companies have been preparing since then for enforcement in 2005. This is the law that is violated when personal data is leaked from companies and organizations. Frequent reporting in the media has made it one of the best publicized laws in the last few years. The act applies to government and private entities that keep records of personal information about more than 5000 individuals. Examples of such records are information sufficient to identify a person by name, birth data or email addresses. In order to maintain such a database, the keeper must inform the individual of what the data will be

used for and seek their consent before disclosing it to other parties. Furthermore, they must ensure that the data is kept secure, and set up a complaint handling system so as to promptly respond to individual requests to have their data updated or deleted.

3.6 Critical Infrastructure Protection Policy

In December 2003 was the Homeland Security Presidential Directive HSPD-7 published. The directive establishes a national policy for Federal departments and agencies to identify and prioritize the critical infrastructures and key resources to protect them (President 2003A). The critical infrastructure (CI) consists of sectors and resources such as Agriculture and Food, Water, Public Health and Healthcare, Emergency Services, Defence Industry, Energy, Transportation Systems, Banking and Finance, Chemicals, Postal and Shipping, National Monuments, Dams and Government Facilities. Strategic improvements in security can make it more difficult for attacks to succeed and can reduce the impact of attacks that may occur, however 80 percent of the US critical infrastructure is private owned. The Department of Homeland Security has established Information Sharing and Analysis Centers (ISAC) to allow critical sectors to share information and work together to better protect the economy and to minimize vulnerabilities. ISAC´s will help the government to understand the impact for different sectors and 14 different ISAC´s are launched for sectors such as energy, telecommunications and food industry (DHS 2005A). The ISAC Council works to promote the cooperation between the ISAC´s and interaction with government. CI protection requires public-private partnerships in combination with governance.

Table 3 Budget for the Department of Homeland Security

Funding by Strategy Mission	**2004**	**2005**
Intelligence and Warning	242	349
Border and Transportation Security	15 840	17 550
Domestic Counterterrorism	3 379	3 944
Protecting Critical Infrastructure	12 279	14 939
Defending Against Catastrophic Threats	2 974	3 399
Emergency Preparedness and Response	6 002	5 765
Total (million USD)	**40 716**	**45 946**

Source: DHS 2005A

The federal budget for 2006 also includes a Targeted Infrastructure Protection Programme of about 580 million USD to assist states and local government in reducing vulnerability relating to critical infrastructure (DHS 2005B). It is considered that state and local homeland security programs would be more efficient if the federal government provided firmer standards and technological practices. The most important part is technological directions and policies rather than the adoption of international standards (GCN 2004A).

The US Committee on National Security Systems (CNSS) provides a forum for the discussion of policy issues, sets national policy, operational procedures and guidance for the security of National Security Systems. National security systems are

information systems operated by the U.S. Government and its contractors or agents that contain classified information. CNSS is also involved in the definition of requirements for Common Criteria certifications.

CNSS have defined policies such as:

- "National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems."
- "National Policy on Securing Voice Communications."
- "National Policy on Secure Electronic Messaging Services."

In the concept of Critical Infrastructure Protection in Japan, thus far only Telecommunications has merited information security protection and discussions are also in progress about strengthening the role of Telecom ISAC-Japan. Telecom-ISAC provides the telecom industry, mainly ISPs, with information, collates information from them, and represents the international point of entry/exit for incident information as information is collected from NIRT, JPCERT, IPA and foreign CERT's and ISAC's. The ISAC provides security information to the general public. The 12 members of the ISAC are leading ISPs and internet-related organizations, while MIC participates as observers. When the committee for essential issues on information security gave their second round of recommendations on conclusion of their work in May 2005, they suggested adding medical services, water and distribution to the list of critical infrastructures, in addition to telecommunications, as being subject to threats and in need of information security protection. "Threats" should also be understood to include unintentional factors, e.g. human error and natural disasters in addition to cyber attacks. The establishment of more ISAC's has already been mentioned as a measure to strengthen the framework of information sharing among such critical infrastructures.

4 Research and Development Programs

4.1 The US National Science Foundation Cyber Trust Program

The Cyber Security Research and Development Act of 2002 authorized 875 million USD between 2003 and 2007 for cyber security programmes at the National Science Foundation (NSF) and at the National Institute of Standards and Technology (NIST). The Act passed the legislation process because the available technology was considered not to provide sufficient protection, and relatively little R&D has been conducted to develop new approaches for protecting computer systems and networks (NSF 2002A).

Table 4 The US Cyber Security Research and Development Act

Program	2003	2004	2005	2006	2007	Total
National Science Foundation Research						
Computer and Network Security Research	35	40	46	52	60	**233**
Computer and Network Security Research Centers	12	24	36	36	36	**144**
Computer and Network Security Capacity Building	15	20	20	20	20	**95**
Community Colleges	1	1	1	1	1	**6**
Graduate Traineeships in Computer Security	10	20	20	20	20	**90**
National Institute of Standards and Technology						
NIST Extramural Research	25	40	55	70	85	**275**
Computer Security Review, Public Meetings	1	1				**2**
Intramural Security Research	6	6	6	7	7	**32**
National Academy of Sciences Study	1					**1**
Total (million USD)	**106**	**152**	**184**	**206**	**229**	**878**

Source: NSF 2002A

The NSF Directorate for Computer and Information Science and Engineering (CISE) is organized in four divisions: the Division of Computing & Communication Foundations (CCF), the Division of Computer and Network Systems (CNS), the Division of Information and Intelligent Systems (IIS), and the Division of Shared Cyber Infrastructure (SCI). NSF funding for cyber security R&D was about 76 million USD in 2004. The NSF Cyber Trust programme, established in 2004, seeks to support relevant research on many fronts, to educate students in how to design and build more trustworthy systems, and to inform the public about safe ways to use the systems on which they depend. In 2004 35 Cyber Trust projects, of 390 research proposals, (NSF 2004A) in 11 different categories received funding of 31 million USD. The funded categories are such as:

A Security of next generation operating system (OS) and networking issues including e.g. the goal of providing new program installation, execution, and management abstractions within the OS. A project for a new operating system design, Asbestos, is funded at UCLA and MIT. A project for a security-aware general-purpose processor is funded at USC ISI.

B Forensic and law enforcement foundations including research into the design and implementation of a Network Forensics System. The project addresses the lack of effective forensic tools for network level investigation of malicious activity on the Internet and other IP networks. Future networks are expected to have forensic support integrated into them to deter cyber crime.

C A human computer interface for security functions including research into exploring risk perception and ultimate trust in online environments The research addresses system interfaces for establishing trust from the perspective of a visually impaired user. The project will specifically seek to identify the factors important in developing visually-impaired consumer trust in online businesses.

D Cross-disciplinary approaches. NSF is funding a project for the study of an Economic Approach to Security. The research is a three-year, multi-institutional, multi-disciplinary research project on the economics of security in networked environments. Specific research topics to be pursued include security of inter-domain routing, adaptability of trusted platforms, the compatibility of "host security" mechanisms.

E Theoretical foundations and mechanisms for privacy, security and trust. Research for a Comprehensive Policy-Driven Framework for Online Privacy Protection Integrating IT, Human, Legal and Economic Perspectives is funded. The project will provide a comprehensive framework for protecting online privacy, covering the entire privacy policy life cycle. Technology for managing federated databases while controlling the disclosure of private data.

F Composable systems and policies. Integrating Security and Fault Error Tolerance in Distributed Systems is the scope of the area. The research focuses on the construction of trustworthy distributed systems: systems that tolerate both malicious attacks and benign faults while preserving data integrity and confidentiality. The goal is new methods for constructing distributed systems that are trustworthy in the event of some nodes in the system have been compromised by malicious attackers.

G Improved ability to certify system security properties. One funded project is: Type Qualifiers for Software Security. The research has the goal of establishing the fact that very large software components are free of specific kinds of security vulnerabilities. The area focuses on the goal of producing high assurance systems, in which the buyer can specify the required software/hardware properties formally and the untrusted supplier can provide machine-checkable proof with the delivered product that the product has the specified properties.

H Improved ability to analyze security designs, and build systems correctly. One research project investigates the use of aspect-oriented programming language techniques as a safe means to update the functions and security policies of a high-confidence computer system while the system is running. Work on a security-typed programming language (Cyclone) that aids the programmer in writing correct, security-critical distributed programs is also funded.

I More effective system monitoring, anomaly detection, attack recognition and defence. One research project is studying the detection of self-propagating malicious codes. Statistical and information-theoretic techniques will be used to develop new methods for the real-time detection of anomalies in network traffic that might have been caused by Malicious Code.

4.2 Cyber Security R&D at US Department of Homeland Security

The Department of Homeland Security (DHS) R&D budget was about 1 billion USD in 2004, but only 18 million USD was for cyber security and only about 1.5 million USD for long-term research (PITAC 2005A). DHS does not have a specific R&D programme for IT security. The Science & Technology Office established the Cyber Security Research and Development Center in March 2004. The Center is the umbrella under which the Department's cyber security R&D activities are coordinated and performed. Charged with creating partnerships between government and private industry, the venture capital community and the research community, the Center develops and fortifies security technology to better protect the cyber infrastructure of the United States. A lot of the Center's work is conducted at SRI International headquarters in Menlo Park, California.

Currently, the Center is involved in the following R&D areas (DHSCSRD 2005A):

- Domain Name System Security Extensions
- Large datasets for cyber security
- Experiment and Exercise Participation
- U.S.-Canada co-operation on wireless security
- Test beds

The US House of Representatives Subcommittee on Cybersecurity, Science and Research & Development was established in 2001 to oversee DHS cyber security and science and technology initiatives. The Subcommittee was working with DHS, the private sector and the academic community to define the most important cyber security-related issues, and to define possible action to make cyberspace safer. The Subcommittee believes that DHS has much work to accomplish in the coming years according to a report published in 2004 (SubCyb 2004A). During recent years many new federal initiatives have been created, but the impact in terms of new R&D funding to the universities is not significant. More robust capabilities need to be established, further outreach sessions with the private sector including users and operators is necessary, and more initiative is needed to work across different infrastructure sectors and with state and local government. The Subcommittee recommendations for DHS are e.g.

- "To update the plan for outreach. The plan should include developing innovative mechanisms for information sharing on cyber security threats, vulnerabilities, best practice and emergency response."
- "Improve performance on cyber risk assessments and remediation activities to include a plan for Internet-related recovery in the event of a disaster."

- "Support research and development and educational activities in order to improve cyber security products and services that are user friendly and keep pace with risk and technology."

4.3 Proposal for Cyber Security R&D in the USA

In February 2005 the President's Information Technology Advisory Committee (PITAC) published a report for the President about cyber security (PITAC 2005A). Members of PITAC are appointed by the President to provide independent expert advice on information technology. The report states that "the growing dependence of the critical infrastructures on the IT infrastructure means that the former cannot be secure if the latter is not". Fundamentally different IT architecture and technologies are needed to secure the infrastructure according to PITAC. How to model, design, and build systems incorporating integrated security attributes is not known today. Issues are e.g. "how can we build complex software-intensive systems that are secure and reliable when first deployed?". PITAC consider there is an imbalance in the current federal cyber security R&D portfolio because of limited support for fundamental research to address larger security vulnerabilities of the civilian IT infrastructure. The current priority is short-term, defence-oriented and classified research. Civilian-oriented cyber security R&D at organizations such as Defense Advanced Research Projects (DARPA), National Security Agency (NSA) and Advanced Research and Development Activity (ARDA) has decreased during last years when the need for new solutions has increased, and long-term economic security is at risk. (PITAC 2005A). Federally sponsored fundamental R&D into information technology has also been important for the creation of billion-dollar segments in the IT industry. PITAC's recommendations are:

- To increase the annual Federal funding of fundamental research into civilian cyber security by 90 million USD at the National Science Foundation in order to support 10 high-priority areas defined by PITAC.
- To intensify Federal initiatives to promote recruitment of civilian cyber security researchers and students, with the objective of doubling the number by the end of the decade. At academic institutions there are fewer than 250 active cyber security specialists today.
- To provide increased support for rapid technology transfer of cutting-edge cyber security technology and strengthen the technology transfer partnerships with the private sector. The federal government needs to develop e.g. test beds.
- Strengthen the co-ordination of the Interagency Working Group on Critical Information Infrastructure Protection (CIIP) and integrate it in the Networking and Information Technology Research and Development Program. Today's government-wide coordination is inefficient.

PITAC has analyzed different cyber security R&D projects and identified 10 priority areas. Further R&D within the areas is considered of core importance in order to be able to secure the IT infrastructure. The areas are:

- Authentication technologies including research on infrastructure and protocols for large-scale public key distribution and management, integration with biometrics and decoupling authentication from identification.
- Secure fundamental protocols. Today's Internet protocols and services such as the Border Gateway Protocol and the Domain Name System have limited security. Basic protocols need to be secured against attacks bearing in mind e.g. trade-offs between security and performance.
- Secure software engineering and software assurance including research areas such as programming languages with security features and technologies for code verification.
- Holistic system security including a new end-to-end architectural approach to security is important. The research topics include building secure systems from trusted and untrusted components and modelling failures in complex systems.
- Monitoring and detection. Tools to understand unanticipated events are important for deployment of the appropriate defence. The research topics are e.g. dynamic protection, global scale monitoring and usable presentation interfaces.
- Mitigation and recovery methodologies. Internet security research needs to learn from the development of other complex systems such as space shuttles to be able to provide increased reliability and redundancy. Research areas include systems for rapid recovery and fault-tolerant systems.
- Cyber forensics for catching criminals and deterring criminal activity. Proposed research topics are e.g. new tools to investigate cyber crimes, tools for traceback of network traffic, and recovering evidence from computing media.
- Modelling and test beds for new technologies. Today there is a lack of test beds to test new security technologies in a real-world environment. Proposed research areas include system simulation environments, gathering and synthesizing very large amounts of data and designing test beds.
- Metrics, benchmarking and best practice to help evaluate new technologies and products. Today's certification criteria are considered antiquated and expensive. Research topics are developing security metrics and benchmarking, economic impact assessment and risk analysis, cost of defense, tools for vulnerability assessments and documentation of best practice.
- Non-technology issues including different factors such as institutional, legal and economic ones that can have an impact on progress in the development of cyber security.

4.4 US Critical Infrastructure Protection R&D

HSPD-7 also requested a national Critical Infrastructure Protection Research and Development Plan (CIPRD) and a comprehensive National Infrastructure Protection Plan (NIPP). The CIPRD was published by the Office of Science and Technology Policy in 2004 and was developed through interagency collaboration. The document (CIPRD 2004A) highlights the target investment necessary to help se-

cure the US key infrastructures and resources from acts of terrorism, natural disasters and other emergencies. The plan developed by the National Science and Technology Council is the first annual version of the R&D roadmap for critical infrastructure protection. The plan has a national scope and integrates cyber, physical and human elements and focuses on "the identification of capabilities, needs and gaps on known threats". The first R&D plan focuses on the creation of a baseline, identification of major R&D investments, and the definition of a vision relating to future needs and identified research gaps. A roadmap and investment plan will be developed in the 2005 critical infrastructure protection research and development planning process.

The vision of the plan (CIPRD 2004A) includes goals such as: "A next-generation computing and communications network with security designed-in" and "Resilient, self-diagnosing, and self-healing physical and cyber infrastructure systems". It is believed that achieving the goals will take more than five years. The R&D plan is structured into nine different scientific and technological themes of importance to critical infrastructure. The themes are:

- Detection and Sensor Systems,
- Protection and Prevention
- Entry and Access Portals
- Insider Threats
- Analysis and Detection Support Systems
- Response, Recovery and Reconstitution
- New and emerging Threats and Vulnerabilities
- Advanced Infrastructure Architectures and Systems Design
- Human and Social Issues

Based on the defined themes and the goals in the vision for the R&D plan the following R&D priorities were defined:

- Improved Sensor Performance including developing improved physical and cyber monitoring and detection systems with e.g. increased sensitivity, higher accuracy, speed enhancement, reduced power requirements and lower cost. Detectors for explosives are particularly important.
- Advanced Risk Modelling, Simulation, and Analysis for Detection Support are important for all CI sectors. Issues included are standardization of vulnerability analysis and risk analysis of CI, quantitative risk assessments and real-time decision support.
- Improved cyber security including developing new methods for protection from, response to and recovery from attacks. Next-generation security for IP-based process control systems and tools to support software assurance is important.

- Improved Prevention and Protection with the focus on low-cost physical perimeter and area defence systems for CI. Develop interpretation systems for automatic protection and detection.
- Improved Large-scale Situational Awareness for Critical Infrastructure with the aim of creating a common, national operating picture of the CI. Issues included are the development of multi-database monitoring systems.
- To develop Next-Generation Designs and Architectures for Devices and Systems including next-generation infrastructural concepts, with designed-in and built-in security.
- To develop a Human-Technology Interface that Allows Better Comprehension and Decision to address the interface between people and technology.

4.5 ICT related R&D at the US Department of Homeland Security

The Department of Homeland Security (DHS) has five major directorates: Border & Transportation Security, Emergency Preparedness & Response, Science & Technology (S&T), Information Analysis & Infrastructure Protection and Management. S&T is the primary research and development arm of the Department with a budget of 1.1 billion USD in 2005 or about 2.8 percent of the total DHS budget. It provides federal, state and local officials with the technology and capabilities to protect the homeland including state-of-the art systems to prevent, detect, and mitigate the consequences of chemical, biological, radiological, nuclear, and explosive attacks. S&T also develops equipment, protocols and training procedures for response to and recovery from attacks. Methods and capabilities to test and assess threats and vulnerabilities are also developed. S&T conducts and funds research in the three main categories: countermeasures such as biological and chemical, department components such as critical infrastructure and cyber security and cross-cutting such as rapid prototyping.

The department components are:

- Border and Transportation Security including the prevention of entry of terrorists. The Container Security Initiative for cargo pre-screening has a budget of about 100 million USD (DHS 2005B).
- Critical Infrastructure Protection including tools to analyze risks and prevent attacks on the critical infrastructure.
- Cyber Security including R&D and testing to improve cyber security.
- Emergency Preparedness and Response including support for planning and response to disasters.
- Threat and Vulnerability, Testing and Assessment including development of solutions to evaluate threats.
- U.S. Coast Guard and U.S. Secret Service including technologies to improve performance and support the mission.

Table 5 Some DHS Initiatives, budget 2006, million USD

Revolutionizing the Borders	**Budget**	**Technology focus**
The Container Security Initiative	138	Pre-screening, RFID
Americas Shield Initiative	51	Surveillance based on sensor networks
US-VISIT	390	Data mining
Long Range Radar	44	Radar for aircraft detection
Leveragning Technology		
The Domestic Nuclear Detection Office	227	Nuclear detection
Low Volatility Agent Warning System	20	Chemical warning system
Portable Air Defense System	110	Anti shoulder-fired missiles research
Cyber Security	73	24/7 cyber threat watch & warning
High Speed Operational Connectivity	174	Improved management of screening
Emerging Checkpoint Technology	50	Checkpoint screening
Homeland Security Data Network	37	Data network for classified data
Homeland Security Operations Center	61	Security Information Network
Strengthening Law Enforcement		
The Integrated Deepwater System	966	E.g. helicopter acqusitions
The Federal Air Marshal Service	688	Air security protection

Source: DHS 2005B

Department of Homeland Security Advanced Research Projects Agency (HSARPA) is an office within the S&T that invests in programmes offering the potential for revolutionary changes in technologies that promote homeland security. HSARPA performs funding by e.g. awarding procurement contracts, grants and agreements to public or private entities. HSARPA also supports rapid prototyping and technology transfer. The Office of Research and Development funds research, development, testing, and evaluation (RDT&E) and has established three University Centres of Excellence (COE). The annual funding to the CoEs is about 15 million USD.

The air, land and marine transportation systems are designed to provide accessibility and efficiency which make them highly vulnerable to different attacks. Aviation security has been a major priority of transportation security policy since 2001 (CRS 2005A). The aviation security strategy is based on a “Risk-Based and Multi-Layered Approach”. Resources should be allocated to where they are considered most needed and redundancies are also established to prevent attacks. The aviation security system includes areas such as Passenger Pre-screening, Passenger Screening, Baggage Screening, Air Cargo Security, Airport and Aircraft Access Controls and In-Flight Security Measures.

Table 6 US IT Security R&D Priority Areas, an overview

DHS Critical Infrastructure R&D Priorities
Improved Sensor Performance
Advanced Risk Modelling
Improved Cyber Security
Prevention and Protection
Large-scale Situational Awareness
Next-Generation Designs and Architectures
Human-Technology Interface
PITAC Recommended Priority Areas
Authentication technologies
Secure fundamental protocols
Secure software engineering and software assurance
Holistic system security
Monitoring and detection
Mitigation and recovery methodologies
Cyber forensics
Modeling and testbeds for new technologies
Metrics, benchmarking and best practices
Non-technology issues
NSF Cyber Trust Program
Security of next generation operating system
Forensic and law enforcement foundations
Human computer interface for security
Cross-disciplinary approaches
Theoretical foundations and mechanisms for privacy, security, trust
Composable systems and policies
Improved ability to certify system security properties
Improved ability to analyze security designs
More effective system monitoring

Source: DHS 2005B, PITAC 2005A, NSF 2004A

4.6 IT Security R&D in Japan

The science part of the R&D budget of the Ministry of Education, Culture, Sports, Science and Technology (MEXT) for 2005 increased 2.6 percent from 2004. MEXT mainly supports basic research at universities and national laboratories and finances through Japan Society for Promotion Sciences (JSPS) and Japan Science & Technology Agency (JST). As for the details of what the 43 billion JPY on R&D into information technology covers, no data are available. There are, however, mentions of specific initiatives, a few of which directly relate to IT security and add up to 2,491 million JPY for 2005, or 5.8 percent of the total IT R&D budget[10] (MEXT 2004A, MEXT 2004B).

[10] *Data were compiled from presentations at MEXT, May 2005. "FY 2005 Budget (1)" and "Major items in the Fiscal 2005 budget"*

Table 7 Ministry of Education, Culture, Sports, Science and Technology, FY 2005 Budget

MEXT Budget, FY 2005	***million JPY***
Education & Science	5 723 400
Science	1 317 000
Strategic promotion of R&D; IT	42 785
Reposted, security related	
Ultrahigh speed network project (National research grid initiative)	1 950
Software for electronic preservation and practical use of intellectual property	470
Sensor technology for a safe and secure society	71
Total, security Related	**2 491**
Reposted, other	
Super computing and basic tech for u-technology	2 974
Promoting fusion field of information science and Nano tech (Nano-IT)	4 572
Promoting R&D to practical applications in the field of IT, (Commercialization)	10 054
Promoting computerization of R&D. Databases & infrastructure	7 450

Source: MEXT 2004A, MEXT 2004B

The Ministry of Internal Affairs and Communication, MIC, expresses its opinions on the most important IT security R&D in their financing of the National Institute of Information and Communication Technology (NICT), and often make mention of wide-area monitoring system technologies, trace-back technologies and countermeasures against Botnets as important fields for R&D. NICT has been newly formed from the merger of the Communications Research Laboratory, CRL, and the Telecommunications Advancement Organization, TAO. Its budget of about 530 million USD is roughly divided between funding NICT intramural labs and university research.

An example of security-relevant ICT-Research is in the field of Quantum Information Science. Progress in this area has implications for security as well as several other aspects of computing. An overview of national R&D programmes in this area was presented in 2004 by ATIP. Over the period of 2000 and 2005, 54 million USD were distributed by MEXT (36.6 USD), METI (6.9 USD), and MIC (10.5 USD) (ATIP 2004).

The National Public Safety Commission regularly surveys what government-funded or supported IT security R&D is being undertaken and in what areas, in compliance with the 1999 law on unauthorized computer access. The following is a list of recently finished and still ongoing projects. Alas, there is no information on the budgets for each of these R&D initiatives (MIC 2005B, NPSC 2005).

Table 8 Ongoing and Completed Research & Development Programmes in Japan, an overview

Ongoing Research & Development Programs	Duration	Organizations
Security vulnerability of Internet applications	2000	AIST Grid Research Center
Information communication risk management	2000-2005	NICT
Wide area monitoring system	2004-2006	Yokogawa, Hitachi, Oki contr. from NICT
Decision making system for secured operation	2004-2006	NTT Comm., Hitachi, NEC contr. from NICT
Mobile security to develop commonly usable and secured base for mobile commerce	2004-2006	Hitachi, NTT DoCoMo, KDDI, and NEC contracted from NICT
Security protection technologies for mobile terminals	2004-2006	Hitachi contracted from NICT
Advanced cryptographic technologies for authentication with smart card aiming for ubiquitous network society	2004-2006	Hitachi contracted from NICT
Recently Completed Research & Development Programs		
Structures for integrated security operation	2002-2004	Matsushita, Kogakuin Univ., Yasukawa Information System, and NTT
Base technologies of cryptography application program interface	2001-2003	NEC contracted from NICT
Secured information communication network which does not allow to send any un-known source packets	2001-2003	NEC contracted from NICT
Base technologies of the next generation authentication	2001-2003	Hitachi contracted by NICT
Data protection technologies for advancement of information security	2001-2003	NEC, Mizuho, Ricoh System, Tokyo Inst. of Tech., and NTT Com. contr. by NICT
Administration technologies of security policy while interconnection of networks	2001-2003	Fujitsu, Kyushu University, Fujitsu Prime Software Technologies
Interoperability of services which use attribution authentication	2001-2003	Hitachi contracted from NICT
Structures for integrated security operation	2002-2004	Matsushita, Kogakuin Univ., Yasukawa Info. Sys., NTT Adv. Tech. contr. by NICT
Development of secured WebDAV (Distributed Authoring and Versioning protocol for the WWW)	2003	SRA Key Technology Laboratory contracted from IPA

Source: MIC 2005B, NPSC 2005

4.7 IT Security R&D in China

The most important IT Security projects have been performed under the 863 programme funded by the Ministry of Science and Technology (MOST). Within the 863 subprogram Information Technology there is a special category of projects called Information Security Technology Projects. Unfortunately, almost no official information about these seems to be available.

Two important governmental actors in the IT security research area are the National Key Lab of IT Security and the Software Research Institute, both under the Chinese Academy of Sciences. The National Key Lab studies how to carry out IT security risk evaluation work, especially study on evaluation tools, while the Software Research Institute does research and development into highly safe operation systems. Development is carried out on a Linux operation system.

Since there is a great shortage of IT security professional people and technicians, China will also invest more in setting up a specialized IT security university or college to provide special IT security-related courses.

Starting from 1999, total investment in China on the development of IT security products has been around RMB 600 million, of which RMB 200 million has come from the National Development and Reform Commission (NDRC) and RMB 400 million from other channels such as venture capital investment, etc. Concern-

ing the future development of products, NDRC will be working on a special plan for the development of IT security from 2006-2010. The plan will be ready by the end of 2005 (NS 2005B).

The Ministry of Science and Technology considers the following areas within IT security to be of special importance:

- Public Key Infrastructure (PKI)
- Anti virus software and secure software based on open sources
- Safety access device
- Special computers having specially designed ICs

The primary sectors for which applications should be developed are financial institutions (banks, stock markets) and government agencies, but also e-medical applications (Liu 2005). Also here there are great difficulties to obtain more detailed information about the technological directions favoured by MOST.

There is an on-going discussion about the future direction of the research initiatives. According to Prof. Zhao Zhansheng at the National Key Lab the R&D work should be focused on the following aspects (Zhao 2005):

- security hardware that can be embedded into the net system
- development trends of the core of the security software, which means work on chip research and development
- research on response systems and computers that can cope with sudden attacks and how to fast spreading information on IT security incidents

Another voice is that of Prof Xu Guangnan, a member of the Chinese Academy of Engineering Sciences. In an article written for *IT Security and Telecommunication Magazine* he argues that the most important thing is to work out China's own basic software. He thinks that basic software is essential to the failure or success of IT security. Basic software such as operating systems, data bases, and some universal functioned software still relies too much on foreign companies. He thinks that the government should provide national resources to support local software development and also provide a market for locally made software (Xu 2004).

Government-funded projects have been the key driver for the development of domestic security products and suppliers. The reason for this is that in most IT security projects initiated by the government only domestic enterprises are permitted to participate. Products supported by the powerful National Development and Reform Committee (NDRC) have been firewalls, safety access equipment, safety data bases, and anti-leaking computers. The principles to acquire support from NDRC for the production of IT security products are:

- Fundamentally upgrading the creativeness of the technology
- Improving the professional service capability
- Being essential to the development of standardization
- Improving the capability of China's self-controlled technology and products

It has often been State Owned Enterprises (SOE) that has been engaged on IT security projects. For example, only three companies: Koal Software, Jilin University Information Technology Co Ltd, and iTrustchina (all SOEs) are involved in providing e-signature-related technology and products for China's national and metropolitan Certification Authority Centres. Some smaller, privately-owned domestic security companies, such as GateGuard and CNNS, have participated in certain government projects, but still face difficulty in securing contracts for large-scale core projects. As mentioned earlier, foreign security are still restricted from participating in most government IT Security projects. The examples below all describe projects where SOEs have been involved.

- **WPKI Core Technology Project** The aim of this project was to develop a functional server system (with wireless certification), a WPKI (Wireless Public Key Infrastructure) security net password, and an embedded safety chip for mobile use. The project was carried out by Changchun Jida Zhengyuan Information Technology Company Ltd and successfully completed at the end of 2004. Government funding was RMB 70 million for three years (2002-2004), and according to reports, all the products produced have met or surpassed their specifications.
- **Information Net Security Check and Response System** The purpose of the project was to check abnormal action on a high speed net. The outcome, in 2004, was three chips (inspection, monitoring and response). The government funded Beijing Qiming Xingchen Information Technology Company Ltd with RMB 60 million of investment (2002-2004) for the project. At present, products from the project are used by customers from 31 provinces and cities in China. MII, MPS, major banks and institutions of the national defense are all users of the product.
- **Intrusion Detection System** During the period 2001-2003 Tianjin Nankai Chuangyuan Information Technology Company Ltd developed China's own solutions to replace foreign software products within IDS (Intrusion Detection Systems). Today, most ministries (both at central and provincial level) and stock exchange centres (approx 85 percent) have replaced their old software with the new type developed in this project.
- **PKI Net Security Platform** The government funded DeAn Computer Technology Company LTD with RMB 50 million (2002-2003) to develop a new PKI (Public Key Infrastructure) platform to replace existing foreign PKI Net Security Platforms. Since completion the project has successfully met the annual revenue target of 200 million RMB.

5 Some Trends within the IT Security Industry

5.1 USA

IT security is a segment within the IT industry and it is also an important business driver to consider. The worldwide market for IT security is estimated at about 13 billion USD in 2004. More and more companies need to provide enhanced security features for offered services and products. The market can be divided into three segments: the largest segment is threat mitigation representing 42 percent of the market and includes products such as anti-virus software, firewalls and application gateways. Command and control including identity management, intrusion detection and event management represent 40 percent of the market and managed security services 18 percent (IW 2004A). Demands on suppliers are increasing and more consumers are requiring them to be legally and financially liable for security vulnerabilities. The implementation of performance-based pricing for software is also an option to increase the vendor accountability but the solutions are not attractive to suppliers. Several business models also depend on secure networking, and security is becoming integrated into the business models. Security is often a prerequisite for the business. The adoption of security solutions is today most of all driven by the need to protect data than because of regulatory compliance and only lastly to prevent downtime according to a study by StillSecure (CN 2005A). IT security budgets increased to about 6 to 9 percent of companies' IT budgets in 2004 from 3 percent in 2000 (SHG 2004A). But increased focus on IT security governance in combination with less cost because of compliance activities can reduce the need for further budget increases.

A single IT security product is not considered sufficient by the IT security industry and the trend within the industry is bundling of security products. Cisco have bundled firewalls, VPN and intrusion prevention, and anti-virus detection into a single device. New, integrated service routers that combine security capabilities with network routing and switching are also provided by Cisco and preferred by customers according to different studies. More security features will become commodity features of the products in the future. If IT security is to be more integrated into other networking products, it will be more of a platform component than a specific segment. Another major trend in the industry during 2004 was the consolidation of companies. One of the leading US IT security companies is Symantec with an annual revenue of about 2.8 billion USD and a revenue growth for the fourth quarter 2004 of 28 percent. Symantech acquired Veritas Software at the beginning of 2005 and has also acquired the companies Brightmail, ON Technology, and TurnTide in 2004. The acquisition of Veritas gives Symantec a better position as a business security software provider

One of Microsoft's priority areas is security and the company acquired several IT security firms last year such as GeCAD Software providing anti-virus, Giant Software providing spyware detection, Pelican Software providing behaviour-based security and Sybari Software. Microsoft gave its concept Trustworthy Computing (Next-Generation Secure Computing Base) high priority in 2002 but the launch of

new functionality is believed to have been delayed. In February 2005 Microsoft launched its Security Cooperation Program with the aim of creating an open dialogue regarding security-incident response, reducing the severity of Internet attacks and fostering educational outreach to citizens (IW 2005B). The program is open to national and state governments worldwide. Multiple IBM-Microsoft specifications for secure Web services are almost ready for submission to standards bodies.

The magazine Red Herring published a list of the 100 "hottest private companies in North America" in May 2005 (RED 2005A) based on an analysis of more than 700 companies according to the magazine. Of the 100 selected companies 16 percent are in the Security and Defence sector, 25 percent in the Computing sector, 24 percent in the Biosciences and 16 percent in the Internet and Services. The list can be seen as an indication of "industrial sectors where technology is exciting, where money is being invested, and where the possibility of long-term growth is strong" according to the magazine. California is the home of 48 of the 100 selected companies, indicating that California is still the major innovative region.

Table 9 Private Security and Defence Companies

IT Security Companies	Focus area
AirDefense	Monitoring of Wi-Fi traffic
AppIQ	Data storage control software
ArcSight	Data -collection and analysis software for security
CipherTrust	Anti-spam software
Crossbeam Systems	Single box security devices
Cyota	Online fraud prevention
Crossbow Technologies	Smart dust motes, open-source TinyOS
eEye Digital Security	Vulnerability management
Elemental Security	Policy management solution
Fortinet	Unified Treat Management
Prolexic Technologies	Denial-of-service attack prevention
Webroot Software	Anti-spyware software,

Source: RED 2005A

5.2 Japan

By July 2004, 99.8 percent of Japanese companies had implemented virus measures. 88.8 percent had firewalls and 11.2 percent have client-side firewall software. As for making IT security policies, 35.6 percent of Japanese companies have already implemented policies, while 20.8 percent are intending to do so, and 32.9 percent are investigating how to do so (MIC 2004B, MIC 2004C). Illegal activities, and the mere threat of it, are making the market for IT security products and service a growth area. The market for PC-security software grew 29 percent to 22 billion Yen for 2004 and the Fuji Kimera Research institute predicts an additional 40 percent growth for 2005, to over 30 billion Yen (NE 2005). Overall, the information security market grew from 72.7 billion yen in 2000, to 222.6 billion yen in 2003, and was estimated at 291 billion yen in 2004 (JETRO 2005C).

According to JETRO[11] (JETRO 2005D), Japan External Trade Organization, Japan's information security market is growing favourably due to strong demand for services as well as products. As most corporate users have taken the necessary steps to protect themselves from external attacks, more attention is being given to strengthening internal security e.g. authentication, and encryption. Implementation of the Personal Information Protection Act has been preparing companies for this since 2003 and certainly also stimulated the demand for information security business through ISMS and P-Mark certification. The estimated value of the "network security business" in Japan was 291 billion yen for 2004, composed of 78 billion yen for services and 213 billion yen for products. Generally, JETRO is identifying a trend of increasing orientation towards information security services, reflected by companies' initiatives to develop service business in co-operation with service suppliers and others.

Whereas the Japanese market for security services is mainly catered for by domestic firms (except for ISS's intrusion service; VeriSign Japan's authentication service; and the firewall services by Juniper and Nokia (FIREWALL-1)), the market for security products is roughly divided 50/50 between domestic and overseas firms. The importance of high name-recognition and trust is thought to be a contributory factor to the strong position of overseas firms.

Table 10 Information Security Market, Annual Sales, by Category. Billion yen.[12]

Services, (Fiscal Year)	**2000**	**2001**	**2002**	**2003**	**2004**
Security inspection, policy formulation and education	3,8	5,3	6,9	17,0	25,6
Illegal access monitoring services	1,4	3,0	5,3	6,8	13,0
Virus monitoring services	0,6	2,1	5,0	9,2	14,0
Firewall operation and management services	1,0	2,5	4,5	7,2	12,0
Electronic authentication services	3,0	2,0	4,5	8,4	13,0
Subtotal (billion JPY)	**9,8**	**14,9**	**26,2**	**48,6**	**77,6**
Products					
Authentication products	8,9	11,8	17,7	20,3	25,1
Encryption products	2,1	3,1	3,9	7,3	13,9
Firewall, VPN and integrated equipment products	24,8	51,5	72,7	68,1	74,4
Security inspection, monitoring and analysis tools	6,4	11,5	14,5	21,1	26,6
Anti-virus tools	18,1	27,7	36,0	47,3	60,0
Filtering software	2,6	4,6	7,4	10,0	12,9
Subtotal (billion JPY)	**62,9**	**110,2**	**152,2**	**174,1**	**212,9**
Total (billion JPY)	**72,7**	**125,1**	**178,4**	**222,7**	**290,5**

Source: JETRO 2005D

[11] *This section is based on the JETRO Report, "Trends in Japanese Information Security Industry (May, 2005)" based on a survey commissioned by Fuji Kimera Research Institute.*

[12] *1. Security inspection, formulation and education services did not include education prior to 2002. 2. Firewall, VPN and integrated equipment products did not include integrated equipment prior to 2002. Source: Fuji Kimera Research Institute, "Comprehensive Survey of the Network Security Business".*

New threats, demands for regulatory compliance, and increasing workloads are making it increasingly difficult for users to manage security measures on their own. This falls in the hands of companies that want to focus less on simple service provision and more on the construction of secure facilities, transforming these to Managed Security Service Providers (MSSP), catering for a growing demand for IT security outsourcing.

The Nikkei Electronics, a bi-monthly technical magazine, surveys Japan's twelve most prominent ICT corporations every January of R&D themes they consider to be the most important ones for the year ahead. In the 2005 edition, five companies explicitly mentioned IT security issues (Toshiba, security-related technologies and intellectual property protection, Fujitsu, secure applications and devices, Mitsubishi Electric, security solutions, NTT, security-related technologies, OKI, security-related technologies). Another five areas mentioned where IT security is bound to be an integral part (Hitachi, sensor networks, digital appliances, Sony, broadband network technologies, NEC, IT & network-integrated solutions, Sharp, ubiquitous network-related technologies, Sanyo, home network technologies), while two made no mention of security (Panasonic (Matsushita), and Canon) (NE 2005A).

There is a strong infrastructural foundation in Japan with the IPv6 roll-out and certainly there are glimpses of outstanding IT security work of Japanese origin, e.g. in cryptography and quantum communications. But the country is not strong on IT security products (or services) on the international market.

5.3 China

Just to remind the reader of the magnitude of the Chinese ICT market two figures concerning the telecom/IP market will be given: there are presently (August 2005) about 600 million (mobile and fixed) telephone subscribers and about 100 million Internet users in China. Increasing Internet penetration, as well as escalating computer and network attacks, is driving the growth of China’s security market. The market value of IT security products in China has increased from RMB 2.1 billion in 2003 to estimated RMB 3.8 billion RMB in 2005, and RMB 5.6 billion in 2007 according to IDC (CCW 2005). Currently, the deployment of security systems in China, especially by domestic companies, is still at a relatively early stage. Foreign enterprises invest an average of 4-5 percent of their total IT budget in security products, while Chinese companies spend less than 2 percent (IFC 2005).

Three major factors have been of great importance for the market development of IT Security. Firstly, the great need of enterprises and the whole of society to speed up the construction of informatization. Secondly, the leading and promotional role played by the Chinese government in creating several key national informatization projects, and, thirdly, the easy access and upgrading of IT Security products. Since 2004 some locally made IT security products have been of a much better quality than earlier, and have been therefore also well accepted by local customers in China.

To date, anti-virus and firewall products have been the most widely adopted security products, reflecting the fact that the two biggest threats for most enterprises in China are virus and hacker attacks.

Table 11 Some Facts about the IT Security Market in China, 2004

Products	%	Customer Segments	%	Suppliers	RMB, million
Firewall	46,3	Finance	20,9	Symantec	34
Anti-virus	26,8	Government	20,6	Cisco	32
IDS	11,7	Telecom	16,7	TopSec	30
AAA	4,5	Energy	7,5	Rising	29
Others	10,7	Manufacture	6,8	Neusoft	29
---		Education	6,2	Jiangming	25
---		Logistics	5,1	Trend	25
---		Transportation	4	NetScreen	23
---		Others	12,2	CheckPoint	21
---		---		Kingsoft	18
Total	**100**	**Total**	**100**	**Total**	**266**

Source: CCW Research

Domestic suppliers (TopSec, Rising, Neusoft, Jiangming, and Kingsoft) accounted during the first quarter of 2004 for 49 percent of the top ten ' total revenues in China.

- *TopSec* was founded in November 1995 and is China's earliest and largest company in the network security area. TopSec developed the country's first domestic firewall in 1996, and subsequently launched security auditing and security management products. In 2003 TopSec launched a wider range of security solutions. TopSec is one of the companies authorized by the Chinese government to evaluate the source code of Microsoft Windows.
- *Rising* Technology Corp Ltd was founded in April 1998. It is a leading anti-virus software provider in China. The company offers anti-virus, firewalls and intrusion detection functionality and security services to enterprise customers and service providers around China.
- *Neusoft* was founded in 1988 on the basis of Software and Computer Department of China Northeast University. The company's major products are software and service on digital medical equipment. At the same time it is also making product of firewalls like Net Eye and provides total net solutions to big companies.
- *Jiangmin* was founded in 1996. It is an IT security technical development and service provider. It is one of the top producers of software for killing viruses.
- *Kingsoft* entered the software industry in 1988, providing application software products and network services in China. Its products include desktop office applications, information security, games and entertainment. In the information security field, Kingsoft's main focus is anti-virus software and on-line anti-virus services for both the customer and enterprise market.

6 Standardization and Certification

6.1 Standardization and Certification in the USA

The National Institute of Standards and Technology (NIST) is responsible for the development of measurements and standards for IT security. Federal agency security programs need to be consistent with NIST guidelines. NIST IT security standards, metrics, tests, validation programs and guidelines are an important part of the federal IT security program according to Office of Management and Budget (OMB) (OMB 2004A). NIST is also involved in raising awareness of IT risks. The activities at NIST also facilitate the transfer of technologies to the market. NIST is engaged in several different IT security initiatives such as system certification, procurement guidelines, security guidelines for e.g. firewalls, developing minimum security standards, maintaining Common Criteria for specifying security requirements used by private laboratories, and operating a security expert assist team. NIST also maintains a website of effective federal agency security practices. Research into cyber security is also performed at NIST. The budget for cyber security research was about 10 million USD in 2004 and is planned to be increased to about 20 million USD in 2005.

The National Information Assurance Partnership (NIAP) is a U.S. Government initiative with the aim of meeting the security testing needs of both information technology (IT) consumers and producers. NIAP is the result of collaboration of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). NIST and NSA have promoted security in commercial off-the-shelf IT products for over two decades. The partnership combines the extensive IT security experience of both agencies in order to promote the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems. NIAP supports the Common Criteria framework for international recognition and acceptance of IT security testing and evaluation results. The purpose of NIAP is to increase trust in information technology with cost-effective testing and certification. The Cyber Security Industry Alliance considers that there are several challenges for NIAP such as reducing the cost and increasing the speed of the certification process, developing the process in line with both government and industrial needs and ensuring that federal procurement policy related to NIAP is applied (CSIA 2004A). Promotion of quality in commercial software is important.

Automatic security functional testing is of importance according to NIST. Experience with security evaluations of products in recent years has shown that such evaluations are a very expensive and time consuming process from the point of view of suppliers of IT products according to NIST. However, security functional testing is an important component of security evaluation, time and cost considerations are less prioritized among overall security evaluation schemes except in the case of High Assurance Products. Improving the economics of security testing is of importance. The formal modelling language Software Cost Reduction (SCR) developed by Naval Research Laboratory (NRL) is used by NIST.

Some other initiatives at NIST are:

- Federal Information Processing Standards (FIPS) have been defined by NIST and some are mandatory for use by the federal agencies. The FIPS 200 Minimum Security Controls will be mandatory for federal information systems in December 2005.
- The Cryptographic Module Validation Program (CMVP) is led by NIST and the Government of Canada's Communications Security Establishment, and provides for the voluntary testing of cryptographic modules.
- NIST has developed an interactive Web-based IPsec tester. IETF asked for an Interoperability Test System for the Internet Security Protocol (IPsec).
- NIST is involved in the development, maintenance, and promotion of a number of standards and guidance that cover a wide range of cryptographic technologies.
- NIST also co-operates with other agencies and the industry to advance the development and use of security configuration checklists including a set of instructions for configuring IT products. Checklists are considered useful particularly for smaller organizations with limited resources. One such guide is for Information Technology Security Services including advice for the selection, implementation and management of security services. The Center for Internet Security with members from the private and public sectors also develops configuration benchmarks for different products in order to lower the cost of e.g. patching systems.
- A publication including technical requirements for verifying electronic identities has been issued by NIST. The Security Assertion Markup Language (SAML) is used for managing identity credentials.

6.2 Standardization and Certification in Japan

The Japan Industrial Standards, JIS, offers requirements (JIS Q 15001) to comply with the Personal Information Protection Act. Furthermore a certificate of compliance known as the Privacy Mark, or P-Mark, is offered by the Japan Information Processing Development Corporation (JIPDEC). The Safe Security ISP-Mark[13] is often used in combination with the P-Mark. The certification scheme does not, however, comply with any established standard. The ISP-Mark was established in 2002 to show compliance with the Telecommunications Business Law of 1983 (No.86) and it was amended in 2005 to comply also with the Personal Information Protection act. This mark is administrated by the Japan Internet Providers Association (JAIPA) and Telecom Services Association (TELESA). 139 ISPs and public and commercial websites bear the mark, 65 of which were added in 2005. Compliance with the P-Mark has more strict terms. It includes the training of staff and establishing the quality of the security of data, equipment, and routines for storing. Companies can do this work themselves or make use of consultants that are available. Companies with branches in the USA may already be certified through the

[13] *www.isp-ss.jp*

BBB-Online Privacy Seal. The Better Business Bureau in co-operation with JIPDEC has ensured that such cases are already in compliance and are eligible for the Japanese P-Mark certificate. Since the P-mark was introduced in 1998, 1200 companies had been certified by May 2005. With the recent enforcement of the Personal Information Protection Act the number of certified companies has risen to 1638 (June 29) and more are expected to follow. (PC 2005) (JIPDEC 2005A) (METI 2005)

6.3 Standardization and Certification in China

The IT Security Standardization Technical Committee of the Ministry of Public Security[14] was set up in 1999. Its main mission is to plan and formulate IT Security standards, and technical standards, as well as monitoring the application of technical standards. The scope of its responsibility to make the related standards covers products, organizational issues, information classified security protection, but also grade evaluation and examination.

In April, 2002, in order to strengthen the work of IT security standards, the China National IT Security Standard Technical Committee[15] was set up (registered as TC 260). It is mainly responsible for standards within the following areas:

- Security technology
- Security system or structure
- Security service
- Security management
- Security risk evaluation

The Information Classified Security Protection Evaluation Center within the Ministry of Public Security[16] was set up in 2003. The main mission of the Center is to evaluate the information security protection status of the national key sectors and provide suggestions for promotion, upgrading or consolidation. In 2004, in order to speed up the work of making China National IT security standards, with the approval of the Central government, a special project named *China National IT Security Strategy Research and Standard Making* was listed as a special project to get all direction support from the government. So far, 47 IT security-related national standards have been published, and 40 IT security-related national standards are under consideration. In addition, the Ministry of Information Industry, the Ministry of Public Security, and the Ministry of State Security, the China National Secret Code Management Committee has also published some IT security industrial standards.

The Chinese government has implemented strict controls on the research, manufacturing, and marketing of security-related products through several approval processes. All IT security-related products sold in China must be certified by the

[14] *Http://www.china-infosec.org.cn/standard*
[15] *http:// www.tc260.org.cn*
[16] *Http://www.cspec.gov.cn*

Computer Information Network Security and Product Quality Supervision Center of the Ministry of Public Security. A *Certificate for Information Security Products* from the China Information Technology Certification Center (CNITSEC) is also necessary for products sold on the civilian market.

The China Information Technology Security Certification Center has four major business scopes, namely

- Certification of IT Security product
- Certification of IT systems
- Certification of service institutions, companies, etc
- Certification of people providing services

For products to be sold to the military sector, manufacturers must have additional certification from the State Secrecy Bureau and the People's Liberation Army Information Security Evaluation and Certification Centre. For some technologies such as Public Key Infrastructure (PKI) and encryption, government regulations are particularly strict, with only state-owned enterprises (SOEs) appointed to engage in product development. However, China worries about the possibility of hidden programs imbedded in foreign products.

6.4 Common Criteria in the USA, Japan and China

The Common Criteria (CC) or ISO standard 15408 is the result of a multi-year initiative by the governments of the US, Canada, United Kingdom, France, Germany, and the Netherlands to develop harmonized security criteria for IT products. Further countries such as Japan and Australia today have a national scheme (Common Criteria Recognition Arrangement (CCRA)) for conducting Common Criteria evaluations. Further countries such as Sweden accept the certificates but not e.g. China. Globally only 22 countries accept the Common Criteria. International recognition of CC certificates only covers assurance levels 1-4. The Common Criteria are a framework for functional security requirements including a standardized means of evaluation with different assurance levels. The US National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme (CCEVS) Validation Body is an activity managed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The focus of the CCEVS is to establish a US programme for the evaluation of information technology products in conformity with the International Common Criteria for Information Technology Security Evaluation. The Validation Body approves participation of security testing laboratories, about 10 laboratories in the US. The Validation Body also provides technical guidance for those testing laboratories, validates the results of IT security evaluations for conformity with the Common Criteria, and serves as an interface for other nations concerning the recognition of such evaluations. IT security evaluations are conducted by a commercial testing laboratories (Common Criteria Testing Laboratories) approved by the Validation Body. Issued Common Criteria certificates only apply to the specific versions and releases of the certified products. Critics say that Common Criteria testing costs too

much and takes too long. According to NIAP 100 percent of the products evaluated for Common Criteria have been approved. About 40 percent of the products evaluated were improved by the addition or extension of security features. Further information about Common Criteria can also be found on the Common Criteria portal.

National Security Telecommunications and Information Systems Security (NSTISS) policy number 11 issued in 2000 and revised in 2003 is a national security community policy governing the acquisition of information technology products. NSTISS is now called the Committee on National Security Systems (CNSS). The policy mandates that, as from July 2002, departments and agencies within the Executive Branch will acquire, for use on National Security Systems, only those off-the-shelf products that have been validated with the International Common Criteria for Information Technology Security Evaluation, the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS), or by the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS). Departments and agencies may wish to consider the acquisition of validated COTS products for use in information systems that may be associated with the operation of critical infrastructures according to CNSS (CNSS 2005A). A problem has been that not enough products have gone through the evaluation process and "many agency officials do not understand how Common Criteria tests fit in with a complete security strategy" according to Federal Computer Week (FCW 2004A). Only 30 products were certified in the US until 2004, but 42 products were also under evaluation. The lack of requirements from civilian agencies makes it more difficult for suppliers to justify the long and expensive evaluation process.

The Japanese Information Security Certification Office, ISCO, conducts ISO/IEC 15408 based certification under the organizational label JISEC, Japan Information Technology Security Evaluation and Certification Scheme. The "ISO/IEC 15408 Evaluation Criteria for IT Security" corresponds to the Japanese JIS X 5070, and are the so-called Common Criteria. This programme awards certification for the security evaluation of IT products and systems conducted by accredited evaluation bodies in accordance with JIS Q 17025:2000. To date, JISEC has certified 24 products under the common criteria (about 10 percent of all CC certified products world-wide), and an additional 5 products are currently being evaluated.[17] (IPA 2005A) (The 6th International Common Criteria Conference, ICCC, is to be held in Tokyo, September 26-29, with IPA and JISEC as main organizers.)

It was agreed in March 2001 at a ministry liaison conference that each ministry and agency should utilize the common criteria certification scheme for public procurement as much as possible. It is not, however, mandatory and its use has been limited. The Defense Agency seems to have similar procedures for IT systems but with higher evaluation assurance levels (EAL), such as EAL 5 and higher, on its own accord (IPA 2005C).

[17] *www.ipa.go.jp/security/jisec/jisec_e/certfy_list200504.html*

6.5 Information Security Certification Frameworks

ISO 17799 is a detailed standard published as an ISO standard in 2002 including a set of controls for best practice in information security. ISO 17799 is the major standard for information security. The standard includes 11 sections such as Communications and Operations Management, Access Control, Information System Acquisition, Development and Maintenance and Information Security Incident Management. COBIT (Control Objectives for Information and related Technology) is used for IT governance and issued by the IT Governance Institute and includes good practice for control over information, IT and risks. COBIT includes a framework for control and measurability of IT. COBIT is also selected by the European Union Commission as an IT systems security standard. Another method is Information Technology Infrastructure Library (ITIL) developed by the British government in the late 1980s as an approach for the cost-effective use of IT resources. The method includes a process for security management with the aim of "ensuring that effective information security measures are taken at strategic, tactical, and operational levels" according to ITIL. ITIL includes a set of best practice examples for managing IT services, and the implementation of ITIL is driven by security concerns, the compliance requirements and possibility for cost reduction. The Security Capability Model is an approach for security evaluations developed by Carnegie Mellon University based on the Capability Maturity Model (CMM). The model includes the four topic areas Risk Management, Management and Policy, System and Network Management, and Physical Security, the purpose of which is to assess the current security level for an organization.

The Conformity Assessment Scheme for Information Security Management Systems (ISMS) and an Information Security Audit are popular solutions for IT security governance in Japan. ISMS is a system for evaluating information security management systems. It has been operated by the Japan Information Processing Development Corporation (JIPDEC) since April 2002. ISMS is based on the ISO/IEC 17799:2000 international standard and harmonize with BS 7799-2 (and the Swedish SS 627799.2:2003). A 2005 revision will rename this standard ISO/IEC 27001:2005 (27004 will be Information Security Management Metrics and Measurement).

The number of ISMS certifications in Japan as of June 5th is 937. This makes Japan the country with the highest number of such certifications internationally (UK 208, US 20, Sweden 7) (ISMS 2005). According to JIPDEC there is now a trend in Japan of acquiring information security certification quite comparable to earlier trends of certifying business for quality (ISO 9001) and environmental work (ISO 14001). Among the drivers of this trend are the facts that METI maintains an ISMS registration, and accreditation scheme for companies working with systems integration and systems operations. Some local governments condition such ISMS certification for procurement. And there is also the factor of peer pressure in the closely knit community of Japanese corporations where the accreditation of one company often requires the accreditation of subcontractors. A final but important reason is the increased focus on information protection and the Personal Information Protection Act of April this year. The 20 or so US companies that are ISMS

accredited are those that operate in Japan. In general, the US lacks a standard for BS 7799-2 (originating in the UK) and thus has no certification body. They have other ISM guidelines to take heed to, according to JIPDEC.

MIC is currently considering X.1051 (ISMS-T) as new standards and guidelines based on the ISO/IEC 17799. It is expected to be more comprehensive and include security policy, information security incident management, business continuity management, and compliance.

7 Organizational Security Processes

7.1 Risk Management, Policy Definition, Life Cycle Management

Risk management is a discipline that enables people and organizations to cope with uncertainty by taking steps to protect its vital assets and resources. The risk management process provides a framework for identifying risks and deciding what to do about them. Risk management is not just about identifying risks, it is about learning to weigh various risks and make decisions about what risks deserve immediate attention. Risk management is a process that should be integrated into all aspects of the organization's management. Some objectives for the risk management process are reducing injuries, avoiding costly claims, preserving non-profit's reputation in the community, freeing up resources for mission-critical activities, and ensuring adequate risk financing. Risks can be categorized into different kind of assets as people, property, information and goodwill. Today information risk management has become a number one priority in most organizations. Information risk analysis is the cornerstone of any program designed to safeguard information assets. Organizational risks can be managed based on a portfolio approach including assets with different risk profiles. Risk management is also important for Homeland Security. DHS has been criticized for having a lack of strategic thinking (WP 2005A). Homeland Security covers a broad area and prioritization is important to get the best return on investment. As an example a study by the organization RAND concluded that airline antimissile systems are not cost-effective.

The process of complying and measuring an enterprise’s adherence to security policies is the single most important step an organization can take to achieve a reasonable level of security. However, in several organizations IT security is still not considered a strategic issue, and the defined policy is often not implemented. The consulting cost for a standard two-week information security assessment is about 40,000 USD (ISPC 2005A). Combining centralized policy management, host configuration, and network access control will give enterprises greater visibility and control over their security compliance. With the various federal and state regulations, organizations must create or re-evaluate their current security policy and process architecture. Some may discover that they have all the pieces spread throughout the current organization, but do not know how to proceed to insure that their security policies and processes comply with various regulations. Privacy, security, and liability also need to be covered within policies.

More and more information technology-based assets are being used by organizations to handle sensitive data that are important for the company’s future. Several industries such as healthcare and financial services are also subject to the data security provisions of legislation such as HIPAA, Sarbanes-Oxley and Gramm-Leach-Bliley. Efficient asset tracking during the entire lifetime of the hardware is an import part of information security. Sarbanes-Oxley requires seven years of asset tracking. Careful processing of the assets at the end of their usefulness is important, and data erasure methods need to be used. The Office of Management and Budget

requires agencies to ensure that security is incorporated in the life-cycle of all IT investment (OMB 2004A).

7.2 Awareness, Education and Certification

The use of information and IT security solutions often places different constraints on the user. In several cases the implementation of IT security solutions can reduce productivity, at least in the short-term. The user of information systems needs to be motivated and be aware of the threats and the impact they can have on the organization. The Information Technology Association of America launched an Information Security Awareness Certification programme in 2004 to help organizations to assess cyber security within the organization. The programme includes e.g. an online test. A common perception today is that greater network security is not worth the cost for individuals and organizations. This perception discourages investment in new solutions for improved security. The perceived value of trust in the IT infrastructure needs to be enhanced according to PITAC (PITAC 2005A).

There is also a lack of competence in IT- and information security. The federal government hiring of employees in the coming years will be driven by jobs concerned with homeland security (WP 2005A). The federal administration will be implementing further requirements on information security certification for employees. Today several different information security certifications exist. One of the most established is Certified Information Systems Security Professional (CISSP). In total there are about 34,000 certified persons in 110 countries. CISSP certification is administered by the International Information Systems Security Certification Consortium (ISC)2. CISSP certification has a policy focus concerned with information security. Other certifications are Certified Business Continuity Planner (CBCP) and Certified Information Systems Auditor (CISA). Fewer than 100 people graduate with a Ph.D in cyber security in the US each year. Purdue University has one of the largest graduate programmes for information security.

The Telecommunications Software Forum in Japan reported in 2003 a shortage of 120,000 people in security administration in Japan. MIC has since 2001 enhanced the development of human resources in this field by promoting security certification[18] and building support programmes for HR development in order to nurture technical experts on security management. IT security awareness is prioritized in Japan.

7.3 Identity and Access Management

User's identities and their level of access are of importance for several organizations and need to be managed in an effective way. The definition and management of identities is rather complex. Identity is a set of characteristics associated with a person and the possibility of confirming identities is also important. Biometrics is one way of confirming identity. Different countries also have different national identity schemes. The increased number of access points, a large number of busi-

[18] *By adding information security to the examination for "Chief Telecommunications engineers licence for Transmission, Switching technology and Line technology", and subsidizing the private security certification scheme "Network Information Security Manager (NISM)".*

ness critical applications and different kind of users such as employees, customers and partners creates an environment with challenges to define access rights. A challenge today is to define personalized and updated security profiles. The large number of users accessing systems remotely as distance workers or with wireless terminals is increasing the complexity further. Today's often complex environment requires an integrated identity and access management solution that supports different applications and platforms. The increasing demand for the integration of access management for physical and information assets is a new challenge for organizations. The use of policy-enforcement solutions is a way to extend access management to also include the examination of patch levels, running processes, security configurations or other end-user machine settings. Dynamic configuration-based access control protects several network mechanisms. The central part of the policy-enforcement system is the policy server. The US federal government approved the Federal Information Processing Standard (FIPS 201) for Personal Identity Verification which will be the basis for a later implementation of smart card-based identity cards. The new card will be used for both physical and IT system access. The new standard does not apply to National Security Systems.

7.4 Incident Management, Business Continuity Planning

Solutions for Vulnerability Management for identifying security holes that attackers can use are considered important for IT security managers. The market for Vulnerability Management in 2008 is estimated at 900 million USD by IDC (RED 2005A). Legislation requires the securing of systems and assessments of the risk of cyber attacks. Vulnerability Management Systems is a particular kind of Intrusion Detection System. The lack of solutions to provide a holistic view of firms IT defence has created a demand for software for the aggregation of different reporting tools to log information. Suppliers also provide different Intrusion Prevention Systems for automated security-management, designed to help firms to monitor and act on security incidents. Some of the suppliers are ArcSight, Intellitactics, NetForesics and OpenService.

Continuous accessibility to important information assets and services is critical to the survival of any organization, but according to Meta Group only 20 percent of Global 2000 organizations have a comprehensive recovery strategy. In the USA September 11th, the Northeast blackout and the California fires have heightened organizations' awareness of the need for planning. The purpose of Business Continuity Planning is to protect organizations from major interruptions of different data processing services. The responsibility includes the formulation, co-ordination, testing and maintenance of recovery plans. US regulations such as HIPAA have imposed requirements on business recovery. A part of the Business Continuity Planning is Business Impact Analysis including definition of the possible impact on different areas and the loss of revenue associated with the particular area (ISPC 2005A). The increased demand for Business Continuity is driving the need for technologies such as high capacity storage networks. Business interruption insurance is also an alternative.

Supporting the availability, survivability, persistence, confidentiality and integrity of information is becoming more and more crucial. This requires secure and reliable data storage systems that distribute information over networks, enabling users to store and access critical data in a continuously available and highly trustable fashion. The long-term archiving of electronically signed documents is also an issue.

7.5 Security Metrics

The measurement of IT security is driven by regulatory, financial and organizational reasons. Federal regulation such as FISMA has defined requirements for IT security performance measurements. FISMA requires annual evaluation, and the Government Reform Committee issues Federal Computer Security Scorecards for the federal agencies based on information from the inspector general of each agency. Agencies need to report their work against a set of security performance measures. The grading standard for the agencies is also expected to be tougher in 2006 and based on the impact a serious threat would have on the agencies' mission (FCW 2005A). Security is also a goal for e-government defined by the Office of Management and Budget (OMB). In 2004 agencies secured 70 percent of their systems, the goal defined by OMB for 2005 is 90 percent.

The National Institute of Standards and Technology (NIST) published a Security Metrics Guide for Information Technology Systems (NIST 2003A) in 2003. The document is a guideline for how organizations can use metrics to implement security procedures. A security metrics programme provides several organizational and financial benefits. The use of metrics is a tool to facilitate improvements in performance and accountability. IT security metrics can be created to measure every dimension of the organizations security. Results of different security-related activities such as risk assessments and penetration testing can be quantified and used as a source for metrics. The development of metrics is also considered important for the evaluation of new products and best practice and a way to facilitate technology transfer (PITAC 2005A). According to NIST a security metrics programme should include the four different components strong management support, practical security policies, quantifiable performance metrics and results-oriented metrics analysis.

Table 12 Examples of Security Metrics

Examples of Security Metrics
Percentage of systems that had formal risk assesments performed and documented
Percentage of systems that have had risk levels reviewed by management
The average time between vulnerability discovery and implementation of action
Percentage of systems that have the cost of security integrated into the life cycle
Percentage of users with special access who have undergone background evaluations
Percentage of laptops with encrypted capabilities for sensitive files
Percentage of used media sanitized before reuse or disposal
Percentage of software change requests approved through change request forms

Source: NIST 2003A

7.6 Societal Issues, Technology Transfer

Several societal issues are concerned with information- and IT security. To increase security and prevent attack it could be necessary to collect more information about the origin of data which could be in conflict with privacy. Some kinds of packet filtering could be considered censorship. Combining security improvements with other requirements is a particular challenge.

PITAC proposes the establishing of a national database of results from federally funded cyber security research projects as a source for suppliers to find ideas that can be implemented into commercial products (PITAC 2005A).

8 IT Security Threat Categories

8.1 The Increasing number of IT-Related Incidents

The US Carnegie Mellon University CERT Coordination Center logged 3,780 new computer security vulnerabilities and about 22,000 incidents in 2004. The number of new vulnerabilities has increased considerably compared to 1,090 in 2000 and 171 in 1995. NIST calculates the US annual cost of software errors to about 60 billion USD. The downtime because of attacks is increasing. The company Symantec has established one of the largest sources of Internet threat data including 11,000 vulnerabilities affecting 2,000 suppliers. The Symantec DeepSight Threat Management System includes sensors monitoring network activities in over 180 countries. The system provides information on a global basis about security incidents. The United States continues to be the top attack source country, followed by China and Germany. The financial services sector experienced the highest ratio of severe attacks (Symantec 2005A). New sources and types of attacks will also form part of IT security. One example is that outsourcing and off-shoring creates new kind of IT security vulnerabilities.

Overall, the incidence of cyber crime in Japan reported by the National Police Agency in 2004 was 2 081 cases. This has more than doubled in five years. A 2003 survey revealed that 72 percent of business Internet users and 34 percent of private users in Japan have experienced security-related damage.[19] Another survey showed that 86 percent of Internet users in 2003 were aware of the necessity for security measures but did nothing (MIC 2004A).

During 2003, 73 percent of all Internet users in China were hit by computer viruses. In the first half of 2004 over 2 million servers and 700 web sites (of which 60 percent were governmental) in China were attacked. Furthermore, during that same year 133 serious confidential leakage cases were officially reported, 40 percent of these leakages were due to the computers or nets being non-protected (NS 2005A). Today in China, many computer systems still have little or no protection.

8.2 Cyber War

An IT-related threat to Japanese society is foreign cyber attacks. At the time of political demonstrations against Japan in Korea and China in 2005, picketing was accompanied by cyber attacks. In April 2005, the Japanese government created the National Information Security Center, NISC, to deal with politically motivated IT attacks from other Asian nations.

The US military has created a programme for cyber war against enemy networks and the unit is called the Functional Component Command for Network Warfare. The unit's responsibility includes defending all Department of Defence networks

[19] *As quoted from a presentation by Mr. Yasuhiko Tanikawi, Japan's telecommunications attaché to the US.*

and for computer network attacks. The existence of the unit is based on the National Security Presidential Directive 16 published in 2002 (Wired 2005A).

8.3 Identity Theft, Cyber Crime and Phishing

Several high profile identity theft incidents disclosed in early 2005 involving companies such as ChoicePoint and Bank of America have increased congressional attention on the issue (CRS 2005C). Tougher disclosure laws and new technologies may be necessary (IW 2005D). Personal information for millions of people has been stolen but not only based on Internet access. The number of annual US Internet victims is estimated at 1 percent of US households and the total cost at about 800 million USD (PITAC 2005A, LAT 2005A). Automated crimes including crime packaged as ready-to-use software solutions could be a future threat. The crime software could include a predefined crime with a particular target (ISPC 2005A). The US Department of Justice has an annual budget of about 7 million USD to fight electronic crime (USDOJ 2005A). Stricter penalties for hacking and cyber terrorism have also been introduced in the US. Internet-based crime is increasing and new kinds of threats such as programmes known as crimeware are emerging. Cyber extortionists who require payment in return for not attacking a firm are also increasing in number. Spyware attackers are teaming with phishers to steal and sell different kind of personal information (UST 2005A).

Leakage of personal information in Japan is reported almost daily, at an average cost of 550 million Yen (5 million USD) per incident. [20](JNSA 2004) The figure is from 2003, but data leakage has continued to the extent of "*shaking the foundations of corporate Japan*" according to JETRO Japan External Trade Organization, and they continue to state that between 2003 and 2004 "*large amounts of personal data were leaked by major telecommunications operators, mail-order vendors, financial institutions, local governments and other organizations*" (JETRO 2005A). In addition to data leakage, virus and illegal access are still current threats, although the Information Technology Promotion Agency, IPA, reports a steady decline. The number of viruses decreased, from 24,261 reports in 2001, to 17,425 in 2003, and illegal access from 550 in 2001, to 407 in 2003. (JETRO 2005B)

Phishing is a way of stealing confidential information such as passwords, credit card numbers, and other financial information. Phishing uses fake websites to get confidential information from consumers. The number of phishing attacks is increasing. By the end of December 2004 the Symantec Brightmail AntiSpam anti-fraud filters were blocking an average of 33 million phishing attempts per week, up from an average of 9 million per week in July 2004. This represents an increase of over 366 percent. Losses due to phishing-related fraud were about 140 million USD in 2004. A new kind of phishing is pharming (UST 2005A). For pharming also malicious software is implanted in the victim's PC which facilitates the collection of data. Spyware for the attacks is widely available on the Internet.

[20] *The figure represents an average for the 51 cases whose claim for damage can be estimated out of the 57 cases for 2003.*

8.4 Malicious code, Viruses, Trojans

Malicious codes include all programs including macros and scripts which are deliberately coded in order to cause an unexpected and usually, unwanted event on a user's PC. Due to the widespread deployment of Microsoft Windows operating systems in enterprise and consumer environments “Windows 32” viruses and worms pose a serious threat to the security and integrity of computer users. In the second half of 2004 more than 7,360 new “Windows 32” virus and worm variants were created. This represents an increase of 64 percent over the previous six-month period. The total number of documented “Windows 32” threats was about 17,500 at the end of 2004 (Symantec 2005A). Organizations are challenged with updating their anti-virus solutions more often than ever before. According to one study the number of viruses increased by 50 percent in 2004. Anti-virus solutions are released weekly or monthly but they operate after the virus was created. The PC has to become infected with the virus before the anti-virus definition can be developed. Tens of thousands of organizations around the world have often been infected before the anti-virus is available. Solutions known as Patch Management are one of the major IT security solutions today. Attacks hidden in embedded content in audio and video images are also expected to increase. This is a problem because image files are ubiquitous, almost universally trusted, and an integral part of modern day computing. The increased use of instant messaging and P2P file-sharing applications is also a security threat, because they can create a gateway for spyware or malicious codes. The increased number of threats on the Internet can be managed by regulation, technology or both. Federal and state lawmakers have proposed different legislation against malicious software program such as the Spyblock Act. Legislation that bans the installation of software without approval from the user is also considered an option by some policymakers.

8.5 Denial-of-Service, Spam, Spyware and Adware

Denial-of-Service attacks (DoS) are one of the most common types of security breach and the most common target for DoSs is specific web sites (Tele 2004A). DoS attacks are also the most expensive problem for organizations. The attacks can originate from anywhere in the world and are often self-distributing and difficult to stop once they start. Another category of incidents is Spam which made up more than 60 percent of all e-mail traffic at the end of 2004 and year-on-year growth has been more than 50 percent (Symantec 2005A). The US CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) creates imposes demands on those who send commercial e-mail. The Act defines penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask e-mailers to stop spamming them. The law became effective on January 1, 2004. A new kind of cyber security threat is Spam over Internet Telephony (SPIT) that could be a challenge when companies are moving to telephony over IP networks.

Several companies are also facing increasing threats from threats such as spyware, adware and other non-viral malicious programs. Spyware steals information about the computer in different ways but also has an impact on system and Internet

access speed. Spyware programs are often bundled with other software. Adware is installed via a Web browser. Spyware can range from simple adware to sophisticated hacker tools. To manage the threat from spyware different anti-spyware solutions are available. Webhancer was the most frequently reported spyware program during 2004. Iefeats was the most commonly reported adware program. Security risks associated with adware and spyware is expected to increase. Some of the anti-spyware solutions are Sunbelt CounterSpy Enterprise and Tenebril SpyCatcher Enterprise. Microsoft also provides an anti-spyware solution.

8.6 Botnets and Web Application Attacks

Botnets or bot (remote control programs) networks are remotely controlled PCs and are a new type of threat. Attackers are hijacking and linking thousands of computers, called botnets, to launch co-ordinated attacks. Large enterprises may have hundreds of hosts being used by a single attacker. The growth of botnets is unbelievable and 30,000 machines are recruited into botnet armies every day. Some botnets have been counted in tens of thousands of compromised computers. Botnets also send more than 70 percent of today's spam. The use of botnets for financial gain is likely to increase and defending against botnet attacks is challenging and complex. Bots are also adopting features to avoid detection.

Web applications are popular targets because they enjoy widespread deployment and can allow attackers to avoid traditional perimeter security measures such as firewalls. They are a serious security concern because they may allow attackers access to confidential information without having to compromise individual servers. Nearly 48 percent of all vulnerabilities documented between July 1 and Dec. 31, 2004 were Web application vulnerabilities, a significant increase from the 39 percent documented in the previous six-month period (Symantec 2005A).

8.7 Mobile Attacks

Today most data losses are caused by the use of laptop computers. Increased mobility and remote network access are imposing new demands on security solutions. Wireless security in general is expected to be an 8 billion US dollar market in 2008, compared to 100 million USD in 2004 according to the market research firm InStat-MCR. Several different wireless threats exist such as peer-to-peer wireless networks and WLAN Rogue access points. The cell phone worm’s task could be as simple as deleting the address book or sending out costly and annoying text message spam. It could create a denial of service attack on your wireless-service provider by making your phone rapidly dial many numbers in succession. As people start using their “smart” cell phones to tap into computer networks, the damage caused by different incidents could grow more severe (Eweek 2005A). Malicious codes targeting mobile devices are expected to increase in number and severity in the future. Worms or other type of malicious code may propagate by Bluetooth-enabled devices. Mobile malicious programs will be able to infect systems not vulnerable to conventional viruses. In the future a car owner may link his Bluetooth-enabled phone to the dashboard computer, but the phone may also be linked to other phones and malicious codes can reach the car and cause severe impact.

New computing architectures such as grid and on-demand computing could be particularly vulnerable to some attacks. For grid computing hundred of computers are linked together and shared by multiple users. Researchers at MIT have shown that a remote access technology based on SSH (Secure Shell) for remote connection to computers can be used for distributing attacks (Eweek 2005A). Nor are the security implications of networked-embedded devices known.

9 Technology Areas

9.1 IT Security Usability and Application Security

User-centred security is an important area and better usability will be necessary in the future. Users need to be able to choose and use the protection they want, that matches their intuitions about security and privacy, and that supports the policies that teams and organizations need and use to get their work done. The increased use of fixed and wireless terminals with always-on access to the Internet is creating a need for improved security. The price for a complete set of security products including anti-virus, VPN, device security, and management can be higher than the cost of the device itself. It should be possible to use the security solutions already up and running in an organisation also for new wireless devices.

The focus on application security has increased compared to network security focus earlier. Web application firewalls, application vulnerability scanners, application code scanners, XML security gateways, and federated identity solutions are all increasing their adoption rates according to Forrester Research. Secure electronic commerce is another important area with several different initiatives such as the standard 3D Secure.

9.2 A system-based approach to security

Several different sources indicate that a more systems-based approach to security is of importance. Today's specialized products do not provide sufficient integration and separate management systems have often made it more difficult to improve security. According to PITAC a broad consensus exists among computer scientists that the approach of patching to enhance security is not suitable in the long run (PITAC 2005A). It is complex to manage all updates and patches in order to provide a system without known vulnerabilities. Continuous manual software patching is not an acceptable long-term solution to information security. The annual cost to business of repairing IT threats such as viruses is several billions of dollars. The cost of patching is about 234 USD per patch per PC (Tele 2004A).

Security cannot easily be added on afterwards. To improve security is it necessary to develop new methods for designing and engineering secure systems. Security as a service is considered to be one direction for development in the future. In May 2005 Microsoft Windows announced OneCare, which is an automated service that will deliver anti-virus, anti-spyware and firewall features. The cost of the service will be an annual fee and the service has not yet been released. However in just one week in 2005 Microsoft issued a dozen security bulletins addressing 17 vulnerabilities.

Adaptive and self-defending networks could also provide a solution for more efficient management of threats. Cisco is promoting the approach Cisco Self-Defending Network including a multi-layered protection system (Cisco 2005A). One objective of the Cisco solution is to provide a better link between end system security and network based security. Cisco aims to "hardwire" more security functions into routers and switch forwarding paths. Further ASIC and processor improvements for

performing detailed packet inspection and application-level control will also be necessary according to Cisco. Cisco considers Policy Enabled Network Security as a proactive approach to security compared to current reactive patching. Security policies need to adapt to new threats and new regulatory requirements. Anti-spam providers have started to launch reputation services in their anti-spam systems. The company Cipher Trust provides a solution for reputation service which can assign a reputation to any IP address on the Internet. The research centre ISI CCSS is working on standards for policy definitions and distribution. For efficient policy management interoperability is based on standards of importance (ISI 2005A). Different standards such as Application Vulnerability Definition Language (AVDL) are also important to simplify integration of solutions from different suppliers. AVDL can be used to send information about detected vulnerabilities to other devices such as a firewall.

9.3 Security in Shared IP Networks

The migration to all-IP networks will probably lead to increased vulnerability, new solutions for security in all-IP networks are of importance. A very high level of security can only be realized on private IP infrastructures. The increased implementation of the all-IP converged operator network will probably decrease network security and may lead to unpleasant security surprises (TeleInt 2005A). On a shared infrastructure, virtual private networks can be created based on technologies such as IPSec, Secure Socket Layer (SSL) tunnels and Multi Protocol Layer Switching (MPLS). MPLS provides logically separate networks which improve security compared with other VPN solutions, but international connectivity with many endpoints is easier to obtain with IPSec.

Operators are likely to offer improved and new services in terms of asset tracking, software management, and configuration control. Managed Security Service Providers (MSSP) provides a higher level of network protection, support and information about threats. Providing security Service Level Agreements (SLA) is a way to improve the security offering for the operator (Tele 2005A). However, some researchers consider that most security developments will be implemented at the endpoints. The increased use of cryptation of traffic based on e.g. IP Sec makes it difficult to inspect the traffic during the transmission between the end points.

The National Police Agency in Japan (Cybercrime Division of Community Safety Bureau) conducted a survey in January 2005, by asking universities and companies what R&D on IT security technologies they considered to be most important now and in the future. The most focused areas for research into IT security for 2005 were said to be Network Security (technologies for protecting and administrating information on networks) and Authentication Technologies (to identify the person who is going to use a computer). The most focused areas in the future were expected to be Security Management (operation and administration for Information Security), Authentication Technologies, and Security Service-related issues, e.g.

evaluation, diagnosis, and monitoring related to information security.[21] (NPA 2005)

9.4 The Next Generation Internet

The Internet was originally built without much consideration of internal attacks, but much attention to external threats such as hurricanes. Technological solutions for several of the problems have existed for some years but it has been difficult to find a consensus to implement them because of e.g. politics, potential profits and intellectual property issues. The interactions between security and advanced networking are complex but are an important part of the agenda for Internet2, a consortium of mostly academic institutions. Performance requirements such as high-bandwidth, end-end transparency, and support of new protocols are essential for the academic mission and innovation, but are considered difficult to manage with current approaches to network security. Applications such as desktop video-conferencing, access to grid-based resources, and remote device control have high priority in the research and education community. Internet2 Security work is focused towards "improving the ability to integrate advanced networking requirements with network security in an insecure world" according to Internet2.

The next version IP protocol, version 6, (IPv6), will provide some new security features but new types of threats could also be created. IPv6 could stop hacking and spam (Tele 2004B). IPv6 is mostly a priority in Asia and particular China. China is encouraging the use of IPv6. China has not been assigned more IP addresses than Stanford University in the US which is a reason for the interest in the new capabilities provided by IPv6. The federal US government will require agencies to use IPv6 in June 2008. The Office of Management and Budget have issue a policy memorandum requiring full federal "IPv6" compliance in an initiative to spur its deployment throughout government agencies. However, most major US federal agencies have not begun planning the transition to Internet Protocol Version 6 in May 2005. Microsoft's next operating system, Longhorn, will be fully IPv6-capable according to Microsoft. The late adoption of IPv6 in the US creates a risk that the US will be bypassed by countries with a quicker adoption of the standard (Tele 2004B).

Some Japanese R&D is relevant to IT security although it is not being pursued with security as the main driver. One such example is the implementation of IPv6, where Japan is very active. The reason for this is not only a matter of security but a perceived future lack of IP addresses. Japan currently has 93 allocated IPv6 addresses, compared to 153 in the US, 36 in Korea, 22 in Sweden, and 21 in China[22] (SIXXS 2005). NICT also recently made a call for proposal of R&D on applications of IPv6 to electronic home appliances, which are necessary to realize the ubiquitous network society. NICT has received 19 proposals from companies and

[21] *Respondent (reply, collection rate) to the survey: 187 (44, 23.5%) universities and 314 (50, 15.9%) companies [501 (94, 18.8%) in total]*

[22] *Six Access, or sixXS, maintains a website that continuously updates national rankings in terms of the number of allocated IPv6 addresses, and currently visible addresses. The national rankings are thus bound to vary depending on the time of day in different countries.*

universities, 11 of which are accepted. Five of the 11 selected R&D projects are concerned with IT security such as tunnelling protocol, cryptography, and secure data transmission (NICT 2005).

Research into the next generation Internet protocol, IP version 6, started in China as early as 1998. In 2002, MII and its Telecom Research Institute set up IPv6 Telecom Trial Net which has been connected with the biggest international commercial trial net named 6BONE. The trial net is located in Hunan Province. The trial consists of testing of technology, equipment, interaction between v4/v6, international interaction, Quality of Service, net safety, and broadband access. Most of the trial work has now been finished, except work concerned with business service models. The idea is to implement IPv6 in the new network CN2.

The importance for China of IPv6 cannot be overstated. For China the implementation of an advanced IT-infrastructure based on IPv6 can be a competitive advantage. The implementation of IPv6 will essentially solve the problem of shortage of IP addresses. After more than ten years of development, the Chinese internet has become the second largest in the world, with approximately 100 million customers. Among the more than 300 million mobile phone users, 30 percent have the mobile internet function. However, China has only approximately 60 million IPv4 addresses. By the end of 2020 the expected number of IP addresses needed in China will be at least about 500 million. Furthermore, IPv6 can greatly improve the net function and quality.

9.5 Secure Networks

A new critical infrastructure for defence purposes is the Global Information Grid (GIG) with the purpose to improve military communications by linking weapons, intelligence and personnel. The GIG is considered to be one of the most ambitious IT projects ever funded by the US federal government. The purpose of GIG is to "provide the users with information superiority, decision superiority, and full-spectrum dominance" for "networked-enhanced warfare". GIG will reduce the military exposure to the insecurities associated with the civilian IT infrastructure. The GIG project is projected to cost 100 billion USD, the cost through 2010 is estimated at 21 billion USD (PITAC 2005A). GIG could be an example of a secure IT infrastructure of the future.

Homeland Secure Data Networks (HSDN) is a network that addresses the requirements for secure data communication of classified information. The project budget for 2006 is about 37 million USD. HSDN will be used for communication within the DHS and with other agencies and organizations. The Cyber Security Industry Alliance proposes the establishment of a "survivable Emergency Coordination Network" (CSIA 2004A) to facilitate the reconstitution of the Internet during a large attack. The alliance considered the DHS activities as not sufficient.

Where there has been a lack of domestic companies with the advanced technology required, the Chinese government has allowed a few foreign companies to participate in important security infrastructure projects, e.g. within the financial and tele-

com sectors. The US 100 million USD ChinaNet Next Carrying Network (CN2) project undertaken by China Telecom Corp. can be taken as an example.

The groundwork for CN2 was done in mid-2004, when China Telecom's Research Institute in Beijing invited bids from many of the world's largest telecommunications equipment suppliers. IT security and monitoring were important issues. Juniper Networks, Cisco, and other firms offered their main frame-class routers. China Telecom awarded six contracts, splitting them up among Alcatel, Cisco, Huawei, and Juniper.

The structure of China's Internet is highly centralized, with three layers, in principle three concentric rings. The innermost ring consists of core routers, from Juniper. The core routers—being installed in eight large, strategically located cities, including Beijing, Shanghai, and Chengdu—are the principal means by which data packets will cross from one region to another or make their way to the outside world. The middle ring consists of metropolitan-area networks. CN2 will upgrade routers in at least 193 of the nation's largest cities, dividing China's provinces, autonomous regions, and municipalities into four regions and giving each of the four suppliers its own territory.

The outermost of the three rings consists of routers located throughout China. CN2 awarded Cisco a nationwide contract for these edge routers, which businesses and institutions will use to make their high-speed connections to one another and to the world. Thus, CN2 gave Juniper and Cisco two contracts each, nationwide ones for core and edge routers, respectively, plus regional contracts. Alcatel and Huawei were each awarded only regional contracts.

9.6 IP-telephony and WLAN Security

When network convergence develops and voice is transported over IP networks several security threats could have an impact on IP-telephony. Threats such as denial-of-service attacks, worms that overload networks and spoofing attacks could seriously disrupt the voice service. The main security issues for IP-telephony is consider to be distributed denial-of-service attacks (TeleInt 2005A). However, the network can be designed to better protect against security threats. There are security issues associated with the configuration of firewalls for IP-telephony. Some IP-telephony protocols such as H.225 and SIP are also considered to have vulnerabilities (NetMag 2005A).

Security for WLAN access has been an issue for several years. The security standard WEP for 802.11 networks has now been improved with the 802.11i standard. But a new *de facto* upgrade for security Wi-Fi protected access (WPA) has also been launched by the industry. But the 802.11i is considered to add latency to communication which is a problem for IP-telephony over WLAN.

Symbian, the company whose mobile device operating system has been targeted by every cell-phone virus so far, has released a version of its software that grants Bluetooth access only to programs tagged with secure digital IDs. The need for wireless anti-virus detection is bound to increase. The security threats to WLAN networks is a major issue, but can be managed by using access point RF-sensors

from companies such as AirMagnet, NetStumbler and AirDefense that monitor the air activity. But it is expensive and complex to monitor all access points. Solutions for RF-scanning are also an option. The company Highwall Technologies also provides a solution for detection of air activity for WLAN network; the company also develops Bluetooth sensors.

Security on IP-telephony, WLAN, ITS-solutions and the mobile system are not really on the radar in Japan. This is perhaps surprising since these are traditional areas of Japanese strength. NTT, as an example, does focus on security, to the extent that "security" is the first in their four key-terms: security, comfort, ease and convenience, and attractiveness. (NTT 2005) Security initiatives at NTT seem to relate less to research and more to service provision. NTT describe their activities for infrastructure protection to cover traffic monitoring, prevention of unauthorized disconnection of BGP sessions with BGP MD5 checksum, decentralization by installing an additional F root name server, and measures for DDOS attack prevention.

The recently issued and controversial security standards for wireless local area networks (WLAN) illustrate the operation of the new standards development system in China. It also clearly indicates why it is contributing to concerns that China is not living up to its obligations under the Technological Barriers to Trade (TBT) Agreement under WTO.

In May 2003 China issued two new mandatory standards for encryption which were to come into effect in December 2003. They were later delayed until June 2004, and have now been postponed indefinitely as a result of protests from the U.S. government and industry The standards apply to both domestically produced and imported equipment such as Centrino notebooks and personal digital assistants (PDAs) and other devices which promise to make wireless technologies the foundation for a multi-billion dollar industry. The WAPI (WLAN Authentication and Privacy Infrastructure) encryption technology, which China is proposing as its standard, "differs significantly from the internationally recognized" version. China has provided the algorithms needed for encryption to 24 Chinese companies, some of which are likely to be competitors with foreign firms. Foreign companies wishing to gain access to the technology will have to work through these Chinese counterparts. This may entail providing "technical product specifications" to potential competitors if they want to market their products in China, and seems to be a clear violation of national treatment under the TBT provisions.

WTO members may not be bound by Annex 3 provisions if standards pertain to matters of national security, and some of the arguments heard from China on the WAPI case do invoke concerns for national security. Representatives of the U.S. IT industry have rejected the national security argument, however, and urged the U.S. government to press China to abandon or modify its policy on the WAPI standard at bilateral trade talks. In response to continuing pressure from industry, the Bush administration then ratcheted up its expressions of concern about this matter to the Chinese government in a letter directed to Vice Premiers Wu Yi and Zeng Peiyan signed by the then Secretary of State Colin Powell, Secretary of Commerce Donald

Evans, and U.S. Trade Representative Robert Zoellick. At talks in April 2004, the Chinese side agreed to postpone implementation of the WAPI standard (Suttmeier 2004).

The development of the WAPI standard nicely demonstrates how a standards policy builds on and reinforces the trends in the development of China. Efforts to explain the genesis of policy supporting the WAPI standard have called attention to the national security interests in the standard, and the likely involvement of Chinese defence and security agencies in its development.

9.7 Software Security

PITAC states that "the software development methods that have been the norm fail to provide the high-quality, reliable, and secure software that the IT infrastructure requires". Several different software components such as ActiveX controls and Web services have security issues. Software development is still not a sufficiently rigorous discipline, and the process in not controlled to minimize the vulnerabilities. The National Cyber Security Partnership recommends action in the area of software vulnerability analysis and particular research funding for the development of better vulnerability analysis or Code Scanning tools that can identify software defects (NCSP 2004A). The Secure Foundations Initiatives is a programme for collaboration between the code analysis suppliers and the universities to train developers in secure software. The programme was launched by the company Ounce Labs in 2004.

The National Security Agency (NSA) has worked for a long time on a way to use operating systems to control how applications and users can access data based on mandatory access-control capabilities. NSA has applied its approach to Linux and created Security Enhanced Linux (SE Linux) which is included in the 2.6 version of the kernel. Both Red Hat and Novel have released packages built on version 2.6 (IW 2005C). Trusted Computer Solutions (TCS) Inc. is developing Trusted Linux, based on NSA SE Linux, a highly secure version of Linux that could compete with Unix in environments in which security is the highest priority. According to TCS officials Trusted Linux will later on be expected to be certified under Common Criteria at Evaluation Assurance Level 4 (FCW 2004A). A paper published at UC Berkeley (UCB 2003A) concludes that "in order to more closely align with national computer systems security objectives, federal agencies should consider adopting open source systems". The paper describes several different reasons for the conclusion, such as that open source reduces complexity and reduces the dependency on the private sector.

9.8 Authentication and Perimeter Defence

Key public infrastructures and electronic signatures are now established and well-known techniques for identifying entities in the digital world, securing digital transactions, and associating digital content with its author. However, there are still many unresolved problems. The company A4Vision, a provider of 3-D facial scanning and recognition software, has received increased attention because the CIA's venture capital firm In-Q-Tel invested in the company in March 2005. The firm

Neven Vision also provides a solution for face recognition for e.g. identity verification and video surveillance. Biometrics is an important part of the US Visitor and Immigrant Status Indicator. The Automated Biometric Identification System is also an initiative at DHS (DHS 2005B). Some of the issues for authentication are e.g. realization of single-sign-on schemes, the association of identity- or role-based rights with authorization and access control.

New solutions for more application-aware perimeter defence are being developed to protect against application layer worms and viruses. The technology Deep Packet Inspection (DPI) is offering the possibility to configure rules on bit patterns inside a packet. A large amount of cyber security research has to date been focused on perimeter defence, but the model is not sufficient. Once the perimeter is breached, the attacker has free access to every connected system in the network. The perimeter approach of inside or outside has also limitations, because a larger number of users are accessing the network from remote locations. A new possible approach is “mutual suspicion” according to PITAC (PITAC 2005A), each system component is always suspicious of every other component and access must be constantly reauthorized.

In general, the implementation of the Personal Information Protection Act has made several Japanese companies focus on developing systems for access prevention e.g. biometric applications and ID management (Toshiba) (TOSHIBA 2005) (NEC). (NEC 2005A) As a measure to strengthen security in the light of the new law, the University of Tokyo Hospitals Department of Planning, Information and Management was recently the first to install the Contactless Palm Vein Authentication technology (CPVA) developed by Fujitsu, which started research on it in 2000 (FUJITSU 2005). According to Asahi Shimbun (July 20), Tsukuba University also uses it for dormitory access control, and Suruga Bank and Tokyo Mitsubishi Bank started to use palm vein pattern recognition for their ATM in July 2004 and October 2004 respectively. Hitachi does research and development into fingertip vein pattern recognition and its technology is said to be employed by Japan Post and Mitsui-Sumitomo Bank. The Asahi Shimbun recently reported that the Japanese Bankers Association is looking to equip Japanese ATMs with both palm vein and fingertip vein readers, and to make available smart cards with information on palm vein patterns and/or fingertip vein patterns, according to the customer’s preference (AS 2005).

9.9 Data Analysis and Modelling

Tools for data gathering and sharing among the federal, state and local agencies have high priority on the federal technology agenda. The US 9-11 Commission states that: "better information sharing would have greatly improved anti-terrorism efforts before the September 11 2001 attacks”. The Commission also notes the need for better collaboration between the different agencies. The Information Analysis and Infrastructure Protection Directorate (IAIP) at DHS were created to analyze threat information and map it against physical and cyber vulnerabilities. The IAIP budget is about 890 million USD in 2005. Several different screening initiatives have been launched by the Department of Homeland Security. The

screening initiatives include e.g. a Secure Electronic Network for Travelers Rapid Inspection, Alien Flight School Checks and Hazardous Materials Trucker Background Checks (DHS 2005B). The Homeland Security Advisory System is a major project for intelligence, information sharing and warning (White House 2005A). IAIP is also working on an initiative to combine bio-surveillance data with threat information to improve the situational awareness (DHS 2005B). The purpose of the Intelligence Reform and Terrorism Prevention Act of 2004 is to improve US intelligence and warning capabilities. The development of better and more integrated systems for identifying and analyzing threats and issuing warnings is a priority. The recently created National Counter-terrorism Center is responsible for threat analysis.

Nikkei.Net reported on May 20th that the Cyber Defense Institute is setting up a commercial research centre to collect and analyze data from cyber terrorism. They claim that there has been a one-sided focus on technological issues and little on who is carrying out such crimes, with what means, and for what purposes. Something they will hire ten analysts to change.

9.10 Cryptology

The Japanese government took the initiative to the Cryptography Research and Evaluation Committee, CRYPTREC, in 2000, to evaluate and recommend cryptographic techniques for e-government activities. It overlaps the EU project NESSIE, and the Advanced Encryption Standard process run by NIST in the USA. CRYPTREC is run by the IT Security Center, ISEC, at the IT Promotion Agency, IPA, with deep involvement by the Security Fundamentals Group at the NICT and Professor Hideki Imai of Tokyo University, recently appointed Director of RCIS. MIC submitted in 2003, a list of recommended ciphers (NICT 2003), and IPA is today continuously upgrading the list with new reports and carrying out research on the reliability of cryptographic techniques. (IPA 2005B)

There is interesting basic research on information security in Japan, such as the work done by NEC. Prof. Imai, the Director of RCIS at AIST, has managed a research project on Quantum cryptography and "super ultrahigh speed communications" together with NEC during 2000-2005. The government, through MIC, sponsored the project with $ 8.7 million during the period. March this year NEC reported the success of the world's fastest continuous quantum cryptography key generation over 14 days, on commercial optical fibre. NEC considers it a breakthrough in commercial applications (NEC 2005B).

9.11 ICT Technology for Security & Safety Solutions

Convergence is on-going between cyber- personal- and physical security. The integration of IT security and physical security is an important issue for industry and the users. The Open Security Exchange is a cross-industry forum dedicated to merging physical and IT security solutions. The lack of integration between different components of enterprise security is considered by the organization to be a major challenge. There are also several projects within DHS with the focus on security applications based on ICT. Americas Shield Initiative is a DHS project for

electronic surveillance along the national borders based on sensor and video equipment and other state-of-the-market surveillance technologies. The project budget for 2006 is 51 million USD (DHS 2005B). People and materials screening and tracking is another major homeland security segment of importance for the development of IT technology including technologies such as biometrics. A Terrorist Screening Center (TSC) was established in 2003 to consolidate screening watch lists and to support federal screeners worldwide. A single point for terrorist screening data was also established. The 2006 budget for TSC is about 100 million USD.

An example where Japan has a very strong R&D position is on most levels of ubiquitous technologies. The MIC has proclaimed “u-Japan” as the new alternative to the e-Japan policy of the last five years. Although the u-Japan policy has not yet received the official support of the PM, and has not been adopted by the IT-Strategy Headquarters either, MIC’s strong influence has positioned the u-Japan initiative in industry, and many companies have taken it to heart. As a result, much government as well as corporate research is in the area of sensor technology, networks and devices. Security takes a natural part in this area of R&D but it is not presented as IT Security R&D in government and corporate statements.

10 Some Research and Development Centres

10.1 USA

The Center for Computer Systems Security (CCSS) at the University of Southern California (USC) Information Science Institute (ISI) is one leading research centre. The Center is working on the security of computer systems, networks, and applications, and focuses on the integration of security policy management and enforcement technologies for distributed systems. CCSS is also a partner in the DETER cyber security test bed providing a supplier-neutral experimental environment for collaboration among researchers. DETER includes an infrastructure for experiments and a research community for public-private collaboration. DETER is funded by NSF and HSARPA. CCSS considers the evaluation of network security mechanisms as important for advances in cyber defence. The test bed is important because new frameworks and methodologies for testing and benchmarking need to be developed (ISI 2005A).

Institute for Critical Information Infrastructure Protection (ICIIP) at USC has the mission to close the gap between the current corporate cyber security risk profile and the requirements for critical infrastructure protection. ICIIP is working with e.g. the creation of public-private partnerships and the centre has developed a process called Systematic Security Management (SSM) including five different security levels. The SSM process includes security from a technology, process, people and organizational perspective with the aim of measuring and benchmarking the security level for different organizations. The organization ISSA has partnered with ICIIP to deliver training programmes for Chief Information Security Officers (USC 2005B).

The Team for Research in Ubiquitous Secure Technology (TRUST) at the University of California Berkeley (UCB 2005A) is working on the development of new science and technology that "will transform the ability to design, build and operate trustworthy information systems for critical infrastructure". The major technical goal of TRUST is "composition and computer security for component technologies". According to TRUST, the development of security technology requires a fundamentally new approach to some of the core areas of information technology in the following areas:

- Software Security. Today's software vulnerabilities reflect software security implementation failures, and software security is directed at removing the problems. The problems need to be addressed by developing the fundamental principles and applications of "language-based security" including code verification, disciplined styles of programming, multi-lingual security, and support for "security by design".
- Trusted Platforms are an important area of development for the security industry (Trusted Computing Group). The composition of the "trusted platform" need to be understood and the vulnerabilities of the systems evaluated.

- Applied Cryptography. Network protocols that use cryptographic primitives are an important part of Internet security. TRUST initiatives are such as protocol design methods and protocol analysis.
- Network Security. TRUST are working on some of the fundamental challenges for securing the Internet such as routing security and structured overlay networks.

The Center for Risk and Economic Analysis of Terrorist Events (CREATE) at the University of Southern California was selected as the first Department of Homeland Security (DHS) Centre of Excellence in a competition between 72 universities in 2003. The mission of the Center is to improve US security by advancing the science of risk and economic analysis. One purpose with the Center is to assist the other DHS centres of excellence in risk analysis and economic modelling. CREATE is also developing tools to be used by emergency response professionals to protect property and lives such as software for resource allocation. Risk analysis is important to prioritize threats and vulnerabilities, for resource allocation, for modelling of the consequences and to quantify probabilities of attacks. Risk analysis is used in combination with cost-benefit analysis of major risk reduction decisions. Modelling is performed for systems such as the electricity infrastructure.

10.2 Japan

NICT Information Security Center was set up in 2004 by MIC. (MIC 2005C) The Security Center has three main objectives: to carry out research, to feed knowledge back to the public, and to promote global standardization. The Information Security Center hosts three research groups totalling 29 researchers, 6 of which are part-time and affiliated to corporations or Universities. They also have at least as many doctoral students, and they plan to hire an additional few researchers over the coming months.

- *The Secure Networks Group*, carry out research into Info-Communications Technologies in Crisis Management, secure communications networking, and info-communications infrastructure for disaster relief (incl. congestion control, a secure Internet overlay network and *ad hoc* wireless networks). This group collaborates with the national research institutes of fire & disaster, and also earth science & disaster prevention. They maintain an operation room for research into Security-Related Decision-Making Rooms. They also maintain a "Monster IAAA" i.e. an experimental info communication system for disaster relief using highly reliable, large-scale, distributed database servers[23]. (IAAA 2005) A RFID test bed and a platform for RFID-based emergency information gathering and delivery are also maintained.
- *The Security advancement group* does research into basic networks to prevent illegal access, DDoS and viruses, research into secure platform to confirm user authentication, and research into network applications bases in order to secure

[23] *The I Am Alive Alliance or I Am Alive System is a disaster victim's information registration and retrieval system. It was developed after the Kobe earthquake in 1995 and has been in use through several disasters since.*

user levels. A unified database system of Internet traffic data and security logs is used for experimental network incident analysis and evaluation. This group also has access to several test beds and counter-measures resources: A high-powered microwave system that is used to estimate the influence of attacks using I-EMI, intentional electromagnetic interference, A DDoS Transaction Generator for simulating attacks. The VM Nebula, which is a simulation system for Internet security using PC emulators and virtual LANs for virtualizing the Internet and targets. The SIOS, Security Integrated Operation Studio, an experimental system for illegal access reproduction composed of a reconfigurable computer cluster to reproduce various network attacks. It includes a vulnerability database. The security advancement group also researches an invisible incident monitoring system and develops a graphical user interface for incident log analysis. These develop new technologies for watermarking or stenography on image data, sound signals and digital documents for the purpose of information hiding (where two meaningless keys of data together become meaningful information), and they work on the security of RFID technology where they have developed prototype system authentication processing framework (APF) that enhances security and privacy in the uses of RFID.

- The third group at the Information Security Center is *the security fundamentals group*, researching cryptographic protocols and symmetric/asymmetric cipher technology and PKI, Tempest and side-channels attacks, and the establishment of secure ciphers for e-government (CRYPTREC). For their assistance this group has a Computer system for trial of factoring large numbers and a TEMPEST receiver, i.e. a receiver that picks up electromagnetic waves emanating from computers.

Besides the Information Security Center, sited in the Information and Network Systems Department of the NICT, there is also an Information Security Unit that spans this department and three other departments of NICT. The Unit gathers in a members' conference that includes not only NICT staff but also officials from MIC, scholars and experts from ISPs, manufacturers and OS & security suppliers.

The Research Center for Information Security at the National Institute of Advanced Industrial Science and Technology (AIST), in Akihabara, Tokyo, was started in April 2005. The Center employs 12 resident researchers and 5 part-timers affiliated to universities. They are in the process of hiring researchers to a total of 30 by April 2006. The Center consists of three teams:

- The Research Team for *Security Fundamentals*, which includes research into Cryptology, Cryptography, Digital Rights Management, and Cryptographic Protocols.
- The Research Team for *Physical Analysis*, including research into the Physical Analysis of IC Cards, Tamper Resistant Hardware, Quantum Computing, - Communication, and Cryptography.
- The Research Team for *Software Security*, focusing on Secure OS, Secure Compilers, Secure Web applications, and the Formal Verification of Software. The team leader is part-time researcher Prof. Akinori Yonezawa of Tokyo University.

The Deputy Director, Hajime Watanabe, considers training and human factors to be very important issues for information security in addition to the three research fields mentioned above. And staff to be recruited will be working in the areas of network security and security management. The Director of the Center, and part-time researcher, is Prof. Hideki Imai, of Tokyo University, a pioneer researcher into cryptographic technology in Japan. Prof. Imai collaborates with Mitsubishi-NEC and the Center is discussing additional corporate collaboration. The government has an influence on the direction of the Center's research, and the Center functions as an adviser to the government on information security issues.

11 Major Organizations

This chapter briefly describes some different organizations of importance for IT security policy, administration and development not mentioned in other parts of the report. (Web sites for the organizations are provided in the appendix.)

11.1 USA

The **National Security Agency´s** (NSA) Central Security Service works on cryptological solutions. NSA is the world expert on cryptology according to the organization. NSA co-ordinates, directs, and performs highly specialized activities to protect US government information systems.

The **CERT Coordination Centre** (CERT/CC) is a federally funded organization at Carnegie Mellon University established in 1988. The Center works on Internet security and was created to "coordinate communication among experts during security emergencies and to help prevent future incidents", but the role for the Center has expanded. CERT/CC works on areas such as Vulnerability Analysis and Incident Response including e.g. analysis of the state of internet security. The Center is also helping organizations to protect and defend themselves, and is collecting information about different security issues. CERT/CC also provides an incident handling certification programme for functions such as incident handlers and system and network administrators.

National Cyber Security Partnership (NCSP) is an organization led by the Business Software Alliance, the Information Technology Association of America and TechNet in voluntary partnership with academics, federal government agencies and industrial experts. NCSP is a public-private partnership for developing strategies for critical infrastructure protection. NCSP works on five task-forces including Cyber Security Early Warning, Corporate Governance, Security Across the Software Development Life Cycle and Technical Standards and Common Criteria (TSCC). The purpose of the task force is to identify gaps and develop recommendations to promote the adoption and implementation of the President's National Strategy to Secure Cyberspace. The TSCC group was formed to develop recommendations for the definition of better security metrics. The group recommended e.g. reduction of the cost of common criteria (CC) evaluations and increase the demand for CC evaluated products (NCSP 2004A).

Corporate Information Security Working Group (CISWG) was formed in 2003 by Congressman Adam Putnam. CISWG is made up of corporate, industry and academic leaders and will promote a private sector-driven approach to enhancing the protection of the nation's corporate computer networks. The group released a report about best practice in November 2004 (CISWG 2004A). The group recommends and proposes the use of a defined set of information security practice and metrics. The usage of metrics will enable enterprise-to-enterprise and agency-to-agency comparisons of information security level and progress.

Cyber Security Industry Alliance (CSIA) is the only CEO public policy and advocacy group focused on cyber security policy issues. CSIA was launched in February 2004 by a group of cyber security software, hardware and services companies. CSIA has the mission to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programmes, technological standards and public education. CSLA has presented a list of proposals for the cyber security policy. The organization recommends the promotion of information security governance within the private sector, the definition of public purchasing requirements, strengthening the information sharing and analysis centres (ISAC) and increasing cyber security R&D (CSIA 2004A).

Information Systems Security Association (ISSA) is an international organization for security professionals with 13,000 members around the world. Other organizations for security professionals are ASIS International and ISACA. ISACA administers certifications as Certified Information Systems Auditor and Certified Information Security Manager.

Internet Security Alliance (ISAlliance) is a non-profit collaboration between the Electronic Industries Alliance, trade associations, and Carnegie Mellon's CyLab. The alliance provides a forum for information sharing and leadership on information security issues. ISAlliance represents the interests of industry rather than legislators and regulators, and aims to identify and standardize best practice in Internet security.

The Liberty Alliance Project (LIP) includes more than 150 companies and government organizations, and is gaining significant attention with its architecture for Identity Federation and, to a lesser extent, its framework for Secure Web Services. The consortium is developing an open standard for network identity to facilitate the control of identity information and promote applications such as e-commerce. LIP has established relationships with other organizations such as the Open Mobile Alliance, the Open Security Exchange and the Network Application Consortium.

11.2 Japan

Computer Emergency Response Team Coordination Center, JPCERT/CC, is a NPO acting as a point of contact for other SCIRT's (Computer Emergency Response Team) in Japan, comparable to the Sveriges IT-Incident Centrum, SITIC. In the Asia-Pacific region, JPCERT/CC has helped to form APCERT (Asia Pacific Computer Emergency Response Team), and provides a secretariat function for it. Globally, as a member of Forum of Incident Response and Security Teams, FIRST, JPCERT/CC co-ordinates its activities with trusted SCIRTs worldwide (where Sweden is represented by TeliaSonera and SUNet).

National Police Agency / Cyber Police "@Police" is an initiative of the government to quickly disseminate information on security issues to the media and the general public. @Police is a portal site with the aim of preventing cyber crime and terrorism by increasing security awareness. Information disseminated here is mainly such as has been compiled by the NPA. Recently, NPA made an agreement with Microsoft Corp. to gain access to information about vulnerable areas before

such information is disclosed to the public. MS will also provide technical information to help investigate computer-related crime. (NIKKEI 2005)

Information Technology Promotion Agency, IPA, is an incorporated administrative agency at the Ministry of Economics, Trade and Industry (METI). METI mainly supports application-oriented research in the same manner as MIC. Funding is distributed through NEDO (mainly hardware-oriented), IPA (mainly software-related), and AIST. IPA's mission is to ensure IT security and reliability. It has included since 1997 the IT Security Center, ISEC and staffs 75, including 28 guest researchers. The ISEC division includes the Information Service Activities, providing information on information security as a public service, The VUAC, Virus & Unauthorized Access Counter-measures group, Secure information promotion activities, assisting METI, LAB, Security engineering lab, CRYPT, Cryptography Research Group (in co-operation with the NICT Security Fundamentals Group), and ISCO, the Information Security Certification Office.

11.3 China

The following governmental bodies are the ones which have the prime responsibility for IT Security policies in China:

- *The National Development and Reform Commission (NDRC)* is the major authority in China in planning key national projects and the layout of industrialization of industries. NDRC is responsible for drawing up the Special Research Plan for IT Security in the 11th five-year plan (2006-2010).
- *The China National Informatization Leading Group* is the highest leading body to co-ordinate the action of different ministries, committees and industrial sectors in regard to work on informatization including work on IT security. The office of this Leading Group is the SCITO (*State Council Informatization Office*).
- *The Ministry of Public Security and Department of Network Inspection* is responsible at different levels of public security bureaus for detecting crime relating to high tech and the Internet and also investigating major accidents and losses.
- *The Ministry of Information Industry* is responsible for making policies and planning ICT development.
- *The Ministry of Science and Technology* is responsible for strategic R&D planning in IT and other sciences in China.
- *The Ministry of State Security* is responsible for the collection of all security-related information both at home and abroad.
- *The State Information Center* deals mainly with information collection but centres around economic information, the *IT Security Research and Service Center also comes under this Center*
- *The National Internet and IT Security Information Reporting Center*. The national level authorities and the management body of the national basic internet

will report to the Center anything that could endanger security. The Center studies and analyzes these reports and sends out information nation-wide.

12 Conclusions and Policy Recommendations

Improving information- and IT security is important because dependence on different information systems and IT networks is increasing throughout society. A broad, top-down approach regarding IT security, including regulation, R&D, standardization & certification, processes and threats is used in this report in order to identify several factors of importance for the future of IT security. Several different policy options exist, and an appropriate balance between short- and long-term initiatives is also necessary so as to create improved IT security.

One fundamental characteristic of IT security is also the international dimension, which increases the importance of international perspectives such as those covered in this study. The need for further international initiatives is also expressed in the Swedish IT Policy Government Act of 2005[24]. This study of IT security in the USA, Japan and China focuses on policy and R&D perspectives adding additional dimensions to the Swedish policy formulation not covered by other reports[25].

The conclusions in this report have been made regarding the complexity and priority of IT security policy, the importance of regulation to drive investment, the possibility for further certification initiatives, the importance of secure software development, the need for new IT security technology concepts, the increasing IT security services business, the creation of new secure networks and the use of IT security test beds.

The report makes policy recommendations relating to the definition of an IT security base level for agencies and the development of new initiatives for increased IT security awareness. Policy recommendations for R&D in this study cover the importance of fundamental IT security R&D, the potential to benefit on the Swedish system knowledge for the growth of the IT security segment within IT and telecoms, and the need for prioritization of initiatives.

Table 13 Policy Recommendations for different IT Security Policy Areas – An overview

IT Security Policy Area	Policy Recommendation
Requirements on agencies	Metrics and benchmarking should be considered
Awareness and education	Learn from the international experience
Research and Development	Focus on fundamental IT security R&D
Research and Development	Benefit on the Swedish system knowledge
Research and Development	Use methods for priortization of efforts

Source: ITPS

[24] *The Government: Från IT-politik för samhället till politik för IT-samhället, proposition 2004/05:175*

[25] *SOU 2005:71; Swedish National Post and Telecom Agency: PTS-ER-2005:7; Swedish Emergency Management Agency: Samhällets informationssäkerhet, lägesbedömning , 2005; VINNOVA: Förslag till en nationell strategi för säkerhetsforskning,, 2005*

12.1 Conclusions

Policy

- **The importance of IT security is increasing.** The functioning of information technology and cyberspace is becoming more and more essential to the economy, because the number of organizational processes that rely on information systems is increasing. Information is one of the most important and valuable resources any organization controls and a majority of the information is managed by information systems. Several critical infrastructures such as electrical transformers are also interlinked with the cyber infrastructure. The frequency, impact and cost of cyber security incidents are continuously increasing and new threats are being created. The development over recent years shows that criminality will move to the digital society if the law enforcement capabilities not are in place. All the possibilities of IT are not utilized because of the lack of trust in the technology solutions.

Table 14 IT Security in USA, Japan and China, an overview.

Policy	**USA**	**Japan**	**China**
IT-Security	Market based	New organization	Document 27
Information Security	Info sec. regulation	Personal Info Act	The Great Firewall
Chritical Infrastructure	Vey high priority	Few initiatives	---
R&D			
Federal, annual, MUSD	~250	(not available)	(not available)
Programs	NSF Cyber Trust	NICT programs	863 Program
Priority areas	Systems approach Secure SW dev. New secure NW Security testbeds	Cryptology App. vulnerability Wide area monitoring Security services	Chinese basic SW Security HW PKI, WPKI Open S. Sec. SW
Technology			
IPv6	Gov. req 2008	High prio.	High prio.
WLAN	RF sensors	Low prio.	WAPI
Other, IT security			
Common Criteria	Only nat. sec.	10% of all CC	Not accepted
Certification	Security metrics	P-mark, ISP-mark	47 nat. standards
Annual Sales, MUSD	~5500	~2500	~500

Source: ITPS

- **The IT security policy formulation is complex.** The increased number of threats on the Internet can be managed by instruments such as regulation, education, market initiatives, R&D and technology. Private-public partnerships are a particular important part of the cyber security strategy process because the majority of the cyber resources are controlled by private organizations. One policy approach is to require companies to report on security preparedness. One alternative is mandatory reporting of certain kinds of security breaches and another approach is to define regulations and use inspectors to monitor compliance. Requirements for product liability and federal purchasing requirements

are an option to drive the industry. Cyber insurance policies are an attractive market solution to the software security problem. Some companies have already begun to issue cyber insurance policies to cover against e.g. hacker intrusion damage and virus infections. Demands on suppliers are increasing and more consumers are requiring suppliers to be legally and financially liable for security vulnerabilities. The implementation of performance-based pricing for software is also an option to increase supplier accountability, but the solutions are not attractive for suppliers. Legislation that bans the installation of software without the approval of the user is also being considered by some policymakers in the US. Some of the US federal policy priorities are increasing R&D, improving the response to cyber incidents and improving the international management of attacks. The policy initiatives are similar in Japan. The Chinese Communist Party decided to regard IT Security as important as political stability, economic safety and national defence in 2004, which is important for future development. The Chinese government has implemented strict controls on research into and the manufacture, and marketing of security-related products through several approval processes. All IT security-related products sold in China must be certified by the Computer Information Network Security and Product Quality Supervision Center. Too much dependence on foreign suppliers is considered a threat to national security and the most important thing is to work out is China's own basic software according to some sources.

- **Low priority for cyber security at the Department of Homeland Security.** Cyber security in the US is considered to be an area of low priority compared to other homeland security issues. The 2006 budget for the National Cyber Security Division at Department of Homeland Security (DHS) is about 73 million USD, only 0.2 percent of the total DHS funding. The low priority can be explained by the fact that IT incidents do not usually cause casualties. There is also resistance in the US by several large companies within the IT-industry to any kind of major government cyber security initiatives. A market-driven approach to IT is a fundamental part of the US IT leadership. However, the total federal budget includes about 10 billion for information technology projects relating to homeland security. Security and safety applications based on ICT are a priority such as screening and surveillance. Over recent years progress in cyber security in the US has been made in areas such as capabilities for large-scale network intrusion detection and for communicating cyber threats, structures for intra-industry information sharing of security-related information, the creation of programmes for cyber security assessments together with the certification and development of best practice guides. Over recent years many new federal initiatives have been created but the impact in terms of new R&D funding to the universities is not significant. China is just beginning to strengthen its IT security in all its aspects. The awakening has been quite rude and the pace of progress is now quite rapid. The research budget IT security in the next five-year plan (2006-2010) will most probably be at least 50 percent higher, albeit starting from a low level of funding.

- **Regulations – an important driver for IT security investments.** Regulation for different industrial sectors is one of the major forces driving technology investment today in information- and IT security in the US. It is important to recognize that general legislation such as the Sarbanes Oxley Act is more important than IT policy for the improvement of IT security in several countries such as the USA. Compliance-related investment is still more important in many ways for the IT security industry than the federal initiatives within Homeland Security. The total cost in 2005 for US companies to comply with the Sarbanes Oxley Act for financial reporting is estimated at 6.1 billion USD including technology costs of 1.7 billion USD. The Personal Information Protection Act of 2003 in Japan is the major regulation to drive focus on information security in Japan. Several high-profile cases of data leakage and the 2005 implementation of the act have contributed to give information security a strong focus in Japan over the last few years. It may be a late awakening but the reorganization in Japan of government work on IT security, the almost simultaneous creation of the IT security research centres at AIST and NICT, and a strong history of making up for lost time, may strengthen Japan as a player on the international arena of IT security. The focus is more on *information security* than *IT security*, both in terms of public debate and public R&D investments. But the former is a driver to the latter, and there is a new general security awareness that Japanese researchers and developers will bring to new technologies, products and services.

Research, Development and Technology

- **Possibilities for R&D Cooperation.** Lacking an approach for growth strategy in IT security R&D policy in Japan, in combination with the future focus on developing technologies in the Ubiquitous-Japan policy programme established by MIC, may offer a window of opportunity for Swedish-Japanese R&D collaboration, where Sweden takes the role of focusing on IT security-related products, services and systems, involving Japanese ubiquitous technologies. From a Swedish perspective there seems at this moment to be very little to learn from China from a technological point of view. There is a general interest on the part of the Chinese authorities in establishing collaboration, more specifically in the areas of IPv6, IP-telephony, and WLAN security areas, where China is relatively strong. The two most important factors that will drive the development of (public and commercial) IT security in China also in the future are: the great need for enterprises and the whole of society to speed up the implementation of IT security solutions. Secondly, the leading and promotional role played by the Chinese government. However, where there is a lack of domestic companies with the advanced technology required, the Chinese government will most probably open up and allow foreign companies to participate in important security infrastructure projects. Areas for R&D co-operation between the USA and Sweden within Homeland Security are described in an earlier

ITPS report[26]. Possible areas for R&D co-operation with the USA within IT security are e.g. IT security test beds, IT security aspects of Open Source, designing secure IT systems and holistic approaches to IT system security.

- **Common Criteria of interest for Critical Infrastructure Solutions.** The lack of requirements from US civilian agencies makes it more difficult for suppliers to justify the long and expensive evaluation process, according to several sources. So far, Common Criteria (CC) is only required in the US for National Security Systems, although recommendations for the use of CC for Critical Infrastructure Systems also exist. The international recognition of Common Criteria certificates only covers the assurance levels 1-4 which may not be enough for several US Homeland Security-related acquisitions. Globally only 22 countries accept the Common Criteria. However requirements for CC certification of the technology used for Swedish Critical Infrastructure solutions such as the Internet should be considered. Countries such as China do not accepted CC. For sales of IT security products in China the products need to comply with particular certification requirements defined by agencies in China. In April, 2002, in order to strengthen the work of IT security standards, China National IT Security Standard Technical Committee was set up, followed by the Information Classified Security Protection Evaluation Center in 2003. So far 47 IT security-related national standards have been published in China.
- **Secure software engineering methods of importance**. The software development methods that have been the norm fail to provide the high-quality, reliable and secure software that is required. Software development is still not a sufficiently rigorous discipline, and the process in not controlled to minimize the vulnerabilities. Security cannot easily be added on afterwards. Next-generation infrastructural concepts, with designed-in and built-in security are one vision. The Secure Foundations Initiatives is a US programme for collaboration between the code analysis suppliers and the universities to train developers in secure software. Vulnerability analysis and Code Scanning tools that can identify software defects are considered important R&D areas. Other R&D areas are "language-based security" including code verification, disciplined styles of programming and multi-lingual security.
- **The importance of new IT security concepts.** Policy Enabled Network Security is a proactive approach to security compared to the current reactive patching. Different ways of defining and managing policies is considered one of the most important IT security R&D areas. The research centre ISI CCSS is working on standards for policy definitions and distribution. For efficient policy management interoperability is based on standards of importance. Anti-spam providers have also started to launch Reputation Services in their anti-spam systems. A large amount of cyber security research to date has been focused on perimeter defence for protection from outside threats, but the model is not sufficient. Once the perimeter is breached, the attacker has free access to every

[26] *ITPS report in Swedish, Samverkansmöjligheter mellan Sverige och USA avseende forskning och teknik inom säkerhets och krishanteringsområdet, Magnus Karlsson, February 2004.*

connected system in the network. A new possible approach is “mutual suspicion”, all network elements need to verify the identity continuously.

- **IT security is emerging as a service business.** Security as a service is considered to be one development direction for the future. The services can facilitate the management of security vulnerabilities by organizations. The IT security product business is to a large extent an international business in comparison with the more domestic service business. However, in May 2005 Microsoft Windows announced OneCare, which is an automated service that will deliver anti-virus, anti-spyware and firewall features. The development in Japan is contributing to a service focus on an already strong market for IT security, as it offers inroads for outsourcing, consulting and certification. The IT services market represents about 26 percent of the total IT security market in Japan compared to about 20 percent in the USA. Tool and equipment suppliers as well as users are increasingly realizing that introducing security products does not automatically eliminate all threats. Products suppliers are therefore starting to emphasize after-sales business and through tie-ups with service suppliers are offering after-sales activities to help clients improve the overall security.
- **When the Internet fails to provide security, new networks are created.** Internet was originally built without much consideration of internal attacks. Today’s Internet protocols provide limited security and migration to all-IP networks will probably lead to increased vulnerability, and new solutions for security in all-IP networks are of importance. Providing security Service Level Agreements (SLA) is one way of improving the security offering for the operator. However, some researchers consider that most of the security development will be implemented at the end-points. The next version IP protocol, version 6, (IPv6) will provide some new security features, but new types of threat could also be created. IPv6 is mostly a priority in Asia and particular China. The federal US government requires agencies to use IPv6 in June 2008. A new critical infrastructure for defence purposes is the Global Information Grid (GIG). GIG will reduce military exposure to the insecurities associated with civilian IT infrastructure. The GIG project is projected to cost 100 billion USD and is one of the largest IT projects ever. Homeland Secure Data Networks (HSDN) is another network that addresses the requirements for secure data communication of classified information. Swedish participation in international co-operation regarding IPv6 such as IPv6 Forum should be considered because the protocol is becoming more important.
- **IT security test beds are considered important.** The Department of Homeland Security Cyber Security Research and Development Centre has test beds as one of five focus areas. DETER cyber security test bed is another example that provides a supplier-neutral experimental environment for collaboration between researchers. DETER is funded by NSF and HSARPA. The researchers consider the evaluation of network security mechanisms as important for advances in cyber defence. The test beds are important because new frameworks and methodologies for testing and benchmarking need to be developed according to several sources in the USA.

- **The convergence of cyber and physical security.** Convergence is on-going between cyber personal and physical security. The integration of IT security and physical security is an important issue for industry and the users. The Open Security Exchange is a cross-industry forum dedicated to merging physical and IT security solutions. America's Shield Initiative is a DHS project for electronic surveillance along the national borders based on sensor and video equipment. People and materials screening and tracking is another major homeland security segment.
- **Product bundling is one trend driving the industry.** A single IT security product is considered to insufficient by the IT security industry. The trend within the industry is towards bundling security products. More security features will become commodity features of the products in the future. Another major trend in the industry during 2004 has been the consolidation of companies.

12.2 Policy Recommendations

There are several reasons for the need to consider policy actions relating to IT security. Stimulating awareness and use of IT security is one way of increasing the trust in IT, which can benefit productivity. Increasing government use of IT security can facilitate the implementation of e-government solutions with benefits for society. Promoting IT security R&D can facilitate growth in the Swedish IT security industry. Developing resources to fight cyber crime is a part of the law enforcement capabilities of society that will support migration to the Information Society[27].

- **New requirements on agencies are an important step.** One way to improve information- and IT security in society is to tighten the requirements on governmental agencies. Improving IT-security at agencies is also an important part of the implementation of e-government. Swedish work regarding the formulation of an IT security base level for the agencies at the Swedish Emergency Management Agency should learn from the initiatives in the USA. The Federal Information Security Management Act (FISMA) of 2002 improved the annual reviews and reporting requirements concerning IT security at the US federal agencies. The act also requires the National Institute of Standards and Technology (NIST) to develop IT security guidelines in a number of areas such as minimum security standards. Recent achievements within cyber security have been made in areas such as the development of best practice guidelines. NIST has also published a Security Metrics Guide for Information Technology Systems. The act also requires the Office of Management and Budget to submit a report to Congress on agency compliance with IT security requirements including performance measurements. Federal Computer Security Scorecards for the federal agencies are issued to track the progress. The measurement of IT security is driven by regulatory, financial and organizational reasons. Metrics, benchmarking and best practice to help evaluate new technologies and products are important. Today’s certification criteria are considered antiquated and

[27] *The Government: Från IT-politik för samhället till politik för IT-samhället, proposition 2004/05:175*

expensive. Beginning in January 2006, US agencies must, according to FISMA requirements, set up a minimum of 17 security controls on all major applications and general support systems.

- **Awareness and usability are a bottleneck for improvements.** Swedish agencies have initiated different initiatives to improve IT security awareness, although Sweden needs to consider further initiatives for improvements of the awareness, and learning from the initiatives in other countries should be an integrated part of ongoing work in Sweden. The use of information and IT security solutions often lays different additional constraints on the user. A common perception today is that greater network security is not worth the cost for individuals and organizations. This perception discourages investment in new solutions for improved security. The perceived value of trust in the IT infrastructure needs to be enhanced. User-centred security is an important area and better usability is necessary in the future. Increasing the motivation to use IT security solutions could be even more important than awareness. The focus on application security has also increased compared to network security focus earlier. In the US awareness certification programmes for organizations have been launched, cyber security education for school children is spreading to a larger number of schools and the National Science Foundation is funding R&D into a human computer interface for security. Japan too has set a priority for initiatives such as IT security education for young people.
- **IT security R&D is the basis for long term trust.** Administrative and legal initiatives for improved IT security in Sweden need to be combined with appropriate R&D initiatives. The development of new approaches to protecting computer systems and networks is considered necessary. Satisfactory long-term trust in information systems requires new solutions based on R&D according to several sources. The US Cyber Security Research and Development Act of 2002 authorized 875 million USD between 2003 and 2007 for cyber security programmes at the National Science Foundation (NSF) and at the National Institute of Standards and Technology (NIST). The Act passed through the legislative process because the available technology was considered not to provide sufficient protection, and relatively little R&D has been conducted to develop new approaches. NSF established a Cyber Trust programme in 2004. The President's Information Technology Advisory Committee considers that there is an imbalance in the current federal cyber security R&D portfolio because of limited support for fundamental research to address larger security vulnerabilities of the civilian IT infrastructure.
- **Benefit from Swedish system knowledge.** Several different sources indicate that a more systems based approach to security is of importance. Holistic system security, including an end-to-end architectural approach to the topic, is one concept. Today's specialized products do not provide sufficient integration and a broad consensus among computer scientists is that the approach of patching to add security is not suitable in the long run. Also usability and design need to be an integral part of the development process from the beginning in the same way as security. The annual cost to business from repairing IT threats such as

viruses is several billion dollars, and in US the annual cost is estimated at 60 billion USD. To improve security is it necessary to develop new methods for designing and engineering secure systems. Swedish telecom system knowledge could be an advantage for the creation of new IT security solutions and architectures based on a systems approach for secure cyber infrastructures. A systems-based approach to IT security is a possible Swedish focus area within IT and telecom.

- **IT security risk – and cost benefit analysis is important.** Several different forms of investment can be made to improve IT security and it is a challenge to select the most efficient initiatives. Risk management is important for Homeland Security in the US because DHS has been criticized for lacking strategic thinking. Homeland Security covers a broad area and prioritization is important to achieve the best return on investment. The total US budget for the department of Homeland Security is about 40 billion USD. The Center for Risk and Economic Analysis of Terrorist Events is involved in risk analysis and was the first Department of Homeland Security (DHS) Center of Excellence which indicates the priority and importance of risk and cost-benefit analysis. The implementation of tools for risk and cost-benefit analysis should also be considered by Swedish agencies involved in the funding of new security technologies such as VINNOVA.

13 Abbreviations and Terms

AIST	National Institute of Advanced Industrial Science and Technology
APCERT	Asia Pacific Computer Emergency Response Team
APEC	Asia-Pacific Economic Cooperation
APF	Authentication processing framework
ASEAN	Association of Southeast Asian Nations
ATIP	The Asian Technology Information Program
ATM	Automatic Teller Machine
BBB	Better Business Bureau
CERT	Computer Emergency Response Team
CPVA	the Contactless Palm Vein Authentication technology
CRL	the Communications Research Laboratory
CRYPT	Cryptography research group
CRYPTREC	Cryptography Research and Evaluation Committee
DDOs	Distributed Denial of Service
DHS	Department of Homeland Security
FIRST	Forum of Incident Response and Security Teams
FISMA	The Federal Information Security Management Act
G8	Group of Eight powers
HR	Human Resources
IAIP	The Information Analysis and Infrastructure Protection Directorate
IDS	Intrusion Detection System
Information Security	The area of protecting and preserving information on a network as well as the network or cyber infrastructure itself.
IAAA	The I Am Alive Alliance
ICCC	International Common Criteria Conference
ICT	Information and Communication Technology
IDS	Intrusion Detection System
I-EMI	Intentional Electromagnetic Interference
IPA	Information -Technology Promotion Agency, Japan

IPv6	IP version 6, the next generation Internet Protocol, today IPv4
ISAC	Information Sharing and Analysis Center
ISC	Information Security Center at NICT
ISCO	Information Security Certification Office
ISEC	The Information-technology Security Center
ISMS	Information Security Management Systems
ISP	Internet Service Provider
ISS	Internet Security Systems
IT	Information Technology
JAIPA	Japan Internet Providers Association
JETRO	Japan External Trade Organization
JIPDEC	Japan Information Processing Development Corporation
JIS	Japan Industrial Standard
JISEC	Japan Information Technology Security Evaluation and Certification Scheme
JPCERT	Japan Computer Emergency Response Team
JPCERT/CC	Japan Computer Emergency Response Team/Coordination Center
JPY	Japan Yen, 100 JPY = 14,5 SEK
JSPS	Japan Society for Promotion Sciences
JST	Japan Science & Technology Agency
LAB	Security Engineering Laboratory
METI	Ministry of economy, trade and industry
MEXT	Ministry of Education, Culture, Sports, Science and Technology
MIC	Ministry of internal affairs and communication
MSSP	Managed Security Service Providers
NDRC	National Development and Reform Commission
NEDO	New Energy and Industrial Technology Development Organization
NESSIE	New European Schemes for Signatures, Integrity, and Encryption

NICT	National Institute of Information and Communication Technology
NIRT	National Incident Response Team
NISC	National Information Security Center
NPA	National Police Agency
NPO	Non Profit Organization
NIST	The National Institute of Standards and Technology
NSA	The National Security Agency
NSF	National Science Foundation
OECD	Organization for Economic Cooperation and Development
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
RCIS	Research Institute for Computational Sciences
R&D	Research and Development
RFID	Radio Frequency Identification
RMB	Renminbi, (People's Currency), currency in China, 1 RMB = 0,9 SEK
SCIRT	Computer Emergency Response Team
SIOS	Security Integrated Operation Studio
SITIC	Sveriges IT-Incident centrum
SOE	State Owned Enterprise
SPREAD	Security Promotion Realizing Security Measures Distribution
TAO	The Telecommunications Advancement Organization
TELESA	Telecom Services Association
TEMPEST	Transient Electromagnetic Pulse Surveillance Technology
UC	University of California
USD	United States Dollar, 1 USD = 7,5 SEK
VUAC	Virus & unauthorized access counter
WPKI	Wireless Public Key Infrastructure

14 Appendix

IT Security in Japan, Timeline of Important Regulations and Policies

IT-security in Japan. Timeline of Central Regulation and Policies

	Gov	Regulation/Policy	Non Governmental Organizations
2005, April	NISC, National Information Security Center. Part of IT-Security office		
2005, April	- - - - - - -	Personal Information Protection Act	
2005, Feb	- - - - - - -	IT Policy Package, 2005	
2004, Aug	- -		IGTF-J, Internet Governance Task Force, Japan
2004, June	- - - - - - -	e-Japan Priority Policy Program, 2004	
2004 Feb	- - - - - - -	e-Japan Strategy II Acceleration Package	
2003, Aug	- - - - - - -	e-Japan Priority Policy Program, 2003	
2003, Sept	- - - - - - -	Implementation of Vulnerability Test on the Information Systems of Ministries, Agencies	
2003, Sept	- - - - - - -	Prompt and Reliable Measures For Incidents Related to IT security	
2003, July	- - - - - - -	e-Japan Strategy II	
2002 , Nov	- - - - - - -	Improvement of IT Security Policies effectiveness	
2002, July	- -		Telecom ISAC Japan
2002, July	- - - - - - -	Enforcement of law concerning specific trade law - action on spam mail problem	
2002, June	- - - - - - -	e-Japan Priority Policy Program, 2002	
2002, April	- -		JPRS starts to manage the JP- domain from JPNIC
2002, April	- - - - - - -	Rule of JP domain name dispute processing - correspondence of domain name to illegal use	
2002, Mar	Establishment of the National Incident Response Team, NIRT, as part of IT-Security office		
2001, Dec	- - - - - - -	Revision of a part of Unfair Competition Prevention Law - illegal use for domain name	
2001, Nov	- - - - - - -	Acceleration of e-Japan Priority Policy Program and e-Japan 2002 Program	
2001, Oct	- - - - - - -	Action Plan for Ensuring e-Government's IT Security	
2001, June	- - - - - - -	e-Japan 2002 Program	
2001, May	- -		NPO-JNSA, Japan Network Security Association
2001, April	- -		IA Japan, The internet Association of Japan
2001, April	- - - - - - -	Law concerning e-signature and attestation business	
2001, Mar	- - - - - - -	e-Japan Priority Policy Program	
2001, Jan	IT Strategic Headquarters established within the Cabinet. Consists of IT-policy- and IT-security office		
2001, Jan	- - - - - - -	e-Japan Strategy	
2000, Dec	- -		JPRS, Japan Registry Service
2000, Dec	- - - - - - -	Special action plan on countermeasures to cyber-terrorism of critical infrastructure	
2000, Nov	- - - - - - -	Basic IT Strategy decided	
2000, Nov	- - - - - - -	IT Basic Law 144, Formation of an Advanced Info- and Telecom. Network Society	
2000, Mar	- - - - - - -	Law concerning protection of individual information	
2000, Feb	IT-security office. Cabinet secretariat that promotes IT-security policies. Supplies IT-HQ		
2000, Feb	IT-security promotion committee , Part of IT-HQ		
2000	- - - - - - -	Law Concerning Electronic Signatures and Certification Services. Law No. 102	
1999, Dec	- -		JAIPA, Japan Internet providers Association
1999	- - - - - - -	Law on Unauthorized Computer Access. Law No. 128	
1997, Mar	- -		Japan Network Information Center
1997	- -		JCSA, Japan Computer Security Association
1994, Aug	IT-HQ, Advanced Information and Telecom. Society Promotion Headquarters, within the Cabinet		
1992	- -		Japan Computer Emergency Response Team

Web Sites for Some Major Organizations

USA

National Security Agency: http://www.nsa.gov

CERT Coordination Center: http://www.cert.org

National Cyber Security Partnership: http://www.cyberpartnership.org

Cyber Security Industry Alliance: https://www.csialliance.org/home

Information Systems Security Association: http://www.issa.org

Internet Security Alliance: http://www.isalliance.org

The Liberty Alliance Project: http://www.projectliberty.org

Japan

JPCERT/CC: http://www.jpcert.or.jp/english/

National Police Agency: http://www.npa.go.jp/english/

Cyber@Police: http://www.cyberpolice.go.jp/english/index.html

Information Technology Promotion Agency: http://www.ipa.go.jp/index-e.html

China

The National Development and Reform Commission: http://www.ndrc.gov.cn

Ministry of Public Security: http://www.mps.gov.cn

Ministry of Information Industry: http://www.mii.gov.cn

Ministry of Science & Technology: http://www.most.gov.cn

State Information Center: http://www.sic.gov.cn

15 References

(AAAS 2004A), AAAS Report XXIV Research & Development FY 2005, Intersociety Working Group, American Association for the Advancement of Science, April 2004.

(AS 2005), Asahi Shimbun, July 12, 2005.

(ATIP 2004), The Asian Technology Information Program, A-QuIST Digest. March-April 2004.

(CCW 2005), China Computer World, May 23, 2005

(CEPRO 2004A), Report written in Swedish, Tillit till IT – en studie av förutsättningarna att öka tilliten till IT och Internet, CEPRO Management Consultants, oktober 2004.

(Cherry 2005), Steven Cherry, The Net Effect, IEEE Spectrum June 2005, p 32.

(Cisco 2005A), Securing the Intelligent Information Network, White Paper, Jayshree Ullal, Cisco Security Technology Group, Cisco, 2005.

(CIPRD 2004A), The National Plan for Research and Development In Support of Critical Infrastructure Protection, The Executive Office of the President Office of Science and Technology Policy, 2004

(CISWG 2004A), Corporate Information Security Working Group, Report of Best Practices and Metrics Teams, November 17 2004.

(Cn 2005A), Communication trends, Communications News, March 2005.

(CNSS 2005A), Committee on National Security systems, National Policy Regarding the Evaluation of Commercial Products, Frequently Asked Questions, 24 March 2005.

(CRS 2005A), Transportation Security: Issues for the 109th Congress, Congressional Research Service, March 2005.

(CRS 2005B), Congressional Research Service, March 2005.

(CRS 2005C), Identity Theft: The Internet Connection, CRS Report for Congress, Congressional Research Service, March 2005.

(CSIA 2004A), Agenda for the Next Administration – Proposals by the Cyber Security Industry Alliance, December 2004.

(DHS 2005A), Department of Homeland Security, Information Sharing & Analysis Centers, webb information, May 2005.

(DHS 2005B), Homeland Security, Budget-in-Brief Fiscal Year 2006, January 2005.

(DHSCSRD 2005A), Cyber Security Research and Development Center, webb information, http://www.hsarpacyber.com, May 2005.

(Ekonomisk Debatt 2003A), In Swedish, Riskperception och attityder, Lennart Sjöberg, Ekonomisk Debatt, årg 31, nr 6, 2003.

(Eweek 2005A) MIT research and grid hacks reveals holes, Eweek, May 2005.

(EU 2004A), Communication from the Commission, Security Research: The Next Step, Commission of the European Communities, September 2004.

(FCW 2004A), Linux wants to earn your trust, Federal Computer Week, October 18 2004.

(FCW 2005A), FISMA tightens criteria, Federal Computer Week, March 16 2005.

(FUJITSU 2005), Fujitsu press release, web information, Fujitsu Limited, www.fujitsu.com/global/news/pr/archives/month/2005/20050511-01.html, May 2005.

(GCN 2004A), Feds: We must set sharing policies, Government Computer News, http://www.gcn.com, November 2004.

(HHS 2002A), Report in Swedish, Sjöberg, Lennart; Risk, politik och näringsliv, SSE/EFI Working Paper Series in Business Administration No 2002:6, Handelshögskolan i Stockholm, 2002.

(IAAA 2005), web information, IAAA, 2005, http://www.iaa-alliance.net/en

(IFC 2005), The ICT Landscape in the PRC – Market Trends and Investment Opportunities, IFC Report March 2005.

(ISMS 2005), web information, ISMS, www.xisec.com/

(IPA 2005A), Certified/Validated Products List (web information: www.ipa.go.jp/ security/jisec/jisec_e/certfy_list200504.html), IPA, 2005

(IPA 2005B), web information, Cryptographic Techniques Evaluation Project (CRYPTEC), IPA, 2005, www.ipa.go.jp/security/enc/CRYPTREC/

(IPA 2005C), IPA Security Center. Appendix in the guide book for public procurement by utilizing ISO/IEC15408

(ISPC 2005A), Donn Parker, Mark Beckmeyer, Information Security Professionals Conference, Dallas, May 2005.

(ISI 2005A), Meeting with Clifford Neuman, Research Scientist, Information Sciences Institute, May 2005.

(ISPC 2005B), Hal Tipton, Information Security Professionals Conference, Dallas, May 2005.

(ISU 2003A), CyberInsurance: A Market Solution to the Internet Secuirty Market Failure, William Yurcik, Illinois State University, 2003.

(ITPS 2003A), Report written in Swedish, IT och tillit, Delrapport till ITPS utvärdering av den svenska IT-plitiken, Institutet för tillväxtpolitiska studier, rapport A2003:015, oktober 2003.

(IW 2004A), IT security Soaring Cost, Information Week, November 2004.

(IW 2005B), Microsoft Pledges to Help Governments, Information Week, February 2005.

(IW 2005C), More Secure Linux Still Needs To Win Users, Information Week, March 2005.

(IW 2005D), Reports of Identity Theft Continue to Rise, Information Week, April 2005.

(IW 2005E), Sarbanes-Oxley compliance may be a burden, but it´s helping some companies, Steven Marlin, Information Week, March 21 2005.

(JETRO 2005A), Japanese Information Security Industry (May, 2005), JETRO, May 2005.

(JETRO 2005B), Trends in Japanese Information Security Industry (May, 2005), JETRO, May 2005.

(JETRO 2005C), Trends in Japanese Information Security Industry (May, 2005), 2005.

(JETRO 2005D), Trends in Japanese Information Security Industry, JETRO, May 2005

(JIPDEC 2005A), web information, JIPDEC, www.jipdec.jp, 2005

(JIPDEC 2005B), web information, JIPDEC, www.isms.jipdec.jp/en/list/org2.html, July 2005

(JNSA 2004), Fiscal 2003, Information security incident survey report, Japan Network Security Association, March 2004, www.jnsa.org/houkoku2003/ incident_survey1_e.pdf.

(KBM 2005A), Report in Swedish, Beredskap mot skadlig kod, Krisberedskapsmyndigheten, 2005.

(KBM 2005B), Report in Swedish, Samhällets informationssäkerhet, lägesbedömning, Krisberedskapsmyndigheten, 2005.

(LAT 2005A), Identity-Theft Prevention Is Needed, LA Times, May 27 2005.

(Liu 2005), Personal communication with Dr. Liu Bing, IT Security Division Chief, MOST, June 27, 2005.

(METI 2005), web information, www.meti.go.jp/english/information/data/IT-policy/privacy.htm

(MEXT 2004A), FY 2005 Budget, Ministry of Education, Culture, Sports, Science and Technology (MEXT), 2004

(MEXT 2004B), Major items in the Fiscal 2005 budget, Ministry of Education, Culture, Sports, Science and Technology (MEXT), 2004.

(MIC 2004A), White paper on information and communication in Japan, 2003, MIC, 2004.

(MIC 2004B), Survey of actual trends on information security, IT Security Office, MIC, 2004.

(MIC 2004C), 2nd survey report concerning with telecommunications service monitor in 2003, MIC, April 2004

(MIC 2005A), Information Security Policies in Japan, Mabito YOSHIDA, IT Security Office, Information and Communications Policy Bureau, MIC, June 2005, www.itu.int/osg/spu/cybersecurity/presentations/session7_yoshida.pdf.

(MIC 2005B), web information, www.soumu.go.jp/s-news/2005/050225_5_2.html

(MIC2005C), Structure of Information Security Center, National Institute of information and Communications Technology (NICT), web information, www2.nict.go.jp/jt/a120/security/page2e.html

(MIT 2004A), Weill, P.; Aral, S., Managing the IT Portfolio, Center for Information Systems Research, Research Briefing, Volume IV, Number 1A, March 2004.

(MS 2005A), Mapping Security Index, Tom Patterson, Information Security Professionals Conference, Dallas, May 2005.

(NCSP 2004A), Report of the Best Practices and Metrics Teams, Corporate Information Security Working Group, 2004.

(NCSP 2005A), The National Cyber Security Progress Report, National Cyber Security Partnership, February 2005.

(NetMag 2005A), Securing the IP Telephony Perimeter, Network Magazine, 2005.

(NIST 2003A), Security Metrics Guide for Information Technology Systems, National Institute of Standards and Technology, July 2003.

(NICT 2003), e-Government Recommended Ciphers List, National Institute of Information and Communications Technology (NICT), February 2003, www2.nict.go.jp/jt/a124/cryptrec_publicity/E-Government%20Recommended%20Ciphers%20List.htm

(NICT 2005), Press release, June 17 2005, www2.nict.go.jp/pub/whatsnew/press/h17/050617/050617.html

(NIKKEI 2004), Nikkei Weekly 13 September 2004.

(NIKKEI 2005), Nikkei Weekly 4 July 2005.

(NE 2005), Nikkei Electronics No 890. Jan 3rd 2005

(NEC 2005A), NEC Journal of Advanced Technology, Vol. 2, No. 1 winter 2005, NEC Corporation, 2005

(NEC 2005B), NEC press release, web information, NEC Corporation, www.nec.co.jp/press/en/0505/3101.html, May 2005

(NPA 2005), report on R&D related to access control technologies, NPA, January 2005

(NPSC 2005), National Public Safety Commission. R&D on unlawful computer access act and access control functions. www.npsc.go.jp/hightech/pdf17.pdf

(NS 2005A), Netinfo Security, No 1, p 39, 2005

(NS 2005B), Netinfo Security, No 3, p 19-25, 2005

(NS 2005C), Gu Jianguo, Netinfo Security, No 4, p 7-9, 2005

(NS 2005D), Netinfo Security, No 1, p 31, 2005

(NSF 2002A), The Cyber Security Research and Development Act, HR 3394, 2002.

(NSF 2004A), National Science Foundation, 2004.

(NTT 2005), NTT Technical Review Jan 2005 & May 2005, Nippon Telegraph and Telephone Corporation, 2005

(OMB 2004A), FY 2003 Report to Congress on Federal Government Information Security Management, Office of Management and Budget, March 1 2004.

(OMB 2005A), Press release, Presidents 2006 Information Technology Budget Supports National Priorities and Focuses on Results, OMB, 8 February 2005.

(ONI 2005), Internet Filtering in China 2004-2005 – A Country Study, http://www.openinitiative.net.

(PC 2005), Japan's Personal Information Protection Act, Privacy council, web information, www.privacycouncil.com/adSvs_japan.php, 2005

(PD 2004), People's Daily 2004, September 18, Statement of the Fourth Session of the Sixteenth Chinese Communist Party' Congress.

(PITAC 2005A), Cyber Security: A Crisis of Prioritization, Report to The President, President's Information Technology Advisory Committee, February 2005.

(President 2003A), Homeland Security Presidential Directive Hspd-7, December 2003.

(PTS 2005A), Report written in Swedish, Strategi förr att säkra Internets infrastruktur, Post- och telestyrelsen, PTS-ER-2005:7, februari 2005.

(PWC 2004A), Rethinking the European ICT Agenda, Ministry of Economic Affairs, The Netherlands, 2004.

(RAND 2004A), Insurance, Self-Protection, and the Economics of Terrorism, Rand Center for Terrorism Risk Management and Policy, WR-171-ICJ, July 2004.

(RED 2005A), Red Herring, The Hottest Private Companies in North America, Vol. 2, No 19, May 2005.

(Regeringen 2005A), Report written in Swedish, Från IT-politik för samhället till politik för IT-samhället, proposition 2004/05:175, juli 2005.

(SCB 2004A), Report written in Swedish, Företagens användning av datorer och Internet, Statistiska central byrån, SCB, December 2004.

(SHG 2004A), A Blueprint for Enterprise Security, Sand Hill Group, March 2004.

(SIXXS 2005), IPv6 DFP's per country, web information, SIXXS

(SOU 2005:42), Report in Swedish, Säker information – Förslag till informationssäkerhetspolitik, Delbetänkande av InfoSäkutredningen, SOU 2005:42, 2005.

(SubCyb 2004A), Cybersecurity for the Homeland, Report of the Activities and Findings, Subcommittee on Cybersecurity, Science, and Research & Development, December 2004.

(Suttmeier 2004), Richard P. Suttmeier and Yao Xiangkui, China's post-WTO Technology Policy: Standards, Software, and the Changing Nature of Techno-Nationalism, NBR Special report 2004, National Bureau of Asian Research

(Symantec 2005A), Internet Security Threat Report, Symantec, 2004.

(Tele 2004A), An Ounce of Prevention, Telecommunications Americas, August 2004.

(Tele 2004B), Latest Version of IP Holds Promise and a Threat, Telecommunications Americas, July 2004.

(Tele 2005A), Network Security Drives Value, Telecommunications Americas, February 2005.

(TeleInt 2005A), Access all areas, Telecommunications International, March 2005.

(TOSHIBA 2005), Toshiba Review, Vol. 60, No 6, Toshiba Corporation, 2005.

(UCB 2003A), Open Source Software Aligns with Strategic National Computer Systems Security Policy, John Han, University California Berkeley, November 2003.

(UCB 2005A), University California Berkeley, Team for Research in Ubiquitous Secure Technology, Web information, May 2005.

(UN 2005A), News Release, UN Panel on Internet Governance Third Meeting, Apr 20, 2005.

(USDOJ 2005A), US Department of Justice, Computer Crime and Intellectual Property Section, webb information, (http://www.cybercrime.gov/), 2005.

(UST 2005A), Thieves hit Internet with sneakier software, USA Today, May 19 2005.

(USC 2004A), Internet Report, USC Annenberg School Center for the Digital Future, 2004.

(USC 2005A), Meeting with Detlof von Winterfeldt, Deputy Dean, Professor, Center for Risk and Economic Analysis of Terrorist Events.

(USC 2005B), Meeting with Charles Meister, Executive Director, Center for Telecom Management, May 2005.

(VINNOVA 2005A), Report in Swedish, Kunskap för säkerhets skull. Förslag till en nationell strategi för säkerhetsforskning, VINNOVA, 2005.

(White House 2003A), The National Strategy to Secure Cyberspace, White House, February 2003.

(White House 2005A), Analytical Perspectives, Budget of The United States Government, Fiscal Year 2006, 2005.

(Wired 2005A), US Military's Elite Hacker Crew, Wired News, April 2005.

(WP 2005A), Disputing Delaying Program Changes, The Washington Post, February 2 2005.

(Xu 2004), Xu Guangnan, IT Security and Telecommunication, No 12, 2004

(Zhao 2005), Zhao Zhansheng, Netinfo Security, No 1, p12, 2005

ITPS, Swedish Institute for Growth Policy Studies
Studentplan 3, 831 40 Östersund, Sweden
Telephone: +46 (0)63 16 66 00
Fax: +46 (0)63 16 66 01
info@itps.se
www.itps.se
ISSN 1652-0483

VINNOVA

itps SWEDISH INSTITUTE FOR GROWTH POLICY STUDIES