Draft October 2009

Draft Background Paper

Cybersecurity: The Role and Responsibilities of an Effective Regulator

9th ITU Global Symposium for Regulators

Beirut, Lebanon
November 2009

Acknowledgements

This draft background paper on **Cybersecurity: The Role and Responsibilities of an Effective Regulator**, was commissioned by the ITU Telecommunication Development Sector's ICT Applications and Cybersecurity Division and Regulatory and Market Environment Division. The paper was prepared by Eric Lie, Rory Macmillan and Richard Keck of Macmillan Keck (Attorneys and Solicitors), for the 9th ITU Global Symposium for Regulators held in Beirut, Lebanon (10-12 November 2009).

The background paper on **Cybersecurity: The Role and Responsibilities of an Effective Regulator** is available online at:

www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/papers.html

For further information on the paper, please contact:

ICT Applications and Cybersecurity Division (CYB)
Policies and Strategies Department
Bureau for Telecommunication Development
International Telecommunication Union
Place des Nations
1211 Geneva 20
Switzerland
Telephone: +41 22 730 5825/6052
Fax: +41 22 730 5484
E-mail: cybmail@itu.int
Website: www.itu.int/ITU-D/cyb/

Table of Contents

1 Introduction

Information Communication Technologies (ICTs) are rapidly evolving while at the same time their usage is expanding. Today, Internet and mobile services have become an indispensible part of daily life for many around the world. While the benefits of ICT adoption have multiplied, the risks and dangers associated with their use have also similarly increased. Cybercrimes such as phishing, spam, computer-related fraud and other similar offences are rapidly increasing and evolving in step with the development and adoption of new ICT services.

In response to this situation, an increased emphasis on enhancing cybersecurity is being placed in all countries. While cybersecurity is a shared responsibility of government, the private sector and individuals alike, only national governments are in a position to lead a collective national cybersecurity effort. Only when governments establish common objectives, define ways to achieve them and clarify the roles and responsibilities of stakeholders can cybersecurity be comprehensively addressed.

As an integral part of government, ICT/telecom regulators play a key role in the national cybersecurity effort of many countries. Their broad competencies in the ICT sector, their familiarity with the ICT industry and their expertise in ICT networks and infrastructure have naturally positioned them as key players in the field of cybersecurity. However, given the constantly changing ICT environment and the dynamics of cybersecurity, the role of the regulator in this area has to evolve and adapt. Institutional improvements and other changes may be necessary to ensure that regulators remain relevant in this dynamic environment. It is in this context that this paper examines and discusses the roles and responsibilities of regulators in the field of cybersecurity.

1.1 What is cybersecurity?

In a discussion of security in the context of ICT, a number of terms are often used to describe different aspects of a common concept. In many instances, terms like cybersecurity and Critical Information Infrastructure Protection (CIIP) are used interchangeably, while in other cases they are used to describe different concepts.

In any discussion of cybersecurity, it is useful to first understand the following terms: cybersecurity, critical infrastructure (CI), critical information infrastructure (CII), critical infrastructure protection (CIP), critical information infrastructure protection (CIIP) and non-critical infrastructure.[1]

While the exact definitions may vary slightly from country to country, CI typically encompass the vital systems, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, economic activity, and/or national security. CI includes physical elements (such as physical infrastructure and buildings) and virtual elements (such as networks and data). What constitutes "critical" varies from country to country, but typically includes elements of communications, energy, public utilities, finance, transportation, public health, and essential government services.

[1] Also see ITU, List of Security-Related Terms and Definitions, available at: http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc .

CII comprises the communications network that enables these elements to operate and deliver their services. Disruption to the CII can have an equally debilitating impact on CI that reaches beyond just the ICT sector.

CIP involves identifying, assessing, and managing risks to deter or mitigate attacks on CI and the promotion of its resiliency. CIIP describes the range of activities that are undertaken to protect the CII. It focuses on the prevention and deterrence of specific ICT related risks and threats.

Cybersecurity is a broad term that encompasses CIIP as well as elements that may not be considered to be critical information infrastructure, such as the computer networks of small and medium enterprises, or home personal computers. Cybersecurity aims to prevent all malicious cyber incidents that affect the critical and non-critical information infrastructures alike. Such incidents can include denial of service attacks, the distribution of spam and malware, phishing and pharming and other cybercrimes.

ITU-T Recommendation X.1205 defines cybersecurity as:

> "the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, users, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity ensures the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The security properties include one or more of the following: availability; integrity (which may include authenticity and non-repudiation); confidentiality".

In addition to the terms defined above, the term "cybercrime" is also used extensively in the discussion of security in the context of ICT. The prevention of cybercrime is a key objective of cybersecurity.

A broad definition of cybercrime describes it as encompassing any activity in which computers or networks are a tool, a target or a place of criminal activity. To better understand some of the implications of cybercrime and the need to criminalize the misuse of information and communication technologies, ITU has developed a set of dedicated cybercrime legislation resources. An ITU publication on Understanding Cybercrime: A Guide for Developing Countries and a Toolkit for Cybercrime Legislation are currently available to assist countries in understanding the legal aspects of cybersecurity and to help harmonize legal frameworks[2].

However, the definition of the term cybercrime is not a uniform one internationally, with different legal instruments in different countries using the term to describe a range of offences. The following categories used by several regional and international instruments illustrate a possible approach:

- Offences against the confidentiality, integrity and availability of computer data and systems (i.e., illegal access, illegal interception, data interference, system interference, and misuse of devices);
- Computer-related offences (i.e., computer related forgery, and computer related fraud);

[2] For more on the definition of "cybercrime" and an in-depth discussion on cybercrime in general, see Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009 available at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html

- Content-related offences (i.e., offences related to child pornography); and
- Copyright-related offences (i.e., offences related to infringements of copyright and related rights);

While some overlap exists between categories, the categories nevertheless serve as a useful illustration of what is involved in the phenomena of cybercrime.

1.2 What is in this paper?

This paper provides a framework for discussion on the role of the regulator in cybersecurity.

Part I focuses on the roles and responsibilities of cybersecurity stakeholders: government, the private sector and individuals. As the role of government frames the eventual role of the regulator in cybersecurity, particular emphasis is paid here to the different aspects of cybersecurity in which government plays a significant part. Part I also looks at the range of international cybersecurity efforts where governments play a large role.

Part II looks in depth into the role of the regulator in cybersecurity. It first traces the evolution of the role of the regulator. It then goes on to discuss the range of roles available to regulators in the context of government involvement in cybersecurity. In that discussion the issues associated with the assumption of those roles and the core competencies necessary on the part of the regulator to fill those roles are highlighted.

Part III highlights some of the main findings of Part I and Part II, and makes some recommendations on the core competencies of regulators in cybersecurity issues.

PART I:

CYBERSECURITY ROLES AND RESPONSIBILITIES - AN OVERVIEW

In today's modern society, ICTs have become an essential component in all aspects of daily life, from the political, the economic and the social. They ensure economic stability, support national security and facilitate social interaction within nations as well as between nations. However, as a largely open, interdependent and interconnected global system, ICTs are by their very nature prone to vulnerabilities and the risk of exploitation.

In order to ensure that society continues to enjoy the benefits that ICTs bring, these vulnerabilities and risks are managed, to some extent or other, through the cybersecurity efforts of the stakeholders that own, develop, operate and use these networks. These stakeholders include government, business, other private sector organizations and individual users.

In the context of this paper, it is important to understand the relative roles and responsibilities of all stakeholders in order to properly situate that of the regulator's.

2 Cybersecurity and the public sector

To a large extent, only national governments are in a position to lead national cybersecurity efforts that involve all national stakeholders. In addition to putting in place substantive measures to counter cybersecurity threats, governments have the central task of establishing, among all stakeholders, a common awareness and understanding of cybersecurity as well as a common recognition of each stakeholder's roles and responsibilities.

2.1 Role and responsibility of government

The role and responsibility of government in cybersecurity is extensive. Given the vital role of ICTs in the nation, the wide range of threats and vulnerabilities and the cross-sector nature of cybersecurity, a large number of national governments assume a variety of roles and shoulder an extensive array or responsibilities ranging from national level policy-making to citizen level capacity-building.

From a brief survey of international practice and by building on the areas emphasized in the pillars of the ITU Global Cybersecurity Agenda (GCA)[3] and the related elements highlighted in the ITU National Cybersecurity/CIIP Self-Assessment Tool[4], the cybersecurity roles and responsibilities of government can be organized loosely into the following categories:

- Policy-making;
- Legal Measures;
- Organizational Structures;
    - Institutional organization and coordination; and
    - Incident management and cybersecurity readiness assessment;
- Capacity building;
- Public-private sector cooperation and industry regulation.

[3] Information on the Global Cybersecurity Agenda (GCA) is available at http://www.itu.int/cybersecurity/gca/.
[4] ITU National Cybersecurity/CIIP Self-Assessment Tool, ITU, 2009 available at http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

To this, the dimension of engagement in international cooperation must also be added as an indispensible element of a government's role in cybersecurity.

A holistic governmental effort that encompasses all these categories is a prerequisite for an effective national cybersecurity response.

2.1.1 Policy-making (and establishing a national cybersecurity strategy)

Leadership in the area of cybersecurity by national governments is manifested largely through the government's national policy-making role. Governmental policy-making in the area of cybersecurity provides, at the highest level, a common understanding and vision of the problem, allowing for coordinated national action that would realize national cybersecurity objectives.

The preparation of a national cybersecurity strategy is an essential first step in addressing cybersecurity challenges. Such a statement typically:

- highlights the importance of ICTs to the nation (e.g. by providing information on the role of ICTs in the economy, society and national security, and the industrial and governmental processes dependant on ICTs);
- identifies and evaluates potential risks and threats (e.g. cyber-attacks, cybercrime, etc.);
- establishes cybersecurity related objectives (e.g. containment of cyber-attacks, detection and prosecution of cybercrime, protection of data resources, etc.);
- identifies the actions to be taken in order to achieve those objectives (e.g. establishment of incident response centers, adoption of cybersecurity standards, building consumer awareness, etc.); and
- sets out the roles and responsibilities of all stakeholders in the process (including a mechanism for information sharing, cooperation and collaboration).[5]

The national cybersecurity strategy can also place cybersecurity efforts into the context of other national efforts, such as homeland security and the development of an information society.

In many countries, national cybersecurity strategy is typically promulgated at a high level of government, often by the head of government, in order to get the buy-in of all stakeholders. For example, in the case of Brazil, the national cybersecurity strategy is led from the Office of the President (see Box 1 below). At the same time, however, national cybersecurity policy is typically developed cooperatively through consultation with all relevant stakeholders, including other government institutions, industry, academia, and civil society. In some countries, such policies also integrate state, local, and community-based approaches that feed into the larger national context.

2.1.2 Legal Measures

An effective cybersecurity effort requires the establishment, review and, if necessary, amendment of relevant legal infrastructures that support modern ICTs.[6] This requires

[5] Ibid. See also ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity, ITU, 2009, available at http://www.itu.int/md/meetingdoc.asp?lang=en&parent=D06-SG01-C&question=Q22/1

[6] For more information on the range of legal measures that can be undertaken in the area of cybersecurity see the section on Legal Matters in the ITU Global Cybersecurity Agenda (GCA) High

updating of criminal laws, procedures and policies to address cybersecurity incidents and respond to cybercrime. As a result, many countries have made amendments in their penal codes, or are in the process of adopting amendments, taking in consideration existing international frameworks and recommendations.[7] As a priority, criminal law, procedures and policy should be reviewed to ensure the prevention, investigation, and prosecution of all forms of cybercrime.[8] In addition, legislation that ensures the security of information and information infrastructures should be introduced[9]. Such legislation typically deals with issues that include the following:

- Security in electronic communications
- Fraudulent use of computer and computer systems;
- Protection of personal data and privacy;
- Certification, digital signatures and Public Key Infrastructure (PKI), among others.

Beyond their enactment, cybersecurity laws must also be effectively enforced. An effective anti-cybercrime effort will require the modernization of law-enforcement agencies, the establishment of dedicated cybercrime units, and the training of prosecutors and judges.

As many instances of cybercrime cuts across borders, participation in international efforts to respond to cybercrime forms an integral part of the national cybercrime prevention effort.

2.1.3 Organizational Structures

Institutional organization and coordination

The institutional organization and coordination of government institutions for cybersecurity is a vital element of a successful cybersecurity effort. In the context of the role and responsibility of government, it typically involves the organization and coordination of cybersecurity roles and responsibilities among appropriate government institutions in order to carry out the actions that are required to meet cybersecurity objectives. A detailed organization and cooperation framework is essential in order to avoid institutional gaps in the national cybersecurity effort as well as to avoid overlaps in responsibilities which can prove just as damaging. Where overlaps in responsibilities exist, there is often either a tendency towards passiveness by the institutions concerned, or at the other extreme, a potential for the introduction of conflicting regulations and approaches.

Universally, a concerted cybersecurity effort at the government level requires organizing and coordinating the work of multiple authorities and government departments, who often have

---

Level Experts Group (HLEG) Global Strategic Report, ITU, 2008 available at http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

[7] To better understand some of the implications of cybercrime and the need to criminalize the misuse of information and communication technologies, ITU has developed a set of dedicated cybercrime legislation resources. An ITU publication on Understanding Cybercrime: A Guide for Developing Countries and a Toolkit for Cybercrime Legislation are currently available to assist countries in understanding the legal aspects of cybersecurity and to help harmonize legal frameworks. These resources are available at http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html and http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

[8] As an example, the Budapest Convention on Cybercrime (2001) includes minimum requirements: substantive laws (i.e. minimum standards for what is criminalized); procedural mechanisms (i.e. investigative methods); and international legal assistance (i.e. procuring of evidence or extradition). The convention is available from the Council of Europe in various languages at http://www.coe.int/cybercrime/

[9] See the UNCITRAL Model Laws on Electronic Commerce and on Electronic Signatures (2001) and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) for example.

different mandates and perspectives on the problem. As such, the delegation of roles and responsibilities among government institutions is a delicate one and in many cases it is undertaken by a government institution with a high-level mandate, such as the cabinet or the presidential office, as is the case with the National Infrastructure Security Co-ordination Centre (NISCC) in the United Kingdom or the Department of Homeland Security in the United States. Such high level oversight is often necessary to efficiently settle potential conflicts where overlaps in institutional jurisdiction and responsibilities exist.

In practice, the actual delegation of cybersecurity roles and responsibilities among the different government institutions varies widely from country to country as such decisions are based on a wide range of considerations. This topic is discussed further in Section 2.2 below.

Incident management and cybersecurity readiness assessment

The capability to detect, to investigate and analyze, and to respond to cyber-threats and attacks is an indispensable component of cybersecurity. In this respect, computer incident response teams (CIRTs) in various forms have been established by a wide range of groups (e.g. operators, businesses, universities, etc.) at the national and international level. [10] CIRTs vary dramatically in the services they provide and the constituents they serve. Some have national responsibility while most belong to private organizations and are established to fulfill specific functions, depending on their situation. A key function that all CIRTs share is the ability to provide (1) timely information about the latest threats and (2) assistance in response to incidents when needed.

While many CIRTs have been created from the bottom-up, it is generally acknowledged that it is important for governments to establish an incident management capability on a national level to prevent, prepare for, respond to, and recover from cybersecurity incidents. National CIRTs also typically assume responsibilities for readiness and response to large-scale attacks.

Such an incident management capability would necessarily extend beyond the traditional CIRT role to include coordination and management capabilities in terms of cybersecurity crisis. It would also make tactical or strategic information available to key stakeholders within the public and private sectors. Examples of such CIRTs can be found in Canada (Integrated Treat Assessment Center) and in Switzerland (Reporting and Analysis Center for Information Assurance, MELANI).

Given the cross-border nature of cyber threats and attacks, active participation in international and regional cybersecurity incident monitoring activities forms a necessary part of the CIRT national effort. Such activities can include active participation in an international CIRT organization (e.g., Asia Pacific Computer Emergency Response Team (APCERT), Forum of Incident Response Security Team (FIRST), etc.) or international incident management exercises. For example, US-CERT has organized major international exercises (e.g. “Cyberstorm”, involving Australia, New Zealand, and Canada), simulating large-scale attacks on critical sectors.

The conduct of cybersecurity exercises to test readiness and responsiveness form part of the larger role of government to evaluate and review the level of cybersecurity preparedness of

[10] The term CIRTs is often used interchangeably with the terms computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs). A CIRT is essentially a team of IT security experts whose main business is to detect, analyze, monitor and respond to computer security incidents. In some cases, these CIRTs also manage outreach, cyber-security awareness, and partnership efforts to disseminate information to key constituencies and build collaborative actions with key stakeholders.

the nation. Such a role typically involves the organization and execution of periodic cybersecurity risk assessments and strategy reviews on both the national and sector-specific (e.g., financial, manufacturing, retail, etc.) levels. The result of such cybersecurity assessments can, in turn, lead to a thorough review of existing cybersecurity-related legislation and regulation as well as sector specific legislation and regulation, such as financial laws and regulation.

2.1.4 Capacity Building

Generally, many end-users (including private enterprises, public entities, and home users) lack the awareness and resources to manage cyber-security risks adequately. Many information system vulnerabilities exist because of a lack of cybersecurity awareness on the part of users.

End user outreach efforts therefore, at the most basic level, entail the development of a concerted strategy to communicate the importance of cyber-security and their role across the country. Such a strategy would identify practical information for dissemination to their target audiences and initiatives to ensure the adoption of those practices.

Capacity-building in the area of cybersecurity is a necessary complement to the building of cybersecurity awareness. For a culture of cybersecurity to be firmly established, the level of cybersecurity competence in general has to be increased. In part, this can be achieved by making basic cybersecurity-related training more readily available to the public (e.g. through interactive websites) and by promoting industry efforts to train personnel and to adopt widely-accepted security certifications.

In addition, governments must encourage academia to provide for the education of a ready pool of trained cybersecurity professionals to meet the increasing demands of both the public and the private sector in the field.

2.1.5 Public-private sector cooperation and industry regulation

A comprehensive national cybersecurity effort requires the establishment of a coordination and cooperation framework through which all stakeholders, from both the public and private sector, can collaborate in the development and refinement of cybersecurity policy and cooperate in the implementation of cybersecurity operational efforts. In particular, such a framework would allow governments, businesses, civil society and individual users to work together to develop and implement measures that incorporate technical (e.g., standards), procedural (e.g., guidelines, standards, or mandatory regulations) and personnel (e.g., best practices) safeguards. Such measures include, for example, promoting government and industry adoption of international standards related to cybersecurity (e.g., ISO 27001 on Information Security Management System) and the implementation of certification schemes (e.g., Public Key Infrastructure).

Governments in almost all countries have recognized the importance of public-private sector cooperation in cybersecurity. The development of a close mutually beneficial relationship facilitates the overall management of cyber threats and cybersecurity. Realistically, many governments actively promote cooperation and information-sharing with the private sector, as large parts of critical infrastructures are owned and operated by private business. Only by understanding the cybersecurity challenges facing the private sector can an effective national cybersecurity strategy and policy be adopted. Cooperation between government and industry is also essential in the response and recovery phase of cybersecurity incidents.

The exact approach countries take to achieve public-private sector cooperation varies based on local conditions and needs. Examples include government-led task forces, industry-led forums, and joint public-private initiatives. In countries such as Switzerland, Republic of Korea, the United Kingdom, and the United States, strong links have already been established between the private business community and various government organizations in the area of cybersecurity.

A key challenge presented to governments and industry alike in this context is the search for a balance between national cybersecurity requirements and business efficiency imperatives. Satisfying shareholder interests by maximizing company profits has often led to minimal security measures on the part of the private sector partly because businesses tend to view cyber-threats as a tolerable risk. In these situations, governments have sometimes found it necessary to introduce measures that compel or encourage the private sector to prioritize cybersecurity and to adopt sufficient safeguards.

To the extent that government supports science and technology and research and development (R&D) activities, some of its efforts should be directed towards cybersecurity and the protection of information infrastructures. Through partnerships with the private sector and academia, governments can help shape the development of cybersecurity related technologies, techniques, standards and processes that further the national cybersecurity agenda.

2.2 Delegating cybersecurity responsibilities among government institutions

Because of the cross-sector nature of cybersecurity, it necessarily means that various key elements of an overall cybersecurity policy will be implemented in practice through a very diverse set of institutional arrangements that differ from country-to-country. Furthermore, countries at different stages of development will have differing perspectives on the overall vulnerability of their own critical information infrastructures. They are likely to be at different stages of institutional development.

As a practical matter, in most countries responsibility for cybersecurity or CIIP is based on an evaluation of national cybersecurity vulnerabilities and a matching of this to the roles and responsibilities of existing government institutions. Relevant cybersecurity responsibilities are then given to the most well-established institution or institutions that appear suitable for the task (e.g. Ministry of Defense, Department of Homeland Security, the ICT regulator, etc.). For example, in Canada, responsibility for CIP and CIIP is delegated to Public Safety Canada, an agency that provides policy advice and support to the minister of public safety on issues related to public safety, including national security and emergency management, policing and law enforcement, interoperability and information-sharing, border management and crime prevention. Public Safety Canada's portfolio also includes the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), and the Correctional Service of Canada among others.[11]

While less common, a number of countries have also set up central management and coordination institutions (e.g. national cybersecurity councils, inter-agency cybersecurity task forces) specifically to meet cybersecurity and CIIP concerns. For example, in Japan, two central management and coordination organizations were established within the Cabinet Secretariat to deal specifically with cybersecurity issues. The Information Security Policy Council (ISPC) plays the central role in developing and reviewing the country's information security strategies and policies while the National Information Security Council (NISC) is the central implementing body for IT security issues.[12]

[11] For more information on the activities of Public Safety Canada, see http://www.publicsafety.gc.ca.
[12] For more information on the ISPC and the NISC, see http://www.nisc.go.jp/eng/index.html

In most countries, different cybersecurity roles and responsibilities are typically spread among multiple governmental institutions and organizations (see Box 1). Depending on their key role (e.g. defense, law enforcement, ICT development), these institutions bring their own perspective to bear on the issue of cybersecurity and shape national policy accordingly.

Box 1: Government cybersecurity framework in Brazil

Brazil has a complex and sophisticated web of institutions involved in cybersecurity. Its experience illustrates the interconnected relationships of public and private stakeholders that are an essential part of an effective cybersecurity framework.

Leadership on national ICT security issues in Brazil falls within the jurisdiction of the Institutional Security Cabinet or GSI (Gabinete de Segurança Institucional), which is part of the office of the President of the Brazilian Republic. GSI is also tasked with crisis management, intelligence, and the provision of advice for the President in military and security issues. It does not directly handle operational security issues, but works through other related organizations such as CTIR-GOV and CGSI.

CTIR-GOV (Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal) is a governmental body that deals with national security incidents that involve the Brazilian federal government.

CGSI (Comitê Gestor de Segurança da Informação) is an information security steering committee created by legislation. It comprises of representatives from every government ministry (justice, defense, health, communication, science and technology, etc). The participants discuss information security issues and through working groups define the cybersecurity policy direction of the Brazilian federal administration.

CERT.br is the Brazilian Computer Emergency Response Team, sponsored by the Brazilian Internet Steering Committee. It is responsible for receiving, reviewing, and responding to computer security incident reports and activity related to networks connected to the Brazilian Internet. Computer Security Incident Response Teams (CSIRTs) have also been established in a number of Brazilian states.

Certain methodologies for dealing with Critical Information Infrastructure Protection have been developed by the Brazilian ICT sector in cooperation with the regulator, ANATEL. These methodologies have been applied to assess the cybersecurity readiness of Brazil's ICT infrastructure.

CEPESC (Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações), a center for research and development for security in communications under the Brazilian intelligence agency, also assists and supports the Brazilian government and the GSI in all aspects related to secure communications.

Source: Adapted and updated from "International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues", TNO, 2005 available at http://www.ists.dartmouth.edu/library/158.pdf

In general, there are at least four overlapping typologies for how cybersecurity issues are viewed[13]:

- an IT-security perspective,
- an economic perspective,

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

- a legal or law enforcement perspective, and
- a national security perspective.

Most countries consider cybersecurity to be a national security issue of some sort. In parallel, however, they also view it from a technological, ICT viewpoint. At the same time, the law enforcement and cybercrime perspective is also found in all countries. While all typologies can usually be found in all countries, the emphasis given to one or more of them varies to a considerable degree.

In countries that view cybersecurity from a national security perspective, cybersecurity efforts are mainly led by the defense and national security establishment. For example, in France responsibility for a large part of cybersecurity falls under the general umbrella of the General Secretary for National Defense.[14] Such nations have had traditionally a significant military or national security presence in the international arena and see cybersecurity as a part of cyber-warfare.[15]

Where cybersecurity is viewed from a law-enforcement perspective, cybersecurity efforts tend to be led by institutions that deal with law enforcement and internal security. In some countries, cybersecurity is also integrated into the overall counterterrorism effort, where the intelligence community plays a large role. For example, in the Republic of Korea the National Intelligence Service (NIS), the chief intelligence agency, serves as coordinator for the private, public, and military sectors in the event of a cyber crisis.

In countries that view cybersecurity from an economic and IT-security perspective, approaches to cybersecurity are often jointly led by the business community and government institutions involved in ICT development, such as the regulator or other institutions involved in the e-economy. In countries such as Estonia, Japan and Singapore cybersecurity is viewed as an integral part of the fostering of an information-based economy. In these countries ICT regulators play a large role not only in the implementation of cybersecurity safeguards but also in policy-making and coordination.

The establishment of these institutions and their location within government are influenced by various factors such as military and civil defense tradition, the allocation of resources, historical precedent and the general perception of where the greatest threat lies by the key policy-makers in this domain. Depending on their influence or their resources at hand, various government institutions shape the cybersecurity issue in accordance with their view of the threat.

It must be highlighted that there is no single strategic approach, organizational and institutional set up, or operational procedure that is right for every country. Between countries there are large differences in political and legal systems, economic development, and public and private sector relationships. What is important, however, is that governments adopt a flexible and adaptive approach to their cybersecurity efforts as threats to cybersecurity are constantly evolving. Sometimes this requires the periodic review and reorganization of the national cybersecurity framework (see Box 2). In adopting a flexible and adaptive approach, governments can also rapidly assimilate and adopt the latest international best practices in the area of cybersecurity without significant delay.

[14] For more information, see the website of the Secrétariat général de la défense nationale at http://www.sgdn.gouv.fr.
[15] For more information on cyber-warfare, see 'Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States', Charles Billo, Welton Chang, ISTS, 2004 at http://www.ists.dartmouth.edu/directors-office/cyberwarfare.pdf

Box 2: Institutional reorganization in the Republic of Korea

As a response to the large scale distributed denial of service (DDOS) attacks on 7 July 2009, the Government of the Republic of Korea confirmed in September 2009 that the National Intelligence Service (NIS) would serve as a coordinator for the private, public, and military sectors in the event of a cyber crisis.

Previously, the ICT regulator, the Korean Communication Commission (KCC), the NIS, and the Ministry of Defense shouldered responsibility separately for cybersecurity in their respective sectors.

When cybersecurity levels pass "normal" and reach "cautionary" levels, the NIS is expected to analyze the threat and implement countermeasures to contain the situation, if necessary.

Source: http://www.hani.co.kr/arti/english_edition/e_national/376585.html

3 Cybersecurity and the private sector

ICT infrastructure is for the most part owned and operated by the private sector in the large majority of countries worldwide. In many countries, the private sector is also typically the first to adopt technological changes and assess its associated vulnerabilities. As such, the involvement of the private sector is indispensible in any national cybersecurity effort.

3.1 The role of the private sector

On an individual basis, businesses are expected to implement an adequate level of cybersecurity safeguards into their business practices. Such safeguards typically involve the installation of technical solutions and the adoption of secure business processes.

Businesses in some economic sectors may be further along in adopting cybersecurity practices. For example, the financial and banking sector, with its dependency on international clearing and central banking, and its links to international financial market systems, cybersecurity concerns are accorded high priority.

On a collective level, the private sector has an important role to play in its own right and in cooperation with government in developing cybersecurity business norms, standards and codes of conduct, as well as in identifying and encouraging the adoption of good practices. By taking part in relevant forums or standards-development organizations, industry plays a critical role in agreeing on technical standards to protect security.

3.2 Cybersecurity and the bottom line

In general it has proved to be a more demanding task to focus resources on the protection of critical information infrastructure which is often subject to private ownership or control. In the competitive global business environment, businesses will necessarily be inclined to reduce or eliminate expenses that do not contribute to the bottom line, such as expenditure for cybersecurity-related systems and technologies.

Some of these business imperatives can be mitigated where government can make the case that additional security-related initiatives are a matter of overriding public concern. As

increased public awareness and government initiatives raise the profile of cybersecurity risks, businesses would be expected to take such matters into account in their operations.

Over time, cybersecurity concerns are expected to become viewed as an integral aspect of a company's product or service, as opposed to a matter of regulatory concern. As public awareness is increased about cybersecurity, consumers will increasingly expect businesses to address cybersecurity concerns in their products and services which, for example, can be seen increasingly in the software industry where consumer operating systems are more commonly being bundled with anti-spyware protection and firewall software.

4 Cybersecurity and the individual

To a large extent, consumers without significant protection against viruses and other malware prevalent in today's computer environment represent the greatest source of vulnerability to the CII. In numerous reported incidents, inadequately protected PCs connected to the Internet have been used to perpetuate cybercrime and mobilized to launch cyber attacks. At the same time, individuals are also the victims of a wide range of cybercrimes and cyber nuisances such as spam, phishing, and computer fraud. [16] As both cybersecurity hazard and victim, the implementation of measures to address the vulnerabilities of individual ICT users is an important facet of any concerted cybersecurity effort.

4.1 The role of the individual

Because the technology generating cyber risks makes it very difficult to fight potential attackers in advance, the adoption of technical and procedural protective measures becomes a crucial element in ensuring security. Here, end-users are in a key position as they alone are in the position to install technical safeguards for IT security at the most basic level.

At its most basic, effective security at the level of the individual involves some degree of familiarity with cybersecurity threats (e.g. viruses, spam, etc.) and the adoption of appropriate technical safeguards (e.g. anti-virus software, firewalls, etc.). As such, a large part of governmental efforts to boost cybersecurity have focused on the dissemination of basic cybersecurity awareness. In this respect, a host of resources from government and the private sector have been made available for individuals to learn more about the role they are expected to play in cybersecurity.

4.2 The role of civil society

Society's range of interests is represented in many countries by a variety of civil society groups that take on various forms and functions. These can range from consumer rights advocacy organizations to environmental groups.

In recent years, civil society groups in a number of countries such as the United States and Canada have taken a greater interest in cybersecurity as they come to understand the range of societal issues cybersecurity raises. These can include human rights, civil liberties, privacy, and consumer protection, among others. A small but growing number of civil society not-for profit organizations have also been established around the issue of cybersecurity and cybercrime itself.[17]

[16] For other examples, "Cybersecurity Guide for Developing Countries", ITU, 2009 available at http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf

[17] See, for example, The Society for the Policing of Cyberspace at http://www.polcyb.org/ and the Open Information Systems Security Group at http://www.oissg.org/

In consultations with government, feedback and other contributions from such groups can serve as an important source of information to policy-makers that seek to create a holistic cybersecurity approach that takes into account interests beyond that of government and business.

5 Cybersecurity and international cooperation

Because of the "borderless" nature of the Internet and cyberspace, cybersecurity crimes, threats and attacks can originate from one country and affect another easily making investigation and law enforcement difficult. As such, there is a strong and pressing need for robust international cooperation in cybersecurity.

Cooperation in cybersecurity can take place on many levels (e.g. regional and international) and across many dimensions (cybercrime, incident response, cyber-terrorism, etc.). International cooperation can involve binding conventions and protocols or they can also involve information sharing (Box 3).[18]

Box 3: The ITU Global Cybersecurity Agenda (GCA)[19]

As facilitator for WSIS Action Line C5 dedicated to building confidence and security in the use of ICTs, ITU is working closely with key stakeholders to respond to the growing cybersecurity challenges in a coordinated manner. As such, the ITU Global Cybersecurity Agenda is designed as an international framework for cooperation and response, and for building partnerships and collaboration between all relevant parties in the fight against cyber-threats. Launched in 2007 by ITU Secretary-General, Dr. Hamadoun I. Touré, the ITU GCA is a framework for international cooperation aimed at enhancing confidence and security in the information society. The GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners and building on existing initiatives to avoid duplicating efforts.

Source: Information on the Global Cybersecurity Agenda (GCA) at http://www.itu.int/cybersecurity/gca/

Because of the multi-sectoral nature of cybersecurity, effective international collaboration requires the involvement of all affected stakeholder groups. An example of such an inclusive approach can be found in the collaboration between ITU and the International Multilateral Partnership Against Cyber-Threats (IMPACT) (Box 4).

Box 4: The ITU-IMPACT Collaboration

Established within the framework of the ITU Global Cybersecurity Agenda, the ITU-IMPACT collaboration aims to bring key stakeholders and partners from governments, private sector companies and academia together to provide ITU Member States with the expertise, resources and capabilities to effectively address cyber-threats.

The key objectives of the ITU–IMPACT collaboration include:

- Real-time analysis, aggregation and dissemination of global cyber-threat information;

[18] For a more detailed discussion of international cooperation on cybersecurity see the section on International Cooperation for Cybersecurity in the ITU Global Cybersecurity Agenda (GCA) High Level Experts Group (HLEG) Global Strategic Report, ITU, 2008 available at http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

[19] Information on the Global Cybersecurity Agenda (GCA) is available at http://www.itu.int/cybersecurity/gca/ .

- Early warning system and emergency response to global cyber-threats; and
- Training and skills development on the various aspects of cybersecurity.

The ITU Telecommunication Development Bureau through its programmes and initiatives facilitates the development and establishment of these resources and capabilities, in line with international cooperation principles while taking into account national and regional requirements. Specific activities are being undertaken, such as:

- Developing a global framework for watch, warning and incident response;
- Establishing appropriate national and regional organizational structures and policies, such as National Computer Incident Response Teams (CIRT);
- Facilitating human and institutional capacity building across sectors; and
- Facilitating global multi-stakeholder international cooperation.

Source: http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html

PART II:

THE EVOLVING ROLE OF THE REGULATOR IN THE AREA OF INFORMATION AND NETWORK SECURITY

6 The role of the regulator

Since the first telecommunications sector specific regulators were established, regulators have assumed a wide variety of roles that differ widely from country to country. Over time, new regulators were established with different mandates while more established regulators had their mandates changed to take into account the phenomenon of convergence and the increasing importance of ICTs to the nation.

6.1 The core duties of the regulator

Regulators in most countries, at their core, perform a traditional set of roles. As highlighted by the ITU-infoDev ICT Regulation Toolkit, the most important duties of the regulator include:

- implementing the authorization framework;
- promoting competition (including tariffs);
- interconnecting networks and facilities;
- implementing universal service/access mechanisms;
- managing the radio spectrum; and
- minimizing the burden and costs of regulation and contract enforcement.[20]

To some extent, the early role of the regulator focused on carrying out these core economic and technical regulation duties in the context of taking the telecommunications market from monopoly to competition. During that period, the scope of these duties typically extended to telecommunications (as opposed to ICT) and was largely focused on a limited number of stakeholders, in particular the incumbent, with less attention paid to consumers and end users. Involvement in policy-making, industry development, and consumer protection were uncommon.

6.2 The evolving role of the regulator

Globally, the role of the regulator has evolved as technology has evolved, and as markets have opened to competition. Notably, this evolution has been marked by:

- A more prominent role for regulators

  Technological changes have dramatically increased the usage and importance of ICTs, in turn bringing the role of the regulator into greater prominence. Regulators in many countries today play an important role in shaping ICT policy. In some cases, regulators also play an active role in managing and promoting ICT sector development.

- A widening of the regulator's scope of regulation (from telecommunications to ICTs)

[20] See ITU-infoDev ICT Regulation Toolkit at http://www.ictregulationtoolkit.org/en/Section.3105.html

Marked by the transition from analogue to digital, narrowband to broadband, voice to data, and circuit switched to packet switched, the phenomenon of convergence has led to an expansion of the regulator's core focus to include services that go beyond just voice. The markets that regulators oversee have also changed dramatically with convergence allowing previously separate industries and entirely new sectors to compete in the same newly expanded market space. The management of a transition to an e-economy has become a key function of many regulators worldwide.

- An expanded regulatory mandate to include the engagement of more stakeholders (e.g. civil society, individuals, etc.)

With ICTs becoming more accessible and indispensible to individuals, many regulators have an expanded role so as to be able to focus on issues such as capacity building, consumer protection and consumer awareness. In many countries, traditional universal access objectives have also been expanded to encompass the national objective of building of an inclusive e-society.

With the larger role regulators play in this current ICT environment, regulators have found themselves increasingly well positioned in terms of mandate, resources and experience to deal with current and emerging cybersecurity challenges.

7 The role of the regulator in cybersecurity

In Section 2.1 above, the different areas of a national cybersecurity effort where government plays significant roles were highlighted and discussed. This Section builds on that discussion by examining the roles regulators already play (or are poised to play) in those areas.

In particular, the discussion will highlight the following issues:

- What role does or can a regulator play in each particular area of cybersecurity?
- What different issues does the regulator need to consider when getting involved in these areas?
- What core competencies and resources of the regulator are critical in this process and what can be done to build the capacity of the regulator in the event it does not possess the necessary resources or competencies?

7.1 Cross-cutting competencies and prerequisites

Before embarking on an area-by-area analysis and discussion, there are a number of cross-competencies that regulators will have to demonstrate before taking an active role in any aspect of cybersecurity. These include:

7.1.1 Institutional maturity

Integrating cybersecurity concerns with the traditional regulatory framework may be a complex task in countries which have only recently established regulatory institutions. These institutions are already burdened with a long list of tasks associated with their core responsibilities such as licensing and interconnection. They also face a complex range of challenges that are associated with convergence and the introduction of new technologies.

In such a situation, it may be more difficult for such regulators with their fledgling status to achieve credibility in significant areas of cybersecurity given its close association with

national security policy. In many countries security issues have been the near exclusive domain of the more established military, law enforcement and the intelligence community.

Regulators in such a situation may have to define their roles carefully and identify ways that they can participate in cybersecurity activities and advise on cybersecurity policy without necessarily being the lead institution. Such regulators would be advised to look closely at the range of cybersecurity roles and responsibilities undertaken by other regulators and to decide which options and approaches are best suited to their own national context. They will need to appraise realistically what they can and cannot do and what needs to be left to others to manage and lead.

7.1.2 Engagement of the private sector

Regulators possess a well established set of mechanisms and processes to facilitate engagement of the private sector for the purposes of consultations as well as for the purposes of facilitating industry self-regulation. Across the globe, examples of regulator initiated public-private sector forums abound. Such forums deal with issues such as infrastructure sharing, interconnection and consumer protection. For example, the Malaysian Communications and Multimedia Commission (MCMC) has facilitated the establishment of a range of industry self-regulation forums focusing on issues such as access, content, consumer protection and technical standards.[21] The same set of mechanisms and processes can be leveraged in the same way when addressing issues related to cybersecurity.

7.1.3 Technical and industry expertise

With technical regulation being a core function of regulators and technological familiarity being a prerequisite for the regulation of the ICT sector as a whole, regulators as an institution possess an in depth technical knowledge of ICTs, often employing technical experts and specialists in their staff. As cybersecurity risk factors are largely technologically driven, regulators are poised to play a leading role in identifying and explaining for cybersecurity policy makers the technicalities involved in potential cybersecurity concerns.

7.1.4 Mandate and jurisdiction

Despite the expanded role of many regulators in general, an extension of the regulator's mandate to cover issues related to cybersecurity cannot be taken for granted. Given the rapid developments in the field of cybersecurity, the cybersecurity policies and frameworks in many countries are constantly undergoing transformation. As such, in many cases there is a lack of clear jurisdictional boundaries that delineate the areas of responsibilities between the different government institutions dealing with cybersecurity issues. In such a situation, the exact scope of responsibility of a regulator with regard to cybersecurity may not be marked out clearly, leaving regulators little guidance as to their role in that field. Such a situation presents both challenges and opportunities.

In a number of countries, regulators have progressively established their role in the field of cybersecurity by building on the clear mandates that they have been given. One good example can be seen in the case of spam. Regulators in many countries have been dealing with the issue of spam as a significant consumer-protection problem and burden on the national ICT infrastructure. For example, the Dutch regulator OPTA deals with the problem of spam and malicious software - and Internet safety in general - under its wider mandate of consumer protection.[22] Spam can also be a vehicle for generating BOT viruses that can lead to DDOS

[21] For more information, see http://www.skmm.gov.my/
[22] See, for more information, OPTA 2008 Annual Report available at http://www.opta.nl/.

attacks against critical information infrastructures. In this light, spam is increasingly being seen as a potential cybersecurity risk and, in turn, a link to the concerns of policy makers concerned with cybersecurity and the protection of critical infrastructure. In this way the spam issue has become an effective vehicle for regulators to become a more integral part of national cybersecurity efforts.

Similarly, the regulator's traditional role in managing communications in times of emergency and crisis can also provide a suitable avenue for its involvement in cybersecurity, particularly in efforts related to incident monitoring and cybersecurity readiness assessments (see Section 7.5.2 below). In many countries, regulators have long exercised responsibilities in the area of crisis-related communications (see Box 5). They may have had roles, at times in cooperation with other agencies concerned with emergency preparedness or national defense, in developing and implementing plans for responding to natural disasters or other civil emergencies where demands on ICT infrastructure may exceed available resources and capacity must be allocated on a system of priorities.

Box 5: Crisis communications and the Norwegian Post and Telecommunications Authority (NPT)

The Norwegian regulator, the NPT is tasked with overall contingency planning with regard to the public electronic communications infrastructure. Its wide range of responsibilities related to communications security includes the following:

- Considering investment in measures designed to increase the robustness of the telecom networks;
- Conducting inspections to see that the required measures are implemented;
- Creating awareness of communications security and contingency planning, improving the necessary related expertise, and offering guidance to operators, users and other players (e.g. through courses, seminars, company visits, establishment of forums of expertise, etc.); and
- Arranging joint exercises and developing cooperation between the operators of telecom networks.

Electronic communications providers who provide essential electronic communications services to users who have socially critical functions must notify the NPT of significant operational and technical problems that could reduce or have reduced the quality of services.

Source: NPT at http://www.npt.no/

As the cybersecurity takes on more national security-related overtones, the jurisdictional claims of regulators may lead to some friction with government institutions that have been more traditionally associated with national security issues. In such a situation, regulators may require a clearer mandate with regard to their cybersecurity role. Such a mandate can be granted by provisions in new cybersecurity legislation, legislative amendments to existing ICT legislation, executive decrees, internal government directives and other similar measures.

7.1.5 Appropriate resourcing

In order to carry out its roles and responsibilities effectively, a regulator has to have the appropriate financial and manpower resources. In an ideal situation, additional financial resources are given in tandem with the assumption of new roles and responsibilities either through general government appropriation or through special grants or funds.[23]

[23] For example, in the United States, under the 2010 Budget, USD355 million in funding was earmarked for cybersecurity and technology R&D that will support the base operations of the National

In the absence of additional funding, regulators in a number of countries have relied on vehicles such as public-private sector partnerships to reduce the costs of cybersecurity initiatives. The consolidation of certain functions and tasks can also result in synergies and cost savings (see, for example, Box 16 below).

7.2 Engagement in international cooperation

Engagement on the part of regulators in a number of key platforms dealing with international and regional cybersecurity cooperation can greatly increase the value of their contribution to the overall national cybersecurity effort.

Through a long history of participation in a wide range of ITU activities, regulators are well positioned to engage in international cooperation and information sharing through, for example, the Global Cybersecurity Agenda which was established by the ITU following a specific mandate from WSIS (see Box 3 above).

In addition, a large number of regulators already actively participate and contribute to the ITU's global cybersecurity-related standardization activities (see Box 6).

Box: 6: ITU standardization activities related to cybersecurity

ITU-T Study Group 17 is the Lead Study Group on Communications System Security and handles security guidance and the coordination of security-related work across all ITU-T Study Groups. It is responsible for studies on security, the application of open system communications (including networking and directory), technical languages and other issues related to the software aspects of telecommunication systems. It has approved over one hundred Recommendations on security.

ITU's Focus Group on Identity Management was established by Study Group 17 to facilitate the development of a generic Identity Management framework with the participation of experts on Identity Management. The Focus Group may analyze other aspects related to such a framework.

Source: ITU at http://www.itu.int/ITU-T/studygroups/com17/index.asp and http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html

Considering the core competencies possessed by regulators, in particular their ICT technical and industry expertise other regional and international cooperation platforms that may be suited for regulator participation include:

- OECD Working Party on Information Security and privacy[24];
- Telecommunications and Information Working Group (TEL) of the Asia-Pacific Economic Cooperation (APEC) (see Box 7) and
- Forum of Incident Response and Security Teams (FIRST)[25].

Cyber Security Division, as well as initiatives under the Comprehensive National Cybersecurity Initiative. More information can be found at http://www.whitehouse.gov/omb/assets/fy2010_new_era/Department_of_Homeland_Security.pdf

[24] For more information, see http://www.oecd.org/department/0,3355,en_2649_34255_1_1_1_1_1,00.html

[25] The "Forum of Incident Response and Security Teams" (FIRST) was established in 1990 and provides a meeting point for CSIRTs worldwide. It promotes active cooperation in incident response. It is comprised of more than 200 public and private sector CSIRTs. Other regional forums and bodies

Box 7: The Asia-Pacific Economic Cooperation (APEC)

APEC is an inter-governmental grouping comprising 21 member economies. It has no treaty obligations required of its participants. Decisions made within APEC are reached by consensus and commitments are undertaken on a voluntary basis.

On May 30, 2002, the Telecommunications and Information Ministers of the APEC economies issued the 'Shanghai Declaration that included a Statement and Program of Action on the Security of Information and Communications Infrastructures. The Statement endorsed action by member economies to combat criminal misuse of information and instructed its Telecommunications and Information Working Group (TEL) to give special priority to work on the protection of information and communications infrastructures.

Initiatives that followed include:

- the APEC Cybersecurity Strategy, which includes a package of measures to protect business and consumers from cybercrime, and to strengthen consumer trust in the use of e-commerce;
- the TEL Cybercrime Legislation initiative and Enforcement Capacity Building Project that supports institutions in implementing new e-security laws; and
- the creation of APCERT, a regional CERT covering APEC member economies.

Source: APEC at http://www.apec.org/

It is also interesting to note that international regulator forums, such as the ITU Global Symposium for Regulators (GSR), as well as regional regulator groupings such as the Asia-Pacific Telecommunity (APT) and the Inter-American Telecommunication Commission (CITEL), are increasing their focus on cybersecurity issues[26]. These international and regional efforts serve to further reinforce the core competencies of regulators in the area of cybersecurity.

7.3 Policy-making

In a large number of countries, regulators play an important part in the development of a national ICT strategy or policy. Although the responsibility for ICT policy making in general is typically delegated to a political body such as a Ministry, regulators often play a key supporting role in policy-making by virtue of their familiarity with the sector that they regulate, the resources available to them, and the processes and mechanisms that have been put in place to engage in consultations with industry stakeholders.

Roles and responsibilities

From a survey of international examples, it is possible for regulators to take on a number of roles in the policy-making area:

- The lead role in cybersecurity policy-making (see, for example, Box 8); and
- Provider of advice and inputs on cybersecurity policy (see, for example, Box 9).

promoting cooperation among CSIRTs include the European Government CERTs group (EGC), NORDUnet, CEENet and APCERT (part of the Asia Pacific Economic Cooperation or APEC).

[26] See, for example, the initiatives undertaken by the APT at http://www.aptsec.org/links/NSS/Default.htm and the ongoing work of the CITEL Rapporteur Group on Cybersecurity and Critical Infrastructure at http://www.citel.oas.org/ccp1-tel/Cybersecurity.asp.

Box 8: Cybersecurity policy-making in Singapore

The Infocomm Development Authority of Singapore (IDA) acts as the national ICT regulator, the ICT development and promotion agency and the chief technology office of the Singapore government.

Singapore's cybersecurity strategy is encapsulated in two Infocomm Security Master-plans launched in 2005 and 2008. These master-plans provide a national strategic roadmap for the development of ICT security capabilities. They were developed through a multi-agency effort led by IDA through the guidance of the National Infocomm Security Committee (NISC).

Source: IDA at http://www.ida.gov.sg/

Box 9: Cybersecurity and the National Broadband Plan of the United States

As part of a wider national cybersecurity reassessment taking place in the United States, a comprehensive draft Cybersecurity Act has been introduced for adoption. Among other matters, the Cybersecurity Act delegates the Federal Communications Commission (FCC) with new responsibilities related to its implementation of the national broadband plan that it must develop under the American Recovery and Reinvestment Act of 2009. Under the Cybersecurity Act, the FCC is required to report on the most effective and efficient means of ensuring cybersecurity of commercial broadband networks. As part of its report, the FCC is required to consider consumer education and outreach programmes.

Source: Cybersecurity Act of 2009 (Introduced in Senate) at http://thomas.loc.gov/cgi-bin/query/z?c111:s773:

Core competencies

In most cases, regulators are poised to play a large role in the design of a national cybersecurity strategy and the formulation of related cybersecurity policies given their core competencies:

- Establishment of the role of the regulator in providing input on ICT policy making in general

As ICT sector specialists, regulators in many countries play a vital advisory role in the formulation of national ICT policy promulgated by national governments. In many countries, such a policy advisory role has been enshrined as one of the functions regulators have been tasked to perform.[27] With cybersecurity being increasingly recognized as a prominent ICT-related issue, regulators with policy advisory functions will increasingly find themselves required to provide inputs on cybersecurity issues. As part of their work on Next Generation Networks, many regulators are already examining the cybersecurity dimension of their introduction.

- Availability of tools vital to policy-making

As part of their ICT market oversight role, many regulators conduct studies and research, and collect and compile important data and information of the status of national ICT

[27] See, for example, Section 7 of the Bahamas' Communications Act (2009) and Section 1(2) of the Danish Act on the National Telecom Agency (Act No. 395 of 10 June 1997).

development and usage.[28] In the context of the formulation of a national cybersecurity strategy, such information can be used to highlight the importance of ICTs to the nation, the threats and vulnerabilities posed by such reliance, and the role cybersecurity plays in mitigating the risks.

- Establishment of mechanisms, processes and relationships for consultation and feedback

As part of the regulatory process, regulators in many countries are required to engage in consultation with sector stakeholders which can include industry, civil society and individuals. With these established mechanisms and relationships in place, regulators are in a position to solicit ICT stakeholder inputs on cybersecurity policy efficiently and quickly.

Observations and recommendations

A number of issues present themselves when regulators assume a larger role in cybersecurity policy-making. In some cases, these issues revolve around concerns to be addressed before a greater level of involvement on the part of the regulator can be assumed.

- Regulator as policy-maker

A greater involvement on the part of the regulator in policy making in general may threaten the traditional separation between policy-making and regulation. In the interest of the widely accepted principle of separation of powers, situations where a regulator formulates policy, implements related regulations, and enforces its application should be avoided.[29]

- Establishing the requisite mandates

While many regulators have been given an express mandate to provide input on ICT policy-making in general, this may not be so in the specific case of cybersecurity policy. In countries where regulators do not possess a mandate to provide input into cybersecurity policy-making, a change in the enabling legislation may be necessary. In most cases, however, such a mandate can be accommodated through the wide wording of existing provisions on the duties and functions of regulators (see, for example, the discussion on spam in the context of mandate and jurisdiction in Section 7.1.4 above).

- Building broad cross-sector expertise and establishing inter-agency relationships

An in-depth familiarity with the ICT sector addresses only one aspect of cybersecurity, albeit an important one. In order to take a prominent or leadership role in cybersecurity policy-making, the regulator also needs to be familiar with the ICT issues that affect other key sectors of the nation such as the finance sector, the energy sector, and the public sector as a whole. Such inter-sector links can be forged through the establishment of working groups, the initiation of informal collaboration on projects and other similar avenues.[30]

[28] For an overview of the ICT statistics and indicators made available through the websites of regulators, see http://www.itu.int/icteye/.
[29] See, in general, the discussion on Separation of Powers in the ITU-infoDev ICT Regulation Toolkit available at http://www.ictregulationtoolkit.org/en/Section.1269.html.
[30] See, for example, the general discussion on the importance of inter-agency links in ICT development in Francisco J. Proenza, "ICT-Enabled Networks, Public Sector Performance and the Development of

- Obtaining appropriate resourcing

As with the execution of any other role or responsibility of the regulator, the regulator must be in possession of the requisite resources and staffing in order to perform its policy-advisory role competently. In the context of cybersecurity policy-making, staffing in particular may be an issue where the regulator's manpower needs in the area of strategy and policy overlap with that of the main policy-maker. Such a situation may become a strain on skilled manpower resources in developing countries. In such a case the options of training or outsourcing may need to be considered (see also Section 7.1.5 above).

7.4 Legal measures

In most countries, the enactment of cybersecurity legislation is largely the prerogative of a country's legislature. The drafting of legislation, while typically entrusted to a legal institution such as the Attorney-General's Office or the Ministry of law, necessarily also takes into account a range of inputs from relevant government institutions.

The compliance and enforcement of cybersecurity laws are entrusted to law enforcement agencies that, in some circumstances, rely on the expert advice from more specialized government institutions. In some circumstances, regulators themselves have law enforcement powers associated with their mandates.

Roles and responsibilities

Regulators have assumed a range of roles and responsibilities in the area of legal infrastructure, compliance and law enforcement. These include:

- Acting in an advisory role in the drafting of cybersecurity related legislation (see Box 10);
- Providing technical training to legislators, prosecutors, the judiciary and law enforcement on the ICT related technical aspects of cybercrime;
- Acting in an advisory role in the development of specialized national cybercrime enforcement units;
- Providing technical assistance in the investigation of cybercrimes;
- Enforcing cybersecurity laws and regulations that are within the regulator's mandate (see Box 11); and
- Participation in international anti-cybercrime efforts (e.g. the 24/7 Cybercrime Point of Contact Network).

Box 10: Cybercrime and the role of the Nigerian Communications Commission (NCC)

The NCC is a member of the Nigerian Cybercrime Working Group (NCWG), an inter-agency group dealing with cyber crime which has the two-fold purpose of dealing with the security of computer systems and networks as well as the protection of the critical ICT infrastructure.

The NCWG has established a cybersecurity forum intended to build consensus among existing agencies and provide expertise to the National Assembly in drafting new computer security legislation (the Computer Security and Critical Information Infrastructure Protection Bill). The working group lays the groundwork for establishing new institutional capacity in Nigeria as well as for global cybercrime enforcement through relations with the Computer

Information and Communication Technologies", 2003 available at http://www.e-forall.org/pdf/ICTEnabledNetworks.pdf

Crime and Intellectual Property Section (CCIPS) of the United States Department of Justice, National High Tech Crime Center (NHTCC) in the United Kingdom and the National Prosecuting Authority (NPA) in South Africa.

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

Box 11: Enforcement of cybersecurity offences under Malaysia's Communications and Multimedia Act (CMA)

Information security and the integrity and reliability of the network of Malaysia are identified as one of the ten national policy objectives in the CMA. Together with the police, the Malaysian regulator, the Malaysian Communications and Multimedia Commission (MCMC) has enforcement powers for offences relating to network security in the CMA.

Source: Malaysian Communications and Multimedia Commission (MCMC) at http://www.skmm.gov.my/

Core competencies

The level and form of involvement of regulators in the area of legal infrastructure, compliance and enforcement can depend on:

- The nature of cybersecurity legislation

In many countries, regulators play a key role in the review and adaptation of a wide range of cybersecurity related legislation by providing input on the nature of cyber threats and cyber crimes. The role of the regulator in providing such advice varies depending on the subjective expertise of the regulator and the cybersecurity-related law at hand. For example, regulators in general would be more familiar providing input on laws dealing with data protection and security in electronic communications (including data transmission, safe data storage, etc.) as opposed to laws dealing with computer assisted fraud.

- Existing legal mandate

A legal mandate to undertake investigations and the enforcement of legal provisions is a basic prerequisite for a regulator's involvement in the compliance and enforcement of cybersecurity laws. In this respect, supportive legislation (e.g. the granting of a wide scope of powers necessary for investigation such as the ability to enter upon premises, seize equipment and retrieve and store incriminating data) is necessary for the regulator to perform such a role (see Box 10 above).

ICT legislation in most countries grants the regulator powers of investigation and enforcement over certain areas. In many cases, these typically extend to the use and abuse of ICT networks, physical damage to ICT installations and similar offences. As highlighted before, some regulators also exercise a mandate to counter malicious activities like spyware and spam under their wider duty of consumer protection.

- Appropriate resources

Even if a regulator is empowered with a mandate to ensure compliance with cybersecurity laws, the enforcement of such laws is often difficult. Frequently, the necessary means to

investigate and prosecute misdemeanors such crimes effectively are lacking due to resource constraints.

The conduct of investigation and enforcement proceedings consumes a significant amount of the limited resources available to regulators. In complex cases, investigations may take a long time to conclude with the process for prosecution taking an equally lengthy period of time. In such situations specialized manpower resources can be tied up indefinitely. In order to avoid the perception of the lack of law enforcement in affected areas, it is therefore important to ensure that regulators have the necessary resources to undertake the enforcement roles that they assume. Regulators can also collaborate with or seek the assistance of other law-enforcement agencies that may have more specialized resources available.

7.5 Organizational structures

7.5.1 Institutional organization and coordination

While regulators are not typically established as high-level governmental institutions (e.g. at presidential or cabinet level), an independent regulator can nevertheless play a significant role in both (1) the organization and coordination of cybersecurity roles and responsibilities among appropriate government institutions and (2) the establishment of coordination and cooperation mechanisms involving private sector cybersecurity stakeholders.

Roles and responsibilities

While it is unlikely for a regulator to take the lead in the delegation of cybersecurity responsibilities among government institutions - such a role is typically reserved for the highest-levels of government - a regulator can nevertheless play a key role in the coordination of governmental cybersecurity activities such as, for example, acting as secretariat for inter-governmental cybersecurity committees or task forces established by the lead cybersecurity institution (see Box 12) or by taking the initiative to forge cybersecurity relationships directly with other government institutions (see Box 13 below).

Box 12: Singapore's ICT regulator as secretariat for cybersecurity policy and institutional coordination

The National Infocomm Security Committee (NISC) was set up to formulate policies and strategic direction for cybersecurity at the national level. With members from various government agencies, it is a platform for the government to coordinate and institutionalize considered policies and mandate strategic initiatives in IT security.

The NISC comprises representatives from the Ministry of Home Affairs, the Ministry of Defence; the Ministry of Information, Communication and the Arts; the Ministry of Finance; and the Defence Science and Technology Agency (DSTA) among others. The ICT regulator, IDA serves as the secretariat for this Committee.

Source: Infocomm Development Authority of Singapore (IDA) at http://www.ida.gov.sg/

Core competencies

The degree to which regulators are adapted to these roles will depend on a number of core competencies:

- Establishment of relationships with national security institutions

A coordinating role in cybersecurity requires a high level of skills in bridge building, in particular with institutions that have intelligence and national security-related portfolios. In many countries policy concerns with cybersecurity are significantly influenced by national security and intelligence policies and the coordinator will have to have significant credibility in this area. In this respect, many regulators enjoy close working relationships with law-enforcement, defense and intelligence institutions in the areas of radio-frequency allocation, legal intercept, and crisis and emergency communications.

- Establishment of inter-agency relationships

The cybersecurity coordinator must be able to bring together other ministries or departments with sector-specific oversight of different critical infrastructure services and sectors. Cybersecurity often involves sectors such as finance (e.g. finance ministries and financial services authorities), energy (e.g. energy ministries and independent energy regulators), and health (e.g. health ministries and health authorities) (see Box 13).

Box 13: Inter-agency cooperation on cybersecurity in the United Arab Emirates (UAE)

In May 2009, the UAE Telecommunications Regulatory Authority (TRA) and the Ministry of Water and Environment signed a Memorandum of Understanding (MoU) on cooperation in cybersecurity. The MoU is expected to assist the Ministry in achieving its goals of enhancing the environmental security, adopting integrated management, increasing biological security, and achieving food security.

Under the MoU, aeCERT, an initiative of the TRA, will provide specific services to enhance the security of the Ministry's ICT infrastructure through the provision of consultancy services, education and awareness; incident monitoring and response; and research and analysis.

A similar MoU was subsequently signed between the TRA and the UAE Community Development Authority (CDA) in September 2009.

Source: UAE Telecommunications Regulatory Authority (TRA) at http://www.tra.gov.ae/.

Regulators that have the mandate of promoting ICT adoption in the public sector may already have mechanisms in place (e.g. working groups) that allow for inter-agency coordination and information exchange.

- Experience with breaking down compartmentalization

An important task of a cybersecurity coordinator will be to break down natural tendencies to "compartmentalize" cybersecurity activities in a series of separate sectors. In cybersecurity incidents in one sector will have potential relevance in other sectors. With their experience in dealing with convergence ICT regulators are in a good position to manage issues that the different sectors may attempt to compartmentalize or exclude. Regulators are also neatly positioned as neutrals in the cybersecurity discussion, with ICT networks and technologies being the common thread that runs through the different issues involved in cybersecurity.

Observations and recommendations

- Establishing inter-agency relationships

As mentioned above, the involvement of the regulator in the organization and coordination of government institutions involved in cybersecurity requires the regulator to have established working relationships with the lead cybersecurity institution as well as other government institutions involved in cybersecurity. Where this is absent, regulators may find it more appropriate to establish such relationships by participating actively in such coordinating bodies, while over time assuming greater responsibilities, such as the role of secretariat or convener. In parallel, independent inter-agency links should still continue to be forged (see the example in Box 13 above).

- Obtaining appropriate resources

The task of organization and coordination in general will compete with other pressing regulatory priorities; therefore regulators should be first assured that they have the resources to support the role that they intend to assume in this area of cybersecurity.

7.5.2 Incident management and cybersecurity readiness assessment

As mentioned in Section 2.1.3 above, one of the most critical aspects of an overall cybersecurity program is the capability to detect, to investigate and analyze, and to respond to cyber-related incidents.

Roles and responsibilities

In the area of incident management, a number of regulators have undertaken the following roles:

- Establishing national cybersecurity incident monitoring facilities (e.g., CSIRTs[31]) (See Box 14) and
- Participating in international and regional cybersecurity incident monitoring initiatives (e.g., Asia Pacific Computer Emergency Response Team (CERT), Forum of Incident Response Security Team (FIRST), etc.).

Box 14: Establishment of the Swedish IT Incident Centre (SITIC)

In May 2002, the regulator, the Swedish National Post and Telecom Agency (PTS) established the Swedish IT Incident Centre (SITIC). Officially launched in January 2003, the SITIC supports national activities for protection against IT incidents by:

- Operating a system for information exchange on IT incidents between public and private organizations and the SITIC;
- Operating a public warning system providing information on threats to IT systems;
- Providing information and advice on security and counter measures;
- Compiling and publishing incident statistics.

Source: Swedish IT Incident Centre (SITIC) at http://www.sitic.se/

In the area of cybersecurity risk assessments, a number of regulators have undertaken the following roles:

- Preparing and implementing periodic cybersecurity risk assessments, audits and reviews on a national or a sector-by-sector level (e.g., financial, manufacturing, retail, etc.) (see Box 15); and

[31] For example, in Finland, CERT-FI was established under the umbrella of the regulator, FICORA. Similarly, in the UAE, aeCERT was also established under an initiative by the regulator, TRA.

- Conducting cybersecurity exercises to test readiness and responsiveness.

Box 15: Critical Infocomm Infrastructure Surety Assessment in Singapore

Under the leadership of the Infocomm Development Authority of Singapore (IDA), the Critical Infocomm Infrastructure Surety Assessment project was established to assess the security readiness of Singapore's critical information and communications infrastructure. Initiated as a public-private sector project, it provides a platform for owners and operators of CII to work together and ascertain the adequacy of their protection measures.

Source: Infocomm Development Authority of Singapore (IDA) at http://www.ida.gov.sg/

Core competencies

- Crisis communications

The role of regulators in crisis related communications was highlighted in Section 7.1.4 above. Nevertheless, while responsibility for cybersecurity related emergencies may have been assumed by some regulators on the basis of their experience in this area, the nature of cybersecurity emergencies and crises are significantly different often requiring a more dedicated approach than might have been the case in the past. As such many regulators have set up CSIRTs that, while under the umbrella of the regulator, function as a specialized independent unit.[32]

- Consolidation of responsibilities and resources

The establishment of a CERT or similar body requires a certain amount of resources to be expended given its round the clock monitoring function. Similarly, the responsibility of regulators to maintain round the clock responsiveness to communications related emergencies and crisis acts as a similar drain on resources. In this respect, the consolidation of all communications related emergency monitoring functions in a single institution may result in synergies that allow for lower resource expenditure (see Box 16).

Box 16: Incident monitoring and alert consolidation in Hungary

Hungary's regulator, the National Communications Authority, is responsible for the National Alert Service (NAS) in the postal and communication sectors. The NAS is based on the cooperation of designated service providers who report incidents affecting their services to the NAS. The main tasks of the NAS are to gather and distribute information based on these reports and to coordinate service provider responses in the case of natural disasters and other emergencies.

Given the significant overlap in terms of incident reporting and timely information dissemination, the operation of the NAS is assumed by the national CERT (CERT-Hungary) that is managed by the Theodore Puskás Foundation. The activities of the Foundation are funded by the private sector and the national government.

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

[32] Ibid.

7.6 Capacity building

In Section 2.1.4 above, the importance of addressing cybersecurity awareness at the level of the end-user (i.e. individual businesses and consumers) was emphasized. In this regard, individual businesses and consumers can be empowered through a variety of means that would promote awareness and improve cybersecurity literacy and skills. Such initiatives increase the likelihood that end-users will consider cyber safety to be an integral part of the use of ICT products and services.

Roles and responsibilities

In the area of consumer awareness and capacity building, regulators can perform the following roles:

- Organization of cybersecurity awareness campaigns (e.g., media campaigns, online information resources, seminars, talks, road-shows, etc.) alone or in partnership with the private sector (see Box 17);
- Identifying cybersecurity education and training needs in the public and private sector and implementing initiatives to meet those needs; and
- Cultivate and develop a pool of cybersecurity professionals (see Box 18).

Box 17: Awareness campaigns in the United Kingdom

Get Safe Online is a public and private sector joint campaign to raise awareness of online security aimed at the general public and small businesses. Get Safe Online is sponsored by the United Kingdom Cabinet Office, the United Kingdom Office of Communications (Ofcom), the Serious Organised Crime Agency (SOCA), Microsoft, HSBC, Cable & Wireless, and Paypal.

The Get Safe Online initiative works with a range of community organizations and aims to give people the confidence to go online securely. The initiative coordinates marketing and PR activities as well as providing a comprehensive website with up-to-date advice, tools and guidance on general internet security. The website includes information on protecting individuals, families and businesses online, as well as advice on topics such as Internet shopping, social networking sites, data theft and identity fraud.

Source: http://www.getsafeonline.org

Box 18: Cybersecurity capacity-building in the Republic of Korea

In response to a spate of DDOS attacks in July 2009, the government of the Republic of Korea intends to train some 3,000 cybersecurity experts as part of measures to enhance Internet security. Announced by the Korean regulator, the Korea Communications Commission (KCC), the new measures, will involve the setting up of new departments in universities that will offer courses on information protection and provide support for the establishment of related research centers.

As part of the overall cybersecurity effort, the KCC will also undertake initiatives to encourage schools and companies to improve cybersecurity training and to raise awareness of Internet terrorism.

Source: Korea Communications Commission (KCC) at http://www.kcc.go.kr/

Core competencies

- Consumer protection initiatives

As part of the overall regulatory mandate of consumer protection, many regulators have been involved in the organization and implementation of consumer awareness initiatives that involve dissemination through a range of media (e.g. TV and newspaper advertising, websites, etc.). The same channels for dissemination can similarly be used for disseminating materials and information on cybersecurity.

- Adequate resourcing

Extensive campaigns involving media outlets such as television commercials, newspaper advertisements and online information involve a significant amount of resources that are likely to tax the resources of the regulator. To the furthest extent possible, such campaigns should be undertaken as part of a public-private partnership where resource needs can be shared between the regulator and the relevant private sector partners. Beyond resource sharing, public-private partnerships can bring significant synergies in the area of promoting end user awareness as businesses typically posses substantial experience in mounting advertising and promotion campaigns.

Observations and recommendations

- Ensuring that consumers as a class are able to have a say in cybersecurity policy

ICT regulators and policy-makers have an important role in dealing with consumers of telecom, ISP, and other ICT-related services. In particular, many regulators are tasked with an ICT consumer protection role, making them well positioned to make the case more broadly to the public and in government circles that consumers have an important role to play in developing an overall cybersecurity framework.

- Regulating to eliminate individual cybersecurity vulnerabilities

Given the significant cybersecurity vulnerabilities present at the level of the individual, the issue of whether regulations should be introduced to ensure a minimum degree of security at that level has been raised (see Box 19). This issue has also been discussed in the context of the mandatory requirement of licensing for end-users of PCs that are connected to the Internet.[33] Such an issue raises a range of policy questions that will require extensive consultations.

Box 19: Ensuring minimum security levels in Korea

Officials at the Korea Communications Commission (KCC), the country's broadcasting and telecommunications regulator, and the Korea Internet and Security Agency (KISA) confirmed they are planning to have Internet service providers, such as Korea Telecom, monitor the security levels of the computers and other devices used by their customers. The companies will limit or cut the Internet connectivity of users with less-than-required software protection, thus forcing them to upgrade their existing programs or download new ones.

[33] For an introduction to that discussion see, for example, "License PC Users? It's a Thought", available at http://www.wired.com/politics/law/news/2001/08/46096 and "Crime expert backs calls for license to compute" at http://www.itnews.com.au/News/154129,crime-expert-backs-calls-for-licence-to-compute.aspx

Government organizations, schools, private companies and "PC-bangs" (or computer gaming centers), will be mandated to install a required level of security programs on their computers and update them when needed.

The KCC will also be granted the rights to suspend the business of software companies that fail to correct the vulnerabilities of their security programs after being ordered to do so by authorities.

The new rules will also grant government authorities the power to shut down "zombie" PCs, or computers infected with malicious software and programmed to spread the cyber attacks. KCC authorities, with the consent of the computer's owner, could inspect the device to track the routes of the cyber attack.

Source: Adapted from the article "Online security steps criticized excessive" available at http://www.koreaittimes.com/story/5007/online-security-steps-criticized-excessive

7.7 Private sector cooperation and industry regulation

Roles and responsibilities

A large number of regulators are in a position to lead cybersecurity coordination and cooperation activities that involve the private sector and industry having both the mandate to engage the private sector in policy consultations (see Box 20) and promote industry self-regulation, and the experience to do so.

Box 20: The Communications Security, Reliability and Interoperability Council in the United States

In 2007, the Communications Security, Reliability, and Interoperability Council (CSRIC) was formed to provide recommendations to the Federal Communications Commission (FCC) to ensure optimal security, reliability, operability and interoperability of communications systems, including public safety, telecommunications, and media communications systems. Among other tasks, its mandate includes:

- Recommending best practices and actions the FCC can take to ensure the security, reliability, operability, and interoperability of public safety communications systems;
- Recommending best practices and actions the FCC can take to improve the reliability and resiliency of communications infrastructure;
- Evaluating ways to strengthen the collaboration between communications service providers and public safety entities during emergencies and make recommendations for how they can be improved;
- Recommending methods to measure reliably and accurately the extent to which key best practices are implemented both now and in the future; and
- Making recommendations with respect to such additional topics as the FCC may specify.

Source: United States Federal Communications Commission (FCC) at http://www.fcc.gov/

In the technical and procedural area of cybersecurity, the regulator is poised to assume a more traditional industry regulation role. These include:

- Encouraging public-private sector efforts to develop cybersecurity standards, procedures, and codes of conduct;
- Developing or enforcing mandatory cybersecurity regulations (see Box 21); and
- Mandating or encouraging the adoption of international cybersecurity standards (e.g., ISO 27001 on Information Security Management System) and recommended best practices.

Box 21: Mandatory cybersecurity requirements in Estonia

The country's regulator, the Technical Surveillance Authority (TJA), oversees companies operating in the field of electronic communications and ensures the compliance of these companies with security requirements.

In this respect, the Electronic Communications Act defines the requirements for the availability of electronic communications networks and communications services. In the area of cybersecurity, the security requirements set out include a requirement for communications undertakings to guarantee the security of a communications network and prevent third persons from accessing the data without legal grounds.

The TJA also oversees the implementation of the Digital Signatures Act and introduces regulations in that regard. It also supervises the certification service providers that provide services under the Act.

Source: Estonian Technical Surveillance Authority (TJA) at http://www.tja.ee/

In some countries where governments support ICT R&D, such support may be channeled through the regulator (e.g. Singapore, Japan). In such a situation, some of that support could be channeled into the research and development of new cybersecurity technologies, techniques, standards and processes in partnership with academia and the private sector (see Box 22).

Box 22: Cybersecurity technology research in Japan

In Japan, the regulator, the Ministry of Internal Affairs and Communications (MIC), is responsible for developing the fundamental national infrastructure of Japan, including information and communications. In order to realize "secure and safe" communications as a social infrastructure, MIC promotes various policies that reinforce information security.

As part of its cybersecurity role, the MIC conducts research related to fundamental technologies related to measures against cyber-attacks and other network security issues and to the protection of personal information in the field of ICT, and carries out measures to upgrade emergency information functions in the telecommunications area.

Source: Ministry of Internal Affairs and Communications (MIC), Japan at http://www.soumu.go.jp/english/ *and* International CIIP Handbook 2008/2009, Center for Security Studies, ETH, Zurich.

Core competencies

- Establishment of appropriate regulatory mandate

Ensuring the integrity of the main pipelines for delivery of ICT services is a key component of an overall cybersecurity program. With their familiarity in mandating and regulating technical standards and requirements, such as quality of service obligations,

regulators in general are well positioned to require or encourage providers of ICT backbone transmission and ISP services to adopt measures to minimize cybersecurity risks.

In a similar fashion, regulators can also play a critical role in providing a first line of defense against a range of new threats arising from the use of poorly protected PCs that are connected to the Internet (e.g. denial of service attacks using zombie PCs[34]) by encouraging or mandating service providers to include, as part of their service offering, access to cybersecurity protection for individual users.

Observations and recommendations

- Self-regulation and soft regulation

In most cases, regulators today have the mandate to require the adoption of standards or procedures in the interest of consumer protection or even general ICT development. Despite this mandate, regulators must constantly weigh, and use with restraint, their ability to impose regulatory obligations or lead industry debates about standards. To a large extent, the issue of cybersecurity is a developing one with technical standards and operational procedures still being defined.

Regulators need to be mindful of the benefits and drawbacks involved in maintaining a balance between regulation and industry self-regulation in the area of cybersecurity. Overzealous regulatory intervention at this stage may result in the adoption of safeguards and measures that are unduly onerous on the private sector, which in turn could affect market entry and the introduction of services. Instead, regulators may be able to leverage existing cybersecurity business practices emerging in the market through public consultations, calls for contributions and forms of "soft regulation", such as the issuance of best practice guidelines, or through self-regulation initiatives taken through public-private sector forums. Regulators in many countries, such as Switzerland, have sought to encourage private consensus building on the matter of cybersecurity standards and operational procedures, leaving decisions about implementation largely to industry.

On the other hand, the number and diversity of operators and service providers involved in certain areas of cybersecurity may be so great that the process of consensus building on certain pressing issues may take too long and regulators may instead need to consider the option of enacting new regulatory requirements.

- Participation in standards setting and coordination activities

The setting of cybersecurity standards is a relatively new field. As opposed to more traditional areas involving standards (e.g. mobile services), many regulators have yet to

[34] Denial of service attacks using "recruited" PCs, involve the following possibilities .The definition of denial of service as per the ITU, List of Security-Related Terms and Definitions available at http://www.itu.int/ITU-T/studygroups/com17/tel-security.html "1) The prevention of authorized access to resources or the delaying of time-critical operations. 2) In the context of message handling, when an entity fails to perform its function or prevents other entities from performing their functions, which may be a denial of access, a denial of communications, a deliberate suppression of messages to a particular recipient, a fabrication of extra traffic, an MTA was caused to fail or operate incorrectly, an MTS was caused to deny a service to other users. Denial of service threats include the following: denial of communications, MTA failure, MTS flooding. 3) This occurs when an entity fails to perform its function or prevents other entities from performing their functions. This may include denial of access to TMN and denial of communication by flooding the TMN. In a shared network, this threat can be recognized as a fabrication of extra traffic that floods the network, preventing others from using the network by delaying the traffic of others."

become established participants in cybersecurity standard setting activities. Ample opportunities, however, do exist for regulators to participate in this field through the established standard setting avenues and other coordinating roles of the International Telecommunications Union (ITU) and other regional bodies such as the Commission Interamericana de Telecomunicaciones (CITEL), and the European Commission.

PART III:

CONCLUSION AND RECOMMENDATIONS

8 The ICT/telecom regulator - a key player in a national team

Looking at the larger national interest, the most effective government led cybersecurity approach would entail each government institution assuming a role to which it is particularly suited for. From the discussion above and the illustrations given by international examples, it is clear that there are a wide range of roles available to regulators in which they can play a significant, if not the lead, part in a national cybersecurity effort.

The actual role a particular regulator can and should play, however, depends in general on a number of variables. In particular, the question of how cybersecurity and cyber threats are perceived as a nation is usually a key determinant of how cybersecurity roles and responsibilities are assigned among government institutions, with a technical, technological ICT focused perception of the problem being the most favorable to a large role for regulators.

The level to which regulators are able to demonstrate a number of core competencies are also critical in determining what role a regulator plays in the national cybersecurity effort. In this respect, the following observations and recommendations can be made:

The **maturity of the regulator** will determine, to some extent, perceptions regarding its efficiency and effectiveness by other more established agencies, especially those dealing with national security, defense and law-enforcement. This in turn will affect the regulator's ability to assume a lead position in a cybersecurity policy-making or organization and coordination role.

A regulator's ICT **technical and industrial expertise** and experience must also be viewed as a core competency. Its familiarity with the technology upon which cybersecurity is built is an asset that can be leveraged in a wide range of roles, from policy-making to reinforcing the legal infrastructure.

Establishing the **relevant mandate and jurisdiction** of the regulator is a key prerequisite in its assumption of roles and responsibilities in cybersecurity. Acting from a clear position of legitimacy will boost a regulator's leadership role especially in the areas of policy-making and organization and coordination. With regards to other areas of cybersecurity such as incident monitoring or building a culture of cybersecurity, it should be recognized that many regulators already have the requisite mandates, often related to responsibilities regarding consumer protection and crisis related communications, to assume the necessary roles and responsibilities.

Ensuring that the regulator has the **appropriate resourcing** for the roles and responsibilities it intends to carry out in the field of cybersecurity is another key prerequisite. While obtaining the necessary funding from appropriations and grants is ideal, the costs of a regulator's participation in cybersecurity roles can also be defrayed by working through public-private sector partnerships and by relying on the consolidation of tasks and roles.

A regulator's mechanisms and processes to facilitate **engagement of the private sector** in consultations and partnerships must also be viewed as a core competency that will be required when assuming a role in cybersecurity. Such a core competency will be vital in carrying out the role of policy making, private sector cooperation, incident management, and building a culture of cybersecurity.

Aside from these general core competencies, a regulator must also possesses core competencies related to a number of the cybersecurity roles discussed. These include:

- Policy making: Providing policy advice in ICT matters;
- Industry regulation: Mandating industry technical standards;
- Legal infrastructure: Investigation and enforcement of ICT related offences;
- Incident management and cybersecurity risk assessment: Managing crisis related communications; and
- Building a culture of cybersecurity: Promoting consumer awareness.

Only when these core competencies can be successfully demonstrated or obtained and prerequisites satisfied can a regulator assume key roles and responsibilities in the national cybersecurity effort.

***

Enhancing cybersecurity and improving CIIP are becoming increasingly important for developed and developing countries around the world in order to maximize societies' benefits from ICTs and manage the risks related to countries' growing dependency on these technologies. Given the changing environment and the specifics of cybersecurity and CIIP, the future role of the ICT/Telecom Sector Regulator and the Regulator's possible areas of responsibility require further discussion and analysis.

The purpose of this background paper was to provide an overview of the challenges that the ICT/Telecom Sector Regulator is facing when dealing with cybersecurity/critical information infrastructure protection (CIIP) issues and discuss how the active involvement of the ICT/Telecom Sector Regulator can positively and negatively impact the initiation, development, and implementation of a national cybersecurity strategy. We look forward to receiving your feedback on the usefulness of the material presented to provide further input and direction to ITU with regards to related activities that could be undertaken in this important and fast evolving area.

Please send any feedback you may have to cybmail@itu.int.
We look forward to hearing from you.

ICT Applications and Cybersecurity Division (CYB)
Policies and Strategies Department
Bureau for Telecommunication Development
International Telecommunication Union
Place des Nations
1211 Geneva 20
Switzerland
Telephone: +41 22 730 5825/6052
Fax: +41 22 730 5484
E-mail: cybmail@itu.int
Website: www.itu.int/ITU-D/cyb/