chapter five

Challenges to building a safe and secure Information Society

5.1 Introduction: Building confidence and security in the use of ICTs

Over the past two decades, the Internet has transformed many aspects of modern life. Use of the Internet continues to grow, with the estimated number of Internet users exceeding one billion worldwide at the end of 2006 and an estimated 113 million websites.[1] People around the globe and from all walks of life have been hearing about the promised improvements the Internet will bring to their lives. While some of these promises have materialized, the full potential of the Internet has not yet been realized. One of the main reasons is that many users lack trust in the Internet for conducting transactions or storing sensitive information. An online survey conducted by ITU in 2006 found that almost two-thirds of respondents had refrained from certain activities online due to security concerns, while users' greatest fears were theft of personal information (e.g., identity theft, credit card fraud etc), computer viruses and spyware.[2] Building trust and confidence is one of the key enablers of future growth and use of the Internet.

The expansion of the Internet is opening up many new opportunities for criminals to exploit online vulnerabilities to commit cybercrime acts or even deliberately attack the critical infrastructures of nation states. Viruses, spyware, phishing, identity theft, zero-day exploits, Denial of Service (DoS) attacks, zombie botnets, and other vulnerabilities are endangering cyberspace and jeopardizing the very future of the Internet. With spam and other exploitation now accounting for up to 90 per cent of e-mail traffic over the Internet, we stand at a critical point in the further development of the Information Society. Unless there is progress in building confidence and security in the use of Information and Communication Technologies (ICTs), users' trust in the Internet may diminish and this could limit its growth and potential.

The term "cybersecurity" is used generically to cover the range of threats to the use of the Internet and ICTs more generally, but it is worth distinguishing three broad areas of concern:

- Threats to individual users posed, for instance, by viruses or identity theft, as well as annoyances such as spam, spyware or pop-ups;
- Threats to businesses, governments or other organizations: for instance, through exploitation of vulnerabilities in their data storage, industrial espionage, system downtime, etc. Corporate users may also have liability in the case of threats to their customers, partners or suppliers;
- Threats to critical public infrastructures, including electronic communication networks, financial systems, emergency services, navigation systems, electrical power grids, air traffic control, water control systems etc.

While these dependencies vary from nation to nation, nearly all nations need to defend and protect their critical network information infrastructures, as the risks are huge, especially in a world in which strife between nations could transmute into electronic warfare. Telecommunications is a critical national infrastructure[3], as vital as the power supply in ensuring the smooth functioning of society. Since the mid-1990s, the rapid growth of ICTs and societal inter-dependency have led to a shift in the perception of threats to cybersecurity. Since then, greater linkages have been made between cybersecurity and Critical Information Infrastructure Protection (CIIP) and, as a consequence, a number of countries have undertaken an assessment of the threats, vulnerabilities and instruments to address them.

With the growing importance of cybersecurity at the national level, cybersecurity has moved onto the international political agenda. During the WSIS, "Building confidence and security in the use of ICTs"[4] emerged as one of the key principles for building an inclusive Information Society. Both the *Tunis Commitment*[5] and *Tunis Agenda on the Information Society*[6] highlight the need to continue the fight against cybercrime and spam, while ensuring the protection of privacy and freedom of expression. In the WSIS outcome documents, Summit participants called for all stakeholders to cooperate to promote, develop and implement a global culture of cybersecurity.

We stand at a critical point in the further development of the Internet. As new technologies are adopted, it is crucial to understand the risks that accompany them in order to maximize the benefits. Growing security threats to security, at the level of the individual, the firm, government and critical infrastructures, make security everyone's responsibility.[7] It is now more important than ever to understand the issues and keep up-to-date on how these challenges are changing.

This Chapter examines the challenges faced in building a safe and secure Information Society.

It reviews the changing nature of cyber-threats and their impact to determine to what extent the future development of the Information Society is at risk. It considers what the different stakeholders can do to build a safer and more secure Information Society, in terms of potential policy responses. Cybersecurity issues are complex and constantly evolving: as a result, coordinated policy action at the international level is needed to address the challenges and the threats to cybersecurity that are emerging.

5.2 The changing cyber-threat environment

5.2.1 From nuisances to real threats

The reliability and robustness of information and communication networks against attack are critical in the future development of the Information Society. The Internet has become such vital part of our society and cultures that it is often difficult to imagine how we ever functioned without it. However, at the same time, the potential for electronic attacks against our networks is growing rapidly. As users demand software with more features and services, and as the underlying source code becomes ever more complex, new opportunities for exploitation continue to emerge. Security is key to users' trust in e-business, e-government and other online applications.

One of the more prominent risks to Internet security is spam, which has mutated from a general annoyance to a broader cybersecurity threat. Spam is now the primary mechanism for delivering viruses that can hijack millions of computers (through so-called "zombie botnets") or launching phishing attacks to capture private or corporate financial information. Phishing refers to spam sent with a fraudulent motive - for instance, to gather credit card or personal banking information. Spam also acts as a platform for many other types of scams. Countries now widely recognize that cybercrime[8] is the fastest-growing form of criminality, including both new criminal offences in relation to computers (such as spam, viruses and hacking) and existing crimes committed using digital or computer technology (such as fraud, harassment, etc.).[9] During the Tunis Phase of the WSIS, participants reaffirmed their commitment to deal effectively with the significant and growing problem posed by spam. However, one problem that all spam-fighters constantly face is that the criminal is always one step ahead.

An additional dimension to consider is the changes taking place in users' online behavior. New ways of using the Internet to communicate, often linked to social networking websites such as MySpace, Bebo, Facebook, etc., are also increasing online security risks, as is the widespread availability of much higher bandwidth connections. The data shared on these sites can make users prey to online attacks. A name, address and birth date, let alone a social security number, provides more than enough ammunition for criminals to hack into financial records and compromise a user's personal information. Fraud, identity theft, computer spyware and viruses (with or without negligent user behavior) can flourish on social networking sites. A recent survey by European Schoolnet[10] indicated that 57 per cent of young people make their online social network profiles public and disclose personal information. Almost a third of youngsters surveyed indicated that they did not know how to choose whether their information should remain public or private on these sites, suggesting greater awareness is urgently needed. Social networking illustrates key trends in the Internet today, with a move away from the centre of the network towards the edges, less centralized control, more user-centric activities and greater user-generated content.

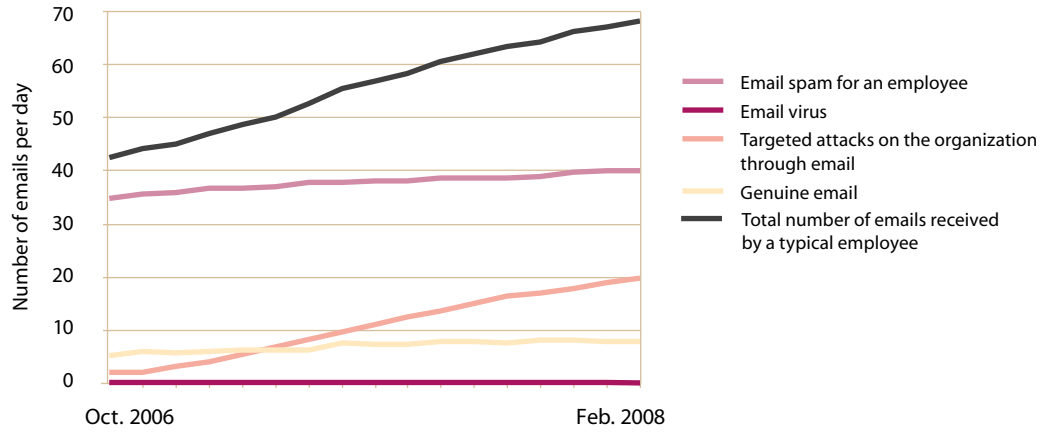
5.2.2 Spam and how the threat from spam is changing in nature

Spam is now worse than ever before.[11] Despite a recent optimistic 'state-of-spam' report by the United States' Federal Trade Commission in December 2006[12] suggesting that spam volumes might have leveled off, in early 2007, it appears that more spam is being sent and received than ever before. Spam now poses a security problem on a colossal scale: some nine out of ten e-mails are considered as spam[13] and both the volume and proportion are increasing steadily (Figure 5.1). Spam has been experienced by nearly everyone who has ventured online. Spam has now reached such a massive volume that experts are warning that spam and related threats could paralyze the Internet. It represents a huge burden on the Internet, clogging critical communication channels and slowing down Internet traffic, especially in developing countries where the capacity of links to the international Internet backbone may be limited.

Spam comprises unsolicited, unwanted and harmful electronic messages[14]: generally, but not exclusively, delivered by e-mail (spam can also

Figure 5.1: Forecast evolution of the changing nature of threats in cyberspace

Based on a typical user



Source: ITU, adapted from MessageLabs.

arrive over mobile phones, instant messaging or IP telephony services, etc). E-mail is considered a business-critical application for many organizations[15], as well as a form of legal documentation in many countries. How do so many spammers succeed in attracting victims and why do people believe the promises offered by spam e-mails? Are people really willing to part with their bank details or invest money in companies that they have never heard of? The answers can be found in the economics driving spam. The cost of sending e-mails is still very low, and if a million scam e-mails can be sent as easily as a single one, there is a likelihood of at least one positive response which will allow the criminal to make a profit. Spam can also be used for indirect profits - for instance, by hyping shares.

Spam - in all its forms - is a drain on resources, time and money. It imposes heavy direct and indirect costs on users, businesses and governments. The direct costs include spam-filtering software, hiring Information Technology (IT) engineers to deal with the problem and the purchase of additional equipment, bandwidth and storage capabilities. More broadly, spam slows messaging services, takes time to deal with (for instance, checking for false positive emails that are detected by a spam filter), reduces employee productivity and increases business costs. In Brazil, 62 per cent of Internet users spend at least five minutes a day dealing with spam, nearly a quarter (23 per cent) spend ten minutes a day and 2 per cent spend more than half an hour a day dealing with spam.[16] According to business surveys, the main justifications for investments in anti-spam initiatives are to compensate for reduced productivity and lost revenues, as well as to reduce the strain on the network and IT resources. Companies may be unwilling, however, to disclose the true costs of spam due to competitive pressures to preserve their reputation. The evidence suggests that costs are heavy, especially for Multi-National Corporations (MNCs) with worldwide operations using e-mail in multiple languages.

The nature of spam is also changing. The e-mail scams asking people to act as intermediaries and move large sums of money through bank accounts are still in circulation, but no longer make up the majority of spam received. More personalized e-mail spam is increasingly common. Pop-ups masked as legitimate warnings from the e-mail software in use on the computer are increasing, as these are currently not picked up by the most commonly-used spam filters. Such pop-ups may state: "Warning: hidden files might have been installed on your computer from the websites you have visited". The person behind this scam wants you to click to accept and download a "safe" program to eliminate the supposed files from your personal computer.

Image spam, or emails sent with embedded images, is a new kind of spam, which is increasing rapidly.[17] By using embedded images instead of text, messages are able to avoid detection by anti-spam filters that rely on the analysis of textual spam content, giving spammers a better chance of having their messages read. A small .gif-file (not

Box 5.1: Threats in cyberspace
Why they deserve increased attention

There are several reasons why cybersecurity is growing in importance to countries and stakeholders around the world, including:

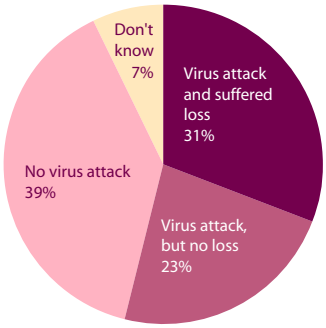
- Inherited architecture: the Internet began as a closed network with a limited number of known users with access, so user authentication was not an issue. The design philosophy of the Internet is now several "generations" behind the latest technological changes (consider, for example, the issue with inherited architecture posed by the 'millennium bug').
- Constant evolution in protocols and technology: the US National Institute of Standards and Technology (NIST)[19] has played a key role in establishing some of the protocols and algorithms used to secure Internet transactions through the use of hash functions. However, in the constant tug-of-war of human ingenuity, many encryption algorithms are eventually compromised. As an example of this, NIST launched an open, blind competition to come up with a fresh algorithm for hash functions in January 2007.
- Evolution of the network: telecommunication networks are evolving towards Next-Generation Networks (NGNs) with decentralized intelligence at the edges of the network and separation of the control layer from the transport layer. The capacity and speed of networks are also increasing. In the absence of specific measures to address network security, the decentralization of intelligence to the edges of the network may make the network more vulnerable.
- Convergence: the combination of different ICTs in converged devices with multiple functions offers opportunities for 'cross-infection', with the problems of one technology feeding into other ICTs. The power and reach of a computer virus would multiply, if it could be transmitted through Internet Protocol television (IPTV) as well as e-mail, to make it much more devastating.
- Size and scale effects: the growth in the size of the network means that chain-reaction network effects are also growing, at an increasing pace.
- Anonymity: the lack of user authentication on the Internet means that it is easy to be anonymous and/or provide false identity information to misbehave online, visit suspicious sites or commit cyber-related crimes without any fear of reprisal ("the easier it is to be bad, the worse people are[20]"). Conversely, anonymity may be one way in which users feel protected, in not giving away information and guarding against attack.
- Internationalization: the availability of the Internet in nearly every country in the world means that the legal framework may have difficulty keeping pace with technological developments: a chain is only as strong as its weakest link. A hacker operating from an unidentified country could use computers in, say, Latvia and the US to attack a Korean government site. Such international attacks are very difficult to guard against.
- Growing dependency on ICTs: modern lifestyles are increasingly dependent on ICTs in work and at play, as well as the storage and transmission of electronic data, for everything from bank accounts to assets to health records. In some countries, the Internet has become such vital part of society that it may be difficult to remember how they functioned without it. Loss of such information could have profound consequences. Very few organizations have the threat-analysis capabilities and strategies in place to address network threats.[21]

Source: ITU.

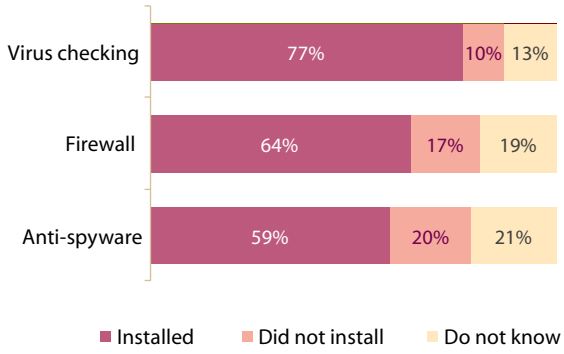
visible in the e-mail received due to its small size) enables the sender of the spam e-mail to know when and if the e-mail message is opened and detect links in pages and e-mails that are opened after the specific spam message. As a result, your personal information could suddenly be in the hands of the spammer. The person or organization behind this e-mail may also want confirmation that the e-mail address is active, so it can be sold to other spammers.

Figure 5.2: Viruses - How worried are you?

Proportion of home users in Singapore that had experienced a virus attack, 2006



Proportions of home internet users that had installed anti-virus software, 2006



Note: The base sample comprised home internet users aged 15-59 who had used the Internet in the preceding 12 months.

Source: Singapore Infocomm Development Authority (IDA), Household Survey, at: www.ida.gov.sg.

Spammers are constantly developing new techniques either in response to, or in advance of, anti-spam software solutions.[18] Variations of spam are developing on different platforms such as spim (spam through instant messaging) and spit (spam associated with Internet telephony). The common thread linking these different platforms is that they have minimal or no marginal costs to sending messages in bulk. Spam is developing from a problem mainly affecting e-mail to attacks on instant messaging, Short Message Service (SMS) text-messaging, blog comments, chat forums, news groups, online games and wikis, with ever-greater costs to users.

Cases of what is called "pump-and-dump" spam and related scams are also increasing: the criminal buys cheap shares in a small company, and creates an interest in the company by sending out spam messages. As a result, the value of the shares rise and the spammer can sell the shares they have acquired at a profit. If undertaken through a real stock exchange, this is an illegal activity with serious consequences; however, in the online world, it is likely that the spammer can get away scot-free without any penalty. The rise of spam still seems to continue unabated and is mutating into more sophisticated threats, often with organized criminal intent. Box 5.1 lists some of the threats in cyberspace and why these deserve increased attention by all stakeholders.

5.2.3 Constantly evolving cyber-threats

We are witnessing a shift in the nature of cyber-security threats with attacks becoming more targeted and sophisticated, using increasingly innovative intrusion methods. Spam is the main vehicle for delivering viruses hijacking millions of computers or launching phishing attacks to capture private financial information. While users are familiar with the time and effort needed to delete spam from e-mail inboxes, the new and emerging threats that spam carries are still quite unknown to the average user. This section reviews some of the more common cyber-threats, their growth and development.

Some users may be sadly all too familiar with the danger posed by viruses and worms to PCs, hard drives and/or files. Viruses and worms can be amusing, annoying or downright dangerous. With connection to the Internet, their transmission by e-mail can multiply their impact many times through a chain reaction branching process. Contrary to previous large-scale virus attacks, where the idea was to attack as many computers as possible, virus attacks are becoming more focused and now rarely occur in a single, large outbreak, to avoid detection.

In Singapore in 2006, over half of all home Internet users experienced a virus attack, with nearly a third of all users incurring a loss as a result. A further fifth of all users had experienced a virus attack, but had not incurred any losses (Figure 5.2). In Brazil, over half of all firms with access to the Internet experienced a virus attack in 2006 (Figure 5.3, left). Viruses were most widely guarded against, with over three-quarters of home users using software to check for viruses (a similar proportion of nearly 70 per cent of household users installing anti-virus software was observed in Brazil, far in excess of the 20 per cent using firewalls or anti-spyware protection). Alarmingly, a fifth of all Singaporean home Internet users did not know about firewalls or anti-spyware. Among all those who had used a home computer but had not installed anti-virus software, 41 per cent were unaware of any need to protect against viruses, while 28 per cent cited the cost of software as being prohibitive. This suggests that consumer awareness is an important issue, with affordable protection the next biggest factor.

Spam often acts as a platform for other scams, with malicious e-mails able recruit your PC to play a role in the activities of a botnet. Botnets are networks of compromised personal computers that can retrieve information such as passwords, credit card numbers, and other personal data stored in the web-browser's auto-fill databases. Botnets are increasingly threatening the smooth functioning of the Internet. Vint Cerf, one of the original developers of TCP/IP, recently stated that up to a quarter of Internet-connected computers are virus-infected components in botnet networks of PCs under the control of hackers, comparing the spread of botnets to a disease that has reached "pandemic" proportions.[19] Large numbers of computers connected in botnets are needed to manage spam campaigns and denial of service attacks. At the 2007 World Economic Forum in Davos, Switzerland, experts in the area mentioned that, at one point, a botnet used about 15 per cent of Yahoo's search capacity.[20] There is also a trend towards smaller botnets, which are much more difficult to detect. In today's business and consumer computing paradigm, the botnet is an emerging tool for various malicious activities. Businesses and consumers are struggling with the best means of protection, and the benefits with implementing different proposed options.[21]

Traditional hacking, or unauthorized access to networked computers, has changed significantly in character over the past few years. Hackers are

Box 5.2: What is malware and what can it do to your PC?

Until recently, designing malware (malicious software) was a competitive form of expression for computer-savvy teenagers. Now, malware techniques are being adopted by organized crime as a goldmine. Malware is very powerful, with low costs and huge returns on investment. Malware, as we know it today, can easily and unknowingly be downloaded by e-mail or Internet websites. This malicious code (which is increasingly targeting mobile phones and portable devices as well as PCs) can install key-stroke logging programs and other software to steal personal information stored on, entered into, or received by these devices. This information, including passwords and other sensitive personal data, is then used in criminal activities, which are increasingly creative and difficult to detect.

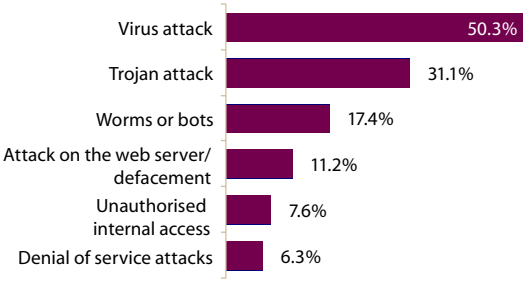
According to SophosLabs, the top five economies hosting web-based malware in 2006 were: the United States, People's Republic of China, Russian Federation, the Netherlands and Ukraine. "The US remains a hot spot for online criminal activity and despite authorities' continued efforts to clamp down on cybercrime, as too many US-hosted websites still have lax security measures in place", according to SophosLabs. "Given the effectiveness of web-based attacks, web-hosting companies in the United States and elsewhere need to step up their policing of published content and ensure that malicious code is quickly removed, before innocent users get hit." Sophos estimates that it sees approximately 5'000 new malicious URLs every day hosting malicious software or "drive-by" downloads of unwanted content.

While policy-makers around the world remain perplexed by this new type of criminal activity, the criminal gangs behind these frauds and scams are getting away with millions of dollars and euros. The stakeholders involved urgently need a better understanding of the impact of malware and how it is used. Only with full awareness of the risks involved can stakeholders take informed decisions on what action needs to be taken. The malware problem is not diminishing, but is constantly changing in character and addressing malware is no easy task, as cyberspace is an increasingly complex place.

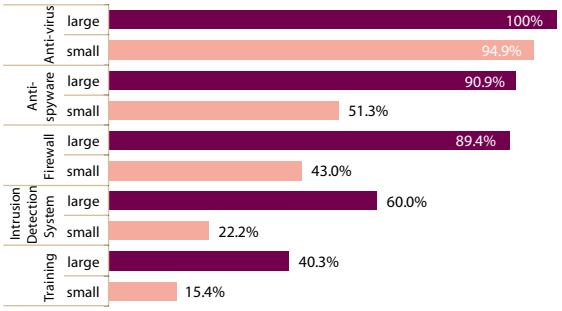
Source: For more information, see MessageLabs and Sophos websites.

Figure 5.3: Cyber attacks on firms in Brazil and action taken

Proportion of firms with Internet access in Brazil that had experienced different forms of cyber attack, 2006



Security measures to promote cybersecurity adopted by firms in Brazil with Internet access, 2006



Note: *'Small' firms comprise businesses of 10-19 employees; 'large' firms include businesses of 1'000+ employees.*

Source: Brazilian Survey on the Use of ICTs, 2005, available from ANATEL, the Brazilian regulator.

developing malicious code more quickly and are becoming more technically sophisticated in the way they circumvent network controls such as anti-virus software and firewalls. Their attacks are more targeted, affecting specific industries, organizations, groups, and people. As an example, denial of service attacks can seek to overwhelm a specific firm's e-mail systems with spam to force the company's system to collapse. Criminals have used attacks like this to blackmail firms into paying them to suspend the attack. Whereas the chance for infamy may have once motivated them, today's hackers often seek financial gain or revenge. Hackers are evolving into well-paid professionals, who can be hired to launch targeted attacks or sell people's private information. According to VeriSign, a US company with specific responsibility for the .com registrar, espionage is likely to prove one of the largest threats to networks in 2007, especially from insiders and direct competitors.[22] MessageLabs, a provider of integrated messaging and web security services, estimates that a key factor in the success of targeted attacks is the distribution of spyware and adware, which has grown into a multi-billion dollar industry and fuelled an increase in the number of botnets.[23]

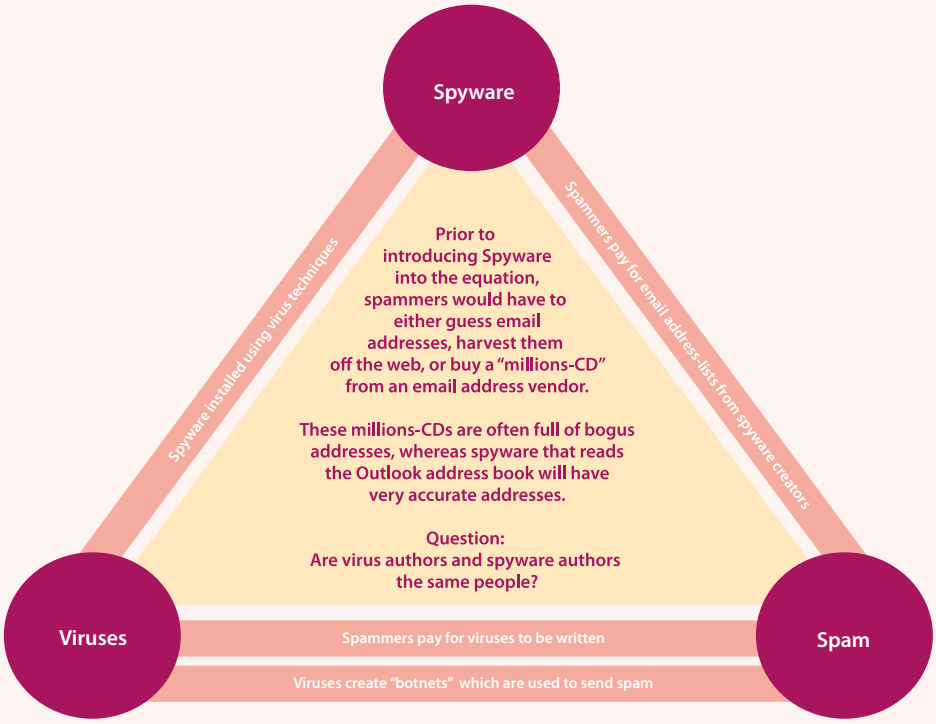
During 2006, there was a steady increase in the number of trojan spy programs designed to steal user data from players in online games and the evolution of trojans encrypting user data using professional encryption algorithms.[24] A trojan horse is a program that appears to have some useful or benign purpose, but really masks some hidden malicious code. Trojan horse programs can hijack a computer without the user's knowledge. In the worst-case scenario, e-mail-hosted spyware can monitor all transactions over the computer, view data stored on the "clipboard" or automatically saved passwords for computers, banks or credit cards, so criminals can take control of these and empty the bank account. Millions of connected computers worldwide are infected with trojan horse programs connecting them to botnets without the users' knowledge. In Brazil, nearly a third of all firms with Internet access had been subjected to a trojan attack in 2005 (Figure 5.2, left). Recently, media articles reported the case of a Russian criminal gang attacking a large Swedish bank using this approach. A trojan horse program, readily sold over the Internet, was used to extract more than USD 1 million from 250 customers of a Scandinavian financial institution.[25] The bank customers' details were stolen and used when they downloaded an attachment from an e-mail that appeared to have been sent from their bank.

Phishing[26] attacks, or false and misleading emails/ websites designed to persuade people to part with personal information and/or money, are also growing threats. An e-mail campaign, or single e-mail sent to many users, directs users to

Box 5.3: The cybercrime ecosystem – spyware, viruses and spam

The financially-motivated, multi-player cybercrime ecosystem is fuelling a rapidly-growing crime wave. Businesses and consumers are suffering financial losses, identity theft and other damages as a result of phishing using botnets and other kinds of threats involving spam, viruses, and spyware.

Box Figure 5.3: The cybercrime ecosystem



It might be described as a "vicious triangle": spammers pay for e-mail addresses and viruses from spyware creators. These viruses are in turn used to create botnets, which are then used to send spam. At the same time, spyware is installed onto "zombified" computers using viruses. Prior to spyware, spammers had to guess e-mail addresses, harvest them off the web or buy a "millions-CD" from e-mail address vendors. Millions-CDs used to be full of computer-generated bogus addresses, whereas spyware reading e-mail address now provides very accurate addresses. Spyware is evolving to become more targeted. Cyber-criminals can now harvest huge amounts of information on user communities. With the information gathered through spyware, it is possible to conduct spear-phishing attacks and gather further confidential business information. Criminals may potentially have access to more knowledge on home users' everyday Internet use than many well-resourced governments. Compromised computers can be used to track user behaviour, record passwords, conduct online purchases and other activities. Any number of applications can be installed on the same computer, each application potentially bundled with different forms of parasitic software so that, over time, the computer becomes overwhelmed by Internet baggage and its performance is severely affected.

Source: MessageLabs presentation; at: www.itu.int/osg/spu/presentations/2006/sunner-lap-cnsa-dec-2006.pdf, available April 2007.

a specific phishing or fraudulent website (multiple campaigns may point to the same web site). In January 2007, for the first time ever, e-mails containing phishing attacks outnumbered e-mails infected with viruses and trojan horse programs.[27] According to security-mail services vendor MessageLabs[28], in January 2007, one in every 93 e-mails (just over 1 per cent) contained some form of phishing attack, compared to one in 120 e-mails (0.8 per cent) that were infected with viruses. Security vendor Sophos[29] confirmed that it had seen more phishing than malicious-software activity/e-mails containing malicious attachments in January 2007. Botnets have been identified as a leading cause for phishing as a very serious form of spam.

Previously, viruses caused massive disruption and users were aware of online assaults. Now, however, targets of phishing attacks may have no knowledge that they have become victims. A carefully targeted phishing attack may go unnoticed for a long time during which the information-gathering continues.

5.2.4 Identity theft and the Internet

In today's business and consumer computing space, a financially-motivated, multi-player cybercrime ecosystem is fueling a rapidly-growing crime wave (Box 5.3). As a result of phishing, businesses and consumers are subject to potential financial losses, identity theft and other damages. The existence of, and interactions within, the botnet ecosystem makes phishing possible, along with its ensuing damage - in particular, the theft of personal or business critical information.

Identity theft is not new. By gaining access to people's personal data and impersonating them, a criminal can pursue a crime in near-anonymity. In the 21st century, with increasing reliance on electronic data and online identification, identity theft has never been easier. Law enforcement experts are concerned that online anonymity is making it more difficult to catch cyber-criminals. Anonymous use of mobile phones is still possible in some countries, using pre-paid cards. Anonymous access to the Internet is offered by service providers, Internet cafés and many wireless hotspots. A degree of anonymity is also facilitated by the use of dynamic rather than static Internet addressing, where addresses are allocated to users for the duration of a session, rather than on a permanent basis.

The Internet has opened the door to countless forms of dishonest but relatively harmless activities, but real criminals looked upon the Internet's shroud of anonymity and saw even greater opportunities. Until now, these criminals have been able to make the Internet a playground for their kind of people, including hackers, spammers and organized criminals. Stories of trojan horse programs stealing passwords, worms burrowing into people's hard drives, and spyware tracking an Internet user's every move barely raise eyebrows anymore. Not only do we accept them, we almost expect them. So, what can be done?

5.3 Towards an International Roadmap for Cybersecurity

5.3.1 Taking Action Against Spam and Related Threats

Spam is a public policy issue that is challenging governments, Internet Service Providers (ISPs), network operators, commercial e-mailers and consumers to work together in new ways, with each stakeholder group playing its part, to solve a problem that threatens the interests of all. But what has been happening in the area of fighting spam and related threats? On the current state of the battle against spam, Neil Schwartzman, Chair of the Canadian Coalition Against Unsolicited Commercial E-mail (CAUCE),[30] recently stated that "the development of spam-fighting is allowing computer-aware criminals to take the upper hand in the fight against what has now evolved into a completely technologically and organizationally merged threat to public safety. If we do not change our strategic approach immediately, the battle, indeed, even the war, may be all but lost".[31] The criminals always seem to be one step ahead in the fight against spam. However, user authentication could dramatically help in reducing spam, as it would require the e-mail sender to verify to the receiver that they are who they claim to be (the current Simple Mail Transfer Protocol (SMTP) "regulating" e-mails is relatively weak).

Work on identity management for activities on the Internet could therefore represent a step in the right direction. The ITU Telecommunication Standardization Sector (ITU-T) has recently established a Focus Group dedicated to identity management (IdM).[32] Its objective is to facilitate the development of a generic identity management framework through the participation of telecommunication and ICT experts. The use of multiple usernames and passwords offers great opportunities for hacking, identity theft and other forms of cybercrime, and is causing substantial financial losses. The ITU initiative on identity management aims to address this problem with a technology-neutral and platform-independent solution.

In today's interconnected networks, threats can originate anywhere, and therefore national, regional and international cooperation and action is needed to address cybersecurity-related threats. At the Tunis Phase of the WSIS[33], participants reaffirmed their commitment to deal effectively with the significant and growing problem posed by

spam. Numerous organizations, businesses, and partnerships worldwide are engaged in this fight; however, spam traffic volumes continue to grow. Consultations have taken place in many different forums over the past few years[34] and the need for a multi-pronged approach to fight spam and related threats has been widely agreed upon. However, prevention, consumer awareness, technical tools such as filtering techniques and national legislation are of only limited use in the absence of a comprehensive international framework.

Limited awareness of the numerous initiatives underway is a significant challenge in promoting international cooperation on countering spam. In December 2006, a meeting on the "Countering Spam Cooperation Agenda"[35] was held in conjunction with ITU WORLD TELECOM 2006[36] in Hong Kong (China). Organizations shared insights into the activities they are undertaking and explained what role their organization is playing in the fight against spam, to give policy-makers ideas for what an international framework countering spam could look like. In countries where legislation for cybersecurity and spam has been enacted and law enforcement procedures have been put in place, prosecutions, fines and prison sentences now apply for spam, creating a deterrent effect. Attitudes are also changing, as more people fall victim to the theft of personal information, identity and assets. The impact of cybercrime-related legislation and the critical role of law enforcement in preventing all different kinds of attacks in cyberspace should not be underestimated.

Overall, however, the anti-spam laws enacted to date around the world have been largely unsuccessful in eradicating spam.[37] In almost every instance, anti-spam statutes have focused on sanctioning spammers for their bad acts. An increasing number of countries and other jurisdictions have created such laws or applied to existing laws on data protection, consumer protection, and protection against fraud to fighting spam. Yet, in many cases, these laws have missed their target entirely, with no perceptible impact on actual spammers. Even worse, some laws have had negative side-effects in higher transaction costs, administrative costs, and restraints on legitimate senders of e-mail.[38] The persistence of the problem of spam has led policy-makers, technologists, academics and many others to come up with a wide range of possible strategies to end it. The least intrusive approach, most consistent with the end-to-end principle of network design, is to leave protection to end-users, through simple technologies, such as spam filters on e-mail clients. While this might be an option for developed countries, the lack of resources in developing economies would not support this kind of approach. An alternative mechanism, which has yet to be carried out in practice on a larger scale, involves enforceable codes of conduct. [39]

Enforceable Codes of Conduct – an alternative approach

Current anti-spam laws exist in around a quarter of countries worldwide[40], but have so far proven relatively ineffective. Enforceable codes of conduct could be used as part of a multi-pronged fight against spam to complement the relevant laws in place. Currently most anti-spam laws are directed at the spammers, not the ISPs that carry spam. On a practical basis, such laws require considerable investigative and enforcement resources – which can be problematic especially for developing countries. Even in developed countries, law enforcement agencies usually have higher priority issues to handle. To date, those promoting legal remedies for the fight against spam have tended to neglect investigation, enforcement powers or resources. And although most spammers and their clients can eventually be found, each investigation can be so time-intensive and costly that the costs often outweigh the benefits. For example, the United States Federal Trade Commission had only brought approximately 70 cases against spammers to court up to the end of 2006.

For developing countries with limited resources for such work, anti-spam laws may be rendered nearly meaningless due to the enforcement challenge. As spam is increasingly used to support fraudulent and criminal activities, different innovative approaches in the fight against spam could prove fruitful. National laws have been designed to address some of the related threats (described earlier in this Chapter), but no law can be , if it is not properly enforced. The move to enforceable codes of conduct offers an alternative approach that would need to be industry-driven. The private sector should first be given the opportunity to develop such codes of conduct. At the same time, it may be beneficial for governments to enforce these codes to ensure that all ISPs operate under the same rules. The ISPs that do not abide by these rules could be held accountable. Examples of such codes of conducts can be found through the Messaging Anti Abuse Working Group (MAAWG), albeit non-enforceable ones.[41] Australia and Italy, among other countries, have also carried out work on developing codes of conduct. Enforceable

codes of conduct could level the playing field in the fight against spam and related threats.

Winning the battle on increasingly sophisticated attacks

In January 2007, in a positive step forward for prosecutors in the fight against cybercrime, the first person was convicted in the United States for running a phishing scheme[42] under the US 2003 CAN-SPAM Act[43] (the federal anti-spam law). The sentence for this crime was set to 101 years in prison. The United States' anti-spam law forbids e-mail marketers from sending false or misleading messages and requires them to provide a way for people to opt out of future mailings. The man had compromised ISP accounts to send e-mails purporting to be from the company's billing department. The e-mails instructed customers to update their billing information on one of several web pages or lose their Internet service.

It is no surprise that phishing[44] succeeds in tricking its victims, as it is able to prey on both the ignorance of many users and their fears (e.g., by claiming that their account information has been compromised and the data should be resubmitted). Increasingly sophisticated, context-aware phishing is making scams more credible, and more successful.[45] To manage such security risks, organizations must examine network vulnerabilities and keep users informed. The Anti-Phishing Working Group (APWG) has been established as an industry association to track and report phishing attacks.[46]

Laws alone though will not make information and communication networks more secure. The problem of computer-related crime can only be solved when makers of computer equipment and technology build more secure systems and when the owners, operators and users on these systems operate in a more secure and responsible manner. The following section looks more closely at some of the other related measures that are being undertaken to build confidence and security in the use of ICTs and promote a global culture of cybersecurity.

5.3.2 Moving forward on a possible Roadmap for Cybersecurity

Today's ICT infrastructure makes it possible to perform illegal activities from almost anywhere in the world, at any time. Attacks are also crossing borders in complex and sometimes surprising ways. It is difficult for any single national or international approach to create trust in so many different infrastructure systems[47]: therefore, a coordinated and multi-layered approach is needed to protect critical network and information infrastructures.

A good way to create trust in global ICT networks is not to rely on a single line of defense, but instead on a set of overlapping defenses comprising national and international strategies, public and private efforts and multilateral and bilateral cooperation.[48] These defenses can help create trust, by giving users confidence that when an attack breaches one or more defenses, other means of protection will step into the gap and contain the attack, preventing the attackers from striking again. However, decision-makers are approaching this challenge from different angles. Depending on their priorities, national agencies and other stakeholders have tried to shape policies through at least four different perspectives:

- Addressing cybersecurity as a technical and operational network or IT issue;
- Looking at cybersecurity as an economic issue (e.g., maintaining business economic advantage, threat to business continuity);
- Focusing on cybersecurity as a legislation and enforcement issue (e.g., cybercrime);
- Concentrating on cybersecurity as a national security issue (e.g., CIIP and possible threats from other states).

An international roadmap for cybersecurity must address all these different perspectives. Through the WSIS process, a practical themed approach has been suggested to facilitate discussions and cooperative measures among governments, the private sector and other stakeholders. This approach includes looking at: information-sharing of national and regional approaches, good practices and guidelines; developing watch, warning and incident response capabilities; technical standards and industry solutions; harmonizing national legal approaches and international legal coordination; and privacy, data and consumer protection.[49] A roadmap, with all these different elements, would serve to engage the relevant actors in what are often seen as siloed communities (stakeholder groups that may not otherwise talk with each other), in order to enhance the opportunity for multi-stakeholder collaboration and partnerships in these domains.

5.3.3 Roles of the different stakeholders in cybersecurity

In a world of intertwined global networks, there is a need for coordinated and sustained approaches to protecting critical network and information infrastructures. Both critical network infrastructures and the attacks that threaten them take a wide range of forms which also cross borders in complex ways. Software written in India controls emergency gas leak repairs in the United Kingdom; an e-mail from Kenya might cross the Atlantic in route to Canada; and a hacker operating from an unidentified country might use computers in Russia and Brazil to attack an Israeli government site. No single national or international approach can create trust in so many different infrastructure systems.[50] All stakeholders have a role to play in the Information Society - and this also applies to cyber-related threats and security issues.

The role of governments

Ultimately, it is the responsibility of each government to ensure that its citizens are protected and, by doing so, to contribute to building a global culture of cybersecurity. Government strategy on information and network security has a major impact on the country's competitiveness. The state has a vital role in the coordination and implementation of national cybersecurity strategy. Currently, countries differ in their readiness to deal with cybersecurity policy issues and to develop a cybersecurity/CIIP strategy. Some countries have developed a comprehensive national strategy, while others are only just beginning to consider the issue.

As threats to cybersecurity are constantly evolving, cybersecurity policy must be flexible and adaptive. As there are many different stakeholders involved, the government needs to determine the roles of institutions and their related responsibilities to ensure cybersecurity at the national level. Typically, implementation of a national strategy requires coordination across many authorities, organizations and different government departments. Each government must determine the level of cybersecurity risk that it is willing to accept and expose its citizens and businesses to. As the different government stakeholders bring different perspectives to the problem, one of the first tasks is to evaluate national vulnerabilities and map these against the roles and responsibilities of the different government agencies. Some states have created a dedicated central organization to deal with the coordination for cybersecurity and CIIP-related issues across government agencies, such as Japan's National Information Security Centre (NISC).

Another important task for governments is the creation of new, or adaptation of existing, legislation to criminalize the misuse of ICTs. At the judicial level, governments need to enforce existing national legislation to curb abuses and protect consumers' rights. In its executive role, the government, with other stakeholders, is responsible for raising awareness on the threats involved, often through public education initiatives. Information on security risks and responses must also be shared with small firms, individual users, and other stakeholders.

To secure infrastructures effectively, national strategies must be matched with an international approach. The creation of frameworks for cooperation across jurisdictions, with the sharing of skills, knowledge, and experience, is vital for a secure online environment. The Council of Europe (CoE) Convention of Cybercrime[51] is one such framework in the area of international cybercrime legislation. The CoE Convention requires signatory parties "to co-operate to the widest extent possible" (Article 23), "to provide for the possibility for extradition for serious offences under Articles 2 to 11" (Article 24), "to provide mutual assistance to the widest extent possible" (Article 25), and "to set up a 24/7 Network" (Article 35),[52] to foster cooperation and collaboration. As mentioned earlier, legislation also requires effective enforcement. Besides direct bilateral cooperation between states, Interpol[53] has undertaken a number of activities to provide a unique range of essential services for the law enforcement community to optimize the impact of international effort to fight cyber-related crime.

The role of businesses and the private sector

As ICT infrastructure is often owned and operated by the private sector, their involvement in promoting a national and global culture of cybersecurity is vital. As hackers become more sophisticated, the time between discovering a vulnerability and developing the malicious code to exploit the weakness is shrinking. Early warning and rapid response is key to protecting business-critical assets. In many countries, the private sector is the first to assess and respond to the rapid technological changes and threats taking place. Large firms are generally more likely to take action than

small firms, as they tend to have greater resources at their disposal and may run greater risk with size (depending on the industry) (Figure 5.3, right). Industry also plays a critical role in agreeing on security standards in industry forums or standards development organizations.[54] Since effective cybersecurity requires an in-depth understanding of all aspects of information and communication networks, the private sector's expertise is crucial in the design of national cybersecurity strategies.

The role of users

The open nature of the Internet and the need for implementing security measures at the edges of the network (on individual computers and devices) make education of end-users is vital. Much remains in the hands of the users themselves, their activities and awareness of security, and how vulnerable they are to different threats.

Unfortunately, users are often unaware of the different threats and dangers in cyberspace and how to protect themselves. Communication systems are increasingly complex and individuals are asked to maintain and trust systems they do not fully understand. Users' lack of unawareness of the risks involved is one of the main reasons why critical infrastructures are increasingly vulnerable to attack (Box 5.3). As mentioned earlier, a large number of PCs are infected with viruses often unwittingly installed by the users themselves. As a result, there are now hundreds of thousands of PCs on broadband networks that have become part of zombie botnets controlled by criminal gangs, used to send spam or launch denial of service attacks. Due to the interconnectivity of modern ICTs, genuine security can only be promoted when users are aware of the existing dangers and threats. It is the responsibility of each user to become aware of the threats, as well as the opportunities, of the Internet. Governments and businesses must help users obtain information on how best to protect themselves.

5.3.4 Information-sharing - a common need

Sharing of information has been a key focus for both governments and private sector players over the past few years.[55] Governments, businesses and non-profit organizations are sharing information on security threats and best practice responses. To protect information infrastructure and fight cybercrime, countries must have systems in place for evaluating threats and preventing, responding to and recovering from cyber incidents. Networked Computer Emergency Response Team (CERT) centres are being established around the world to research modern techniques of cyber-intrusion and network security, security alerts, etc. and provide guidance and support.

Another approach adopted by some governments is the support of privately-funded information-sharing agencies. These agencies address everything, from overall network concerns to meeting sector-specific needs. One example is the United Kingdom's work on establishing Warning, Advice and Reporting Points (WARPs)[56] to establish an interdisciplinary network for the sharing of critical security information. In other countries, industry-specific information-sharing and analysis centres serve a similar purpose.

At the regional level, in 2005, the European Commission established the European Network and Information Security Agency (ENISA)[57] to coordinate national efforts on cybersecurity and to serve as an advisory unit to the Commission on information- and network security-related matters. International bodies including the OECD, ITU, APEC, the EU[58] and private sector and not-for-profit organizations are also working together to fight cybercrime.

5.3.5 Cybersecurity and developing economies and countries in transition

A globally interconnected information network makes it clear that cybersecurity cannot be effectively addressed by individual nations or even groups of industrialized countries as it requires a combined effort by government, industry, law enforcement, and citizens of all countries worldwide. Developing countries face unique challenges in developing security policies and approaches appropriate to their circumstances. In developing countries, ICTs also bring new challenges that need to be addressed in order to conduct electronic transactions securely and maintain the integrity of information systems and resources. Ensuring that developing nations reap the full benefits of the Internet to foster economic, political and social development involves assisting these countries (which make up the majority of the countries around the world) to address the challenges related to cybersecurity. As security is an important component of the policy framework for the Internet, developing countries need to: ensure that their laws cover cybercrime, develop

partnerships between government and the private sector to address cybersecurity, improve the sharing of information and raise security awareness among all users.[59]

Some important first steps in providing cybersecurity-related assistance to developing countries and countries in transition include awareness-raising, providing platforms for information-sharing and overall capacity-building in specific areas related to cybersecurity; setting up the necessary building blocks for a national strategy on cybersecurity; establishing a legal foundation and encouraging regulatory development; technical expertise in incident response, watch, warning, recovery, etc. In addition to these, the benefits of partnerships between industry and government in this area need to be explored in order to promote a culture of security involving all stakeholders.

Assistance on laws and legislation and enforcement

The overall development of cybersecurity strategies, information-sharing and outreach to the public is often encouraged when advising developing and emerging economies for enhancing national cybersecurity efforts. There are, however, many resources where developing countries can get immediate assistance in this area:

- To obtain support and assistance with drafting cybercrime statutes, examples of multilateral contacts that can be consulted include the Asia Pacific Economic Cooperation (APEC), the Organization of American States (OAS), the Council of Europe and ITU, as well as individual countries. Private critiques of draft cybercrime statutes can also be obtained from different stakeholders.
- For awareness-building (including for policy-makers), multilateral organizations such as APEC, Interpol, ITU, OAS and OECD, as well as individual states, can again provide good contacts.
- To obtain training for law enforcement in cybercrime, cyber-forensics and how to set up a cyber-investigation unit, interested parties can consult APEC, OAS, the G8 (to a limited extent) and Interpol, among other multilateral groups.
- In addition, developing countries themselves have valuable information to share with each other. The development banks (both global and regional institutions) and the private sector are expanding their activities in this area. There is also growing interest in routine formal training of law enforcement by companies, groups of companies, national trade associations, as well as interest by the private sector in talking to national policy-makers. It is important to remember that in cyberspace, any nation is only as secure as the least secure country.

5.4 WSIS Action Line C5: Building confidence and security in the use of ICTs

Fresh thinking and innovative solutions, together with solid commitment by governments and all stakeholders, are now needed to move forward to ensure global cybersecurity. The WSIS outcome documents[60] emphasize that building confidence and security in the use of ICTs is a vital foundation in building a safe and secure Information Society. The ITU has been appointed as the sole facilitator for WSIS Action Line C5, to assist stakeholders in building confidence and security in the use of ICTs. In this role, ITU is responsible for assisting stakeholders in the implementation process, at national, regional and international levels.

5.4.1 Action Line C5 Facilitation and Partnerships for Global Cybersecurity

The first Action Line C5 meeting was held in Geneva 15-16 May 2006, in conjunction with World Information Society Day on 17 May 2006. This meeting was dedicated to Promoting Global Cybersecurity. Three main focus areas were endorsed as the basis for future work programmes[61]:

- **Focus Area 1 -** National Strategies: The development of a generic model framework or toolkit that national policy-makers can use to develop and implement a national cybersecurity or CIIP programme.
- **Focus Area 2 -** Legal Frameworks: Capacity-building in the harmonization of cybercrime legislation, the Council of Europe's Convention on Cybercrime, and enforcement.
- **Focus Area 3 -** Watch, Warning and Incident Response: Information-sharing of best practices on developing watch, warning and incident response capabilities.

To stress the importance of the multi-stakeholder implementation, ITU has launched the Partnerships for Global Cybersecurity (PGC) initiative.[62] PGC is an open, multi-stakeholder platform that seeks to advise and share information with, and between, governments and other stakeholders on the different dimensions of building confidence and security in the use of ICTs. It aims to promote the use of ICTs to achieve the internationally-agreed development goals and to facilitate the implementation of WSIS Action Line C5, as well as providing a forum for policy dialogue and action.

The upcoming meeting for C5 facilitation in Geneva, Switzerland, on 14-15 May 2007[63], will assess the progress of worldwide initiatives to promote cybersecurity and seek ways to move forward in the five main themes[64] of: (1) information-sharing of national approaches, good practices and guidelines; (2) developing watch, warning and incident response capabilities; (3) technical standards and industry solutions; (4) harmonizing national legal approaches and international legal coordination; and (5) privacy, data and consumer protection. Specific attention will be given to activities in the Action Line C5 focus areas, as mentioned above.

ITU has also launched the Cybersecurity Gateway[65] as an easy-to-use online information resource on cybersecurity activities and initiatives worldwide. This gateway provides access to a vast number of resources. Organizations are invited to join in partnership with the ITU and other stakeholders to build confidence and security in the use of ICTs.

Specifically in the area of spam, the StopSpamAlliance[66] has been launched as a joint initiative to gather information and resources on countering spam. This initiative has been jointly launched by APEC, OECD, ITU, the European Union's Contact Network of Spam Authorities (CNSA), the London Action Plan, and the Seoul-Melbourne Anti-Spam group. The StopSpamAlliance.org website contains an overview on these organizations' activities in countering spam and related threats. In line with the *Tunis Agenda for the Information Society*[67], the StopSpamAlliance web pages link to initiatives in anti-spam legislation and enforcement activities, consumer and business education, best practices and international cooperation.

5.5 Conclusion –Towards a safer Information Society

Due to society's greater dependency on ICTs, the challenges related to creating a safe and secure networked environment are very real. ICTs are now indispensable in all areas of life: individuals, institutions, governments and firms around the world are investing in technologies, introducing security management procedures and launching campaigns to enhance network and information security. There are today more than four billion users of ICTs around the world, with increasingly powerful devices in terms of data storage, processing power and transmission capabilities. Technologies are also converging. Mobile phones are now becoming computers in their own right, offering greater opportunities for 'cross-infection' and damage.

5.5.1 Is the Information Society really at risk?

As the speed and connectivity of the devices used to commit cybercrime increase, the network itself has become vulnerable. The availability of information, the speed of information exchange and with the relative anonymity of online transactions complicates security vastly. The Information Society and business, based increasingly upon the digital economy, are in growing jeopardy. A growing number of security breaches have already incurred substantial financial losses and undermined user confidence.

Today, the Internet is largely anonymous - some argue that this core value of anonymity is one reason why the Internet has flourished. However, as cyber-threats become more disruptive and pose a serious menace, some wonder whether the Internet can remain anonymous, as we try to build a safe and secure Information Society? They claim that the drawbacks and negative aspects of anonymity are starting to outweigh the advantages. There are compelling reasons to authenticate and validate user names and addresses (e.g., for servers, domains, etc.) and to establish a more secure structure for the Internet. In contrast, proponents of anonymity for the Internet are quick to point out the virtues of anonymity in freedom of expression and the risks and costs of introducing strict identification and authentication in the networks.

5.5.2 How can we build a safe and secure Information Society?

For a normal citizen today, it is already difficult to keep personal computers secure from spam, spyware, viruses, phishing, let alone protect the personal data stored on the computer and other devices. Living in the digital world in 2015, users will be surrounded by pervasive devices, embedded sensors and systems, all connected to an IP-based network. Trust, privacy, and security are vital to the further development of the Information Society. Cybersecurity is a major consideration for the development of NGN[68], which will require increased international cooperation as well as the involvement of governments working on harmonized legislation and mutual enforcement.

An "updated" Internet (Web 2.0) could offer new and improved services with better security against viruses, worms, denial-of-service attacks and zombie computers. Other services requiring high levels of reliability (such as medical monitoring) and services that cannot tolerate network delays (such as voice and video-streaming) would be better supported in this new environment. However, the constant ebb and flow of technological change means that we cannot just rely on technological solutions: new issues are bound to surface. To provide these advanced services, both the architecture of the Internet and the business models through which the services are delivered, need to change.[69]

The benefits of the Information Society as a whole are at stake, if networks are insecure. As no single country or entity can create trust, confidence and security in the use of ICTs, international action is needed to address cybercrime. The protection of critical information infrastructures needs a joint effort by governments, industry, law enforcement and citizens worldwide. Time will tell if governments, businesses and citizens are willing to undertake this challenge. Encouraging each participant in the Information Society to become aware of the risks involved and assume responsibility for the security of information systems is one of the main challenges going forward. Building confidence and security in the use of ICTs requires a coordinated and focused effort from all stakeholders in the Information Society.

Annex to Chapter Five

Glossary

Adware – Advertising-supported software, or adware refers to any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.

Botnets/Bots – Botnets are networks of compromised personal computers that can retrieve information such as passwords, credit card numbers, and other personal data stored in the web-browser's auto-fill databases. The program is similar to worms in their propagation methods, but allows attackers to communicate with and control access to compromised machines. A Bot is a computer that has been broken into (compromised) and misappropriated by a criminal (2007 United States Contribution to ITU-D Study Group 1/Q22).

Blog – blog is short for "Web log"

Denial of Service (DoS) attack – Denial of Service is an attack on a computer or network meant to deny legitimate users access either to that computer or network. When the attack comes from multiple sources it is known as a Distributed Denial of Service (DDoS).

Malware – Malware is a general term for software code or program inserted into an information system in order to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners. Malware is a tool which facilitates a range of crimes. Compromised computers, like the malware installed on them, can become both components of the cyber attack system and the targets of attack.

Phishing – Phishing is a fraudulent attempt to trick an individual into revealing sensitive information such as bank account numbers, national insurance identification numbers, or user names and passwords. Spam is a primary vehicle for Phishing. An example would be an email that purports to be from one's bank but directing an individual to an illegitimate web site for the purposes of stealing that person's credentials.

Spam – Spam has multiple definitions that vary from one administration to another. For example, in some jurisdictions, it is unwanted, fraudulent email while in others it is simply unwanted email. An email message is determined to be spam either by a recipient, or his or her agent.

Spyware – Spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

Trojan horse – A trojan horse is a program that appears to have some useful or benign purpose, but really masks some hidden malicious code.

Url - A url is a universal resource locator. It is the address on the network of a given web page.

Viruses – A virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user.

Worms – A worms is a computer programe capable of self-propagation, sending copies of itself from computer to computer, through the exploitation of existing vulnerabilities or configuration flaws.

Notes for Chapter Five

1 Netcraft (www.netcraft.com) runs a monthly survey of websites. In April 2007, it registered some 113,658,468 sites, an increase of 3.2 million sites from the previous month's survey. Of these sites , around 50 million were "active" at the time of the survey. For more information, see: http://news.netcraft.com/archives/2007/04/02/april_2007_web_server_survey.html.

2 ITU Trust and Awareness Survey, March-May 2006; www.itu.int/newsarchive/press_releases/2006/09.html.

3 Melani security resources; www.melani.admin.ch/index.html?lang=en.

4 Information on WSIS Action Line C5 - Building confidence and security in the use of ICTs; www.itu.int/wsis/implementation/c5/ and www.itu.int/pgc/.

5 WSIS Tunis Commitment; www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|0.

6 WSIS Tunis Agenda on the Information Society www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

7 Michigan Online Security Training resources; www.michigan.gov/cybersecurity/0,1607,7-217--108238--,00.html.

8 Different terms are used in countries around to globe for criminal activity over the Internet, but cybercrime is the most widely used (cf. Council of Europe Cybercrime Convention).

9 Report by London's Metropolitan Police Service, 2007; www.mpa.gov.uk/committees/mpa/2007/070125/10.htm#fn001.

10 European Schoolnet coordinates the European Safer Internet network, Insafe (www.saferinternet.org), which aims to empower citizens to use the Internet. The results of the survey can be found here: www.saferinternet.org/ww/en/pub/insafe/news/insafe_survey.htm, December 2006.

11 Red Tape article on "Spam is back and worse than ever", 19 January 2007; http://redtape.msnbc.com/2007/01/spam_is_back_an.html.

12 United States' Federal Trade Commission; www.ftc.gov/.

13 Article in The Sydney Morning Herald, "2006: The year we were spammed a lot", 16 December 2006; www.smh.com.au/news/security/2006-the-year-we-were-spammed-a-lot/2006/12/18/1166290467781.html.

14 Spam as per the Anti-Spam Toolkit www.oecd.org/dataoecd/63/28/36494147.pdf.

15 Gartner Inc.; http://mediaproducts.gartner.com/webletter/blackspider/issue1/article3.html, 2004.

16 Brazilian survey on the Use of ICTs in Brazil, 2005, available from the Brazilian regulator, ANATEL.

17 Secure Computing; www.securecomputing.com/image_spam_WP.cfm and SPU Newslog; www.itu.int/newslog/.

18 Often, image spam is created using animated GIFs to bypass spam filters. Layering multiple images loaded one on top of another adds disturbances or "noise", which can complicate the message and make every message unique.

19 Interview for the WEF at Davos, 2007, available from: www.weforum.org/.

20 Article in The Register, "Botnet 'pandemic' threatens to strangle the net", 26 January 2007; www.theregister.co.uk/2007/01/26/botnet_threat/.

21 Paper on "Botnet threats and solutions – Phishing"; http://antiphishing.org/sponsors_technical_papers/trendMicro_Phishing.pdf, available April 2007.

22 VeriSign, "A Holistic Approach to Security", 2006, www.verisign.com/static/037640.pdf.

23 MessageLabs press release, 2006: the Year Spam Raised the game and Threats Got Personal, 13 December 2006.

24 Kaspersky Security Bulletin 2006, "Malware Evolution"; www.viruslist.com/en/analysis?pubid=204791924,.

25 Article in The New York Times, "Online Nordic Banking Theft Stirs Talk of Russian Hacker" by Andrew E. Kremer, 25 January 2007; www.nytimes.com/2007/01/25/technology/25hack.html?ex=1327381200&en=5699048fce2742b2&ei=5090&partner=rssuserland&emc=rss.

26 Phishing Guide from the United Kingdom's National Infrastructure Security Co-ordination Centre (NISCC); www.cpni.gov.uk/docs/phishing_guide.pdf.

27 CNET News article, "Phishing overtakes viruses and Trojans by Tom Espiner; "http://news.com.com/Phishing+overtakes+viruses+and+Trojans/2100-7349_3-6154716.html, January 2007.

28 MessageLabs resources; www.messagelabs.com/.

29 Sophos resources; www.sophos.com/.

30 Website for the Canadian CAUCE; www.cauce.ca/ and for links to all CAUCE globally; www.cauce.org.

31 Article in Spam Fighter blog, "Trench Warfare in the Age of Laser-Guided Missile .html", 26 December 2007 ; http://spamfighter666.blogspot.com/2006/12/trench-warfare-in-age-of-laser-guided.html.

32 The scope of the ITU-T Focus Group is Identity Management (IdM) for telecommunications/ICT in general; and specifically to facilitate and advance the development of a generic IdM framework and means of discovery of autonomous distributed identities and identity federations and implementations. IdM Focus Group website at: www.itu.int/ITU-T/studygroups/com17/fgidm/index.html, available April 2007.

33 WSIS main website; www.itu.int/wsis/.

34 ITU WSIS Thematic Meeting on Countering Spam, 2004, www.itu.int/osg/spu/spam/meeting7-9-04/index.html, ITU WSIS Thematic Meeting on Cybersecurity, 2005, www.itu.int/osg/spu/cybersecurity/2005/index.phtml, First Meeting for WSIS Action Line C5, 2006, www.itu.int/osg/spu/cybersecurity/2006/index.phtml, available April 2007.

35 StopSpam Alliance resources; www.stopspamalliance.org, available April 2007.

36 ITU Telecom World resources; www.itu.int/WORLD2006/forum/index.html, available April 2007.

37 WSIS Thematic Meeting on Countering Spam, July 2004, ITU Discussion Paper by Matthew Prince, "How to Craft an Effective Anti-Spam Law"; www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf, available April 2007.

38 Trends in Telecommunication Reform 2006 , Stemming the International Tide of Spam; www.itu.int/ITU-D/treg/publications/Chap%207_Trends_2006_E.pdf.

39 Trends in Telecommunication Reform 2006 , Stemming the International Tide of Spam; www.itu.int/ITU-D/treg/publications/Chap%207_Trends_2006_E.pdf,

40 ITU Survey on Anti-Spam Legislation Worldwide 2005; www.itu.int/osg/spu/spam/.

41 Messaging Anti Abuse Working Group, Code of Conduct, 2005; www.maawg.org/news/maawg050510,

42 Article in Mercury News; www.mercurynews.com/mld/mercurynews/news/breaking_news/16482522.htm,.

43 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act); http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf.

44 Phishing Guide from the United Kingdom's National Infrastructure Security Co-ordination Centre (NISCC); www.cpni.gov.uk/docs/phishing_guide.pdf, available April 2007.

45 Study on "Designing Ethical Phishing Experiments: A study of (ROT13) rOn", 2006, www2006.org/programme/files/pdf/3533.pdf, available April 2007.

46 Phishing Attack Trends Report, November 2006; http://antiphishing.org/reports/apwg_report_november_2006.pdf

47 ITU Background Paper on "International Coordination to Increase the Security of Critical Network Infrastructures", 2002; www.itu.int/osg/spu/ni/security/docs/cni.04.pdf, available April 2007.

48 ITU Background Paper on "International Coordination to Increase the Security of Critical Network Infrastructures", 2002; www.itu.int/osg/spu/ni/security/docs/cni.04.pdf, available April 2007.

49 See more details on the different themes in the Cybersecurity Gateway; www.itu.int/cybersecurity/.

50 ITU Background Paper on "International Coordination to Increase the Security of Critical Network Infrastructures", 2002; www.itu.int/osg/spu/ni/security/docs/cni.04.pdf.

51 Council of Europe (CoE) Convention on Cybercrime; www.coe.int/economiccrime.

52 Council of Europe (CoE) Convention on Cybercrime; www.coe.int/economiccrime.

53 Interpol resources; www.interpol.int/Public/TechnologyCrime/default.asp.

54 ITU-T Study Group 17 is the main ITU Study Group on telecommunication security and related standards activities; www.itu.int/ITU-T/studygroups/com17/index.asp.

55 Information on the benefits of information sharing; www.itu.int/cybersecurity/info_sharing.html,.

56 Warning, Advice and Reporting Points (WARPs) resources; www.warp.gov.uk/.

57 European Network and Information Security Agency (ENISA) resources; www.enisa.europa.eu/.

58 Information from the ENISA website on security-related activities taking place in the European Union; www.enisa.europa.eu/pages/01_01.htm.

59 ITU WSIS Thematic Meeting on Cybersecurity, Chairman's Report, 2005; www.itu.int/osg/spu/cybersecurity/chairmansreport.pdf.

60 WSIS outcome documents; www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2316|0.

61 2006 Chairman's report available at www.itu.int/osg/spu/cybersecurity/2006/chairmansreport.pdf.

62 Partnerships for Global Cybersecurity and WSIS Action Line C5 Facilitation; www.itu.int/pgc/.

63 Partnerships for Global Cybersecurity and the second meeting for WSIS Action Line C5 Facilitation; www.itu.int/pgc.

64 WSIS Thematic Meeting on Cybersecurity 2005 resources; www.itu.int/osg/spu/cybersecurity/2005/ .

65 ITU Cybersecurity Gateway; www.itu.int/cybersecurity/.

66 The StopSpamAlliance initiative; www.StopSpamAlliance.org.

67 Tunis Agenda for the Information Society; www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2316|0,.

68 ITU resources related to Next Generation Networks (NGNs); www.itu.int/ngn/.

69 Washington Post article, "Hold Off On Net Neutrality" by David Farber and Michael Katz, 19 January 2007; www.washingtonpost.com/wp-dyn/content/article/2007/01/18/AR2007011801508.html.