GSR 2010 Discussion Paper

10th Global Symposium for Regulators
10-12 November 2010
Dakar SENEGAL

Comments are welcome and should be sent by 30 November 2010 to GSR@itu.int

ITU

International Telecommunication Union

GSR 2010 Discussion Paper

The role of ICT regulation in addressing offenses in cyberspace

Work in progress, for discussion purposes

Please send your comments on this paper at: gsr@itu.int before 30 November 2010.

TABLE OF CONTENTS

1 THE ROLE OF ICT REGULATION IN ADDRESSING OFFENSES IN CYBERSPACE

Authors: Marco Gercke, Director and Tatiana Tropina, Researcher, Cybercrime Research Institute; and Christine Sund, Technical Officer and Youlia Lozanova, Regulatory Analyst, BDT/ITU

1.1 Foreword[1]

In many countries around the world, information and communication technology (ICT) in all its forms has become a critical driver for growth and innovation. Breakthroughs in the development of ICTs and the innovative use of these technologies and applications play a pivotal role in helping governments respond to a number of unprecedented challenges, ranging from improving healthcare and education to addressing climate change to dealing with natural disasters. In this regard it is necessary to highlight that in many ways, societies have become highly dependent on ICTs. With the growth in the number of private users and businesses relying on ICTs for the functioning of their everyday lives, ICTs should be seen as a critical part of national infrastructures. This growing dependence on ICTs represents a major potential vulnerability as even brief interruptions to ICT-based services can cause significant economic or social damage. As a result, as countries' reliance on ICTs increases, there is a growing awareness that cybersecurity and the fight against cybercrime must be taken more seriously. Given the link between ICTs and political, social, and economic growth, cybersecurity and cybercrime are now being considered as an important element in national development agendas. Drawing on the experiences of both developed and developing countries, this discussion paper underlines some of the major challenges and considerations.

Many countries are currently in the process of developing legal and regulatory frameworks for cybersecurity, including legislative frameworks for addressing cybercrime. Because of its nature, addressing cybercrime challenges traditional regulatory approaches and criminal law paradigms. Cybercrime and offenses in cyberspace traverse national borders and impacts multiple sectors and industries. Its crime scenes are in the virtual world and evidence is typically electronic rather than physical in nature. The "neighborhood" where cybercrime occurs is the global network and thus it is – just like in the real world – impossible to contain or to monitor at all times. The diffuse and global nature of the Internet implies that many, including international stakeholders must be involved in coordinated responses to cybersecurity and cybercrime as criminals are able to exploit vulnerabilities in one area to attack users in many other places. Moreover, because cybercrime stems from the use of evolving technologies, those charged with policing cybercrime must be nimble enough to keep pace with a rapid element of change.

In this context, traditional centralized models of regulation – with the government at the top of hierarchical decision-making structures – might not be the only solution for responding to cybercrime since modern global digital networks have evolved beyond direct governmental influence. The Internet has eroded old models of division of responsibilities between government, private sector and civil society. In this regard, the Internet requires the fight against cybercrime to be based on multi-stakeholder involvement. This raises new issues and concerns with regard to the roles and responsibilities of various actors. Moreover, due to the international nature of offenses in cyberspace there is a pressing need for international harmonization of law, standards, and protocols and for cross-border cooperation in investigating and prosecuting cybercrimes. At a domestic level, policy makers and regulators from different sectors must coordinate their activities, while legislators must work to close loopholes in existing national legislation that facilitate cybercrime. The tools and actions required to respond effectively to cyberthreats and to address cybercrime are evolving and must be assessed within a wider context of national and in-

ternational cross-sector approaches and collaborative arrangements.

The urgent need to criminalize the misuse of ICTs goes hand-in-hand with another trend – namely, the ongoing transformation of the traditional role of ICT regulators. Due to convergence and the rapid evolution of ICTs, ICT regulators must now strive to address factors that impede ICT development and undermine consumer trust while creating an enabling environment for investment, fostering market growth, and ensuring digital inclusion for all. As a result, many ICT regulatory authorities have found themselves involved in a range of activities related to tackling offenses in cyberspace. In some cases, these activities involve new duties and responsibilities, while other activities are direct expansions of normal tasks of the ICT regulator. From this point of view, fighting cybercrime can be seen as a part of the broader trend of moving from strictly centralized models of regulation towards more flexible and non-hierarchical structures.

1.1.1 Purpose, scope and value of the paper

Maintaining cybersecurity and responding effectively to cybercrime requires cooperation and coordination among a wide variety of stakeholders both within and between countries. In light of the importance of the ICT sector and the threats posed by cybercrime, this paper seeks to develop an understanding of the nature of the cybercrime ecosystem and to consider how the mandates of ICT regulators are changing accordingly[2].

The involvement of regulatory authorities in the fight against cybercrime is a relatively new trend, which is one of the reasons there is a basic lack of research on the issue. This paper seeks to contribute to filling that gap and to facilitate the discussion on the evolving roles of ICT regulators in addressing offenses in cyberspace. It provides ICT regulators and other interested parties with examples of how regulators around the world are becoming involved in addressing cybercrime, together with some practical suggestions for how regulators may address the challenges associated with this changing mandate. The growth in cybercrime globally is raising a number of challenges for regulatory frameworks that these frameworks were not initially intended to address. It is hoped that the ideas presented through this paper will assist countries in better understanding what steps need to be taken to put in place the necessary regulations to effectively respond to these offenses. These steps include ensuring that a system of policies, laws and other resources are in place that criminalize the misuse of ICTs and to investigate, prosecute, and punish offenders.

To provide context for the discussion, the first part of this paper (**Sections 1.2 and 1.3**) provides an overview of the cyberthreat environment, gives a general introduction to cybercrime threats and challenges, and explains their relevance for ICT regulation. **Section 1.4** discusses the cybercrime ecosystem with a view to exploring the roles that different stakeholders have in fighting cybercrime and the position of the ICT regulator in this multi-stakeholder environment. **Section 1.5** outlines some regulatory approaches and tools to addressing cybercrime. **Section 1.6** explores in greater detail the roles that the ICT regulator may play and the contributions that the ICT regulator may make in the fight against cybercrime both at present and going forward. **Section 1.7** concludes.

1.2 *Introduction to cybersecurity, cyberthreats and cybercrime*[3]

1.2.1 What constitute cybersecurity and cybercrime?

The term "cybersecurity" refers to various activities such as the collection of tools, policies, security safeguards, guidelines, risk management approaches, training, best practices, and technologies that can be used to protect the cyber environment and the assets of organizations and users. These assets include connected computing devices, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity initiatives aim to protect the security of the assets of organizations and users against relevant security risks in the cyber environment.[4] The growing number of initiatives launched by international organizations, national governments, and industry players is a sign of the importance of cybersecurity. Today enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer for both service providers and users has become integral to the development of new services as well as government policy.[5]

With countries' growing reliance on ICTs, cybersecurity has risen to the top of some countries' development agendas. This trend goes far beyond the usage and reliance of private users and businesses. ICTs are increasingly used to manage critical national information and networks. The growing dependence on ICTs

makes critical infrastructures more vulnerable to attacks, as even short interruptions to services can cause significant damage. For instance, in 2004, when the "Sasser" computer worm affected computers running versions of Microsoft's operating system Windows, US-based Delta Airlines had to cancel several trans-Atlantic flights because its computer systems had been swamped due to the worm; the same worm also disabled electronic mapping services of the British Coastguard for a few hours.[6] The result of the first analysis of the Stuxnet computer worm, which was discovered in 2010, highlights that the impact on critical infrastructures may not only be a side effect of the attacks but the key function of certain types of malicious software.

Cybersecurity is not only an issue for industrialized nations that rely heavily on ICT infrastructure. It is an important issue for developing countries. There is a common misconception that developing countries have too many basic "bread and butter" problems[7] to worry about (e.g., food and water supply, fighting traditional crime, poverty reduction, etc.), and thus do not need to attend to building a culture of cybersecurity or implementing cybercrime legislation. Yet, the lack of appropriate regulation in the area of cybersecurity and cybercrime can hinder these countries from reaching fundamental development goals and risks opening a new gap between developed and developing countries and creating what could be termed as "the cybersecurity divide". This potential gap can deepen the digital divide, undermine other efforts put in place to facilitate economic and social development, and, as a result, open a new schism "between (the) haves and have nots".[8]

Deploying ICT infrastructure and establishing an access point to global telecommunications networks should be accompanied by measures to make these networks secure, resilient, and robust. In addition, promoting awareness amongst consumers about the threats that accompany the use of ICTs[9] and developing appropriate legislation are necessary components of ICT infrastructure and services rollout. Developing countries need to address the call for international solutions to fight cybercrime. Unless this is considered in conjunction with the deployment of new technologies, developing countries might find themselves confronting the problem of being safe havens for cybercriminals and unable to protect Internet users within their territory, in addition to dealing with 'bread and butter' problems. Putting in place the necessary framework to take action against cyberthreats includes ensuring that a country has policies, laws, and other resources in place to criminalize the misuse of ICTs, as well as to investigate, prosecute, and punish offenders.

Once a country is connected to the global network, it is likely that the users become targets for cybercrime and the network's vulnerability increases as a result. This is an additional reason for developing countries to attend to the issue of cybersecurity, particularly since many such countries have focused on the deployment of advanced technical solutions such as of wireless networks. Although wireless networks enable the implementation of affordable ICT solutions, using relatively cheap technology and without huge infrastructure investments,[10] they are also considered generally more vulnerable to attack than wired networks. In addition, the vulnerability of developing countries is heightened by the absence of legal and regulatory frameworks to combat cybercrime; the lack of an inherent culture of cybersecurity and awareness among individual users and businesses; and inadequate financial, technical and human resources. Ultimately, in light of the interconnectedness of ICT networks, the vulnerability of developing countries in this regard represents a global concern.[11]

Although the term 'cybercrime' is used to discuss the issue of cybersecurity in the broader context, a clear line between cybersecurity and cybercrime can be drawn. 'Cybercrime' is often defined as criminal acts committed within computer networks, by the means of computer networks, or against them,[12] while the term 'cybersecurity' refers to as a complex set of measures, tools, policies and concepts to prevent cybercrime and related offenses. Deterring and preventing cybercrime can thereby be seen as an integral part of a cybersecurity and critical information infrastructure protection strategy. However, analysis of cybercrime focuses the investigation and criminalization of certain offenses, as well as their prevention and deterrence, while cybersecurity includes topics that extend beyond merely fighting cybercrime. Moreover, cybersecurity deals with the organizational, technical and procedural aspects of protecting the integrity of ICT networks against attacks, such as developing less vulnerable technologies.[13]

The legal, technical and institutional challenges posed by threats to cybersecurity and cybercrime are global and far-reaching and can only be addressed through a coherent strategy. In this regard, the ITU Secretary-General launched the Global Cybersecurity Agenda (GCA)[14] on 17 May 2007, alongside partners from governments, industry, regional and international organizations, and academic and research institutions. The GCA establishes a global framework for dialogue

and international cooperation with seven main strategic goals[15], built on five work areas:

- "Legal measures" focuses on how to address the legislative challenges posed by criminal activities committed over ICT networks in an internationally compatible manner.
- "Technical and Procedural Measures" focuses on key measures to promote the adoption of enhanced approaches to improve security and risk management in cyberspace, including accreditation schemes, protocols, and standards.
- "Organizational Structures" focuses on the prevention, detection, response to and crisis management of cyberattacks, including the protection of critical information infrastructure systems.
- "Capacity Building" focuses on elaborating strategies for capacity-building mechanisms to raise awareness, transfer know-how, and boost cybersecurity on the national policy agenda.
- "International cooperation" focuses on international cooperation, dialogue, and coordination in dealing with cyberthreats.[16]

The GCA notes that the development of adequate legislation is an essential part of a cybersecurity strategy. This requires first of all the necessary substantive criminal law provisions to criminalize acts such as computer fraud, illegal access, data interference, and child pornography.[17] The fact that provisions exist in a country's criminal code that are applicable to similar acts committed outside the network does not mean that such provisions can be applied to acts committed over the Internet.[18] Therefore, a thorough review and analysis of current national laws are vital to identifying any possible legislative gaps.

In addition to the need for appropriate substantive criminal law provisions, law enforcement agencies require the necessary tools and instruments to investigate cybercrime. Such investigations themselves present a number of challenges. Perpetrators can act from nearly any location in the world and take measures to mask their identity.[19] The tools and resources needed to investigate cybercrime are quite different from those used to investigate ordinary crimes. Furthermore, as an increasing number of cybercrimes have an international dimension,[20] the legal framework must therefore also facilitate international cooperation.[21] One of the key demands of investigators handling transnational investigations is an immediate reaction of their counterparts in the country where the offender is located.[22] Traditional instruments of mutual assistance do not, in most cases, meet the need for speedy action required by investigations dealing with the Internet.

Creating a criminal law framework for addressing cybercrime must be complemented by other measures. The ICT sector is highly decentralized, and responding effectively to cybercrime requires a decentralized approach. As a result of the shift from monopoly to competition, ICT infrastructure is owned and operated by a diverse group of service providers and private infrastructure owners. The interdependence between the providers of backbone services and the providers of dependent services is increasing. Moreover, peer-to-peer technologies allow millions of end-users of ICTs to become service providers in their own right allowing them to share music or any other files.[23] Centralized approaches to cybersecurity alone cannot be effective in such a decentralized network environment. An effective cybersecurity strategy therefore requires a comprehensive approach that includes engaging a variety of different stakeholders in the task of protecting and maintaining the integrity of global ICT networks.

Deterring cybercrime extends beyond the implementation of an appropriate criminal law and enforcement framework; it can include preventive measures, as well as self-regulatory and co-regulatory approaches. Although the adoption of appropriate legislation against the misuse of ICTs for criminal purposes is one of the most important prerequisites to building cybersecurity, at the national level, a cybersecurity strategy should be considered a shared responsibility among policy makers, regulators, the private sector, and citizens. There must be coordinated action related to preventing cybercrime and preparing for, responding to, and recovering from cybersecurity incidents.

The development and sustainable functioning of a country's ICT network in general implies that the ICT regulator has a central role to play with respect to cybersecurity. In many countries, Internet consumer safety and consumer protection[24] have already become an issue for the ICT regulator. Consumer protection, for example, has now broadened beyond quality of service issues to include protection from cybercrime.[25] Moreover, the end-users of ICT services are both targets for cybercriminals and simultaneously a security risk to the integrity of the network by acting as unwittingly entry points to the network for dissemination of malicious software, viruses, worms and the like. Indeed, end-users probably represent the principal security risk to the network.[26] ICT infrastructure and service providers

can safeguard most of the physical components of the network, but they cannot guard against the potentially destructive data and software placed on the network by end-users. ICT regulators are thus becoming increasingly involved with various activities associated with cybercrime, including investigation, enforcement, prevention and awareness raising.

1.3 Setting the scene[3]

1.3.1 Offences in cyberspace

There is no single definition of cybercrime[27] but there are certain categories of offences that are linked to it. Box 1.1 summarises the different categories of offences representing a growing concern for ICT regulators.

Box 1.1: Different types of cyber-offences

Illegal access
Illegal access is one of the most traditional offences, often associated with the term "hacking".[28] One example of such an offence is the circumvention of a password requirement or other protection mechanism in order to access a system or data, without authorisation. Following the development of computer networks, this crime has become a mass phenomenon.[29]

Data espionage
Data espionage refers to the act of obtaining data without authorisation. As sensitive information is often stored in computer systems that are connected to networks, offenders can try to access this information remotely. As a consequence, the Internet is increasingly used to obtain trade secrets.[30]

Illegal interception
With the increasing use of email in general and the use of wireless Internet access, often non-secured and un-encrypted, the opportunities for illegal interception multiply.

Data interference
Data interference, like illegal access, involves attempts to destroy or alter data by inserting malware such as viruses or worms, and is among the more traditional cybercrimes. Offenders can manipulate data to create backdoors through which a computer can be accessed or controlled from outside or install spyware or key loggers, which record the keystrokes of users, and send this information to criminals.

System interference
As with computer data, computer systems can be manipulated. The insertion of malware, as one type of system interference, can affect the functioning of a computer system. Another example is a denial-of-service attack, where a massive number of requests or "hits" are sent to a computer system in order to hinder its operation. Such attacks can be committed through powerful distributed botnets.[31]

Fraud and computer-related fraud
Fraud and computer-related fraud constitute typical offences related to cybercrime. Credit card fraud, advance fee fraud, Internet marketing and retail fraud and auction fraud involving electronic auctions platforms over the Internet are just some examples of fraudulent means of using the Internet and other technology.

Illegal content
The activities of criminals in disseminating illegal content range from making available child pornography and hate speech, to running illegal gambling websites. The dissemination of illegal content such as instructions on how to make explosions or organize terrorist attacks is also a serious concern.

Spam
Spam refers to the emission of unsolicited bulk messages. Today, e-mail provider organizations report that as much as 85 to 90 per cent of all e-mails are spam.[32]

Copyright violations
Copyright violations have moved online to sharing systems like peer-to-peer-based networks providing direct connectivity between participants in networks instead of communicating over conventional centralized server-based structures. This enables users to share files and data, often with millions of other users. File-sharing systems can be used to exchange any kind of computer data, including photos, music, movies, software, and even sensitive personal documents.[33]

Identity-related crimes
While most thieves still obtain personal information through traditional rather than electronic channels[34], this type of offence represents a growing concern as more data, services, and transactions are moved to global networks.

All the crimes outlined above either target end-users or represent a threat to the normal functioning of ICT networks. Some of these offences such as fraud, scams, spam, illegal or harmful content, especially content related to child pornography, are recognised as being Internet security concerns for consumers. [35] Although many ICT regulators have responsibility for consumer protection, they often do not have sufficient powers and resources to address these types of concerns, many of which are treated primarily as criminal law, rather than regulatory, matters. Some of the crimes also fall within the jurisdiction of other national regulatory bodies such as data protection agencies. When various agencies have overlapping mandates related to a certain type of crime, then these agencies must work together to coordinate their activities with respect to the crime. For example, in the Netherlands, the ICT regulator OPTA cooperates with the Data Protection Authority on the issue of addressing spam.[36]

The impact of various cyber crimes is different for developed and developing countries. For instance, in developed countries, spam is not only a nuisance but also poses a risk due to the malware and harmful content it can contain; spam also poses a threat to users' privacy and to the security of users' personal identities through phishing and the like.[37] Developing countries face these same spam-related issues. However, in developing countries, spam represents a major problem for the general functioning and use of ICT networks, as it constitutes a heavy drain on resources that are scarcer and costlier in developing countries than elsewhere.[38] Due to the limited availability of Internet resources, many users in developing countries rely on free, web-based email services with generous storage limits, which are particularly targeted by spammers. The cost of receiving and deleting spam over low-speed lines, for which charges often accrue on a minute by minute basis, also represents a significant cost for the users in developing countries. In essence, this means that the growing level of spam has the same overall effect as a denial-of-service attack.[39] Moreover, because developing countries have less effective security measures and protection, computers on broadband networks are often compromised and hijacked to send spam and to perpetrate other undesirable activities. In some cases, the emails of entire networks are rejected ("blackholed") by recipients due to the failure of the networks to deal with these problems.[40] ICT regulators in a number of developed states have already become involved in addressing this problem at both the national and international levels. For stakeholders in developing countries, focused capacity building is still needed.

1.3.2 Challenges related to fighting cybercrime

There are unique challenges associated with investigating, prosecuting, and preventing cybercrime. Existing approaches to regulating the ICT sector and to policing criminal activity are not well-adapted to the particular nature of cybercrime. These existing approaches have been designed to address issues in the "real" world, as opposed to the virtual world, and are generally country-specific, as opposed to the borderless nature of the Internet. This section outlines the main challenges related to fighting cybercrime; strategies for addressing cybercrime must take into account these issues.

1.3.2.1 Number of users

The popularity of the Internet and its services is growing fast, with over 2 billion Internet users worldwide by the end of 2010.[41] In 2005, the number of Internet users in developing countries surpassed the number in industrial nations.[42] The rising number of Internet users poses a challenge for law enforcement agencies since there are literally millions of people who have the means and opportunity to perpetrate cybercrimes. Developing a suspect list for a particular cybercrime is thus very difficult given the potential number of individuals who could be involved. At present, it is difficult to automate the process of vetting suspects. Thus, investigating who may be involved in a cybercrime is a labour-intensive and time-consuming process.

The large number of Internet users who do not have a good understanding of how to protect themselves while on-line also poses a significant problem with respect to preventing cybercrime. This lack of understanding is exploited by criminals.[43] Those engaged in cybercrime prevention, consumer protection, and general awareness-raising, including ICT regulators, face the challenge of educating an ever-growing number of users.

1.3.2.2 Availability of tools and information

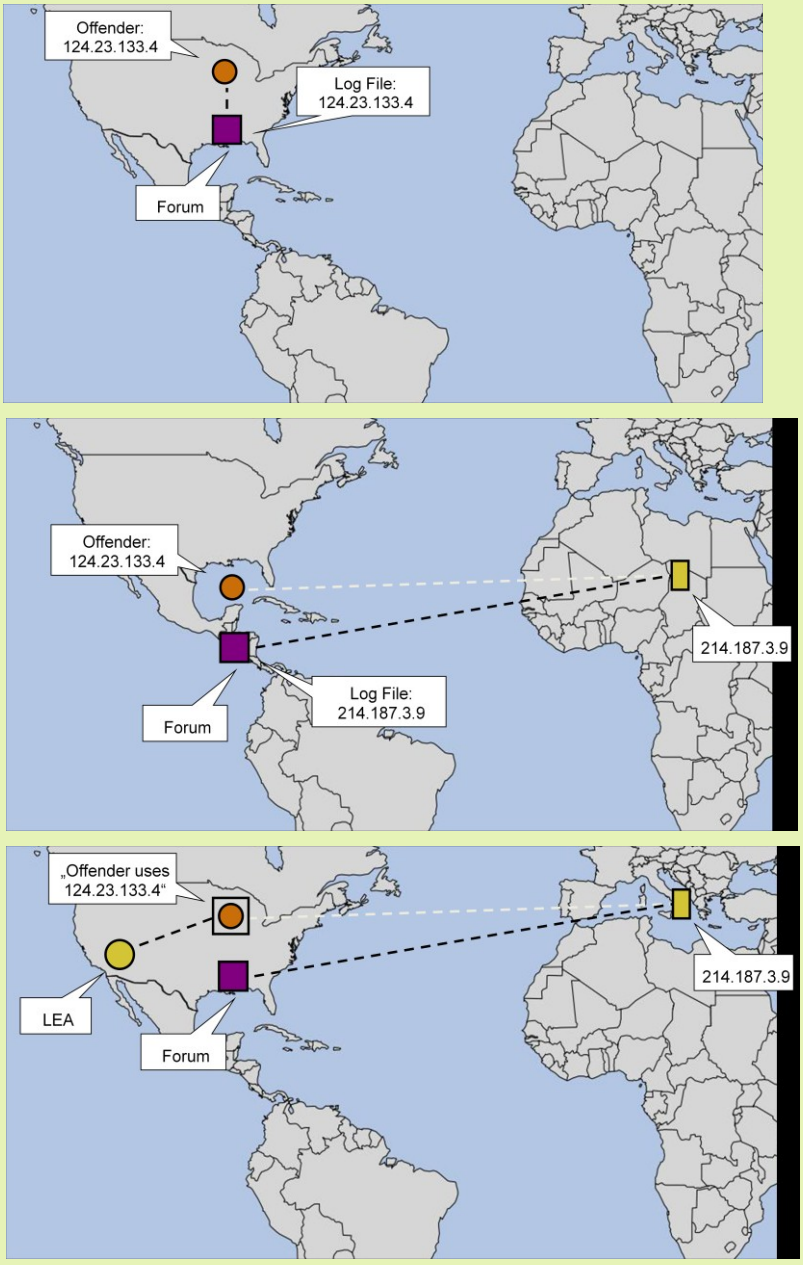
There are ample materials available on the Internet that provide guidance on how to commit various types of cybercrimes. Cyber criminals do not require in-depth technical knowledge; they are able to commit a range of cybercrimes by employing easy-to-use software devices and tools that are designed to locate open ports or break password protection.[44] This problem is compounded by the fact that it is difficult to contain the

availability of these devices and tools due to mirroring techniques and direct peer-to-peer exchanges.[45] Thus, virtually any computer user has access to the means necessary to commit cybercrime. Moreover, in addition to specific software, potential offenders can find a range of instructions on how to commit online as well as offline crimes on the Internet. "Googlehacking" or "Googledorks", for example, describes the use of complex search engine queries to filter many search results for information on computer security issues.[46]

1.3.2.3 Difficulties in tracing offenders

It is difficult for law enforcement agencies to identify offenders who use public Internet terminals or open wireless networks. Offenders may also hide their identities by using anonymous communication services.[47]

Figure 1.1: Difficulties in tracing offenders



In response to this challenge, some countries have put in place procedures and measures to restrict the free use of public Internet access points. These kinds of preventive measures illustrate how cybercrime can indirectly disrupt the facilitated availability of ICT technologies. This approach can be dangerous for countries, especially for developing states that are developing and promoting access to Internet technologies for consumers who do not have the opportunity to obtain Internet access in any other way but through public points such as cyber-cafes, Internet access points in libraries and schools, etc. The real challenge for ICT regulation is to find a balance between strict preventive measures availability and access to Internet services.

1.3.2.4 Missing mechanisms of control

As is often pointed out, the Internet was originally designed as a military information network[48] based on a decentralized network architecture designed to maintain functionality even when components of the network were attacked. As the Internet was not originally designed to facilitate criminal investigations or to prevent attacks from inside the network, undertaking investigations that require a centralized means of control poses unique challenges.[49] One example of the problems posed by the decentralized nature of the Internet is the ability of users to circumvent filter technology[50] by using encrypted anonymous communication services. Developing centralized mechanisms of control requires the cooperative participation of a range of stakeholders at the national, regional, and international levels in formulating cybersecurity strategy.

1.3.2.5 International dimension

Cybercrime often has an international dimension. One consequence of the protocols used for Internet data transfers that are based on optimal routing is the fact that many data transfer processes affect more than one country. Moreover, offenders do not necessarily need to be located in the same jurisdiction as their targets. (See Section 1.3.2.6, below). Where cybercrime crosses national borders, the related cybercrime investigations need the cooperation of law enforcement agencies in all of the affected countries since international law principles related to national sovereignty[51] do not permit investigations within the territory of other countries without the permission of local authorities.[52] However, the formal processes, requirements, and time needed to collaborate with foreign law enforcement agencies often hinder investigations[53] as cybercrime investigations tend to be very time-sensitive. As a consequence, offenders may deliberately include more than one country in their attacks to make investigation more difficult.[54]

The international dimension of cybercrime has implications for the strategies adopted by ICT regulators to promote cybersecurity. Where the regulator has responsibilities that relate to cybercrime, for example, policing spam, the regulator will face the same sort of challenges to effective enforcement experienced by law enforcement officials and intelligence agencies.[55] Government actors, whether the ICT regulator, law enforcement officials, or intelligence agencies, face the same critical issue: it is nearly impossible to ensure effective crime prevention within one country or one region due to the interconnectedness of networks.[56] ICT regulators must cooperate with agencies in other countries when investigating cybercrimes, and therefore will face the same challenges related to coordinating responses to cybercrimes and the consequent time delays as law enforcement officials and intelligence agencies.

The international nature of cybercrime also has implication for legislators. Governments must seek to harmonize national legislation, regulations, standards, and guidelines in order to create effective regional and international frameworks for fighting cybercrime. Cybercriminals often exploit inconsistencies in the legislative and regulatory approaches of different countries to avoid detection, prosecution, and conviction.

1.3.2.6 Independence of location and presence at the crime site

Another challenge for law enforcement agencies is that cybercriminals do not necessarily need to be present at the same location as the target. Offenders can therefore act from locations where there is a lack of effective cybercrime legislation or weak enforcement of such legislation, or both. Preventing “safe havens” is therefore one of the key goals when considering international approaches to fighting cybercrime.[57]

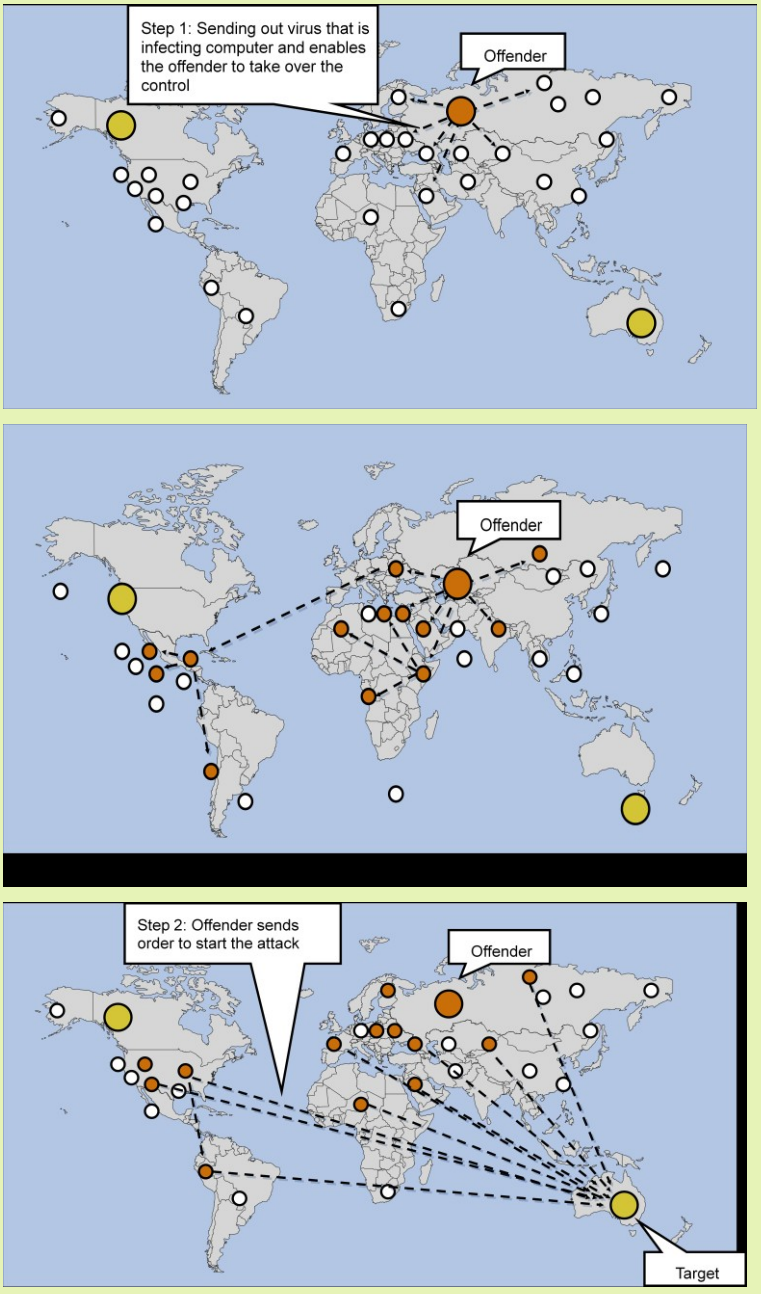
1.3.2.7 Automation and resources

Cybercrime offenders can often use automation to scale up their activities. As an example, many millions of bulk spam messages can be sent out using automated processes within a short time frame. Hacking attacks are also often automated,[58] with as many as 80 million hacking attacks occurring every day.[59] This is possible with the help of software tools that can attack

thousands of computer systems in hours. Offenders can make great profits by automating processes and designing scams that are based on a high number of offences with a relatively low loss for each victim.[60] However, it is not only the automation that causes difficulties in investigating and preventing cybercrime.

Offenders can use botnets to commit powerful attacks, such as the attack against computer systems in Estonia.[61] Analysis of the Estonian attack suggests that it was committed by thousands of computers within a "botnet" or group of compromised computers running programs under external control.[62] Over the past few years, botnets have become a serious risk to cybersecurity.[63] The size of a botnet can vary, from a few computers to more than a million computers working together.[64] The figures in Box 1.3 give an indication of how a botnet operates and the scale and power of the networked structure of an attack.

Figure 1.2: Example of a botnet attack



Botnets represent a threat for both network security and consumer protection. As such, botnets fall within the mandate of many ICT regulatory authorities.[65] ICT regulators thus need to be involved with developing regulatory instruments to fight botnets. Regulators should also endeavour to cooperate with the ICT industry to take down botnets and to raise consumer awareness about botnets, the risk posed by them, and measures that should be taken to guard against them. Raising consumer awareness in this context extends beyond mere consumer protection to encompass measures to ensure the overall security of ICT networks.

1.3.2.8 Encryption technology and innovation

Another factor that can complicate the investigation of cybercrime is encryption technology,[66] which protects information from being accessed by unauthorised people. Like anonymity, encryption is not new,[67] but computer technology has transformed the field. It is now possible to encrypt computer data with a simple click of the mouse or keyboard, making it difficult for law enforcement agencies to break the encryption and access the data. Offenders are already widely using encryption technology to mask their activities. Likewise, it has been reported that terrorists are also users of encryption technologies.[68] The availability of technologies designed to break encryption codes constitutes a key tool in the fight against cybercrime.[69]

The rapid pace of innovation in the ICT sector can result in gaps in the legislative and regulatory cybersecurity framework. The challenge for the legislator is the delay that exists between the recognition of new types of offences and the adoption of amendments to applicable legislation. Furthermore, as discussed above, this legislation cannot be drafted in isolation due to the cross-border and truly international nature of cybercrime. Participation in the process of regional and international harmonization of laws, regulations, standards, and guidelines must therefore be an ongoing activity.

The unique nature of cybercrime poses challenges that traditional approaches to preventing, investigating, and prosecuting crimes are not well-adapted to meet. Legislators, law enforcement agencies, ICT regulators, and other stakeholders must devise and deploy new approaches and tools to fight cybercrime while keeping an eye on adverse effects of ever more complex technologies (see Box 1.2).

Box 1.2: Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH)

Cybersecurity has become a major concern across the world. The number of attacks, the sophistication of the attackers, and the monetary damage have all been increasing at exponential rates for several years.

Rather than attempting to eliminate or mitigate the risks associated with today's IP-networks, an alternative approach may be to act at the root of the problem by rethinking computer systems we use today in order to make them more resilient in the face of cyber-attacks. This involves completely new ways of designing computer systems (both hardware and software) so that computers adopt the survival strategies of organisms and societies. The immune systems of higher organisms, for example, include "innate" elements that are fast and deadly, but deal with a fixed set of pathogens that are always in the environment. But they also include a second "adaptive" system that responds more slowly but can mount adaptive responses to novel pathogens. Moreover, these systems interact. Such biological systems invest enormous resources into self-defence at a level that any self-respecting computer designer would regard as untenable. But according to some analysts, the trade-offs for computers are today more like those for biological systems: resources are abundant and the lack of adaptive self-defence can be fatal.

As aggressive scaling takes micro-electronics to ever finer geometry, soon devices will not work like "ideal" and "perfect" switches but will rather begin to be unreliable. These "attacks from nature", transient errors, and high device failure rates, are different from cyber-attacks; cyber attacks are conscious attacks on specific targets that have value to the attacker. Thus if we are to continue to reap the benefits of Moore's law, we will have to begin to design processors to be resilient to device failure. In both cases the standard tools of self-adaptive computation will prove to be key: self-monitoring, diagnosis, and repair.

Source: Adapted from DAPRA paper on "Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH), June 2010, at:
www.darpa.mil/tcto/docs/DARPA_CRASH_BAA-10-70.pdf

1.4 The cybercrime ecosystem: An overview of roles and responsibilities[70]

Fighting cybercrime requires effective international cooperation and coordination on cyber-related issues in order to ensure that cybercrime policies are coordinated at the national level.[71] Moreover, an effective strategy to combat cybercrime requires a multi-stakeholder approach that is implemented at the national level. Efforts by national governments to establish policies and legal measures should be supported by the technical and economic expertise of the private sector and the readiness of civil society, and should be facilitated by the activities of intergovernmental and international organisations.[72] This section briefly discusses the cybercrime ecosystem and highlights the roles, responsibilities and activities of the main stakeholders in this field, as well as the tools to fight cybercrime. This discussion will provide a framework for further analysis of the role of the ICT regulator in combating cybercrime.

1.4.1 Cybercrime ecosystem

The cybercrime ecosystem is a multi-stakeholder environment where the tasks to be undertaken can be performed by different stakeholders or shared by two or more stakeholders. Naturally, some of the roles are determined by the authority and the power of the stakeholders. For instance, at the level of the state only a few actors can exercise the mandate of policy-making or law-making. However, with the rising importance of co-regulation and self-regulation, more and more players within industry are becoming involved in various processes related to regulating cyberspace and addressing cybercrime.

With regard to the regulation of different sectors and services that are affected by growing cybercrime, such as banking (including mBanking and eBanking) and telecommunications/ICTs, regulatory spheres can overlap (e.g., finance and mobile technologies). Countries often give multiple agencies overlapping mandates to deal with the same issue. For example, addressing spam may come under the jurisdiction of the ICT regulator, crime units, and/or data protection agencies. Critical information infrastructure protection is another example of an issue for which multiple agencies such as national security services, utility agencies and ICT regulators,[73] have overlapping responsibilities. In this case, not only is there a need for cooperation between the agencies, but different areas of regulation also overlap with international matters, thus creating the need for coordination with international and regional bodies.

In order to illustrate the interactions between the different stakeholders, the focus of analysis should be shifted to the functions that need to be executed rather than on the actors and the specific institutions involved. A networked model[74] could be applied to illustrate the truly cross-sector and multi-linked stakeholder ecosystem and to promote the concept of what should be done instead of who should do it (see Figure 1). In this regard, each country can determine which actor or institution is best suited to hold this responsibility in light of the country's specific circumstances and situation.

1.4.2 The role of the State (public sector)

"National governments" are typically identified as being among the principal stakeholders in fighting cybercrime because of their mandate to lead in the development of the national cybercrime and cybersecurity strategy and to distribute responsibilities and duties among the other stakeholders involved.[75] In this coordinating role, the government must ensure that there is a framework comprised of policies, laws, and other resources to protect the integrity of ICT networks and to investigate, prosecute, and punish cybercrimes. A 2007 Working Group on Internet Governance (WGIG) report highlights the role of the national government in addressing the issue of cross-border jurisdiction and in developing tools and mechanisms such as treaties and inter-agency cooperation to allow effective criminal investigation and prosecution of cybercrimes.[76]

While it is clear that there is a role for "national governments", it is necessary to consider what this term means in practice. "National governments" can refer to the government as a symbol of national sovereignty, the highest level of government institutions that deal with policy-making, or to different governmental institutions and agencies working in the area of policy implementation. Different states have different agencies involved with addressing cybercrime and these agencies also have different institutional designs. It is therefore difficult to define the role of the "national government" within the cybercrime ecosystem and to identify which institutions are associated with this role. Nevertheless, it is possible to distinguish between "high level policy making", where only a few government actors are involved in the decision-making processes, and "policy implementation", where a variety of different agencies may be involved.

The roles and duties of the national government in fighting cybercrime include:

At the high policy making level

- Conceptualize and develop cybercrime policy and establish a national cybercrime/cybersecurity strategy;
- Coordinate policies and strategies on broader ICT policies at the national level and coordinate efforts to fight cybercrime at the national level;
- Develop policy and coordinate efforts to fight cybercrime at the regional and international levels;
- Develop and adopt cybercrime laws and standards; and
- Take part in the process of international harmonisation of cybercrime laws (this task may be assigned to agencies at lower levels of authority when the mandate for enforcement has been determined).

At the policy implementation and institutional level

- Implement cybercrime policy;
- Coordinate cybercrime efforts at the regional and international levels for policy implementation;
- Identify gaps in national legislation (e.g., in criminal law statutes) and adopt measures to fill these gaps;
- Enforce cybercrime laws and regulation
- Build capacity among other stakeholders and build awareness of cybercrime-related issues and cybercrime prevention strategies;
- Foster international, regional and sub-regional cooperation;
- Develop mechanisms for collaboration with the private sector, for example, through public-private partnerships.

As policy- and law-maker, the national government at the high level has the authority to give priority to the problem of cybercrime. The government at the high level also delegates the authority that flows from its national sovereignty to a variety of ministries and agencies and equips these bodies, in addition to other stakeholders, with the necessary legal and regulatory measures to address cybercrime.

It is becoming extremely difficult for governments to prevent and prosecute cybercrime on their own.[77] With the rapid changes in ICT technologies and the ongoing developments in this sector, government cannot and should not be expected to compete with the private sector's expertise and resources.[78] Instead, government is increasingly engaging in partnerships with the private sector to fight cybercrime.[79] While governments dominate the process of establishing and enforcing legal provisions, particularly where the use of coercive power is necessary, non-governmental stakeholders that have practical experience in the ownership and operation of ICT infrastructure have valuable skills and knowledge to contribute.[80]

Due to the low reporting rates on cybercrime[81] and to a lack of resources, government authorities can do little more than investigate and prosecute a "tiny fraction"[82] of cybercrime. Accordingly, there is a growing emphasis on the importance of adopting proactive measures that seek to prevent cybercrime and to promote cybersecurity rather than relying on reactive measures that address cybercrime once it has already been committed (e.g., investigations and prosecutions). Preventive measures include technical measures that are aimed at protecting information systems and communications (e.g., encryption, electronic signatures and certificates, etc.), as well as efforts to foster understanding among users about cybercrime and current threats (e.g., awareness-raising campaigns, guidelines, alerts, etc.). The effective implementation of these types of proactive, preventative measures requires the engagement of non-governmental actors. Thus, while the national government must take the lead in the fight against cybercrime, the government cannot effectively protect ICT infrastructure and the users of ICT services without the involvement of non-governmental industry stakeholders and the general public.

1.4.3 The role of businesses and the private sector

Private actors have played a dominant role in driving innovation and in the overall development of the ICT sector. As owners and operators of the infrastructure itself, industry players have a key role in the fight against cybercrime. While government has the power to establish the legal and regulatory framework for addressing cybercrime, the private sector understands the changing and converging nature of the ICT environment and has greater adaptability to new technologies and their utilization. The competences and resources of the government and the private sector thus complement each other, creating a fruitful environment for voluntary collaboration.

An important contribution that can be made by private sector actors such as Internet Service Providers (ISPs) relates to monitoring of the Internet. The government does not have the capability and resources required to monitor the full volume of Internet communications and transactions taking place at all times; furthermore, the government is not in a position to collect and store all existing ICT-related data. ISPs and other sector actors are better placed to manage the monitoring of potential threats such as viruses and botnets and to store digital records of ICT-related data. Successful prosecutions of and convictions for cybercrimes depend on a combination of the monitoring and data management of ISPs and other sector actors[83] and the government's authority to enforce criminal law and regulatory provisions related to cybercrime. Recent cases, like Microsoft's initiative to shut down a botnet through court procedures[84], illustrate that sector actors are extremely interested in stopping criminal activities taking place online and are willing to cooperate with the government to do so.

Collaboration between government and industry can be pursued in the form of public-private partnerships that may be conducted either as operational cooperation for specific cases or as more long-term initiatives. For example, ongoing collaborative efforts could include joint initiatives to deliver training on cybersecurity and to monitor and block illegal content on the Internet; collaboration might also include setting up networks of contact points in both the private and the public sector.[85]

Collaboration between the state and sector actors requires that care be taken to avoid breaching the rights of private users. For example, efforts to monitor Internet communication to detect threats must be balanced with the privacy rights of users. The importance of cybersecurity cannot be used to circumvent the privacy rights that users have in their personal information and communications. Moreover, where the government seeks access to data held by sector actors such as ISPs, the government should be required to obtain a warrant for such data. Sector actors should also be aware that their collaboration with government may render them an agent of the state for criminal law purposes and that they may therefore be required to uphold the criminal procedural rights of their end-users, including, for example, the right to be free from unreasonable search and seizure.

The ICT sector can make an important contribution to cybersecurity by implementing forms of co-regulation and self-regulation.[86] Co-regulation involves regulation of industry by government and industry working together, while self-regulation involves industry regulating itself. Co-regulation represents a tougher approach to regulation since there is still a threat of enforcement; by contrast, self-regulation is based on voluntary commitments that industry players make due to industry self-interest (e.g., industry voluntary codes of practice) or brand self-interest (e.g., unilateral codes of conduct).[87] One example of co-regulation is the Australian Cybercrime Code of Practice that was developed as a result of joint efforts between the Information Industry Association (IIA) and the Australian Securities and Investments Commission (ASIC). The Cybercrime Code outlines procedures for interaction between Internet stakeholders, particularly ISPs, and law enforcement with regard to e-crime. It also sets base criteria for the retention of records.[88] The Cybercrime Code provides the private sector with a clear framework for collaboration both within industry and externally with law enforcement agencies.

There are a range of potential benefits that flow from collaboration between industry and the state. As a number of papers have noted, such cooperation, along with the development of co- and self-regulation, has the potential to deliver even better results than criminal law enforcement.[89] Moreover, self-regulation and co-regulation have become necessary complements to centralized regulation in light of the decentralised architecture of the Internet and its borderless nature. Centralized state intervention is readily frustrated since criminals can easily bypass traditional regulatory frameworks.[90] At the same time, over-regulation can hamper the development of ICT networks and the availability of ICTs. In this context, co-regulation and self-regulation offer sensible approaches to managing cybersecurity.

However, self-regulation and co-regulation have their limitations when it comes to deterring cybercrime. For instance, the enforcement by industry of codes of conduct for regulating child pornography cannot alone guarantee that the appropriate investigation of the crime and prosecution of offenders is undertaken. The protocols adopted by industry cannot completely prevent certain forms of cybercrime, such as the distribution of child pornography. Thus, a proper legal framework is necessary to prosecute offenders who are able to circumvent industry protocols. Nevertheless, the self-obligations adopted by the private sector can ensure that safe havens for cyber-criminals do not exist or emerge.

1.4.4 The role of civil society, academia and individual users

The various interests of civil society are usually represented by different groups performing a variety of functions. Consumer groups, trade associations, non-profit organizations, and mass media can play a key role in raising awareness about cybercrime and in helping citizens to understand that each person is an important part of a larger 'security chain'. These groups and organizations can also pressure the government to address cybercrime issues. Civil society already plays an important role in consumer protection campaigns and in promoting cybersecurity awareness, tools and practices.[91]

As a part of civil society, academia can also be an important player in addressing cybercrime. Both industry and government appreciate input and analytical studies on cybercrime-related topics from academic communities, especially with regards to projections for the future and 'over-the-horizon' perspectives.[92] Universities are also carrying out research in cybercrime and developing solutions based on new understandings and emerging technologies. For example, academic researchers have developed many key security algorithms used to encrypt confidential data exchange and online transactions. Universities are increasingly becoming involved in joint industry-academia-government partnerships for delivering training programs.[93] Independent experts from academia, such as university professors, can contribute to the harmonization of cybercrime legislation and can assist countries with implementing international standards.

Academic experts can also be involved in the activities of international organizations.[94] The ITU High-Level Expert Group on Cybersecurity is an example of a partnership between academia and international organizations. The ITU High-Level Expert Group on Cybersecurity included academia, research institutions and individual experts.[95] It was established as an advisory body to assist ITU's Secretary General in addressing concerns related to cybersecurity and cybercrime.

Cooperation with academia has become especially relevant in the area of critical information infrastructure protection. Some national Computer Incident Response Teams (CIRTs), Computer Emergency Response Teams (CERTs) or Computer Incident Response Teams (CSIRTs) are even established and run by academic institutions.[96]

The end-user is also a critical component in the cybercrime chain of actors. Many of the opportunities exploited by the criminals in cyberspace directly result from human error or a lack of understanding about the importance of protecting personal data. Since cybercriminals constantly develop sophisticated social engineering techniques and new kinds of malware, end users need to be aware of how to create the necessary level of individual security and how to keep this security up to date.[97] For individual users, prevention cannot be limited to technical protection alone. On the contrary, awareness campaigns should also focus on social engineering techniques and other means that cybercriminals use.[98]

1.4.5 The role of regional and international organizations

The trans-border character of cybercrime calls for counter-actions that are coordinated on different levels – national, regional, and global. Many international and regional organizations are already engaged in dealing with threats to cybersecurity and fighting cybercrime. This includes the following organizations: ITU, Council of Europe (CoE), INTERPOL, United Nations Office on Drugs and Crime (UNODC), G8 Group of States, Organization of American States (OAS), Asia Pacific Economic Cooperation (APEC), The African Union, The Arab League, The Organization for Economic Co-Operation and Development (OECD), The Commonwealth, European Union, Association of South East Asian Nations (ASEAN), North Atlantic Treaty Organization (NATO) and the Shanghai Cooperation Organization (SCO). More information on the specific activities of the various regional and international organizations active in this area can be found in ITU's publication Understanding Cybercrime: A Guide for Developing Countries[99].

1.5 Addressing cyberthreats: Understanding regulatory issues and available tools[1]

This section explores the regulatory issues raised by cyberthreats around the world today, as well as the tools that may be used to address those issues. As will be seen, the various stakeholders in the cybercrime ecosystem can make use of a range of tools to fight cybercrime. These tools can be administered under different policy and regulatory approaches, which will in turn determine the scope and nature of the tools.

The main regulatory issues involve adopting consistent and streamlined policies and regulations that in-

clude clear definitions, unambiguous division of responsibilities among government agencies involved in fighting cybercrime, and clear enforcement mechanisms. At the same time, however, regulators and policy-makers should be mindful to avoid excessive and disproportionate interventions in the market in order not to stifle market players and ultimately market growth. Moreover, an overly rigid legal and regulatory framework for addressing cyberthreats will be unable to adapt to new forms of cybercrime, thereby creating gaps that can be exploited by cybercriminals.

In an ideal world, all countries, regardless of the maturity of their markets, would adopt a full-fledged set of policies and regulations to ensure the highest level of protection against cyberthreats and cybercrime. However, in the non-ideal world in which we live, a host of difficulties, both political and practical in nature, prevent ICT markets from achieving a high level of cyberthreat readiness. This is especially true in developing countries, where policy-makers often consider that there are more pressing development issues to address before developing a framework for cybersecurity. Greater priority must be given to cybersecurity in these countries. Indeed, cybersecurity needs to be integrated in a holistic way as a fundamental component of a wider development strategy that includes using ICTs to promote positive development outcomes. The lack of human and institutional capacity and the lack of sufficient expertise in this highly specialized field may be a constraint in so doing, however. A detailed discussion of this matter is contained in Section 1.6.1.2 below.

One way to address the lack of adequate resources and expertise necessary for building an effective cybersecurity framework is to adopt a staggered or phased approach to addressing cyberthreats. Table 1.1 outlines various policy and policy implementation outcomes that may be adopted at various stages as a country's ability to respond to cybercrime matures. The proposed checklist of policy and policy implementation outcomes is neither exhaustive nor prescriptive, and should be regarded as an attempt to capture some of the specific regulatory issues related to forging a framework to address cybercrime.

1.5.1 Regulatory approaches

The high-level regulatory and policy approach adopted by a country to respond to cybercrime is typically based on a set of strategies and goals. These can be specific to cybersecurity and cybercrime or stem from broader national strategies and priorities, such as economic development and national security.

Current practices related to regulatory approaches to cybersecurity issues fall broadly into five categories, depending on the level of readiness (policy, regulatory, and institutional) of countries to address cyberthreats. These categories do not necessarily imply the adoption of a regulatory approach to cybersecurity; indeed, some categories are characterized by the lack of approach or overall strategy, while other can be described as pre-approaches or elements of a nascent approach:

- Laissez-faire (no framework, no specific policies or regulation in place such that country will address issues later on or when faced with concrete threat/crime); the majority of developing countries unfortunately fall into this category.
- Loose consensus (no legal text or related policies, no entity explicitly mandated by law to deal with cybercrime but some efforts deployed outside the regulatory framework); found in some developing countries.
- Elements of policy and regulatory framework in place (e.g., policy document or declaration, individual regulations on concrete topics), but no mechanisms for implementation; both developing and some developed countries follow this model;
- Policy and legal framework and implementation mechanisms in place, including an entity or entities with a mandate in this field; at least 44 countries, including a handful of developing countries, have adopted cybersecurity-related legislation or regulations and at least 53 countries had an entity or entities in charge of addressing cybersecurity issues, as of the end of 2009.[100] (See also the discussion in Section 1.5.2 below.)
- Sound and streamlined regulatory and legal framework in place complemented by effective enforcement; this is a moving target as cyberthreats continue to evolve; no countries have yet achieved this stage.

Although very few countries have applied streamlined regulatory approaches to cybercrime to date, it is clear that there are diverging visions with regard to the degree of regulatory intervention required.

Table 1.1: A phased approach to addressing regulatory issues related to cyberthreats

Phase 1	Phase 2	Phase 3
• Define cyberthreats. • Develop and adopt a national broadband strategy or ICT master plan, etc., incorporating and addressing cybercrime and setting broad cybersecurity goals. • Develop a national cybersecurity strategy that addresses in detail the broad cybersecurity goals identified in the national ICT plan. • Awareness raising among lead ICT users (government officials, public servants, educational institutions, organizations, small-and-medium sized enterprises, etc.), target user groups (youth, children), and the general public. • Review existing legislation to assess whether it is capable of holding people accountable for criminal/fraudulent activities conducted using ICTs. • Develop the necessary legislation to address gaps in the legislative and regulatory framework. • Develop an understanding of the different tasks and mechanisms required to address threats to cybersecurity. • Identify actors on the national level that can implement and maintain some of the required activities/functions. • Consider the possibility of establishing a national computer incident response team (CIRT).	• Create incentives for infrastructure and service providers to address cyberthreats and to collaborate with the regulator and other government agencies. • Pass more comprehensive legislation to criminalize harmful activity in cyberspace. • Develop and enforce technical regulations (i.e., setting security requirements for ISPs; adopting/transposing internationally agreed cybersecurity standards (ITU-T, ITSO, etc.) and work toward eventually integrating them into existing Quality of Service (QoS) standard requirements. • Train experts in the various aspects of cybercrime/cyberthreats and build institutional capacity (i.e., regulator, specialized agencies, etc.). • Develop an understanding of the mandates and practices of the various agencies in charge of cybercrime-related issues and how to facilitate coordination between entities. • Ensure that the national cybersecurity/cybercrime entities are linked to existing sub-regional, regional and global networks pertaining to cybersecurity and fighting cybercrime. • Ensure that national legal measures enable the cooperation between law enforcement agencies in different countries.	• Strengthen the incentives for infrastructure and service providers to prevent cybercrime and protect consumers. • Impose specific obligations (i.e., in licences, related to QoS or consumer protection) on infrastructure and service providers to address cyberthreats and collaborate with the regulator and other government agencies). • Develop an operational network for collaboration among government agencies in charge of cybersecurity, cybercrime, or specific aspects of cybersecurity (data protection, privacy, etc.) and all stakeholders. (See also Section 1.5.2.1.) • Develop or extend Internet content regulation focusing on, inter alia, illicit and offensive content, hatred and obscene speech, and protecting minors (including banning child pornography), etc. • Develop intellectual property rights (IPR) legislation and regulations. • Put in place effective mechanisms for assessing readiness of national infrastructure to withstand cyberthreats, prevention, early warning detection, etc. • Enhance mechanisms to investigate cybercrime (cyber forensics, etc.) and ensure enforcement mechanisms for penalizing cybercriminals.

Note: Some countries implement activities from different phases simultaneously.

Source: Authors.

An additional layer of complexity is added by the lack of international harmonization and the very different regulatory treatment of cybercrime in different national jurisdictions. In the event of cross-border incidents, the lack of a harmonized regulatory approach and/or the competition between national regulatory agencies seeking to impose their own approaches may pose serious obstacles to the prompt and concerted response by all concerned parties.

1.5.2 Tools for addressing cybercrime

As public access to and use of the Internet has grown, so has cybercrime and cybersecurity-related concerns. Policy-makers and regulators have responded to the growth of cybercrime and the need for more robust cybersecurity by reforming the legal frameworks governing the use of ICTs, by amending criminal law provisions, by introducing new legislation and regulations focused on cybercrime, or a combination of these types of reforms. Given the nature of cybercrime, reform of ICT legislation is increasingly coordinated with legislative reform that affects other sectors of the national economy. In some cases, more holistic approaches are taken that feature the adoption of legislation and regulations designed to apply across all sectors of the economy and throughout society generally. Countries that have not integrated cybersecurity measures into the legislative frameworks governing a variety of economic sectors tend to have fewer regulatory tools available to deal with cybercrime and, consequently, are less effective in addressing cybercrime. As a result, such countries may not realize the full benefits of the development of broadband networks and the take up of advanced services by the market. For instance, if reforms developed in the ICT regulatory framework are not integrated into the regulatory frameworks governing other sectors, end-users of ICT services will be reluctant or unable to make full use of all ICT capabilities due to security-related issues; this, in turn, will impact market performance.

Although there are a multitude of tools available to address cybercrime, no one tool is sufficiently powerful to address all issues, let alone resolve all such issues. A combination of tools is necessary. Adopting complementary general-purpose and specialized tools represents the most effective approach to fight cybercrime. Once a general cybersecurity strategy has been adopted at a national level, regulators and policy-makers must carefully pick and choose among tools and mechanisms in order to develop an integrated and coherent approach to policy implementation that balances policing cybercrime with promoting network deployment and use.

The tools available to regulators and policy-makers in this regard can be classified using the "5Ws" analytical framework, as follows:

1. **What is the nature of the tools?** Ranging from broad policies through specialized rules and regulations to individual customized incentives or remedies, the available tools can activate a national strategy and enable an effective response to cyberthreats.
2. **For what purpose are the tools applied?** The *ex ante* tools for preventing cybercrime and assessing the specific risks associated with ICT development in a country as well as the *ex post* tools for enforcing rules and regulations and penalizing cybercriminals are equally important to ensure the integrity of networks and organizations, and the private sphere of individual users.
3. **In which area can the tools be applied?** The variety and sophistication of existing and emerging cyberthreats require a high degree of caution and coordination as well as fine-tuned, flexible and modular tools in each and every target area, from botnets to e-fraud and intellectual property rights violation.
4. **Who can apply the tools?** There is no unanimity to date on the unique entity that should be responsible for handling cyberthreats and various national models co-exist across regions. Typical examples are described in the related sub-section below.
5. **How are these specific tools different from traditional regulatory tools?** The open nature of the Internet has led to fundamental changes in the architecture of and the service delivery over communication networks, which require the centralized regulatory models from the past to be rethought and reinvented. The different threat scenarios that countries are faced with require not only more efficient technology, but also dedicated laws and regulation (including data protection and privacy laws), and the appropriate enforcement mechanisms.

A practical overview of the key aspects of these tools is presented in the following sub-sections.

1.5.2.1 What is the nature of the tools?

There is a range of complementary and sometimes overlapping tools that can be applied to enable an effective response to cyberthreats.

Policy tools

In the 2000s, the ICT sector became the nexus point where virtually all other sectors of the national economy meet. The overall economic performance of a country is now directly impacted by the integration of ICTs (and increasingly broadband, in particular) into public governance, industrial and commercial processes, and social lifestyles. The productivity gains and other non-economic efficiencies of this integration are likely

to boost the national economy if the necessary enabling framework is put in place[101]. Consequently, countries have begun to pay closer attention to ICTs in policy development; a number of countries have also adopted broad national strategies related to the ICT sector and the digital economy.

Both policies related to economic development in general and policies that focus specifically on ICTs have key roles to play in establishing an effective governance framework for addressing cyberthreats. In addition, general political support for ensuring a healthy ICT sector and increased public awareness of cybercrime-related issues can propel cybersecurity to a more prominent place on the national political agenda. This increased prominence of cybersecurity in turn can pave the way for a concerted and more efficient response to cyberthreats.

ICT policy goals have evolved considerably over the past decade. While initial targets for Internet and broadband service provision typically focused on public access (e.g., telecentres and cybercafés),[102] private access to such services has increasingly become a major part of overall policy objectives. This transformation of policy goals has drawn greater attention to issues related to cybercrime and the responsibility of citizens to protect themselves online. Increased attention to cybersecurity and cybercrime issues has also been driven by the awareness that a minimum level of cybersecurity readiness is essential for the massive uptake and ultimately universal availability of ICT services. Specific targets included in national strategies and policies and the tools for implementation need to be selected carefully in accordance with best practices and standards and in light of national circumstances. This may be challenging, as targets must be realistically achievable, yet forward-looking and not unduly limited or prone to becoming outdated as the market and technology develops. Most general policies are designed to last at least for five to ten years but in view of the rapid development of the ICT sector in general and of cyberthreats in particular, it might be more practical to set targets for three to five years. Needless to say, policies should allow for a process of review and update so that targets may be adjusted as necessary.[103]

There is no single or universally recognized model of addressing cybercrime at the national policy level. Rather, countries have adopted a variety of different policy frameworks, depending on their specific national circumstances, priorities and perceived needs. For example, cybersecurity and cybercrime can be addressed in the National ICT Development Plan or the National ICT Strategy, given its cross-cutting nature and paramount importance but criminalization requires specific measures. A growing number of countries are developing national broadband strategies that include elaboration on how to secure broadband networks and ensuring a safe and secure user experience. Increasingly, cybercrime is being addressed in national security policies and plans. Alternatively, at least a quarter of countries worldwide, both developed and developing, have adopted specific cybersecurity policies or legislation.[104] In countries where more than a single policy document exists (i.e., a national ICT strategy and a broadband plan), a consistent and effective interplay between those documents must be ensured. In the foreseeable future, separate cybercrime policies may come into being as a result of greater political awareness of the underlying issues.

Legal and regulatory frameworks

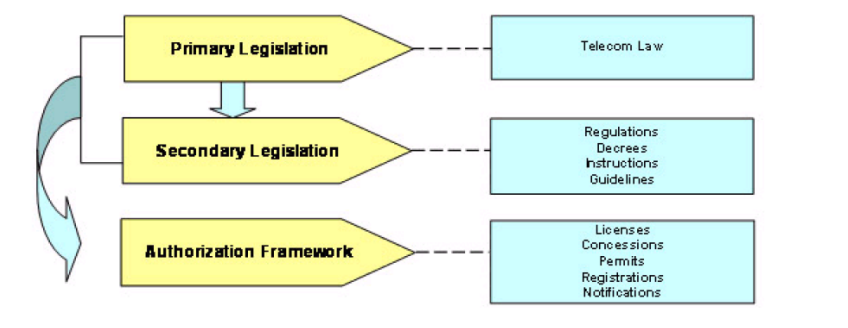
As Box 1.4 illustrates, the design of the legal and regulatory frameworks used to regulate the ICT sector typically involves a hierarchy that allows the need for certainty and stability in the sector to be balanced with the need to be able to adapt regulations in response to technological developments.

a. Primary legislation and legal measures

Some ten years ago, cybercrime was not addressed through any legal or regulatory instruments governing the ICT sector. More recently, however, telecommunication/ICT legislation and/or national penal laws have been amended in many countries to address cybercrime. The introduction of provisions targeting cybercrime into such telecommunication/ICT and criminal legislation has a number of benefits. For instance, once written into law, the process of implementing policy objectives becomes easier. More dedicated resources become available for policing cybercrime. Furthermore, the legislative provisions typically identify clear roles and responsibilities for different agencies involved in responding to cybercrime and specify implementation mechanisms available to such agencies. In this regard, amendments to telecommunication/ICT legislation and criminal law can enhance a country's ability to respond effectively to cybercrime.

Box 1.3: Hierarchy of regulatory frameworks

Generally, the legal framework governing the ICT sector follows a hierarchy, which is depicted in the figure below. The primary legislation for the sector, such as laws and decrees, should establish the broad framework that will be used to regulate the sector. The more detailed dimensions of regulatory regime is typically best addressed in secondary legislation, which can be amended and modified more easily to complement the pace of technological development without the intervention of the legislature. Secondary legislation, in turn, provides the legal basis for the regulator or the relevant ministry to issue authorization instruments such as licences, concessions, and permits to operators. This legal hierarchy provides certainty and predictability to consumers and other stakeholders because it specifies the rights and obligations (i.e., the rules of the game) that apply to the sector.



Source: ITU-infoDev ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org

There is no established approach for introducing cybersecurity and cybercrime-related matters into national and regulatory frameworks, though some useful tools exist. Since cybercrime-related amendments to telecommunication/ICT legislation and criminal law are relatively recent developments, it is not yet possible to evaluate the impact of different approaches to legislating in relation to cybercrime.

There are two principal ways of introducing cybercrime issues into ICT legislative and regulatory frameworks. First, amendments can be made in a piecemeal fashion, responding to issues as they arise. Second, countries can introduce entirely new legislation to regulate the ICT sector that includes provisions relating to cybercrime. The latter, more radical approach may offer a more practical way to integrate cybercrime issues into existing telecom and ICT laws, allowing for a common, coherent approach to current issues facing the sector and a single, consistent legal point of reference with regard to available means and tools. A third way is to integrate cybercrime issues into a general criminal law.

Whatever option is chosen by countries, a legal framework for fighting cybercrime should include:

- Updated criminal legislation;
- Criminal procedural legislation;
- Legislation to facilitate international cooperation; and
- Legislation to deal with cybercrime-related issues, such as data protection legislation, ISP liability legislation, etc.

The range of legal measures that countries should adopt include, first of all, substantive legal provisions to criminalize acts such as illegal access, illegal interception and data interference, the violation of copyright and related rights, computer fraud and electronic forgery, and offences related to the distribution of child pornography over the Internet.[105] As has been discussed above, gaps in national legislation must be identified and amendments introduced to close these gaps. Criminal law provisions, for example, frequently must be amended to facilitate the laying of charges in contexts where the criminal act takes place online or in a digital format.

Next, countries should adopt amendments to procedural law and regulations in order to ensure that law enforcement agencies have the powers and tools necessary to conduct cybercrime investigations. These investigations are significantly different from investigations of traditional crimes due to the transborder nature of networks, the international dimension of most cybercrimes, and the "virtual" nature of cybercrimes as opposed to the "real world" nature of traditional crimes. The international nature of cybercrime also highlights the need to ensure that national legal measures facilitate the cooperation between law enforcement agencies in different countries.[106] Despite

the challenges that are bound to lie ahead, regulators could encourage the adoption of an anti-cybercrime law or legal provisions in general communication legislation that are harmonized as much as possible with those of other countries.

Although criminal law is an essential component of the legal and regulatory frameworks for combating cybercrime, these legal and regulatory frameworks should not be limited to criminalization. For example, non-criminal law provisions were used by the court to order VeriSign Inc., a domain name service provider, to take down the "Waledac" network in early 2010 and to deactivate domain names administered by VeriSign that had been used by a botnet. In the future, botnet operations are very likely to use top level domains hosted by different naming service providers in order to make it more difficult to get such a court decision. Developing a legal framework that enables the shutting down of domain names hosted by different naming service providers is one of the examples of future legal frameworks.

b. Regulatory tools

Adapting a country's regulatory framework to respond to cybercrime-related issues takes time and often repeated attempts. Effective adaption depends on the provisions contained in existing sectoral or general policies and in primary legislation. Moreover, the roles and responsibilities of government agencies and other potential partners in this field must be defined at a higher level and adequate authority to discharge these responsibilities must be delegated to government agencies in order to ensure that these agencies and partners can develop the necessary regulatory tools to respond to cybercrime.

A critical challenge for government agencies dealing with cybercrime is keeping pace with cybercriminals who have proven to be adept at using new technological developments and fats-adapting techniques to perpetrate new forms of cybercrime. Regulatory frameworks for cybercrime therefore must be flexible and forward-looking, while still well-defining the issues, offences and remedies in order to be proved effective.

c. Co-regulation and self-regulation

In addition to enacting anti-cybercrime legislation, other alternative regulatory approaches such as co-regulation and self-regulation may be adopted in order to enhance the readiness of the sector to address cyberthreats.[107] National telecommunication/ICT legislation can mandate the development of co-regulatory practices, such as ISP codes of conduct. Adherence to such codes could be a licence condition or the obligation could be imposed in regulations or in other instruments adopted in a rulemaking proceeding. For example, obligations related to adherence to industry codes of conduct may be imposed on ISPs in much the same way that facilities-based operators have been required to interconnect with competing carriers: through interconnection regulations, terms of licence, orders to develop a reference interconnection order, and the like, with an emphasis on collaboration with industry stakeholders to determine the terms of interconnection.[108] As markets mature, many regulators encourage industry self-regulation such as industry self-reporting for enforcement purposes and reliance on alternative dispute resolution techniques to resolve conflicts. These forms of industry self-regulation help regulators to successfully oversee the multiple players in the dynamic the ICT sector.[109]

Practices related to fighting spam provide a potential model for co-regulatory initiatives related to cybercrime.[110] Just as regulators have required ICT service providers to develop and to implement guidelines and standards for fighting spam, regulators could require ISPs to establish co-regulatory initiatives related to cybercrime such as an industry code of conduct. The enabling legislation underlying the order to develop such a code should stipulate that the regulator has the authority to enforce the code against any ISP in violation of it. Although not yet very common, such practices could prove very useful to regulators as they discharge their responsibilities both to rely on market forces to the greatest extent possible and to protect the sector and ICT networks from various forms of threats and market failures. As essential players in developing the digital economy, ISPs have generally been left alone by legislatures, administrative agencies, and judges. They may be licensed and overseen by regulators in some contexts, but ISPs have largely been immune from prosecution for criminal acts committed by people using their services.

Over the past decade, ISPs around the world have taken an active role in attacking spam at the source, before it reaches customers' premises. Pursuant to codes of conduct, ISPs have committed themselves to denying service of any kind to spammers, phishers, spoofers and other actors who violate spam-related policies.[111] Where such codes are in place, they could be extended to cover a wider range of offences and can be trans-

formed into functional barrier to cybercrime. An important advantage of this type of industry involvement is that by acting at the root of the content distribution network, ISPs can rapidly and effectively counter a number of cybercrime threats. Regulators need to be careful, however, not to over-burden ISPs by imposing overly onerous obligations and requirements related to co-regulation.

As an alternative to a mandated code enforced by regulators, governments might encourage ISPs to develop their own, industry-enforced codes of conduct. In fact, such self-regulatory practices have already emerged to address issues related to cybercrimes such as spam. In the case of spam, the terms and requirements adopted in self-regulatory mechanisms are often built into "acceptable use" policies for customers and peering arrangements.[112] Under this voluntary, self-regulatory model, regulators could advise the industry in developing the codes. The corporate responsibility of participating ISPs can effectively be used as a promotional strategy to attract consumers from other, less secure ISPs, and can actually prove to be a sound business strategy in itself. Strong involvement in the fight against cybercrime is not necessarily incompatible with a desire to increase revenue and subscriber growth. ISPs are very much aware that cybercrime and cyberthreats in general are likely to considerably compromise their financial and operational sustainability and thus have incentives to partner with government agencies to counteract cybercrime. In this regard, regulators should carefully study and analyze market realities and peculiarities with a view to designing and adapting targeted incentives for industry players, especially to ISPs, to work with them to fight against cybercrime.

Partnership tools: Regulating with the assistance of the private sector, other regulatory agencies, and industry stakeholders

a. Contracting out specific tasks

Ensuring the capacity of government agencies to cope with unexpected incidents requires leading edge technological expertise and highly specialized knowledge of the latest trends in encryption technologies, threat analysis, and layered preventive measures. This is particularly challenging for ICT regulators, as their mandate and field of oversight is broad and multifaceted. More often than not, ensuring that the institutional arrangements for addressing cybersecurity and cyberthreats are effective requires new ways of operating in order to address the rapid pace of evolution in cybercrime, the international dimensions of cybercrime, and the "virtual" world in which cybercrime occurs. What are some of the steps that the ICT regulator or the any government agency can take to build cybersecurity and cybercrime capacity when these fall under its mandate?

Drawing on past examples from other utilities and industries and under different circumstances[113], the regulator could consider contracting out some of the specific tasks. Here are some of the reasons why this may be useful:

1. **To supplement limited in-house capacity**. ICT regulators are often faced with sharp peaks in their workload or need small amounts of specialized inputs and technical skills that tend to be in short supply, particularly in the public administration and especially in the areas of cybersecurity, cybercrime, and countering spam.
2. **To reduce costs**. When looking at security from an innovative point of view, providing a specialized service is almost never considered as a means of reducing costs. However, strategically contracting out some of the cybersecurity tasks may help reduce the costs of procuring expertise or, for a given cost, increasing regulatory competence. Third parties can spread the fixed costs of acquiring specialized experience over large markets, both nationally and globally.
3. **To improve the quality and credibility of the regulation**. Contracting out tasks related to cybersecurity may assure investors of the independence of the regulatory process from short-term political capture, particularly in countries with institutions in transition. Cybersecurity and cybercrime is a growing concern and external expertise may also be useful to assure investors that the regulator is capable of developing and adopting the measures necessary to protect their investments in the sector.

Agencies may decide to contract out different tasks at various stages in the development of their institutions and for different reasons. New ICT regulators, for example, may need extra support when they are first established to build credibility and competence; as cybersecurity and cybercrime is a highly specialized area, engaging experts at an initial stage may be preferable so that the regulator can concentrate on its other core duties. More experienced and established ICT regulators may contract out a particular task, like analysis and research into malware and spam, because doing so is less expensive than performing it in-house. From a risk

management perspective the institution needs to consider thoroughly what activities should be performed in-house and which tasks can be outsourced.

b. Institutional cooperation: Memoranda of Understanding and Cooperation Protocols

It is not commonplace for an ICT regulator to have complete and exclusive jurisdiction over all legal and regulatory aspects of cybersecurity or cybercrime. In many cases, there are a number of government agencies that share the responsibility of overseeing this area (see also Section 1.4 above and Section 1.5.2.4 below). The relationship between the ICT regulator and sector ministries are often well defined in legislation. The coordination with some other specialized bodies such as the national data protection agency and the consumer protection agency are often much less clear or may be missing entirely. Cooperation with courts and the national police are unfortunately often not codified in legislation but instead established through administrative procedures[114].

When the existing legislative framework does not define clear roles and responsibilities for the agencies involved with fighting cybercrime, inter-agency cooperation may be hampered, especially if two or more agencies have concurrent jurisdiction set out in different legislative frameworks. This situation creates uncertainty and confusion for industry stakeholders and risks inconsistent regulatory approaches; moreover, it can result in a waste of scarce regulatory resources as various agencies complete the same or similar tasks.[115] It may even result in competition between regulatory agencies to assert jurisdiction and control, to the detriment of all sector stakeholders.

In other, more traditional areas of regulation, a number of regulators have responded to the need to coordinate their actions in matters of concurrent jurisdiction by adopting Memoranda of Understanding or cooperation protocols.[116] For example, the separate Dutch ICT regulator and competition authority have established a cooperation protocol to provide clarity on how they will cooperate on matters of mutual interest.[117] Similarly, the Nigerian Communications Commission (NCC) and the Nigerian Consumer Protection Council (CPC) have adopted a Memorandum of Understanding that establishes how the agencies will collaborate on matters related to consumer protection.[118]

This mode of cooperation may usefully be replicated to enable enhanced interplay among peer agencies in the area of cybercrime. One advantage is that there is no need for action or involvement of higher level institutions such as the ministry or legislative body, and therefore no additional delay and administrative procedures before the agreement is enacted. On the other hand, the memoranda or protocols used provide a supple framework for joint action while limiting the wide discretionary scope of general administrative laws. Thus, complexity and bureaucratic hurdles are reduced and the collaborative processes are smoothened, hastened, and focused on the topical issues rather than on procedural ones. Such frameworks also allow for greater predictability of the actions of the agencies involved and better guarantees that the objectives set in laws and regulations will not be distorted.

c. Mechanisms for stakeholder involvement

No matter how many resources have been mobilized through official government channels to prevent and to police cybercrime, they may prove limited and partial. The exploding amount of online traffic significantly complicates addressing cybercrime incidents. Every additional piece of information or indication that responsible agencies can get allows them to better understand cybercrime, to better monitor evolving cyberthreats, and ultimately to better respond to incidents. In this respect, it is important to involve users in addressing cybercrime and to put the appropriate participative mechanisms in place. Free hotlines (through the web, by email or by telephone) for users to make complaints or report fraud and other abuses may be set up to get real-time feedback and allow for rapid responses to incidents and potentially minimize their impact. User feedback may also be sought on a continuous basis in order to better monitor and understand imminent threats in cyberspace and to anticipate harmful or malicious acts.

d. International cooperation

Cybersecurity is as global and far-reaching as the Internet. Since threats can originate anywhere around the globe, the challenges are inherently international in scope and require international cooperation, investigative assistance, and common substantive and procedural provisions. Therefore solutions need to be harmonized to the extent possible across all borders and for many of the different measures put in place.[119] This necessarily entails international cooperation, not only at government level, but also with industry, non-governmental and international organizations. Due to the differences in national laws and the limitations of

existing instruments and tools, international cooperation is considered of the major challenges in the fight against cybercrime. As noted in Section 1.4.5 a number of international and regional organizations collaborate and undertake activities in the areas of cybersecurity and fighting cybercrime. This further underlines the importance of the prosecution of cybercrime, including cybercrime committed in one jurisdiction, but having effects in another. There is a need for effective and efficient tools and actions, at national and international levels, to promote international cooperation among the different stakeholders, including law-enforcement agencies.

There are several international and regional initiatives working towards harmonizing the legal frameworks of various countries. For example, the Tunis Agenda for the Information Society adopted during the second phase of the World Summit on the Information Society in 2005 highlighted the need for international cooperation in the fight against cybercrime and called upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime[120]. The Group of Eight (G8) adopted Ten Principles to combat cybercrimes, which included commitments to 1) ensure that there would be no safe havens for cyber criminals anywhere in the world and 2) implement a coordinated international legal framework capable of investigating and prosecuting cybercrimes regardless of where the harm has occurred.[121] The Council of Europe has established the Convention on Cybercrime, which sets out measures to be implemented by Member States to help ensure that domestic laws regarding confidentiality, integrity and availability of computer data and systems, such as illegal access or interception, were consistent.[122] The Council of Europe Convention on Cybercrime also requires Member States to establish rules related to extradition and mutual assistance in order to guarantee international cooperation.[123] Additional regional commitments to the prevention and prosecution of cyber crimes have been implemented through APEC, the African Union, the Arab League, ASEAN, and OAS. [124] Although there are multiple organizations working towards a harmonized framework, developing countries may face a variety of different challenges in implementing effective domestic and international frameworks for the prevention and prosecution of cybercrimes, which may require specialized strategies.

Despite these international initiatives, there has been little harmonized action in fighting cybercrimes, with countries divided over how to best approach a unified framework. For example, in April 2010, nations at the 12th UN Congress on Crime Prevention and Criminal Justice failed to agree on the necessary response to take to cybercrimes. While some countries supported expanding the European Union's Convention on Cybercrime, others have argued for new multilateral negotiations.[125] However, the generally agreed upon principles of implementing international cooperation include:

- providing cooperation in international investigations to the greatest possible extent;
- facilitating extradition for cybercrimes; and
- requiring mutual legal assistance in order to expedite communications among law enforcement agencies in multiple countries, including designating contacts within agencies that process requests for assistance.[126]

The main obstacles to a globally harmonized cybercrime framework are time and money. While cybercrimes occur quickly, the development and implementation of international agreements take time. Furthermore, enforcement and technical protection measures are costly, particularly for developing countries. However, the commitment of sufficient resources to ensure online security is necessary to protect consumers, businesses and the government against cybercrimes.

Technical tools and technical standards

At the network level, a range of tools exist to impede or to terminate activities that constitute cybercrime offences. Technical measures can usefully complement legal and regulatory measures and substantially enhance the cybercrime readiness and response of a country. One example is the technical measures applied by ISPs (i.e., restricting Internet access to offenders) in or outside the framework of co- and self-regulatory practices.

Government agencies need to be clear on what their responsibility is with regards to website applications that feature software that installs itself on users' computers and that automatically reports back to remote computers with information on users' specific behaviour. Cookies are an example of such an application; cookies install automatically on users' computers and report back to the companies that created them, for example, search engines, about the users' online activities. The trend in this area shows that some countries are taking steps to protect consumers' privacy by enacting legislation that requires such website applica-

tions to request the users' permission and to specify what the application does (e.g., report back to the creators of the application with information about online activities) before the software installs on the users' computers. However, the creators of such applications have already developed methods of circumventing the requirement to obtain explicit user approval such as the simple addition of a button in the browser for the acceptance of cookies.

Table 1.2: The purposes of anti-cybercrime tools

Purpose	Tools				Examples
	Policy	Legal and regulatory	Technical	Cooperation	
Preventing cybercrime	X	X	X	X	• Awareness campaigns through media and Internet • Adoption of anti-spam regulation (which often takes the form of a provision in the national telecommunication/ICT legislation, e.g., regulating the sending of unsolicited e-mail for "commercial, ideological or charity" purposes (in The Netherlands), not limited to bulk mail.)
Assessing the cybersecurity readiness			X	X	• Regular reporting and assessment of cybercrime incidents, their impact, and scope • National cybersecurity drills
Limiting the scope or impact of cybercrime/ mitigating cybercrime		X	X	X	• Enforcing the anti-spam regulation • Issuing warnings and discontinuing service to offenders' IP addresses • Enforcing technical measures to take down unlawful content from the web
Rendering cybercrime uneconomic	X	X			• High fines for unlawful behaviour
Resolving disputes		X		X	• Provide redress for consumers and/or organizations • Applying alternative dispute resolution mechanisms (mediation, arbitration, etc.)
Investigating cybercrime		X	X	X	• Preservation of the crime scene, cyber-forensics
Penalizing cybercriminals		X	X	X	• Impose fines and other sanctions as prescribed by law

Source: Authors.

What types of duties does the ICT regulator have when obligations to notify users about ICT and telecommunication security breaches are put in place? One example of a measure to provide Internet users with more protection is the establishment of mechanisms that informing such users when their online bank account has been used by a non-authorized party. There are different ways this can be done such as through an email, text messaging or a telephone call. Such protocols would very likely increase users' and businesses' willingness to conduct more of their everyday activities online.

Standards development bodies have a vital role to play in addressing security vulnerabilities in protocols. Today there are security guidelines for protocol authors, security specifications for IP-based systems, guidance on how to identify cyberthreats, and countermeasures to mitigate risks, etc. and many more standards are being developed to help address growing threats. ITU's Telecommunication Standardization Sector (ITU-T) holds a unique position in the field of standardization as its work brings together the private sector and governments to coordinate work and to promote the harmonization of security policy and security standards on an international scale.[127]

1.5.2.2 For what purpose are tools applied?

As in other regulatory and legal areas, each tool for addressing cybercrime has its own role and its own use and limitations. Most tools are single-purpose in nature; accordingly, in order to address all aspects of cybercrime, government agencies need to be equipped with a full set of complementary instruments.

As shown in the table above, regulatory tools can be used on a continuous basis, in parallel with regular regulatory work related to stimulating investment and market growth, preserving competition, and ensuring affordable services to consumers. As a matter of implementation strategy, an integrated approach to addressing cybercrime will be characterised by a combination of *ex ante* and *ex post* tools, applied simultaneously in a range of target areas. But such an approach should not be perceived as a sort of pervasive regulation and certainly should not be understood as a move towards "more regulation" or additional regulatory burdens or strings. Instead, an integrated approach should feature smart, adaptive regulation, which builds protection mechanisms around vulnerable areas. More onerous enforced measures should only be applied when a cyberthreat is imminent or a cybercrime has been committed. Of paramount importance are the framework conditions (both regulatory and technical) that must be put in place to ensure a maximum level of resilience is enabled over networks, services, applications and consumer behaviours (described in Section 1.5.2.1).

1.5.2.3 In which areas are tools used?

There are heated debates over the exercise of regulatory authority to specific individual fields of cybersecurity/cybercrime such as network security, spam, phishing, denial-of-service attacks, and content regulation. The extent to which each of these particular fields are being regulated varies from country to country, and it is difficult to ascertain whether certain types of regulatory treatment are better than others. Nevertheless, adopting cybersecurity-related legislation is considered today a mainstay of a sound strategy for making cybersecurity mechanisms work better.

To present some insights into the range of issues that merit the attention of ICT regulators, it may be interesting to explore the specific areas in which countries around the world have adopted cybersecurity-related legislation or regulations. Experiences of selected countries in different regions are presented in Table 1.3 below.

1.5.2.4 Who can apply those tools?

In recent years, the Internet and the innovative ICT services it enables have challenged this traditional sector-specific approach to regulation, and have engendered a call for new regulatory models able to respond to the complexity, breadth, and heterogeneity of the modern Internet phenomena. Cybersecurity and cybercrime illustrate the need for current regulatory frameworks to move towards more decentralization and cooperation among government bodies and all stakeholders in the cybercrime ecosystem (see also Section 1.4).

According to ITU's data, at least 33 regulators (22 per cent of established regulators world-wide) have been explicitly given the mandate to deal with cybersecurity, as of the end of 2009.[128] Half of them, or over 10 per cent, have jurisdiction over cybercrime issues, while in a quarter of all countries, the specialized body responsible for cybersecurity is an agency other than the ICT regulator.

Table 1.3: Examples of countries that have adopted legislation or regulations in cybersecurity-related areas, 2009

Country	Cybercrime	Data protection	Online privacy	Online fraud	Online gambling and gaming	Child online protection	Critical information infrastructure protection	Network security	Spam
Australia	X	X	X		X	X		X	X
Brazil	X					X			
Croatia	X	X	X	X		X		X	X
Ecuador	X	X	X	X		X	X	X	X
Finland	X	X	X			X	X	X	
France							X	X	
Georgia	X	X	X			X	X		X
Germany	X	X	X	X	X	X	X	X	X
Ghana	X	X	X	X	X	X	X	X	
India	X	X	X	X	X			X	
Kenya	X	X	X	X					
Latvia	X	X	X	X		X			X
Moldova		X	X				X	X	
Nicaragua	X	X	X	X		X			
Pakistan	X	X	X	X					X
Peru	X	X	X	X		X			X
Poland	X	X	X	X	X	X	X	X	X
Saudi Arabia	X	X			X	X			X
Senegal	X	X				X			
Singapore	X	X				X			X
St. Vincent and the Grenadines	X	X	X	X		X	X		
Turkey	X		X	X	X	X	X	X	X
Zambia	X	X	X	X				X	

Note: This table is based on self-reported information provided by countries through the ITU World Telecommunication/ICT Regulatory Survey 2009. Definitions may vary across countries.

Source: ITU World Telecommunication Regulatory Database

Apart from the ICT regulator, the responsible body is often the sector Ministry (e.g., in the Czech Republic, India, and Japan), but it may also be the National IT Agency (e.g., in Ghana) or the police (e.g., in Singapore). A handful of countries have created a specialized cybercrime agency (e.g., the National Response Center for Cybercrimes in Pakistan) and others have assigned the mandate to the government agency responsible for Internet-related issues (e.g., the Brazilian Internet Steering Committee). In a number of countries, more

than one entity has responsibilities in one or more areas of cybercrime, for example network security, critical information infrastructure protection, and child online protection (e.g., in Qatar, Q-CERT and ictQatar, the regulator; in Austria, the ICT sector Ministry jointly with the Ministry of Justice and the Data Protection Commission; and, in Hungary, the ICT regulator and the national consumer protection agency).

1.5.2.5 How are those tools different from traditional regulatory tools and where is regulation headed?

Because of the large and growing number of players in the ICT sector and the complexity of their interactions, effective mechanisms for cooperation and communication should be established in order to ensure synergies and ultimately ensure resilient cybersystems and safe online experience. On the other hand, these mechanisms need to allow for enough flexibility and openness in order to be capable of responding to a large array of circumstances without locking in the agencies or stakeholders involved in regulation.

Cybersecurity and cybercrime cannot be treated as any other regulatory topic or subject matter. Although it is fair to include cybersecurity as a type of public good, the mechanisms for delivering it differ substantially from other public goods in the ICT sector such as ubiquitous connectivity. There is a need for the design of new mechanisms that support cooperation among stakeholders and the dynamic development of a shared understanding of cyberthreat phenomena. Therefore, the cybersecurity ecosystem cannot be regarded as simply a network of institutions, entities, and individuals following the same goals, but rather should be viewed as a community of interdependent and interacting constituencies. In a sense, regulation is only likely to be effective if distributed across the ecosystem or delivered through peer-to-peer mechanisms — the functioning and performance of which implicitly requires coordination and cooperation between peers.

A new generation of peer-to-peer regulation is likely to promote collaboration and better performance. Typically, performance will be closely related to responsiveness and willingness to cooperate among peers. Nevertheless, there is also a need for alternative mechanisms or routes for cooperation in regulation in case of a breakdown in cooperation or occurrence of conflicts.

In short, what would a comprehensive regulatory framework for cybercrime look like? Contrary to what many may believe, it is not necessary to invent a completely new regulatory regime to accommodate the aforementioned concerns, but it does require the involvement of additional stakeholders and new forms and channels of cooperation at the national and international level. From the analysis carried out in the previous sections, it appears that the following elements should be designed, applied and enforced:

- **Adaptive and scalable mechanisms**: there are increasing issues stemming from the accelerated pace of cybercrime and the cutting-edge technology used to harm networks and consumers. The regulatory mechanisms put in place should be flexible, forward-looking, and able to adapt quickly to new threats and offences. In fact, new measures may need to be conceived "on the fly" in order not to become overwhelmed by new generations of malicious attacks. In the meantime, agencies have to decide which regulations and requirements are important to retain and which should be replaced.
- **Modular approach**: the ability of agencies in charge of cybercrime oversight and response to regulate efficiently in this area has major implications for investment in both communication networks and services and a country's long-term competitiveness. Therefore, it is important to engineer a modular approach to regulating the various types of offences in a differentiated way to allow for a greater or lesser degree of intervention and coercion according to the magnitude of the offence and the nature of the offender. The rationale behind this is not to overload market players and consumers with extra burdens (and ultimately not to harm the market) while preserving the ability to fight back and block offences without delay.
- **Dynamic decentralized control**: the regulation of cybercrime is an ongoing process that requires regular attention as new issues emerge. As these issues can occur at all network layers and at the end user level, the response to cybercrime can only be effective if it is distributed across the cybercrime ecosystem. A pure top-down, centralized approach to regulation is unlikely to prove efficient unless combined with more open and dynamic models of cooperation with a host of agencies, network, and service providers, as well as consumers.
- **Agile procedures and protocols**: ultimately, cooperating agencies need to ensure that all known cybercrime offences fall under the jurisdiction of at least one agency and that in areas of concurrent ju-

risdiction, the procedures and protocols of the relevant agencies are non-controversial, complementary, and provide for concerted collaboration. As mentioned above, it is vital to ensure that there are no administrative or other hurdles to the smooth applications of rules and regulations and their effective enforcement.

1.6 Role of the ICT regulator in addressing cyberthreats[70]

Traditionally, ICT regulators were not assigned a significant role in addressing cyberthreats since cybercrime was mainly considered the domain of lawmakers and law enforcement agencies. However, with the increasing ubiquity and openness of ICT networks, the ICT sector and ICT users have become ever-more vulnerable. This vulnerability stems not from issues of dominance or anti-competitive practices,[129] but from concerns about harmful and offensive content and innumerable cyberthreats to critical infrastructures, to privacy, and to the integrity of computer systems and networks, to name but a few. When exploited by criminals, the vulnerabilities in question threaten not only to harm individual users, businesses and financial institutions but also to undermine the development of the ICT industry and related products and services.

What is the role of the ICT regulator in this complex ecosystem? The ICT regulator can leverage certain core competencies and its position within the ICT sector to make a material contribution to safeguarding cybersecurity, particularly with respect to facilitating the mobilization of various stakeholders and coordinating the efforts of these stakeholders in the fight against cybercrime. The long-term sustainability of the ICT industry depends on it. Consequently, ICT regulators in some countries have already explored the possibility of extending regulatory duties from dealing with universal access and competition and authorization issues to addressing consumer protection, industry development, cyber safety, and participation in cybercrime policy making and implementation. While some new regulatory authorities have been created with mandates and responsibilities that include cybercrime (e.g., the Korea Communications Commission)[130], older and more established ICT regulators have extended their existing tasks to include various activities aimed at tackling cyber-related threats (e.g., the Swedish regulator, PTS)[131].

However, the exact mandate of ICT regulators in this field has not yet been clearly defined. With the field of vision and involvement for regulators expanding, only a few ICT regulatory bodies have effective powers to go beyond traditional telecommunication regulation and deal with wider ICT sector issues. Being active in a rapidly changing and developing sector exposes the ICT regulators to new fields that have traditionally been considered the domain of other government departments and agencies or possibly even no one's domain.[132] Even if the regulator has enough competence and industry expertise to be involved in addressing specific problems, it should nevertheless have a clear understanding about its mandate and of the responsibilities and mandates of other stakeholders in order to interact and collaborate with them.

The following discussion highlights some potential areas in which the ICT regulator can be involved and analyzes activities that are generally handled by other stakeholders. The analysis in this section provides insight into some of the current trends and country examples. The section will answer the following questions in order to probe the issue of extending the involvement of the ICT regulator in issues related to cybersecurity and to make some suggestions on specific functions and duties that the regulator could undertake:

- What could be the reasons behind and the prerequisites for extending the mandate of ICT regulators to address cybercrime?
- What are some of the specific areas where the ICT regulator has already been involved and/or can be potentially involved?
- What role can the ICT regulator play in each area when it is involved?

1.6.1 Extending the regulatory mandate to address cybercrime: Areas of involvement, skills and competences

1.6.1.1 Extending the mandate of the ICT regulator

As ICT regulators, especially in developing countries struggle to bridge the digital divide and to improve access to information and communications technology, they must prioritize the implementation of measures aimed at detecting and responding to vulnerabilities, the adoption of an appropriate cybersecurity strategy, and awareness raising among consumers about online threats.

At the same time, while there are reasons to support extending the ICT regulator's mandate into the area of cybersecurity, there are also reasons to be cau-

tious in expanding the regulator's mandate. When the responsibilities of the ICT regulator in this area are not clearly defined or supported by the appropriate mandate, it will be challenging for the ICT regulator to determine how it can participate in the fight against cybercrime alongside of other agencies and stakeholders. The jurisdiction of other agencies with respect to cybercrime must be ascertained and assessed to determine if activities undertaken by these other agencies should be transferred to the ICT regulator or possibly shared with the ICT regulator. The main areas of regulatory involvement that should be analyzed in each particular case are discussed in the following sections.

An analysis of country practices in selected countries suggests that the mandate of ICT regulator can potentially be usefully extended or strengthened into the following areas:

1) **Implementing consumer protection duties.** The Dutch Independent Post and Telecommunication Authority (OPTA) highlights the fact that Internet safety is a key area for regulation under the mandate of consumer protection. This is considered together with the task of addressing spam, spyware and botnets as threat to the privacy of anyone who uses a computer. OPTA defines three key areas under its consumer protection mandate:[133]

   - **Prevention is better than cure.** The ICT regulator can work together with ISPs and other industry stakeholders to ensure the fulfilment of article 11.3 of the Dutch Telecommunications Act, which makes it mandatory for ISPs to secure their networks properly and to inform their customers of the risks that are peculiar to the Internet.

   - **Spam prohibition.** The Dutch regulator has been given the authority to address any contravention of the prohibition on unsolicited communication pursuant to its duties to provide Internet safety for consumers.

   - **Fighting dissemination of malware.** OPTA has the power to take action against anyone who has contravened the prohibition of spam and unsolicited software by imposing fines.

   In 2009 OPTA raised the issue of a growing gap between cybersecurity and cybercrime for agencies that deal with both issues. OPTA pointed out that it is necessary to bring together competent national authorities that deal with cybersecurity problems like spam and/or malware (ICT regulators, Data Protection Agencies, Consumer Protection Bodies) and police, public prosecutors, and other agencies fighting cybercrime. From the Dutch regulator's point of view, a bridge 'between the world of cybersecurity and cybercrime' should be built in order to effectively address both issues.[134] The extension of regulatory power to address cybercrime provides the ICT regulator with a clear mandate for further collaboration with different agencies investigating and preventing cybercrime and for developing legal and technical measures to address threats in cyberspace. This in turn strengthens the links between actors involved with cybersecurity and facilitates capacity building within the whole ecosystem.

2) **Taking over the responsibility for information security or network security.** As a converged regulator, the Malaysian Communications and Multimedia Commission (MCMC) has an Information and Network Security (INS) department to ensure information security and network reliability and integrity within the communications and multimedia industry, and in particular the critical communications and multimedia infrastructure. The department's mandate includes the promotion of education and awareness raising on information and network security best practices.[135]

3) **Granting a newly established regulator with the operational mandate for Internet safety.** The Korea Communications Commission (KCC) was formed after consolidating the former Ministry of Information and Communication and the Korean Broadcasting Commission in February 2008. Among other duties, the Commission is responsible for the protection of Internet users from harmful or illegal content.[136]

It should be noted that these activities and responsibilities may in some cases overlap with the responsibilities of other agencies. In the case of established ICT regulators, the regulator's existing authority to address certain issues such as consumer protection and ICT infrastructure protection and development may be extended to include addressing cybercrime. For a newly established regulator, the jurisdiction of other agencies should always be taken into account to determine what areas could fall under the responsibility of the ICT regulator. This is necessary to ensure the establishment of viable mechanisms for collaboration among government agencies rather than creating redundant jurisdictions.

1.6.1.2 Regulatory capacities and the extension of the regulator's mandate

There are number of competencies and capabilities that an ICT regulator should possess before its mandate is extended to include addressing cybercrime. These competencies and capabilities are necessary for the effective participation in the fight against cybercrime and include:

- **Maturity of the regulator.** Exercising duties and responsibilities in the area of cybercrime may be a difficult task for a newly established ICT regulator, particularly when such duties and responsibilities are added to the long list of conventional regulatory duties and the challenge of dealing with emerging issues such as convergence and introduction of new technologies. Newly created ICT regulators may be in a weak position as a newcomer, a factor that may have implications for its credibility amongst other stakeholders to take on a leading role in areas associated with domain of other authorities.[137] For mature ICT regulators, it may be easier to assess if there is room to extend the mandate, how the mandate can be extended within the regulator's existing activities, and what resources or specific competences will be necessary to deal with cybercrime issues.
- **Links established within the ICT industry.** The mature ICT regulator constantly interacts with other stakeholders within ICT industry such as businesses, consumers, other governmental agencies, and international organisations through different mechanisms, including public consultations and consumer-feedback tools.[138] The ability to leverage existing links and mechanisms of collaboration to reach out to different ICT industry stakeholders is a prerequisite to addressing cybercrime.
- **Technical expertise and industry expertise.** Cyberthreats are technology-driven.[139] The ability of the ICT regulator to address cybercrime effectively depends to a large extent on its industry competency, technical knowledge, and perceived industry expertise.
- **Availability of appropriate resources.** Possessing the right financial and human resources, or being able to acquire them through collaboration with industry (public-private partnerships) or international organisations, is necessary for the ICT regulator to be able to play an effective role in fighting cybercrime.

If a regulatory authority does not possess all of these competencies and capabilities, extending regulator's mandate to cybercrime-related issues is likely to prove challenging and even inefficient.

The institutional design of the regulator also influences its ability to effectively take on broader mandate, depending on whether it is a multi-sector regulator (like utility commissions), a sector-specific telecommunication/ICT regulator, or a converged regulator (also in charge of broadcasting regulation). While every model of institutional design has its advantages and disadvantages from the perspective of ICT industry regulation,[140] the type of institutional design should be taken into account when assessing how and in what areas the ICT regulator should be involved.

Converged regulators have responsibility for broadcasting transmission and/or content as well as ICT services. Such regulators already face a challenge by taking on extensive and often complex workloads. However, converged regulators may be well-suited to deal with cybercrime because of their broader mandate to address content issues (see Box 1.4); a converged regulator thus has expertise that is relevant to fighting cybercrime. In a converged environment where traditional telecommunication regulators may struggle to resolve certain issues such as the consolidation between online content and telecommunications service providers, the converged regulator seems to be in a better position to address regulatory issues related to content. Furthermore, the converged regulator is likely to avoid imposing unequal regulatory interventions on different content delivered over various platforms.[141] .

Although the converged regulator has greater adaptability and expertise in dealing with complex ICT issues, the sector-specific regulator traditionally has substantial technical knowledge and understanding of the industry. Both types of regulators can potentially perform well in addressing cybersecurity and cybercrime issues. However, the greater institutional flexibility[142] of the converged regulator can provide distinct advantages with regards to detecting areas of cybercrime activity and managing the ICT industry stakeholders due to their broader regulatory involvement. This is not to suggest that sector-specific regulators cannot play an important and effective role in cybersecurity. Indeed, the reality is that there are fewer converged regulators while many sector-specific regulators are actively involved with addressing content-related offences.

Box 1.4: Content regulation as an essential component of fighting cybercrime

The digitalization of content allows it to be transmitted on different media, including cable, satellite, and over the Internet. Despite digitalization, rules applied to broadcasting content usually do not apply to content delivered over the Internet. This raises concerns about regulating the same type of content differently based on the platform used to deliver the content. It also raises concerns about the unequal treatment of telecommunications, broadcasting, and Internet services, which are regulated by different bodies pursuant to different laws. However, it is the lack of regulation of Internet content that raises the most concerns from the perspective of cybercrime.

Content regulation is an essential part of fighting cybercrime since the unregulated or under-regulated Internet environment facilitates different infringements of intellectual property rights and provides extended access to various kinds of illegal or harmful information, including child pornography, hate speech, and terrorist propaganda.

Source: Authors.

The rationale for creating multi-sector regulators relates to the network structure of the sectors (many of which were at one time subject to monopoly control) that are regulated by these agencies.[143] Multi-sector utility regulators can be less flexible and ICT-oriented than converged or sector-specific regulators. However, due to the concerns related to critical information infrastructure protection and protection against cyber-attacks, multi-sector regulators are in a good position and hold the right competencies to play a central coordinating role as they typically regulate utilities that are considered to be part of national critical infrastructure. Consequently, the mandate of multi-sector regulators can often be extended to address cybersecurity and cybercrime on the basis of such regulators' responsibility to protect the critical infrastructures. On the other hand, however, these regulators are much less prepared to address content-related issues.

1.6.1.3 Areas of involvement

Since the ICT regulator must interact with all stakeholders involved with the functioning of the ICT sector, the regulator can be involved in many duties in almost every area that concerns addressing cyberthreats or cybersecurity. Although some fields or efforts are usually considered to be the domain of other governmental bodies, nevertheless the regulator's core competencies and its experience in international cooperation on ICT issues suggest that the ICT regulator could possibly be involved in many associated activities, for example as an advisory body. The activities include the following:

- Policy-making and developing policy approaches to address cyberthreats;
- Contributing to the development of cybercrime-related legislation and regulation;
- Detecting and investigating cybercrime incidents;
- Contributing to law enforcement activities;
- Facilitating national coordination to address cybercrime;
- Facilitating international cooperation to fight cybercrime; and
- Awareness raising and capacity building among industry and consumers.

Since the activities of the ICT regulator and the degree of intervention differ from country to country and depend on various factors such as the current mandate of the ICT regulator and the jurisdiction of other agencies, the nature of the participation of the ICT regulator in fighting cybercrime could be considered as an evolving process.

1.6.2 Role of the ICT regulator in policy making and policy approaches

Although the traditional concept of delegation of power within the state tries to separate policy making from policy implementation, it is nearly impossible to attain the complete independence of the ICT regulator from the ICT policy–making process.[144] ICT regulators in many countries play an important role in shaping the policies and strategies for ICT industry development. While the power of policy-making is traditionally granted to the higher level of governmental bodies, such as government ministries, the ICT regulator enjoys clear advantages with respect to the formation of ICT policy given its industry expertise and existing communication channels with other stakeholders.[145] In some countries, one of the main tasks of the ICT regulator is providing inputs to the ICT policy-making process.[146] It is quite likely that those ICT regulators will also be expected to provide input into the cybercrime policy-making process.

When the ICT regulator's mandate is extended to include cybersecurity and related issues, the regulator can be involved in the policy-making process by:

- Taking (or being given) the leading role in developing and shaping the policy approaches in areas that fall under its mandate (i.e., enforcement of regulations to ICT service providers; content), or
- Playing an advisory role by providing inputs into the development of policy, based on its expertise and competencies.

The input that regulators provide to cybercrime policy-making can constitute a step in the process of extending the mandate of ICT regulatory authority to address cybercrime. This was the case in Finland, for example. The Finnish government set up an Advisory Committee for Information Security (ACIS) under the Finnish Communications Regulatory Authority (FICORA) to develop the country's national information strategy.[147] The proposal released by ACIS in 2002 identifies goals and measures to promote the information security strategy, including measures that can be considered as cybercrime–related. The proposal also highlights the importance of the development and improvement of appropriate legislation, facilitating international cooperation, and increasing information security awareness among end-users.[148] The government decision empowers FICORA to act within the framework of implementing the strategy as the national information security authority with different responsibilities, including pursuing computer incident response (CERT/CSIRT) activities, supervising observance of the Act on the Protection of Privacy and Data Security in Telecommunications, and encouraging national and international cooperation.[149]

Degree of involvement:

ICT regulators can use their core competencies to offer help in shaping policy approaches and to provide specific input into the cybercrime policy-making process.

1.6.3 Role of the ICT regulator in developing cybercrime legislation and regulation

While the power to drafting and to formally adopt cybercrime statutes is the prerogative of legislators, analysis of country practices shows that the ICT regulator can play an important role in the process of cybercrime legislation enactment. Although ICT regulators in general are designed to regulate industry, meaning they are not typically familiar with criminal law, some domains exist where the ICT regulatory body can assist legislators. The areas where the regulator can be involved vary from country to country, depending on regulator's field of expertise. However, what can be seen is that ICT regulators mainly participate in developing or reviewing legislation when the data protection, data transmission, spam, and ISPs responsibilities are being considered.[150] As an entity that possesses technical knowledge, ICT industry expertise, and experience in conducting public consultations, ICT regulators can be involved in the process of developing cybercrime regulation by:

1) **Acting as an advisory body.** This is especially relevant for developing countries that have limited or no legislation to address cybercrime. When dealing with ICT network deployment, ICT regulators should also promote cybersecurity and deliver a clear message to other sector actors that the problems of illegal use of global networks can undermine the benefits that Internet can bring to society. An analysis of developing countries' experiences in the area of drafting cybercrime legislation shows that the ICT regulator can be responsible for facilitating the development of legal frameworks to address crime in cyberspace. Some examples are provided below.
    - The Ugandan Communications Commission has played an advisory role in the process of drafting cybercrime legislation by being involved in the multi-stakeholder National Task Force which was established in 2003 to formulate cybercrime-related laws. Moreover, the Ugandan National Task Force on cybercrime legislation is now part of a regional initiative called the East African Countries' Task Force on Cyber Laws which is dedicated to an ongoing process of development and harmonisation of cybercrime laws in the East African region.151
    - In Zambia, the Zambia Information and Communications Technology Authority (ZICTA, formerly CAZ) assisted in the activities of the National Working Group on Cybersecurity (NWG). This Working Group is in charge of drafting new cybercrime-related legislation[152], namely the Electronic Communications and Transactions Act 2009.[153] This Act assigns the ICT regulator the role of facilitating the creation of secure communications systems and net-

works; it also makes ZICTA one of the leading agencies with responsibilities for dealing with cybersecurity and cybercrime related issues.[154]

- The Nigerian Communication Commission participated in the Nigerian Cybercrime Working Group (NCWG) established in 2004 within the framework of the National Cybersecurity Initiative. One of the tasks of NCGW was the criminalization of cyber-infringements through the drafting of cybercrime-related legislation, namely the Computer Security and Critical Information Infrastructure Protection Bill.[155]

2) **Initiating reviews and amendments of cybercrime legislation within the regulator's area of expertise.** This opportunity is more relevant to countries with developed ICT networks, mature institutions dealing with cybercrime problems, and existing legislation to address the problem of cybercrime. The ICT regulator in this case deals with specific problems that emerge within its areas of competence such as the responsibilities of ISPs, blocking of harmful content, and data retention (see Box 1.5).

Degree of involvement:

Since the input that ICT regulators can provide into the development of legal frameworks depends on the current state of the cybercrime legislation in a particular country, it is very likely that the degree of intervention in this area will change once the initial bills are drafted and approved.

1.6.4 Role of the ICT regulator in detecting and investigating cybercrime incidents

As the ability to monitor, detect, analyze and investigate cyberthreats and cyber-incidents is a critical element in fighting cybercrime, the need to enhance the ability to respond promptly and properly to computer incidents have led to the creation of Computer Incident Response Teams (CIRTs) both at the national and international levels. Due to the multi-sector nature of cybercrime, different CIRTs have been established by a range of stakeholders, including governments, businesses, telecommunication operators, and academia, to fulfil various functions.

ICT regulators in both developed and developing countries can be responsible for creating, running and supervising national CIRTs. These CIRTs are usually considered the main entities responsible for detecting and investigating cybercrime incidents at the national level and key participants in enhancing cybercrime cooperation at the international level.

One of the first CIRTs established as an initiative under an ICT regulator was the Finnish national Computer Emergency Response Team, launched in January 2002 under the auspices of the Finnish Communications Regulatory Authority (FICORA).[156] Today, more ICT regulators have created CIRTs with national responsibility for monitoring and detecting cyberthreats, reacting to cybercrime and cybersecurity incidents and investigating them. (See Box 1.6 below.)

Degree of involvement:

If the decision to create a CIRT under the umbrella of the ICT regulator has been taken, the regulator could exercise this mandate by maintaining the activities of CIRT and collaborating with other stakeholders in this area.

Box 1.5: Reviewing cybercrime-related regulation in Belgium

In 2006, the Belgian ICT regulator (BIPT) was involved in the amendment of some specific areas of cybercrime legislation. BIPT had detected the necessity of amending the data retention legislation and prepared a draft transposition of an EU directive related to data retention into Belgian national law. The draft amendments were developed in cooperation with the Federal Public Service of Justice and the Federal Computer Crime Unit. During the development process, the draft passed public consultation. In addition, in 2008, BIPT announced that it was considering the possibility of rephrasing the legal provisions with respect to privacy in the electronic communications sector.

Source: Annual report 2008 of the Belgian Institute for Postal Service and Telecommunication[157]

Box 1.6: CIRTs under the umbrella of the ICT Regulator

- **Sweden** - Sweden's IT Incident Centre (Sitic) is located in the ICT Regulator PTS.[158]
- **United Arab Emirates** - aeCERT created as initiative of UAE Telecommunications Regulatory Authority to detect, prevent and respond to the current and future cybersecurity incidents in the UAE.[159]
- **Zambia** - Zambia CERT was initially a project of Zambian Information and Communication Technology Authority, supported by the ICT Regulator, ITU, and COMESA.[160]
- **Qatar** - National CERT (qCERT) was established by and acts on behalf of the Qatari ICT Regulator (ictQatar).[161]

1.6.5 Role of the ICT regulator in law enforcement

The involvement of the ICT regulator in the enforcement of laws related to cybercrime requires a clear legal mandate granted to the regulator to exercise and enforce particular legal provisions. While in some countries government departments or agencies dealing with traditional criminal offenders were assigned the lead role in dealing with cyberthreats such as online fraud, identity related crimes and child pornography, the ICT regulators are increasingly being granted law enforcement powers in cybercrime-related areas such as anti-spam laws enforcement, content regulation, or enforcing co-regulatory measures.

1) Under the mandate of **anti-spam law enforce-ment,** some European ICT regulators are already part of a contact network of anti-spam enforcement authorities established by the European Commission in 2004 to fight spam on a pan-European level.[162] At the global level, many ICT regulators are listed as contact points for enforcement agencies in the OECD Task Force on spam.[163] As the law enforcement body responsible for spam regulation, ICT regulatory authorities can co-operate closely with other law enforcement agencies. For instance, there are cooperation agreements between ICT regulators and hi-tech crime police units in the Netherlands and Romania.[164]

Box 1.7: The ICT regulator as a law enforcement body: Spam regulation and malware

Australia

The Australian Communications and Media Authority (ACMA) is responsible for enforcing the 2003 Spam Act which prohibits the sending of 'unsolicited commercial electronic messages' with an 'Australian link'. A message is seen as having an 'Australian link' if it originates or was commissioned in Australia or originates overseas but was sent to an address accessed in Australia. In the case of a breach of the Spam Act, ACMA can take any of the following enforcement actions:[165]

- Issue a formal warning.
- Accept an enforceable undertaking from a person or company. Undertakings usually contain a formal commitment to comply with the requirements of the Spam Act that ACMA has found person or company has breached. A failure to abide by an undertaking can lead to the ACMA applying for an order in the Federal Court.
- Issue infringement notices.
- Seek an injunction from the Federal Court to stop a person sending spam.
- Prosecute a person in the Federal Court.

The Netherlands

In addition to being the enforcement agency for addressing spam, the Dutch Independent Post and Telecommunications Authority (OPTA) is the designated enforcer of a malware ban in the Netherlands.[166] OPTA imposes fines in the case of malware and spyware dissemination. For instance, in 2007 OPTA imposed a fine totalling 1 million Euro on three Dutch enterprises operating under the name of the biggest spyware distributors in the world for illegally installing spyware and adware on more than 22 million computers in the Netherlands and elsewhere.[167]

2) **Content regulation** is the area where converged ICT regulators can exercise a mandate in the area of law enforcement. For example, ACMA, the Australian ICT regulator, administers a national regulatory scheme that includes the investigation of complaints about prohibited online content and mobile phone content. ACMA has the power to direct the content service provider to remove or prevent access to the content hosted in Australia[168].

3) Some ICT regulators consider the power to impose and monitor cybersecurity requirements within the industry as a future **mandate for implementing and enforcing co-regulatory measures**. For example, the Korea Communications Commission (KCC), the broadcasting and telecommunications regulator, and the Korea Internet and Security Agency (KISA) were planning to have ISPs monitor the security levels of the computers and other devices used by customers. The suggested solution was to limit or cut the Internet connectivity of users with less-than-required software protection to force them to upgrade their existing programs or install new ones.[169]

   In a similar way, ZICTA announced that it is taking measures to punish ISPs that continually fail to provide security measures for their Internet services after Zamnet's operations were paralyzed by hackers. In 2009, ZICTA was considering reviewing licence conditions for all ISPs in order to ensure that they are effectively prepared to protect their customers.[170]

The degree of intervention by the ICT regulator in law enforcement can only be determined at the higher decision-making level of the national government. The challenge for ICT regulators is to strike the right balance in maintaining the idea that ICT sector stakeholders all share responsibility for network protection. In this regard, care should be taken to avoid targeting ISPs alone with strict obligations related to network protection.

Degree of involvement:

Regulators should bear in mind that it is better to avoid over-regulation in fields where less enforcement would suffice and should also to try to find the areas for shared responsibility for cybersecurity rather than impose and enforce strict requirements on a narrow set of actors.

1.6.6 Role of the regulator in facilitating national coordination

If the ICT regulator has developed mechanisms for cooperating with industry players, it can play a lead role in organizing various forms of partnerships between public agencies and private actors to deal with cybercrime.

Efforts by ICT regulatory bodies to facilitate national coordination and cooperation on cybercrime-related issues may focus on specific cyberthreats. For example, in 2008 the Japanese multi-sector Ministry, the Ministry of Internal Affairs and Communications (MIC), launched an Anti-Bot Project in collaboration with Ministry of Economy, Trade and Industry (METI) to promote a prompt and effective approach to stopping cyber attacks by bot-program-infected computers.[171] The Cyber Clean Centre (CCC), the operating body established for the project, analyzes the characteristics of bots and provides information on the disinfestations of bots from users' computers. In addition, the Cyber Clean Centre is the main organization responsible for promoting bot cleaning and preventing the re-infection of users' computers. This work is done in cooperation with ISPs.[172] When the ICT regulator can identify its capability and has interest in addressing specific problem, such ad-hoc partnerships can be established in the any area of regulator's competence.

When the responsibility for facilitating national coordination has not yet been delegated to one specific national body, the ICT regulator can support the wide range of the efforts undertaken at the national level. For example, since NWG's creation in 2008, ZICTA acts as a coordinator of different efforts to fight cybercrime at the national level. It has coordinated stakeholders on national level for a range of different actions to address cybercrime – from capacity building to implementation of legal frameworks.[173]

In the capacity as mediator between government agencies and industry players, the ICT regulator can play a significant role in coordinating child protection initiatives such as the Child Online Protection (COP) initiative launched by the ITU in order to address legal, technical, organizational and procedural issues and to engage in capacity building and international cooperation.[174]

ITU's call for action for all stakeholders (policy makers, regulators, operators and industry) to promote the adoption of policies and strategies that will protect

children in cyberspace and promote their safe access to online resources, at the 2009 World Telecommunication and Information Society Day made under the COP initiative, exemplifies how the ICT regulator can help to coordinate national stakeholders' efforts in child online protection:[175]

- Creation of public awareness on the issues related to protecting children in cyberspace, identification of policies, best practices, tools and resources for adaptation/use on national level.
- Support for ongoing work aimed at developing guidelines on protecting children online for policy makers and regulators.
- Identification of risks to and vulnerabilities of children in cyberspace as the Internet and other online resources continue to expand.
- Build resource repositories for common use.
- Promote capacity building aimed at strengthening global response in protecting children as they venture into cyberspace.

The experience gained by the ICT regulator from participating in such initiatives (see Box 1.8) can further be leveraged in other areas of collaboration at the national level.

Though the coordination of national stakeholders is usually undertaken by governmental institutions at a higher level of decision-making, there are instances when the ICT regulator is the only body at the national level that can initiate, facilitate, and coordinate the national initiatives. Even when such initiatives are started from scratch and are eventually taken over by another entity, the ICT regulator would still be likely to have a solid contributory role in national coordination.

Degree of involvement:

When the ICT regulator can coordinate national efforts on specific issues related to cybercrime such as spam and child online protection, this effort should be encouraged.

1.6.7 Role of the regulator in facilitating international cooperation

ICT regulators have a long record of being involved in a range of activities at the international level,[176] especially with regard to the ITU standardisation efforts[177] and also through the activities of regional organisations such as the European Commission, APEC[178], the BEREC (formerly the European Regulatory Group)[179], and the Arab ICT Organisation[180].

Box 1.8: Child Online Protection: Example of how national efforts are coordinated to contribute to a global appeal

Australia – ACMA Cybersafety Program includes:

- An 'Internet Safety Awareness' presentation on the risks faced by children online and effective strategies for helping to keep young people safe online;
- 'Professional Development Programs for Teachers' on how children use technology, digital literacy, cyberbullying, identity protection, and the legal responsibility of schools to minimise risk; and
- 'Cybersmart Detectives' events for primary school age children.

Indonesia – Activities of the Directorate General of Posts and Telecommunications, Ministry of Communications and Information technology include:

- Conducting socialization in schools and workshops featuring the theme of applying healthy, safe and wise internet;
- Internet publications on the theme of 2009 WTISD *Protecting children in cyberspace;* and
- Gathering around 500 representatives of regulators, telecommunication operators and other actors in telecommunication community, as well as concerned society for WTISD 2009 on 17 May 2009 to demonstrate the using of healthy and safe Internet for children.

Suriname - Activities of the Telecommunications Authority Suriname (TAS) include:

- Participation in an annual 4 day walk through the streets of Paramaribo promoting the theme;
- A 15 minute film to alert the youth of the possible dangers on the Internet; and
- Administering the course: "Diploma Veilig Internet" (Diploma Safe Internet).

Source: ITU WTISD 2009: Worldwide Initiatives[181]

Such ongoing involvement and familiarity with the process of cooperation at different levels – national, regional and global – provides the ICT regulator with valuable experience to contribute to the process of responding to the truly international nature of cybercrime. In facilitating international cooperation, ICT regulators can either:

- Cooperate on the international level in some cybercrime related fields in the exercise of their own mandates, such as consumer protection or spam legislation enforcement (such as activities supported by the London Action Plan, a platform established in 2004 for international public-private cooperation on spam enforcement and addressing spam-related problem,[182]) or
- Facilitate regional and global efforts for addressing cyberthreats by being involved in different groups that take part in international cooperation. Examples include the collaboration among Kenya, Tanzania and Uganda within East Africa Communications Organization (EACO, formerly EAPRTO) (See Box 1.10).

As international (e.g., ITU) and regional (see Box 1.9) organizations are increasingly turning their attention to the issue of cybercrime, it is very likely that ICT regulators will start becoming directly involved in international cooperation in this field. ICT regulators can also raise the problem of cyberthreats through existing mechanisms for international cooperation within the ICT industry such as the Independent Regulator's Group (IRG)'s Informal working group for IT security that listed cybersecurity as a priority issue at the suggestion of Danish ICT regulatory authority in April 2004.[183] This group is also cooperating and exchanging experiences with ENISA and other international organisations.[184] This creates the platform for further international collaboration – both within the ICT sector and on the cross-sector level.

As mentioned above, a platform for global cooperation is provided by the ITU Global Cybersecurity Agenda[185], which is designed to enhance cooperation and efficiency based on existing initiatives to avoid duplicating efforts. It has already fostered projects such as the Child Online Protection initiative and, with the support of leading global players, is currently deploying cybersecurity solutions to countries around the world.[186]

Box 1.9: International cooperation on cybersecurity and cybercrime: APEC

APEC is an inter-governmental, non-binding organization consisting of 21 Member States in the Asia-Pacific. Since the development of the APEC Cybersecurity Strategy in 2002, the Telecommunication Working Group (APEC-TEL) has focused on fulfilling the strategy's goals on combating cybercrime and maintaining cybersecurity.[187]

As a part of strategic cooperation, APEC also pursues collaboration on cybersecurity and cybercrime issues with other international and regional organizations such as ITU, OECD, and ASEAN.[188] Due to the involvement of regional ICT regulators, APEC can be considered to be a prospective platform for regional cooperation that gives ICT regulators a more evolving role in addressing cybercrime.

Box 1.10: Harmonisation of cybercrime efforts in the East African region: EACO

Kenya, Tanzania and Uganda collaborate within EAPRTO, the East Africa Regulatory, Postal and Telecommunications Organization (now East Africa Communications Organization (EACO)).[189] This organization aims to promote confidence and security in the use of cyberspace in the East Africa (EA) region[190] through collaboration amongst all the stakeholders, including ICT regulators, by facilitating regional coordination, implementing the appropriate cybercrime legislation, developing and harmonizing cybercrime legislation on East Africa regional level, and establishing National CERTs; regional and international partnerships.

The EACO Cybersecurity Taskforce can be considered to be an inter-regional platform for collaboration as it cooperates with EU countries. For example, in December 2009 members from Kenya and Tanzania participated in benchmarking visits to CERT-FI and CERT-Hungary in order to share experience and in an effort to develop relevant frameworks for the establishment of national CERTs.

Degree of involvement:

The increasing participation of ICT regulators in different international initiatives is likely to develop further in the future. This suggests an evolving role for ICT regulators in addressing cybersecurity and managing cyberthreats on an international basis. International organizations increasingly offer opportunities for ICT regulators to contribute to and facilitate international cooperation regionally and globally.

1.6.8 The role of the regulator in building capacity to address cyberthreats within the ICT industry and among end ICT-users

As one of the key actors in the ICT industry, the regulator can focus some of its efforts on building capacity and raising awareness on cyberthreats among end-users and ICT industry players. Raising awareness among end-users flows naturally from the consumer protection mandate of ICT regulators. Extending the regulator's mandate to include raising awareness about cyberthreats leverages some of the regulator's core competencies and eventually allows these competencies to be mobilized in the fight against cybercrime. Efforts to raise awareness may include organizing various campaigns and distributing useful consumer information through different channels. In order to optimize the outcome of awareness-raising campaigns, it is important that the ICT regulator has the means to receive end-users' feedback. The ability to receive such feedback allows to monitor how effectively information about cybersecurity and cybercrime is received and understood by the general public, as well as to identify areas where more efforts to educate the public are required.

Many regulators already have undertaken responsibility for building user awareness about cybercrime. Awareness-raising activities are largely focused on providing customers with guidelines and tips to help them avoid becoming victims of cybercriminals. In addition, regulators can provide timely warnings about new and emerging threats, such as viruses, malware, and other vulnerabilities of the end-user. Examples of how regulators are engaged in providing such warnings to the public as part of their responsibility to build awareness of cybercrime-related issues among the public include:

- In Finland, CERT-FI, which functions as the national Finnish Computer Emergency Response Team under the Finnish Communications Regulatory Authority (FICORA), publishes warnings about cybercrime threats aimed at increasing awareness among Internet users. One example of CERT-FI's activities is the CERT-FICORA memorandum on data-stealing malware, which was issued in 2010. This memorandum includes general guidelines on the procedures users may apply in order to prevent data theft and procedures for data theft victims; the memorandum aims to increase the overall awareness of users about cybercrime and to share information on useful tools with stakeholders.[191]
- The Belgian ICT regulator BIPT provides consumers with information and alerts on the latest viruses and critical vulnerabilities.[192] In addition, it has also come out with "general public" user guidelines intended to describe some of the IT risks, possible remedies and preventive measures that users can adopt to avoid becoming victims of cybercriminals.[193]
- In 2009, the United Kingdom's ICT regulator Ofcom became one of the sponsors of the cross-sector online safety initiative, GetSafeOnline.org. This initiative was established to provide a source of unbiased, user-friendly advice about online safety to UK consumers and small businesses. Since its inception, it has operated as a joint initiative between the government, the Serious Organised Crime Agency (SOCA), and private sector sponsors from the retail, technology and finance sectors.[194] Its role in GetSafeOnline.org forms part of Ofcom's wider media literacy strategy designed to provide citizens with confidence to use communications technologies effectively and safely.[195]

The ICT regulator's ability to dialog with industry players makes it also well-suited to undertaking capacity building within the ICT industry. In this role, the regulator can encourage private sector stakeholders to implement measures to protect industry itself and consumers against cybercrime. This could include encouraging industry players to establish voluntary codes of conduct (see Box 1.11) or to adopt technical requirements that help preventing cybercrime. It may also include promoting the adoption of best practices and international security standards.

Degree of involvement:

As the responsibilities for awareness raising and capacity building fall under the general domain of consumer protection, if these responsibilities are not already assigned to another national player, there are benefits to assigning these responsibilities to the ICT regulator. Of course, the degree of intervention and/or participation will vary, depending on the ability to leverage core regulatory competencies to the cybercrime issues.

Box 1.11: User awareness and capacity building in Australia

ACMA, the Australian ICT Regulator, is involved in several initiatives aimed at raising awareness and building capacity among different stakeholder groups:

1. The 'Cybersmart' initiative[196]: a national cyber-safety education program managed by ACMA, as part of the Australian government's commitment to promoting online safety for children and young people.
2. Australian voluntary E-Security Code of Practice[197]: the Code has been developed by Internet Industry Association (IIA) with input from the ACMA and the Department of Broadband, Communications and the Digital Economy. The E-Security Code of Practice is intended to provide guidelines for ISPs related to the delivery of consistent messages to their customers when ISPs receive compromise reports from ACMA and to adopting consistent approaches to customers who do not take remedial action when they are notified of a compromise.
3. Australian Internet Security Initiative (AISI)[198]: this initiative was launched to help address the emerging e-security threat posed by networks of 'zombie' computers. ACMA developed the AISI software and obtained the support of ISPs to enable its operation. AISI helps fight against spam and related e-security threats and provides information to participating Australian ISPs about 'compromised' computers residing on their networks.

1.7 Summary of findings and conclusions[1]

1.7.1 Maintaining a balanced approach to ICT regulation

While it is generally recognized that ICT regulators should maintain a balanced approach to regulation to ensure sound development of the sector and to meet social goals, in practice, this is never an easy task. This is especially true when it come to devising a sound strategy and national approach to fight the growing number of offenses in cyberspace. The battle against all forms of cybercrime requires immediate attention from all relevant actors in the cybercrime ecosystem, including the ICT regulator, and close collaboration and coordination among relevant parties. Analysis shows that innovative approaches to fighting cybercrime adopted by the ICT regulator can have a positive impact on end-users' trust and confidence, which underpins the development of today's digital society and economy. Given the potential implications of cybercrime and threats to cybersecurity for the uptake of ICT services by citizens, businesses, and governments in developing countries, ICT regulators can be a key stakeholder in developing and implementing national strategies to respond to cybercrime.

Looking back some ten years, cybercrime was rarely addressed in the legal and regulatory frameworks governing the ICT sector. Integrating cybercrime-related offenses into either telecommunication/ICT legislation or national criminal laws is thus a fairly recent practice. Implementation mechanisms, including the assignment of clear roles and responsibilities to the different stakeholders involved, would surely facilitate the work that countries must undertake to fight against cybercrime. There is no one model for developing a legal and regulatory cybercrime framework. While countries have begun to respond to cybercrime, insufficient time has elapsed to assess the relative strengths and weaknesses of various approaches. In the past, important reforms in the telecommunication sector have been introduced through piecemeal legislative amendments over a period of time and through major reforms of the telecommunication regulatory framework that featured the introduction of entire new pieces of legislation. The latter, more radical approach may prove to be the most practical for responding to cybercrime since it would allow for a common, coherent approach to the full range of current issues facing the sector today and a single, consistent legal point of reference with regards to available means and tools for regulating the sector.

As noted in this paper, in addition to general telecommunication/ICT laws and other sector-specific legislation, ideally a legal framework for fighting cybercrime should include updated criminal legislation, criminal procedural legislation, legislation for international cooperation, and specific legislation to deal with cybercrime-related issues, such as data protection legislation, ISP liability legislation, at a minimum. It should be noted that although criminal law is an essential component of legal frameworks aimed at fighting cybercrime, these frameworks are not limited to criminalization. Some forms of cybercrime can be addressed effectively through use of non-criminal legal and regulatory sanctions, such as the deactivation of domain names used by a botnet.

Regardless of the approach adopted to creating a legal and regulatory framework to respond to cybercrime, the challenge will remain the same. These frameworks must be flexible and forward-looking so that they do not quickly become outdated by the rapid pace of change in the sector. At the same time, they should offer sufficient structure and certainty in how offences and sanctions are defined to enable effective investigations, prosecutions, and conviction of cyber criminals. Of course, telecommunication/ICT regulators have always had to strike such delicate balances. Regulators must provide the sector with certainty without inhibiting growth and innovation; they must protect and encourage investment in the sector while simultaneously protecting consumers and ensuring that ICTs serve a multitude of socially desirable ends. At the present, the task of the ICT regulator is to strike these delicate balances in a nimble way given the rapid pace of technological innovation and the exponential growth of the variety, sophistication, and impact of offenses in cyberspace. In this regard, ICT regulators have recourse to a variety of tools and mechanisms that can be used alone or in combination to address this issue. Not the least of these tools and mechanisms is the involvement of industry itself, as well as end-users and other stakeholders, to play central roles in the cybercrime regulatory framework. In the cybercrime ecosystem, maintaining a balanced approach to ICT regulation increasingly involves balancing interest among the actors who are engaged in the battle against cybercrime. As this paper has argued, ICT regulators are well-placed to actively contribute to efforts to bring stakeholders together in cooperative and coordinated responses to cyberthreats.

1.7.2 Future challenges and future roles for ICT regulators

This paper concludes by outlining some of the challenges facing ICT regulators and the roles that these challenges may create for regulators. These challenges can broadly be grouped into the following categories: general challenges related to the nature of cybercrime; the existence of "safe havens" for cybercriminals; content regulation; inter-agency cooperation and concurrent jurisdiction over the Internet; degree of regulatory intervention; and maintaining the separation of powers and regulatory independence.

One of the biggest issues for ICT regulators and other stakeholders involved in responding to different kinds of offenses and threats in cyberspace is the rapid pace of change in the ICT sector and in technology itself. The types of cyber offences and the manner in which cybercrime is perpetrated continues to evolve rapidly. Moreover, as noted above, cyberthreats are growing in variety, sophistication, and so is their impact. The Internet itself has grown significantly in importance over the past ten years and its importance is unlikely to diminish going forward. In this environment, the role of ICT regulators evolve and their involvement should respond to the specific needs of the national ICT ecosystem, and especially of users and the industry. ICT regulators often share the heavy responsibility of ensuring the reliability of the Internet and avoiding disruptions to its current and future uses by consumers, businesses and governments that may result in significant loss to the community and/or economy. Discharging this responsibility requires the ICT regulator to be capable of acting quickly to respond to cyberthreats and suggests that there is a high value to adopting preventative measures. As the ICT regulator's mandate continues to evolve, it will be crucial to ensure that the regulator is equipped with the tools and resources necessary to detect cyberthreats, to engage in awareness raising among all stakeholders, to mobilize particular stakeholders to play their roles in fighting cybercrime, to coordinate its responses with authorities from the public and private sector, and to contribute to fostering cooperation and coordination between countries and across regions.

The general challenges associated with cybercrime are compounded by the existence of "safe havens" for cyber criminals. The international nature of cybercrime allows cyber criminals to exploit the existence of countries that do not have the necessary regulatory frameworks, laws, and related enforcement capability in place to police cybercrime effectively. The ICT regulator has several important roles to play in an environment that is prepared to deal with cybercrime and that has harmonised cybercrime legislation, trained police and law enforcement officials, a national computer incident response team, and a well coordinated national strategy. However, in countries where this capacity has not yet been developed, the ICT regulator has a role to play to help the country develop and put in place the required capabilities to begin to respond to cybercrime. The regulator can leverage its technical knowledge of the ICT sector, its connections with industry stakeholders, its experience in dealing with other government agencies, and its regional and international ties to facilitate the development and implementation of a national strategy that is coordinated and harmonized with regional and international approaches.

Convergence has already forced ICT regulators to begin to grapple with content regulation, which has lead to the establishment of a number of converged regulators in all regions. Cybercrime presents regulators with a new dimension of content regulation: the existence of harmful or offensive content on the Internet. The establishment of a converged ICT regulator can help to avoid unequal intervention in regulating content delivered over various platforms. Moreover, a converged regulator combines expertise in content with expertise in carriage of such content. In this regard, the converged regulator is well-placed to tackle cybercrime related to harmful content and can prevent the duplication of efforts related to protecting consumers and fighting illegal or harmful content.

The cybercrime ecosystem is complex and often involves overlapping mandates of various regulatory agencies. Moreover, as discussed above, there is a pressing need to engage a variety of stakeholders, from industry to end-users to academia to government, in coordinated and cooperative efforts to fight cybercrime. In this context, questions arise about how to manage overlapping mandates and which agencies should take the lead in regulating various aspects of the Internet and online activities. For example, one should ask which agency or agencies (ICT regulator, financial regulator, data protection agencies, general consumer protection agency, privacy commissioners, and so forth) should regulate services such as e-commerce, e-learning, mobile- and e-banking, as well as how they could do undertake these responsibilities, and whether or not there is a need for cross-sector regulation. Since ICT regulators have jurisdiction over electronic communications networks, they will almost certainly be involved in one way or another in any national strategy to respond to cyberthreats. ICT regulators must work to ensure that they coordinate their efforts with other agencies and may even take the lead in shaping cross-sectoral cybercrime strategies.

Issues surrounding concurrent jurisdiction raise important questions about the degree of regulatory intervention in the ICT sector. Concerns arise when two areas of regulation – one with less intervention and another which is more heavily regulated – are merged since the outcome may be that both areas are ultimately regulated more strictly. This can happen even where the underlying intention was to decrease the level of intervention, as was the case with the transfer of existing telecommunication regulation to the Internet arena.[199] In the context of responding to cybercrime, there is a risk that cross-sectoral and coordinated responses to cybercrime will ultimately result in a much higher level of regulation over the Internet than is ideal for promoting ongoing investment and innovation in the ICT sector. Despite ongoing discussions about the necessity of self-regulation and co-regulation, some fields tend to be regulated with the maximum degree of intervention because of the criminal component of cybercrime. A future challenge will be to maintain balance in regulation, as the development of smart regulatory approaches will determine areas where it is reasonable to make regulation stricter while avoiding overregulation and unnecessary intervention in other areas.

There are also concerns that a leading role for the ICT regulator in the fight against cybercrime may undo the separation of power and undermine regulatory independence by bringing the regulator closer to either the government or industry. This issue is especially relevant where the mandates of other stakeholders in this area have not yet been clearly defined or when the ICT regulator is involved as a leading actor in cybersecurity policy making, the development of cybercrime legislation, or law enforcement. However, the analysis of practices in such countries as Finland suggests that once a general strategy to fight cybercrime has been developed and once ICT regulator's mandate within that strategy is established, a separation of power can still be maintained and regulatory independence safeguarded. Nonetheless, this issue should be always taken into account when assessing the responsibilities of ICT regulator in fighting cybercrime.

A credible ICT regulatory framework that protects consumer interests, but also those of the public and investors, operators, and service providers, remains a key requirement going forward. Regulators must grapple with crumbling consumers trust in ICTs and telecommunication services due to concerns about privacy, security, and fraud, as well as industry players that are occupied with attempting to make convergence in the market place work for them. At the same time, governments are seeking to engage public and private stakeholders in close partnerships to respond to growing ICT needs and expectations amongst consumers and businesses. In this context, the need both for functioning regulatory institutions and viable cooperation among stakeholders has never been stronger.

[1] Sections 1.1, 1.5 and 1.7 of this paper were written by Christine Sund and Youlia Lozanova, BDT/ITU.

[2] This paper intends to provide ICT stakeholders with a greater understanding of the evolving cyberthreats and criminal offences in cyberspace. It builds on a GSR09 background paper on "Cybersecurity: The Role and Responsibilities of an Effective Regulator", available at: http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf

[3] Sections 1.2 and 1.3 of this paper were written by Dr. Marco Gercke, Cybercrime Research Institute.

[4] ITU-T Recommendation X.1205, "Overview of Cybersecurity". Also see ITU, List of Security-Related Terms and Definitions, online: www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

[5] See e.g. ITU WTSA Resolution 50: Cybersecurity (Rev. Johannesburg, 2008), online: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52: Countering and combating spam (Rev. Johannesburg, 2008), online: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45: Mechanism for enhancing cooperation on cybersecurity, including countering and combating spam (Rev. Hyderabad, 2010), online: www.itu.int/publ/D-TDC-WTDC-2010/en; European Union Communication, "Towards a General Policy on the Fight Against Cyber Crime" (2007), online: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf; National Science and Technology Council, President's Information Technology Advisory Committee (U.S.), "Cyber Security: A Crisis of Prioritization" (2005), online: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

[6] See Heise News, 04.01.2005, available at: www.heise.de/newsticker/meldung/54746http://www.heise.de/newsticker/meldung/54746; BBC News, Sasser net worm affects millions, 04.05.2004, available at: http://news.bbc.co.uk/1/hi/technology/3682537.stmhttp://news.bbc.co.uk/1/hi/technology/3682537.stm.

[7] *Yeo*, Lack of cybercrime laws impedes Asia's cross-border efforts?, available at: www.zdnetasia.com/lack-of-cybercrime-laws-impedes-asia-s-cross-border-efforts-62040170.htm.

[8] *ITU,* Cybersecurity Guide for Developing Countries. ITU, 2009, available at: www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf.

[9] *ITU,* Cybersecurity Guide for Developing Countries. ITU, 2009, available at: www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdfhttp://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf.

[10] *ITU*, Cybersecurity Guide for Developing Countries, Edition 2007; *Cieslikowski*, Key Trends in ICT Development; *Hafkin*, Gender Issues in ICT Policy in Developing Countries: An Overview http://old.apc.org/english/capacity/policy/mmtk_gender_ictpol_hafkin.pdfhttp://old.apc.org/english/capacity/policy/mmtk_gender_ictpol_hafkin.pdf

[11] *Schjølberg/Ghernaouti-Hélie*, A Global Protocol on Cybersecurity and Cybercrime – An initiative for peace and security in cyberspace. Cybercrimedata, 2009; *ITU,* Cybersecurity Guide for Developing Countries. ITU, 2009, available at: www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdfhttp://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf.

[12] This is however a broad definition. There is no single definition of cybercrime. For an overview of the various offences that fall within the definition of "cybercrime", see Box.1.

[13] *ITU*, Cybersecurity Guide for Developing Countries. ITU, 2009.

[14] For more information on the ITU Global Cybersecurity Agenda (GCA), see: www.itu.int/cybersecurity/gca/.

[15] The seven goals of the GCA are: 1) Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures. 2) 2Elaboration of global strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime. 3) Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for hardware and software applications and systems. 4) Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives. 5) Development of global strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials across geographical boundaries. 6) Development of a global strategy to facilitate human and institutional capacity building to enhance knowledge and know-how across sectors and in all the above-mentioned areas. 7) Proposals on a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

[16] For more information see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[17] *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141, for an overview on the most important substantive criminal law provisions.

[18] *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, 245 et. Seqq.

[19] For example, to use the anonymous communication services. See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999; Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 et seqq., available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

[20] *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289, available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension - in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et seq., available at: http://media.hoover.org/documents/0817999825_1.pdf.

[21] *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol 9, page 451 et seq., available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.pdf.

[22] *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141.

[23] *Bruce, at al*. TNO Report. International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues. 2005.

[24] See more about consumer protection as an ICT regulatory concern: Trends in Telecommunication Reform 2009. Hands-On or Hands-Off? Stimulating Industry Growth through Effective ICT Regulation. Summary, 2009, available at: www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.11-2009-SUM-PDF-E.pdf.

[25] See more about this trend: *Macmillian*, Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf; *Stevens*, Consumer Protection: Meeting the expectation of connected Consumer. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Consumer-protection_Stevens.pdf.

[26] ITU Cybersecurity Gateway. Civil Society, available at: http://groups.itu.int/Default.aspx?tabid=933&language=fr-FR.

[27] Regarding approaches to define and categorise cybercrime see for example: Cybercrime, Definition and General Information, Australian Institute for Criminology, available at: www.aic.gov.au/topics/cybercrime/definitions.html; Explanatory Report to the Convention on Cybercrime, No. 8. *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf.

[28] *Levy*, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: www.aic.gov.au/publications/htcb/htcb005.pdf.; *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, 2001, page 61.

[29] According to HackerWatch statistics, on the 23rd of April, 2010, 195,000,000 incidents were reported for the last 30 days. Source: www.hackerwatch.org.

[30] Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2003, page 1, available at: www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf.

[31] Botnets is a short term for a group of compromised computers running programmes that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf.

[32] The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails were spam. See: www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf.

[33] *Johnson/McGuire/Willey*, Why File-Sharing Networks Are Dangerous, 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf.

[34] Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf.

[35] *Stevens*, Rosalind, Consumer Protection: Meeting the expectation of connected Consumer. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Consumer-protection_Stevens.pdf.

[36] See *OPTA*. Joint ruling of the CBP (Dutch Data Protection Authority) and OPTA (Independent Post and Telecommunications Authority) concerning "tell-a-friend systems" on websites. 2004.

[37] ITU WSIS Thematic meeting on countering spam. Spam in the Information Society: Building frameworks for international cooperation.

[38] OECD, Spam Issues in developing countries. 2005.

[39] ITU WSIS Thematic Meeting on Countering Spam CICG, Geneva, 7–9 July 2004.

[40] ITU WSIS Thematic Meeting on Countering Spam CICG, Geneva, 7–9 July 2004.

[41] ITU ICT Eye, at: www.itu.int/ITU-D/icteye/.

[42] See Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

[43] See, e.g. *Rash, et al.* Crime Online. Cybercrime and Illegal Innovation. NESTA. Research Report. July, 2009.

[44] *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9.

[45] In order to limit the availability of such tools, some countries criminalise the production and offer of such tools. An example of such a provision can be found in Art. 6 of the European Convention on Cybercrime.

[46] *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006.

[47] *ITU/Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU 2009, page 75.

[48] For a brief history of the Internet, including its military origins, see: *Leiner/Cerf/Clark/Kahn/Kleinrock/Lynch/Postel/ Roberts/Wolff*, A Brief History of the Internet, available at: www.isoc.org/internet/history/brief.shtml.

[49] *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

[50] Regarding filter obligations/approaches see*: Zittrain/Edelman*, "Documentation of Internet Filtering Worldwide", available at: http://cyber.law.harvard.edu/filtering/, and Reidenberg, "States and Internet Enforcement" (2004) 1 University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 et. Seq.

[51] National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1.

[52] *Putnam/Elliott,* International Responses to Cyber Crime, in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 et seq; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et seq.

[53] See *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16.

[54] See: Lewis, Computer Espionage, Titan Rain and China, page 1, available at: www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf.

[55] Bruce, at al. TNO Report. International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues. 2005.

[56] ITU. Cybersecurity Guide for Developing Countries. ITU, 2009. Page 5.

[57] This issue was addressed by a number of international organisations. The UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the Resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies".

[58] *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 et seqq., available at: www.212cafe.com/download/e-book/A.pdf.

[59] The Online-Community HackerWatch publishes regular reports on hacking attacks. Based on their sources, more than 250 million incidents were reported in only one month (August 2007). Source: www.hackerwatch.org.

[60] Nearly 50% of all fraud complains reported to the United States Federal Trade Commission are related to a amount paid between 0 and 25 USD. See Consumer Fraud and Identity Theft Complain Data – January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

[61] Regarding the attacks, see: *Lewis*, Cyber Attacks Explained, 2007, A cyber-riot, The Economist, 10.05.2007, available at: www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163598; Digital Fears Emerge After Data Siege in Estonia, The New York Times, 29.05.2007.

[62] See: *Toth*, Estonia under cyber attack, www.cert.hu/dmdocuments/Estonia_attack2.pdf; *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, page 3.

[63] See Emerging Cybersecurity Issues Threaten Federal Information Systems, GAO, 2005, available at: www.gao.gov/new.items/d05231.pdf.

[64] *Keizer*, Duch "Botnet Suspects Ran 1.5 Million Machines", TechWeb, 21.10.2005.

[65] Whether a particular ICT regulator will have responsibility for cyber security and consumer protection depends on the legislative framework governing the ICT regulator in the country in question. Most ICT regulators have been assigned responsibility for these matters.

[66] Regarding the impact on computer forensic and criminal investigations, see: See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6.

[67] *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology.

[68] *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37*Flamm*, Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography, available at: www.terrorismcentral.com/Library/Teasers/Flamm.html.

[69] 74 per cent of respondents of the 2006 E-Crime Watch Survey mentioned encryption technology as one of the most efficient e-crime fight technologies. For more information, see: 2006 E-Crime Watch Survey, page 1.

[70] Sections 1.4 and 1.6 were written by Tatiana Tropina, Cybercrime Research institute.

[71] WGIG Report, 2005, available at: www.wgig.org/docs/WGIGREPORT.pdf.

[72] The importance of roles of all stakeholder mentioned here is especially highlighted in WSIS Declaration of Principles, 2003, available at: www.itu.int/wsis/docs/geneva/official/dop.html.

[73] See e.g. ENISA country reports, available at: www.enisa.europa.eu/.

[74] The World Bank Group. Global ICT Department. Cybersecurity: A New Model for Protecting the Network, available at: http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/CyberSecurity.pdf

[75] See WGIG Report, 2005, available at: www.wgig.org/docs/WGIGREPORT.pdf and *Lie/ Macmillan*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

[76] WGIG Report, 2005, available at: www.wgig.org/docs/WGIGREPORT.pdf.

[77] *Sieber*, Internet Crimes – Annex 1 to the Questionnaire for the 18th International Congress of the IACL. 2009.

[78] See: *Marsden at al*, Options for an Effectiveness of Internet Self- and Co-Regulation. Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet. RAND Europe, 2007; *Sahel*, A new policy-making paradigm for the Information Society, TPRC conference, 2006, available at: http://web.si.umich.edu/tprc/papers/2006/635/NewParadigmInfoSociety.pdf.

[79] *Vogel*, Towards a Global Convention against Cybercrime. World Conference on Penal Law, Guadalajara, Mexico, 2007, available at: www.penal.org/IMG/Guadalajara-Vogel.pdf.

[80] For details of the discussion on loosing governmental control on ICT sector see: *Sahel*, A new policy-making paradigm for the Information Society, TPRC conference, 2006, available at: http://web.si.umich.edu/tprc/papers/2006/635/NewParadigmInfoSociety.pdf, See also ITU Cybersecurity Gateway , available at: www.itu.int/cybersecurity/gateway/.

[81] See e.g. *Guillaume*, Fighting Cybercrime: Technical, Juridical and ethical Challenges. Virus Bulletin Conference, September, 2009. Page 69.

[82] *Vogel*, Towards a Global Convention against Cybercrime. World Conference on Penal Law, Guadalajara, Mexico, 2007, available at: www.penal.org/IMG/Guadalajara-Vogel.pdf.

[83] *Vogel*, Towards a Global Convention against Cybercrime. World Conference on Penal Law, Guadalajara, Mexico, 2007, available at: www.penal.org/IMG/Guadalajara-Vogel.pdf.

[84] In February, 2010 Microsoft Corp won a U.S. court approval of deactivation of global network of computers that the company accused of spreading spam and harmful computer codes. Microsoft request to deactivate 277 Internet domains, which the software maker said is linked to a "botnet," was granted by a federal judge in Alexandria, Virginia. See details: Microsoft Wins Court Approval to Topple "Botnet": Report. NY Times, 25th February, 2010, available at: www.nytimes.com/reuters/2010/02/25/technology/tech-us-microsoft.html.

[85] *Vogel*, Towards a Global Convention against Cybercrime. World Conference on Penal Law, Guadalajara, Mexico, 2007, available at: www.penal.org/IMG/Guadalajara-Vogel.pdf.

[86] The use of self-regulation and co-regulation as a tool for responding to cybercrime is discussed in more detail below, in Section 3.2.1.2(c).

[87] *Marsden at al*, Options for an Effectiveness of Internet Self- and Co-Regulation. Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet. RAND Europe, 2007.

[88] The Attorney-General's Department Submission Parliamentary Joint Committee on the Australian Crime Commission Inquiry into Cybercrime, 2003.

[89] See *Sieber*, Legal Regulation, Law Enforcement and Self-regulation, Protecting Our Children on the Internet, J.Watermann, M. Machill (eds.), 2000, pp. 319-399.; *Sieber*, Internet Crimes – Annex 1 to the Questionnaire for the 18th International Congress of the IACL, 2009.

[90] Brousseau, Internet Regulation: Does Self-Regulation Require an Institutional Framework, DRUID Summer Conference on "Industrial Dynamics of the New and Old Economy - who is embracing whom?" Copenhagen/Elsinore 6-8 June 2002, Page 1.

[91] ITU Global Cybersecurity Agenda. HLEG Global Strategic Report, ITU, 2008.

[92] *Rash et al.* Crime Online. Cybercrime and Illegal Innovation. NESTA. Research Report. July, 2009.

[93] *Callanan /Jones*, Co-operation between LE, Industry and Academia to deliver long term sustainable training to key cybercrime personnel, 2009, available at:

www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20interface%202009/if_2009_presentations/LEA-ISP%20Training%20Strategy%20v1.0.pdf.

94 *Sieber*, Internet Crimes – Annex 1 to the Questionnaire for the 18th International Congress of the IACL, 2009.

95 See information on the High-Level Experts Group on Cybersecurity (HLEG), available at: www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

96 Bruce, at al. TNO Report. International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues. 2005.

97 *Rash et al.*, Crime Online. Cybercrime and Illegal Innovation. NESTA. Research Report. July, 2009.

98 *Brenner/Clarke,* Distributed Security: a New Model of Law enforcement, 2005, available at: http://ssrn.com/abstract=845085.

99 The guide is available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html.

100 ITU Telecommunication Regulatory Database, available at: www.itu.int/icteye/.

101 An in-depth analysis of the impact of broadband on the economy and the related policy and regulatory issues can be found in the GSR10 discussion paper on the topic, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR10/documents/documents.html.

102 ITU-infoDev ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org.

103 ITU-infoDev ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org.

104 ITU World Telecommunication Regulatory Database, available at: www.itu.int/icteye/.

105 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141.

106 *ITU/Gercke*, Understanding Cybercrime: A Guide for Developing Countries. ITU, 2009, page 85.

107 The value of co-regulation and self-regulation was discussed above in Sections 4 and 5.

108 ITU Trends in Telecommunication Reform 2006, Regulating in the Broadband World.

109 ITU-infoDev ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org.

110 ITU Trends in Telecommunication Reform 2006, Regulating in the Broadband World.

111 ITU Trends in Telecommunication Reform 2006, Regulating in the Broadband World.

112 See for example MAAWG's industry-wide codes of conduct, available at: www.maawg.org/about/.

113 Regulating Utilities: Contracting out Regulatory Functions, infoDev 2006, available at: www.ictregulationtoolkit.org/en/Publication.2352.html.

114 In general, in common law countries, a regulatory agency must have the authority to seek the assistance of the court in enforcing an order or determining a matter, etc. It is an important issue since a court may not have jurisdiction to hear a matter if there is not legislation that establishes this jurisdiction. This is not a matter that should normally be left to administrative type procedures; it should be set out in legislation (either that of the regulator or that of the court or both). The administrative procedures typically address how a matter may be referred to a court by the regulator.

115 ITU-infoDev ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org.

116 ITU-infoDev ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org.

117 OPTA, NMa Cooperation Protocol, available at: www.globalcompetitionforum.org/regions/europe/Netherlands/OPTA.PDF.

118 NCC, Memorandum of Understanding between Consumer Protection Council and the Nigerian Communications Commission, available at: www.ncc.gov.ng/RegulatorFramework/MOU%20BETWEEN%20NCC%20AND%20CPC.pdf.

119 ITU Global Cybersecurity Agenda (GCA), available at: www.itu.int/cybersecurity/gca/.

120 WSIS, Tunis Agenda for the Infromation Society, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

[121] ITU Global Cybersecurity Agenda (GCA), High-Level Experts Group, Global Strategic Report (2008) at www.cybersecurity-gateway.org/.

[122] Council of Europe, Convention on Cybercrime, Budapest (Nov. 23, 2001, entry into force July 1, 2004), available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[123] Council of Europe, Convention on Cybercrime, Budapest (Nov. 23, 2001, entry into force July 1, 2004).

[124] ITU Global Cybersecurity Agenda (GCA), High-Level Experts Group, Global Strategic Report, ITU, 2008.

[125] 12th UN Congress on Crime Prevention and Criminal Justice, *Delegates Consider Best Response to Cybercrime as Congress Committee Takes Up Dark Side of Advances in Information Technology*, UNIS/CP/605E, Brazil (13 Apr. 2010) at www.un.org/en/conf/crimecongress2010/pdf/pr100413-1.pdf.

[126] *ITU/Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009.

[127] ITU-T Study Group 17 is the lead ITU Study Group on telecommunications security and identity management. It is responsible for studies relating to security, including cybersecurity, countering spam and identity management and handles security guidance and the coordination of security related work across all ITU-T study groups. More information can be found at: www.itu.int/ITU-T/studygroups/com17/index.asp.

[128] ITU World Telecommunication Regulatory Database, available at: www.itu.int/icteye.

[129] *Macmillian*, Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf.

[130] e.g. Korea Communications Commission established in February, 2008 (formed after consolidating the former Ministry of Information and Communication and the Korean Broadcasting Commission) announced among other core regulatory duties protection of Internet users from harmful or illegal content. Korea Communications Commission: http://eng.kcc.go.kr.

[131] e.g. Swedish ICT Regulator PTS addresses cyberthreats and cybercrime under user protection mandate and network security mandate. See: *PTS*. Secure communications, available at www.pts.se/en-gb/About-PTS/Operations/Secure%20communications/.

[132] Trends in Telecommunication Reform 2009. Hands-On or Hands-Off? Stimulating Industry Growth through Effective ICT Regulation (Summary), 2009, page 11, available at: www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.11-2009-SUM-PDF-E.pdf.

[133] *OPTA*. Regulatory areas, available at: www.opta.nl/en/about-opta/regulatory-areas/.

[134] OPTA Reaction on the Consultation Concerning the Future of ENISA, 14/01/2009, available at: http://ec.europa.eu/information_society/policy/nis/docs/pub_consult_nis_2009/public_bodies/OPTA.pdf.

[135] See: *MCMC*, What do we Do. Information Network Security, available at: www.skmm.gov.my/what_we_do/ins/feb_06.asp.

[136] Korea Communications Commission: Important Issues, available at: http://eng.kcc.go.kr.

[137] *Lie/Macmillan*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

[138] ITU-infoDev ICT Regulation Toolkit - Public Consultation Processes, available at: www.ictregulationtoolkit.org/En/PracticeNote.756.html; *Labelle*, ICT Policy Formulation and e-strategy development, 2005, available at: www.apdip.net/publications/ict4d/ict4dlabelle.pdf.

[139] *Lie/Macmillan*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

[140] ITU-infoDev ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/en/Section.2033.html.

[141] ITU-infoDev ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/en/Section.2033.html.

[142] ITU-infoDev ICT Regulation Toolkit - Converged Regulator, available at: www.ictregulationtoolkit.org/en/PracticeNote.2557.html.

[143] *Henten. at al.* The Next Step for Telecom Regulation: ICT Convergence Regulation or Multisector Utilities Regulation?

[144] ITU-infoDev ICT Regulation Toolkit. Section 6.3. 6.3 Separation of Power and Relationship of Regulator with Other Entities, available at: www.ictregulationtoolkit.org/en/Section.1269.html.

[145] ITU-infoDev ICT Regulation Toolkit - Public Consultation Processes, available at: www.ictregulationtoolkit.org/En/PracticeNote.756.html; Labelle, ICT Policy Formulation and e-strategy development, 2005, available at: www.apdip.net/publications/ict4d/ict4dlabelle.pdf.

[146] For example, Botswana Telecommunications Authority is imposed to provide the input to government efforts of policy making. See: Case Study Single Sector Regulator: Botswana Telecommunications Authority (BTA). ITU-infoDev ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/en/PracticeNote.2031.html.

[147] International CIIP Handbook 2008/2009, Center for Security Studies, ETH, Zurich, 2009, available at: www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663, page 133.

[148] National Information Security Strategy Proposal, November, 2002, available at: www.mintc.fi/fileserver/national_information_security_strategy_proposal.pdf.

[149] Ministry of Transport and Communications, Finland. Government resolution on National Information Security Strategy. Helsinki, 4 September 2003, available at: www.oecd.org/dataoecd/38/0/36406236.pdf.

[150] *Lie/Macmillan*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

[151] See, e.g. Report of the Second EAC Regional Taskforce Meeting on Cyber Laws. June, 2008, Kampala, Uganda, available at: http://r0.unctad.org/ecommerce/event_docs/kampala_eac_2008_report.pdf.

[152] *Mukelabai*, Cybersecurity Efforts in Zambia. Presentation at ITU Regional Cybersecurity Forum for Africa and Arab States 4-5 June 2009 Tunis , Tunisia, available at: www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mukelabai-caz-zambia-lusaka-aug-08.pdf.

[153] *Hatyoka*, ZICTA Corner - Defining ZICTA's new mandate. Times of Zambia, 2009, available at: www.times.co.zm/news/viewnews.cgi?category=12&id=1262768483.

[154] Zambia Electronic Communications and Transactions Act 2009, available at: www.caz.zm/index.php?option=com_docman&Itemid=75; see also *ZICTA*. Cybercrime Penalties (Part 1), available at: www.caz.zm/index.php?option=com_content&view=article&id=76:cyber-crime-penalties-part-1&catid=34:column&Itemid=38.

[155] *Maska*, Building National Cybersecurity Capacity in Nigeria. Presentation to the ITU Regional Cybersecurity Forum for Africa and Arab States, Tunis 2009, available at www.itu.int/ITU-D/cyb/events/2009/tunis/docs/maska-nigeria-cybersecurity-june-09.pdf.

[156] *FICORA*, www.ficora.fi/.

[157] Annual report 2008 Belgian Institute for postal service and telecommunication, BIPT, 2009, available at: http://bipt.be/GetDocument.aspx?forObjectID=3091&lang=en.

[158] See: *PTS*. Secure communications, available at: www.pts.se/en-gb/About-PTS/Operations/Secure%20communications/.

[159] *Bazargan*, A National Cybersecurity Strategy aeCERT Roadmap. Presentation at Regional Workshop on Frameworks for Cybersecurity and CIIP 18 – 21 Feb 2008 Doha, Qatar, available at: www.itu.int/ITU-D/cyb/events/2008/doha/docs/bazargan-national-strategy-aeCERT-doha-feb-08.pdf.

[160] *Mukelabai*, Cybersecurity Efforts in Zambia. Presentation at ITU Regional Cybersecurity Forum for Africa and Arab States 4th – 5th June 2009 Tunis , Tunisia, available at: www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mukelabai-caz-zambia-lusaka-aug-08.pdf.

[161] *Lewis*, Q-CERT. National Cybersecurity Strategy Qatar, available at: www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/lewis-Q-CERT-incident-management-brisbane-july-08.pdf.

[162] *Time.lex.* Study on activities undertaken to address threats that undermine confidence in the Information Society, such as spam, spyware and malicious software. SMART 2008/ 0013, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf. Page 21.

[163] E.g. ICT regulators are involved in law enforcement efforts with regard to combating spam in the following countries: Australia, Finland, Greece, Hungary, Japan, Malaysia, Mexico, Netherlands, Portugal, Turkey. See: *OECD* Task Force on SPAM. Enforcement authorities contact list, available at: www.oecd-antispam.org/countrycontacts.php3.

[164] *Time.lex.* Study on activities undertaken to address threats that undermine confidence in the Information Society, such as spam, spyware and malicious software. SMART 2008/ 0013, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf. Page 21.

[165] *ACMA,* How the ACMA fighting SPAM. Legislation & Enforcement, available at: www.acma.gov.au/WEB/STANDARD..PC/pc=PC_310309.

[166] OPTA Reaction on the Consultation Concerning the Future of ENISA, 14/01/2009, available at: http://ec.europa.eu/information_society/policy/nis/docs/pub_consult_nis_2009/public_bodies/OPTA.pdf.

[167] Commission welcomes fast and effective intervention by Dutch regulator OPTA against spyware and malware placed on 22 million computers. Europa Press Releases Rapid. 20/12/2007, available at: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/1971.

[168] *ACMA*,Regulating on-line content, available at: www.acma.gov.au.

[169] *Lie/Macmillan*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

[170] *Malakata*, Zambia authorities crack down after Zamnet hack www.computerworld.co.ke/articles/2009/01/23/zambia-authorities-crack-down-after-zamnet-hack.

[171] *MIC*, Anti-Bot Presentation for ISP is to be Held. Press release Telecom, July, 17, 2008, available at: www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/news080717_1.html.

[172] What is Cyber Clean Center?, available at: https://www.ccc.go.jp/en_ccc/index.html.

[173] See: *Mukelabai*, Cybersecurity Efforts in Zambia. Presentation at ITU Regional Cybersecurity Forum for Africa and Arab States 4th – 5th June 2009 Tunis , Tunisia, available at: www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mukelabai-caz-zambia-lusaka-aug-08.pdf.

[174] ITU Child Online Protection (COP) Initiative, available at: www.itu.int/osg/csd/cybersecurity/gca/cop/so-whats-cop.html.

[175] See: WTISD-2009. Call for action, available at: www.itu.int/wtisd/2009/call-for-action.html.

[176] *Lie/Macmillan*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

[177] See ITU-T, available at: www.itu.int/net/ITU-T/info/Default.aspx.

[178] Working Group APEC-TEL, available at: www.apectelwg.org/.

[179] European Regulatory Group, available at: http://egr.eu.int.

[180] Arab ICT Organisation, available at: www.aicto.org/.

[181] WTISD 2009: Worldwide Initiatives, available at: www.itu.int/wtisd/2009/initiatives.html.

[182] The London Action Plan serves as a network of national spam enforcement agencies (including ICT regulators, Data Protection Agencies, Consumer Protection Agencies) and promotes the effective coordination of public and private efforts on combating

spam by including ICT industry. The London Action Plan involves ICT regulators from Australia, Japan, Lithuania, Malaysia, Mexico, Taiwan, the Netherlands, United Kingdom (ICT regulator OFCOM participates with observer status). See: London Action Plan, available at: www.londonactionplan.com/?q=node/1.

183 *Weiss*, Sicherheit im Netz –Was kann der Gesetzgeber tun? Europäische Ansichten und Aussichten, available at: http://subs.emis.de/LNI/Proceedings/Proceedings17/GI-Proceedings.17-2.pdf.

184 National IT and Telecom Agency Denmark. International collaboration, available at: http://en.itst.dk/it-security/international-collaboration.

185 ITU Global Cybersecurity Agenda, available at: www.itu.int/osg/csd/cybersecurity/gca/.

186 ITU Global Cybersecurity Agenda (GCA), available at: www.itu.int/osg/csd/cybersecurity/gca/.

187 See: APEC TEL Working Group, available at: www.apectelwg.org/, APEC Telecommunication and Information Working Group, available atwww.apec-ecba.org/english/info/Article_New.jsp?a_no=4280&col_no=43&dir=200710&siteid=english.

188 APEC TEL Working Group, available at: www.apectelwg.org/.

189 See: East Africa Regulatory, Postal and Telecommunications Organization (EARPTO), available at: www.cck.go.ke/earpto_issues/.

190 *Njiraini*, Report on Recommendations for an Effective Regulatory Framework for Cybersecurity in Kenya, 2010, page 6, available at: www.commonwealthigf.org/cms/images/pdf/mwende_njiraini_recommendations_regulatory_framework_cybersecurity_kenya.pdf.

191 *FICORA*. News 29/01/2010. Memorandum on Data Stealing Malware is Published, available at: www.ficora.fi/en/index/viestintavirasto/uutiset/2010/P_6.html.

192 See *BIPT*. Warning. Viruses, available at: www.bipt.be/en/13/VirusAlertLast/Last_warning/Last_virus_alert.aspx.

193 See *BIPT*. Some Advice, available at: www.bipt.be/en/16/ShowContent/1584/Some_advice/Introduction.aspx.

194 Ofcom joins GetSafeOnLine, 2009, available at: www.getsafeonline.org/ngcontent.cfm?a_id=1500.

195 See: *Ofcom*. Media Literacy, available at: www.ofcom.org.uk/advice/media_literacy/.

196 *ACMA*. Cybersmart Program, available at: www.acma.gov.au/WEB/STANDARD/1001/pc=INT_PUB_CONTENT_PARENTS.

197 The ACMA plays a leading role in E-Security Code of Practice, available at: www.acma.gov.au/WEB/STANDARD/1001/pc=PC_311830.

198 Improving e-security for Australian internet users, available at: www.acma.gov.au/WEB/STANDARD/pc=PC_310225#4.

199 ITU-infoDev ICT Regulation Toolkit. 3.5.2. Organisational Issues.