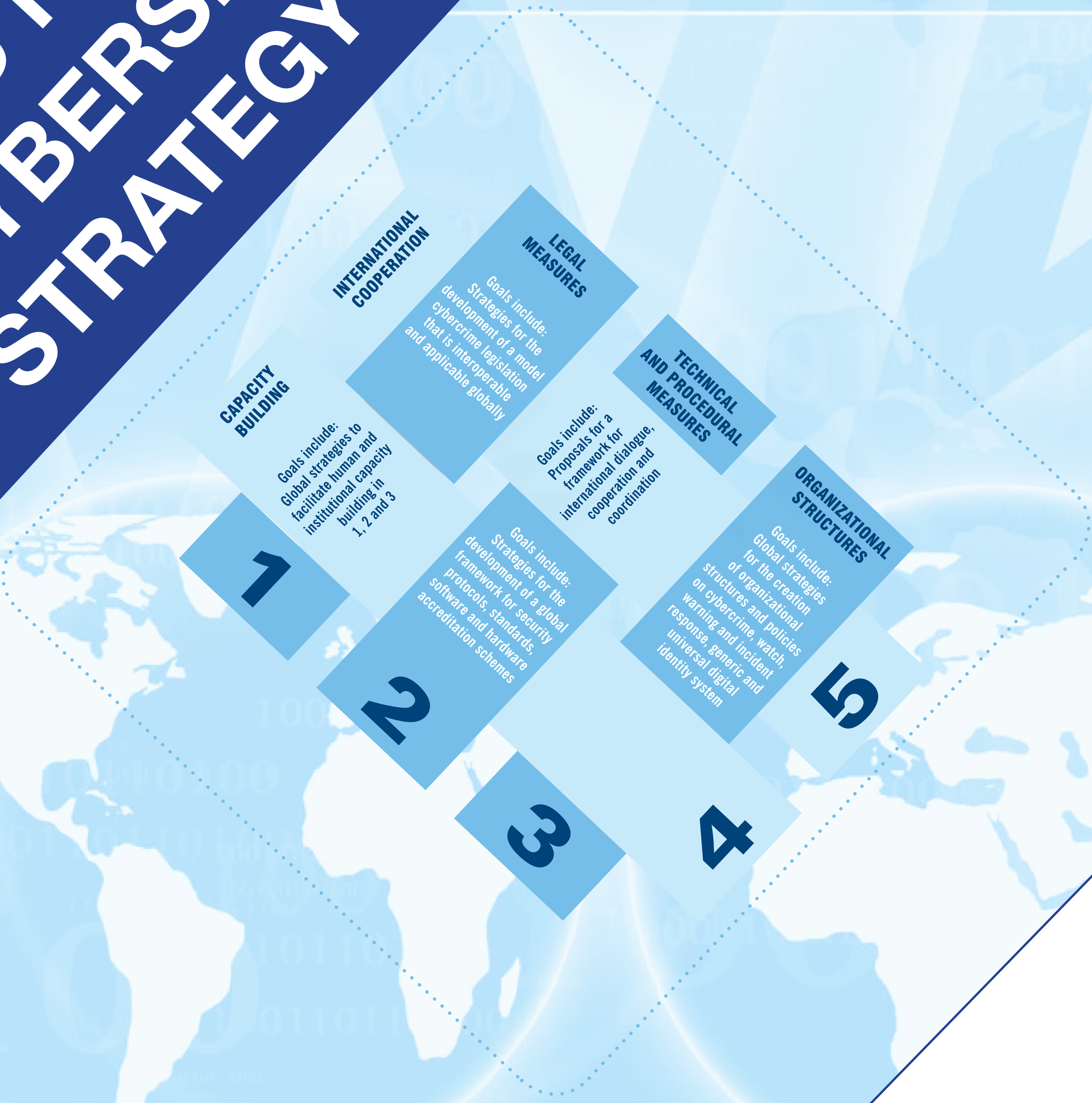
ITU NATIONAL CYBERSECURITY STRATEGY GUIDE

September 2011



1 CAPACITY BUILDING

Goals include: Global strategies to facilitate human and institutional capacity building in 1, 2 and 3

2 INTERNATIONAL COOPERATION

Goals include: Strategies for the development of a global framework for security protocols, standards, software and hardware accreditation schemes

3 LEGAL MEASURES

Goals include: Strategies for the development of a model cybercrime legislation that is interoperable and applicable globally

4 TECHNICAL AND PROCEDURAL MEASURES

Goals include: Proposals for a framework for international dialogue, cooperation and coordination

5 ORGANIZATIONAL STRUCTURES

Goals include: Global strategies for the creation of organizational structures and policies on cybercrime, watch, warning and incident response, generic and universal digital identity system

International Telecommunication Union

THE ITU NATIONAL CYBERSECURITY STRATEGY GUIDE

Dr. Frederick Wamala (Ph.D.), CISSP®

I. EXECUTIVE SUMMARY

1 EXECUTIVE SUMMARY

1.1 OVERVIEW

We use the term cyberspace to describe systems and services connected either directly to or indirectly to the Internet, telecommunications and computer networks. Modern life depends upon the timely, adequate and confidential performance of cyberspace. Thus, cybersecurity is important to all States because it endeavours to ensure that cyberspace continues to work when and as expected even under attack. We argue that cybersecurity is no longer a pure computer security issue. Instead, we see cybersecurity as a national policy matter because the illicit use of cyberspace could hamper economic, public health, safety and national security activities. Since governments mainly exist to maintain social order, protect the lives and property of their citizens and enable commerce, then national leaders are accountable for cybersecurity as it supports all the aforementioned services. We, thus, recommend that governments use all instruments of national power to reduce cyber risks appropriately. In particular, national leaders have accountability for devising a cybersecurity strategy and fostering local, national and global cross-sector cooperation. This document is a reference model for national cybersecurity strategy elaboration. We discuss what constitutes a national cybersecurity strategy; the typical ends it seeks to accomplish and the context that influences its execution. The Guide also discusses how States and other relevant stakeholders such as private sector organisations can build capacity to execute a cybersecurity strategy and the resources required to address risks.

1.2 SCOPE OF GUIDE

This document focuses on the issues that countries should consider when elaborating or reviewing national cybersecurity strategies. As national capabilities, needs and threats vary, we recommend that countries use national values as the basis for strategies for two main reasons. Firstly, culture and national interests influence the perception of risk and the relative success of defences against cyber threats. Secondly, a strategy rooted in national values is likely to gain support of stakeholders such as the judiciary and private sector. Cognisant of the multi-stakeholder nature of cybersecurity, we derive principles from the ITU Global Cybersecurity Agenda (GCA). The GCA is a holistic framework for coordinating, developing and implementing a robust global culture of cybersecurity. Since we consider cybersecurity as a national policy issue, we adopt the Ends-Ways-Means strategy paradigm due to its popularity with national policy makers. Lastly, since cybersecurity is a branch of information security, we adopt global security standards.

1.3 AUDIENCE

The primary audience for this Guide are parties that have responsibility for, or an interest in, cybersecurity. Inevitably, this audience is broad as cybersecurity touches practically all forms of social, economic and national security activity. Thus, this Guide will benefit anyone interested in the considerations for elaborating a national cybersecurity strategy. Beneficiaries include top government leaders, legislators, regulators, service providers and accreditors. We consider it important, at the outset, to emphasise that the success of strategies depends upon focusing on the right risks and involvement of all stakeholders.

1.4 CYBERSECURITY PROGRAMME ELEMENTS

Below is what we consider the main features of a holistic, multi-stakeholder and strategy-led cybersecurity programme. We focus on these elements throughout this Guide.

# ITEM	ELEMENTS OF A NATIONAL CYBERSECURITY PROGRAMME
1	**Top Government Cybersecurity Accountability** Top government leaders are accountable for devising a national strategy and fostering local, national and global cross-sector cooperation.
2	**National Cybersecurity Coordinator** An office or individual oversees cybersecurity activities across the country.
3	**National Cybersecurity Focal Point** A multi-agency body serves as a focal point for all activities dealing with the protection of a nation’s cyberspace against all types of cyber threats.
4	**Legal Measures** Typically, a country reviews and, if necessary, drafts new criminal law, procedures, and policy to deter, respond to and prosecute cybercrime.
5	**National Cybersecurity Framework** Countries typically adopt a Framework that defines minimum or mandatory security requirements on issues such as risk management and compliance.
6	**Computer Incident Response Team (CIRT)** A strategy-led programme contains incident management capabilities with national responsibility. The role analyses cyber threat trends, coordinates response and disseminates information to all relevant stakeholders.
7	**Cybersecurity Awareness and Education** A national programme should exist to raise awareness about cyber threats.
8	**Public-Private Sector Cybersecurity partnership** Governments should form meaningful partnership with the private sector.
9	**Cybersecurity Skills and Training Programme** A programme should help train cybersecurity professionals.
10	**International Cooperation** Global cooperation is vital due to the transnational nature of cyber threats.

Figure 1 – Elements of a National Cybersecurity Programme

1.5 HOW TO READ THIS GUIDE

This Guide aims to assist States as they build capacity to identify goals, constraints and stakeholders of a national cybersecurity strategy. We structure the document as follows:

1.5.1 Section I: Executive Summary

The Executive Summary presents the main proposals we make in the Guide.

1.5.2 Section II: Global Cybersecurity Context

In this section, we explore the value of cyberspace to global and national economic well-being and security. First, we contrast the terms cybersecurity and information security. We then consider the growing sophistication, frequency and gravity of cyber attacks. Thereafter, we discuss the cybersecurity concepts and themes that we use frequently in the Guide. Lastly, we explore the global nature of cybersecurity and the activities of the international community at the United Nations. We conclude with an evaluation of the ITU's role in cybersecurity as encapsulated in the Global Cybersecurity Agenda (GCA).

1.5.3 Section III: National Cybersecurity Context

The concepts of critical national infrastructure and critical information infrastructure allow us to explore the transformation of cybersecurity from a pure technical domain into a strategic national policy area. We then discuss the value of a national cybersecurity strategy. We follow on with reflection on the steps in the strategy formulation process. This section covers the conditions that influence national cybersecurity formulation and execution. We note typical stakeholders and their role in national cybersecurity strategy.

1.5.4 Section IV: National Cybersecurity Strategy Model

In this section, we present a model for visualising the national cybersecurity domain. The model could also support organisational and global cybersecurity programmes. We use the Pillars of the GCA and the Ends-Ways-Means strategy paradigm as the foundations for our dynamic view that grounds cybersecurity strategy in national values and interests.

1.5.5 Section V: Ends – Cybersecurity Objectives

Ends are the cybersecurity objectives that national administrations seek to accomplish. Cybersecurity ends cover economic, social and national security matters. This aligns with national interests as cybersecurity aims to keep States secure and prosperous.

1.5.6 Section VI: Ways – Priorities

In this section, we identify the approaches to executing the strategy. The GCA is ITU's overall cybersecurity framework. Thus, we present the ways in terms of the GCA Pillars.

1.5.7 Section VII: Means – Actions

We cover the resources that countries typically have to devote to achieving cybersecurity ends. The actions have a direct link to the priorities/GCA pillars.

1.5.8 Section VIII: Assurance & Monitoring

In this section, we discuss the activities required to validate that the cybersecurity tasks performed actually comply with the national cybersecurity strategy. We present ideas on how you may monitor the success of the cybersecurity programme.

1.5.9 Section IX: Annexes

This section concludes the Guide with a National Cybersecurity Strategy template.

Table of Contents

List of Figures

II. GLOBAL CYBERSECURITY CONTEXT

2 GLOBAL CONTEXT OF CYBERSECURITY

2.1 CYBERSECURITY AND INFORMATION SECURITY

It is a good bet that you are reading this Guide because you have responsibility for, or an interest in, cybersecurity. We are sure, therefore, that you know the terms cybersecurity and information security. Perhaps, even at expert level. For the benefit of all readers, we contrast the terms. We deem it an important exercise because the views formed about the two terms might either lead to a false sense of security or panic about cyber risks. Both concepts aim to attain and maintain the security properties of confidentiality[1], integrity[2] and availability[3] (ITU 2008d). However, the global reach of the Internet gives cybersecurity a unique character. First, whilst information security started when most systems were standalone and rarely traversed jurisdictions, cybersecurity works on global threats under legal uncertainty. Thus, laws created for information security are woefully inadequate[4] in the Internet era. Second, cybersecurity has to contend with an Internet architecture[5] that makes it virtually impossible to attribute an attack[6] to an actor (Sinks 2008). Third, due to its origins in the military and diplomatic services, information security typically focuses on confidentiality. Whilst WikiLeaks[7] underlined the import of confidentiality, cybersecurity focuses more on integrity[8] and availability[9]. Thus, cybersecurity is information security with jurisdictional uncertainty and attribution issues.

2.2 THE AGE OF CYBER ATTACKS

As we see later, a cyber attack occurs if a threat successfully breaches security controls. Evidence shows that cyber attacks are growing in sophistication, frequency and gravity. Our ever-growing reliance upon cyberspace places all Governments, businesses, other organisations and individual users at the risk of computer-enabled fraud, sabotage and vandalism. Accordingly, cyber threat actors routinely access, steal and corrupt sensitive corporate and government information. The ITU notes[10] that even prominent tech-savvy companies are not immune anymore. Reported victims of cyber attacks include Google, RSA, Sony, Lockheed Martin, PBS, Epsilon and Citibank. This list of victims includes security companies, defense contractors and some of the brightest lights in technology. We expect the list to be longer as many organisations do not report cyber attacks due to legal and reputational risk concerns. Worse still, a worrying number of organisations lack the capacity to detect attacks. Awareness of an attack is not an issue if the perpetrators

[1] Confidentiality focuses on providing assurance that access to information is restricted to authorised parties only

[2] The integrity principle deals with the prevention of unauthorised modification of information. Integrity also covers trust in the accuracy, completeness and thus reliability of information.

[3] Availability aims to provide assurance that assets will be accessible to authorised users in a timely manner if required.

[4] The UK Computer Misuse Act 1990 is a prime example. The law came into force well before the widespread use of the Internet and in particular the World Wide Web. The UK updated its cybercrime law under Police and Justice Act 2006.

[5] IPv6, the upgrade from IPv4 will significantly reduce the anonymity of online transactions

[6] Find the ITU Security Manual here: http://www.itu.int/dms_pub/itu-t/opb/hdb/T-HDB-SEC.04-2009-PDF-E.pdf

[7] WikiLeaks enabled one of the largest unauthorised computerised disclosures of classified government information.

[8] Integrity is a focus due to low trust in the accuracy, completeness and hence reliability of information.

[9] Availability is critical in cyberspace due to concerns that information, systems and assets may not be available to authorised users in a timely manner if required.

[10] Obtain the ITU “Making the Online World Safer” document here: http://www.itu.int/net/itunews/issues/2011/05/38.aspx

are hacktivist[11] groups such as Anonymous and Lulzsec that seek notoriety. However, cybersecurity and national security strategists are extremely concerned about targeted compromises or 'Advanced Persistent Threats (APTs). McAfee describes APTs as:

> "More insidious and occur largely without public disclosures. They present a far greater threat to companies and governments, as the adversary is tenaciously persistent in achieving their objectives. The key to these intrusions is that the adversary is motivated by a massive hunger for secrets and intellectual property; this is different from the immediate financial gratification that drives much of cybercrime, another serious but more manageable threat (Alperovitch 2011)."

Independent researchers[12] have identified attacks similar to the McAfee discovery that targeted high value diplomatic, political, economic and military targets. In common with McAfee, victims included governments, businesses and international organisations[13]. As expected, researchers were unable to attribute the attacks to a particular actor.

2.3 CYBERSECURITY: A GLOBAL CHALLENGE

Policy makers are only waking up to the challenges of cyberspace (Drew and Snow 2006). In contrast to land, air, sea and space, cyberspace poses the following unique difficulties. First, due to the global reach of ubiquitous networks, threat actors can launch distressing attacks far from victims and often in jurisdictions with weak laws and/or no enforcement. Second, fast connection speeds give victims little time to defend against attacks. Thus, at best, States and organisations only know about an attack when it is process. At worst, victims do not discover the compromise of their critical systems. Indeed, a report from a major security company alleged that many of the 72 States[14] and public and private sectors organisations subjected to a five-year campaign of cyber attacks were unaware of the targeted compromises. Third, whereas States pursue national interests through a rules-based international system, cyberspace does not have accepted norms and principles of proportionality. Indeed, whilst a country typically requires the approval of the United Nations to participate in the activities of the community of nations, any actor can setup in cyberspace and do whatever they please. Actors such organised criminals, insurgents and terrorists do not worry about norms and do not fear retaliation chiefly due to the difficulty of attributing an attack to a given actor. The lack of accepted norms in cyberspace is reducing confidence in the use of ICTs. Indeed, the United Nations Resolutions that we discuss in section 3 show that cybersecurity has been a concern of the international community for many years.

[11] Hacktivism (a portmanteau of hack and activism) is the use of computers and computer networks as a means of protest to promote political ends, according to Wikipedia, the online encyclopaedia.

[12] GhostNet report here: http://www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/

[13] Shadows Report: http://www.infowar-monitor.net/2010/04/shadows-in-the-cloud-an-investigation-into-cyber-espionage-2-0/

[14] The "Operation Shady RAT" report is here: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

2.4 CYBERSECURITY CONCEPTS

We shall now define the cybersecurity concepts that we use throughout the Guide.

2.4.1 CYBER THREATS

The term cyber threat is part of the popular press lexicon. Whenever we use this phrase in this Guide, know that we mean a potential violation of security properties (ITU 2009f). We further differentiate threats by character, impact, origin and actor as follows:

2.4.1.1 Accidental or Intentional Threats

Accidental threats occur without premeditated intent. For example, system or software malfunctions and physical failures. However, intentional threats result from deliberate acts against the security of an asset. Intentional threats range from casual examination of a computer network using easily available monitoring tools, to sophisticated attacks using special system knowledge. Intentional threats that materialise become *attacks*.

2.4.1.2 Active or Passive Threats

Active threats are ones that result in some change to the state or operation of a system, such as the modification of data and the destruction of physical equipment. Conversely, passive threats do not involve a change of state to the equipment. Passive threats aim to glean information from a system without affecting the resources of the system. Common passive threat techniques include eavesdropping, wiretapping and deep packet analysis or inspections. Successful passive threats become passive attacks.

2.4.1.3 Threat Source

We regard a threat source as an entity that desires to breach information or physical assets' security controls. The threat source ultimately aims to benefit from the breach for example financially. We identify what we regard as the main threat sources in Figure 2.

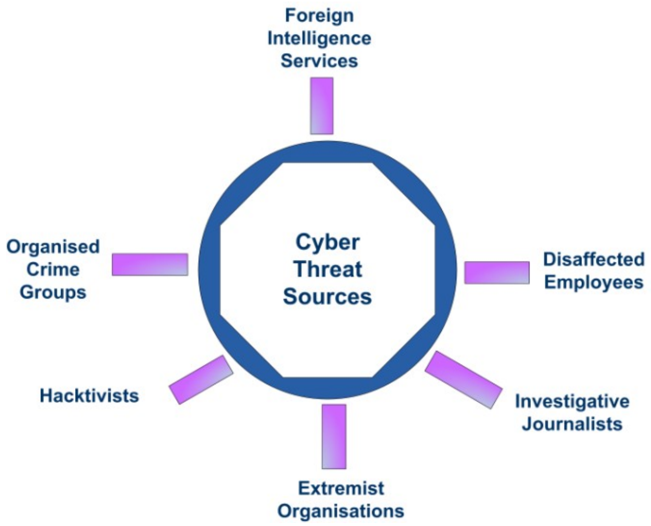


Figure 2 – Common Cyber Threat Sources

2.4.1.4 Threat Actor

A threat actor is an entity that actually performs the attack or, in the case of accidents, will exploit the accident. For example, if an organised crime group corrupts an employee, then the group is the *Threat Source* and the employee is the *Threat Actor*.

2.4.1.5 Vulnerability

The intentions of threat sources and threat actors often materialise into attacks largely because they exploit weaknesses in the security controls. The weakness may include lack of software patching and poor configuration. Even sound technical controls may fail if social engineering attacks dupe staff with weak knowledge into breaching security.

2.4.2 SECURITY RISK

Whenever you see phrases security risk or cyber risk, know that we mean the probability that a threat will exploit a vulnerability to breach the security of an asset. It is important for States to manage cyber risks. However, as most readers know, functional IT systems operate with a degree of exposure to threats because full elimination of risk is either too expensive or undesirable. As such, a national cybersecurity strategy is the first step in ensuring that all stakeholders assume responsibility for and take steps to reduce risk.

2.4.3 CYBER ATTACKS

A cyber attack occurs when a threat breaches security controls around a physical or an information asset. We categorise cyber attacks by state and origin as follows:

2.4.3.1 Active and Passive Attacks

An "active" attack aims to alter system resources or affect their operation. Conversely, a "passive" attack seeks to use information from a system but does not affect system resources of that system (IETF 2007). Instead, passive attacks aim to obtain data for an off-line attack. For example, hackers typically use packet inspection and analysis to facilitate offline review of security protocols and thus fine-tune exploits.

2.4.3.2 Inside and Outside Attacks

We may also characterise attacks according to their initiation point. The Internet Security Glossary describes an “Inside Attack” as one that is initiated by an entity inside the security perimeter (an "insider"). Insider attacks are difficult to defend against because the culprits misuse the access privileges obtained for legitimate business functions. In contrast, unauthorised or illegitimate users initiate "outside” attacks outside the security perimeter. Outsider attackers include hackers, organised criminal groups and States. The attack types are not mutually exclusive as outsiders often rely on insiders.

3 UN CYBERSECURITY ACTIVITIES

3.1 RESOLUTIONS ON CYBERSECURITY

Cybersecurity has been high on the agenda of the United Nations (UN) for a number of years. The UN took up the subject out of recognition that building trust and confidence in the use of ICTs is crucial to the socio-economic well-being of humanity. As a result, the UN General Assembly (UNGA) has expressed itself on cybersecurity matters in five major Resolutions. Next, we explore the relevant Resolutions to assess the views of the international community on cybersecurity.

3.1.1 A/RES/55/63: COMBATING CRIMINAL USE OF ICTs

The Resolution issued on 4th December 2000 focused on combating the criminal misuse of information technologies. It draws on the United Nations Millennium Declaration[15] and asks States to ensure that the benefits of the new technologies are available to all. The Resolution is relevant to this Guide as follows. It recognises that free flow of information can promote economic and social development, education and democratic governance. Indeed, the Resolution warns that unless addressed, the increasing criminal misuse of information technologies may have grave impacts on all States.

[15] Obtain a copy of the UN Millennium Declaration here: http://www.un.org/millennium/declaration/ares552e.htm

3.1.2 A/RES/56/121: COMBATING CRIMINAL USE OF ICTs

Issued on 19th December 2001, the Resolution covers similar ground to A/RES/55/63. It calls on States to coordinate and cooperate against criminal misuse of ICTs. Crucially, the Resolution calls for national law, policy and practice to combat computer crime.

3.1.3 A/RES/57/239: CULTURE OF CYBERSECURITY

The Resolution focuses on the creation of a global culture of cybersecurity. Issued on 20th December 2002, it notes the growing depending of Governments, businesses, other organisations and individual users on information technologies. The Resolution notes that cybersecurity requirements increase as countries increase their participation in the information society. The Resolution makes it clear that government and law enforcement cannot address cybersecurity alone without the support of all stakeholders.

3.1.4 A/RES/58/199: CRITICAL INFRASTRUCTURE

This Resolution also deals with the creation of a global culture of cybersecurity and the protection of critical information infrastructures. Issued on 23rd December 2003, it notes the growing reliance on information infrastructures by critical national services in areas such as energy generation, transmission and distribution; air and maritime transport, banking and financial services, water supply, food distribution and public health. Thus, the Resolution invites UN Member States to develop strategies for reducing risks to critical information infrastructures, in accordance with national laws and regulations.

3.1.5 A/RES/64/211: GLOBAL CULTURE OF CYBERSECURITY

This Resolution covers similar ground to the preceding four Resolutions. The Resolution considers the outcomes of the two phases of the World Summit on the Information Summit (WSIS). As we shall see next, the WSIS appointed ITU as the sole moderator of Action Line C5 focusing on “Building Confidence and Trust in the use of ICTs.” This Guide is in support of ITU’s obligations under the WSIS Action Line C5.

4 ITU CYBERSECURITY ACTIVITIES

ITU has played an important role in global telecommunications, information security and standards setting in different capacities since its formulation in 1865. ITU became the United Nations’ specialised agency in the field of telecommunications, information and communication technologies ICTs in 1949. As the leading UN Agency on ICTs, ITU is the global focal point for governments and the private sector in developing networks, services and mechanisms against threats and vulnerabilities. Therefore, ITU implements

UN Resolutions aimed at spreading benefits of the new technologies to all nations. Next, we explore ITU's cybersecurity mandate and concomitant activities.

4.1 WORLD SUMMIT ON THE INFORMATION SOCIETY (WSIS)

The UN General Assembly Resolution 56/183 (21 December 2001) endorsed the holding of the World Summit on the Information Society (WSIS) in two phases[16]. The first WSIS phase took place in Geneva, Switzerland from 10 to 12 December 2003. The second phase took place in Tunis, Tunisia from 16 to 18 November 2005.

4.2 WSIS ACTION LINE C5

The WSIS Tunis Agenda underlined the value of multi-stakeholder action at international level. The Agenda took into account the themes and Action Lines in the earlier Geneva Plan of Action. The two Summits asked UN Agencies to facilitate Action Lines in areas of their expertise. As noted above, ITU is the specialised UN ICT agency. Therefore, world leaders participating in WSIS entrusted the ITU with the role of sole Moderator/Facilitator of Action Line C5, "Building confidence and security in the use of ICTs." On 17 May 2007 newly elected ITU Secretary-General Dr. Hamadoun I. Touré launched the ITU Global Cybersecurity Agenda (GCA). The initiation of the GCA was in response to the WSIS Action Line C5 mandate as well as the instructions of the ITU Membership.

4.3 GLOBAL CYBERSECURITY AGENDA (GCA)

The GCA is a framework for international multi-stakeholder cooperation on cybersecurity. It aims to build synergies with current and future initiatives and partners towards a safer and more secure information society. The GCA encourages collaboration with and between all relevant partners and builds on existing initiatives to avoid duplicating efforts (ITU 2010f). The 2010 Plenipotentiary Conference in Resolutions 130 and 170 reaffirmed the importance of the GCA and ITU's role in public policy issues related to the illicit use of ICTs respectively. Within ITU, the GCA aggregates cybersecurity activities in the three[17] sectors. Figure 3 below illustrates the five Pillars/Work Areas of the GCA:

[16] This paragraph is an extract from the WSIS website. For more information visit: http://www.itu.int/wsis/index.html

[17] The ITU operates in three sectors namely Development (ITU-D), Standardization (ITU-T) and Radiocommunication (ITU-R).

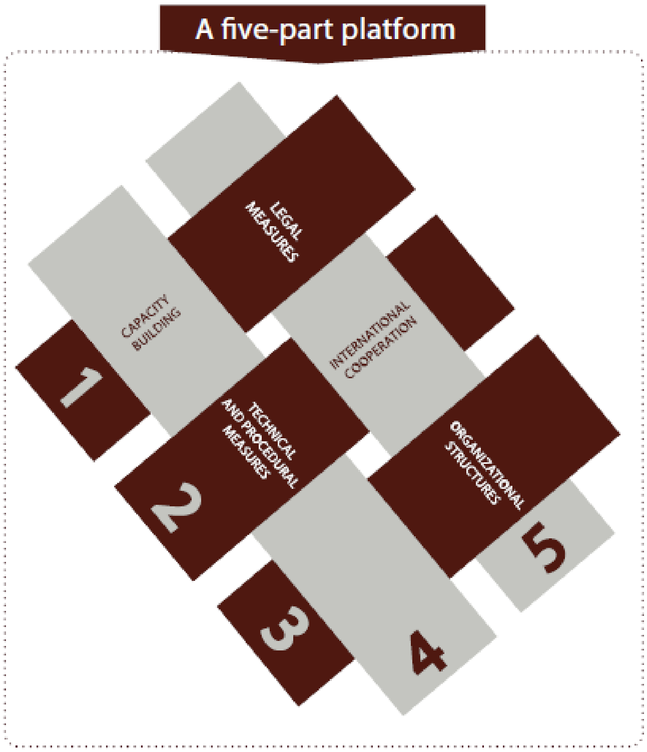

A five-part platform
LEGAL MEASURES
CAPACITY BUILDING
INTERNATIONAL COOPERATION
TECHNICAL AND PROCEDURAL MEASURES
ORGANIZATIONAL STRUCTURES
1
2
3
4
5

Figure 3 – Pillars of the Global Cybersecurity Agenda (GCA)

4.3.1 Pillar 1 – Legal Measures

This Pillar seeks to elaborate strategies for the development of model globally applicable and interoperable cybercrime legislation. The overall goal of the Pillar is to develop advice and internationally compatible processes for handling crime committed over ICTs.

4.3.2 Pillar 2 – Technical and Procedural Measures

This Pillar focuses on measures for addressing vulnerabilities in software products. The pillar aims to devise globally acceptable accreditation schemes, protocols and standards.

4.3.3 Pillar 3 – Organizational Structures

The Pillar aims to create organisational structures and strategies to help prevent, detect and respond to attacks against critical information infrastructures.

4.3.4 Pillar 4 – Capacity Building

This Pillar seeks to elaborate strategies for enhancing knowledge and expertise to boost cybersecurity on the national policy agenda.

4.3.5 Pillar 5 – International Cooperation

The Pillar focuses on strategies for international cooperation, dialogue and coordination.

4.3.6 GCA Strategic Goals

On top of the five Pillars, the GCA contains seven strategic goals. These are:

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

4.4 THE CHILD ONLINE PROTECTION (COP) INITIATIVE

The Child Online Protection[18] (COP) Initiative is the first specialised GCA programme. ITU Secretary General, Dr Touré states that the ITU launched COP to "kick-start the process of forging international consensus and focus.[19]" Dr Touré adds, 'This says to the world: "we need to start to get agreement on these issues, and it's clear that we can all agree on the need to protect children as a first step." COP will serve as a template for future negotiations and consensus in cybersecurity issues.' The initiative aims to: (a) identify risks and vulnerabilities to children in cyberspace; (b) create awareness; (c) develop practical tools to help minimise risk; and (d) share knowledge and experience.

As a GCA initiative, COP takes a multi-stakeholder approach to defending children's best interests. A collaborative approach is necessary because child online protection issues are global in nature and thus must take into account the role of different stakeholders as well as existing initiatives. The holistic approach aims to tackle risks to children through the five GCA pillars without duplicating effort. COP has created a network to promote the

[18] For more information on ITU's Child Online Protection Initiative please visit the website: http://www.itu.int/cop/
[19] Questions & Answers – Dr Hamadoun I. Touré, ITU Secretary-General at http://www.itu.int/net/pressoffice/facts/sg.aspx

online protection of children worldwide by providing guidance on safe online behaviour in conjunction with other UN agencies and partners. The UN Secretary–General, Heads of State, Ministers and heads of international organisations have all endorsed the Initiative.

4.4.1 Online Child Protection Guidelines

Creating awareness and sharing knowledge and experience are two of COP's key objectives. COP sees the risks facing children online as including inappropriate content; violence; online gaming and addiction; online fraud; cyber bullying and racism. As such, COP has issued a set child online protection guidelines[20]. The guidelines are the work of ITU, ICT sector contributors and child online safety institutions. The four guidelines are for children; parents, guardians and educators, industry and policy makers.

4.4.2 COP New Phase

On 17th November 2010, the ITU launched a new COP phase. The new phase aims to encourage the development of national COP centres, awareness campaigns and community forums to create a safe environment for young users of the Internet. Building on the Guidelines, the phase focuses on the development of industry codes of conduct; national hotlines; national roadmaps and legislative toolkits; training and collaboration through online platforms. We should note that national online child protection strategies follow the same approach as this Guide since COP is a GCA initiative.

4.5 GCA PARTNERSHIPS

4.5.1 ITU-IMPACT Alliance

The GCA is both a framework for visualising the global cybersecurity domain and a tool for guiding national action. Therefore, on 3rd September 2008, ITU and the International Multilateral Partnership Against Cyber Threats (IMPACT) signed an agreement that made IMPACT the GCA operational home and executing arm on behalf of ITU. The venture avails expertise and resources to detect, analyse and respond effectively to cyber threats to over 136 ITU Member States[21]. The coalition is of particular benefit to countries that lack the resources to develop their own cyber response centres. However, we encourage developed nations to consider joining the alliance because it provides a superb snapshot of potential or real cyber risks, threats and vulnerabilities. ITU-IMPACT also offers managed security services to the United Nations family. The activities of IMPACT match the GCA Pillars and Goals as follows:

4.5.1.1 GCA Pillars and IMPACT Activities

IMPACT activities support the GCA in the following ways. First, the IMPACT Centre for Policy and International Cooperation[22] supports ITU's Legal Measures objectives as

[20] Obtain copies of the Online Child Protection guidelines at: http://www.itu.int/osg/csd/cybersecurity/gca/cop/
[21] Visit the IMPACT website for a current list of participating ITU Member States at http://impact-alliance.org/home/index.html
[22] Explore Centre for Policy and International Cooperation: http://www.impact-alliance.org/services/centre-for-policy-policy.html

outlined in GCA Pillar one. Second, IMPACT's Global Response Centre[23] supports GCA Goal four that focuses on strategies for the creation of a global framework for watch, warning and incident response. Third, IMPACT's Centre for Security Assurance and Research[24] supports GCA Goal two. The goal sits between the Legal Measures and Organisational Structures GCA Pillars. Fourth, IMPACT's Centre for Training and Skills Development[25] supports GCA Goal six. In common, with the next Goal, facilitation of human and institutional capacity building cuts across all GCA Pillars and Goals. Lastly, IMPACT's Centre for Policy and International Cooperation supports GCA Goal seven.

4.5.2 UNODC Agreement

On 19th May 2011, the ITU signed an agreement with the United Nations Office on Drugs and Crime (UNODC). The organisations signed Memorandum of Understanding (MoU) at the WSIS Forum 2011 event in Geneva. The organisations will collaborate in assisting ITU and United Nations Member States mitigate the risks posed by cybercrime. Areas of collaboration include legal measures; capacity building and technical assistance; organisational structures and international cooperation. Other areas are knowledge and data mechanisms; intergovernmental and expert meetings and the comprehensive study of cybercrime. The two organisations – within the UN system – further agreed to organise joint assessment missions, conferences and training activities.

4.5.3 Symantec Partnership

The ITU draws its Membership from public and private sectors. Therefore, in keeping with the public-private partnership tradition, ITU has also signed a MoU with Symantec Corporation. The company is a provider of security, storage and systems management solutions. Under the agreement, Symantec will avail quarterly Internet Security Threat Reports to increase awareness of and readiness for cybersecurity risks among the ITU Membership. ITU will distribute the reports to interested Member States to help improve response to cyber threats. Raising awareness and transferring knowledge complements the work of ITU and strengthens its effectiveness as the sole Moderator/Facilitator of the WSIS Action Line C5 dealing with "Building confidence and security in the use of ICTs."

[23] Explore the Global Response Centre at: http://www.impact-alliance.org/services/grc-introduction.html
[24] Centre for Security Assurance and Research here: http://www.impact-alliance.org/services/centre-for-security-igss.html
[25] Explore Training and Skills Development at: http://www.impact-alliance.org/services/centre-for-training-overview.html

III. NATIONAL CYBERSECURITY CONTEXT

5 NATIONAL CYBERSECURITY CONTEXT

In the previous section, we explored the global nature of the cybersecurity challenge. We noted that cybersecurity has been a worry of the international community for many years. We considered five United Nations cybersecurity Resolutions that warn that failure to fix the issue may lead to grave impacts on all States. Next, we explore how cyberspace has graduated from a technical to a strategic domain. The reliance of States on cyberspace for daily tasks, commerce and national security underlines the domain's strategic value.

5.1 CRITICAL INFRASTRUCTURE

Cybersecurity requires coordinated cross-sector cooperation because cyberspace both supports and constitutes critical infrastructure (CI). ITU-D Study Group 1[26] defines CI as "the key systems, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of these (ITU 2008a)." Whilst what comprises CI varies across States, in this Guide we regard typical infrastructure sectors as including health, water, transport, communications, government, energy, food, finance and emergency services sectors.

5.1.1 Critical Information Infrastructure

ITU-D Study Group 1 notes that all the critical infrastructure sectors rely upon physical infrastructure such as buildings, roads, plants and pipes. Increasingly, the critical sectors also rely on cyberspace[27] and the information and communication technologies (ICTs) that enable it. The Study Group classifies cyberspace and its supporting ICTs as critical information infrastructure (CIII). The CII operates and controls the critical sectors and their physical assets. Consequently, ensuring the reliable functioning of cyberspace is a strategic[28] national objective because the lack of trust and confidence in the use of ICTs could hinder daily life, commerce and national security. Cybersecurity is a strategic domain because the complexity and interconnectedness of CII across critical sectors makes it difficult to predict the outcome of a cyber attack. ITU Study Group 1 sees a critical information infrastructure protection programmes (CIIP) as about protecting the virtual aspect of CII. In this Guide, we use the phrase CIIP interchangeably with national cybersecurity programmes. Figure 4 shows how Study Group 1 visualises the domain.

[26] The ITU-D Study Group 1 addresses telecommunication policies and regulatory strategies, which best enable countries to benefit from the impetus of telecommunications as an engine of economic, social and cultural development.

[27] We use the terms cyberspace, cyber environment and critical information infrastructure interchangeably. Recommendation ITU-T X.1205 contains a detailed definition of terms. Obtain a copy here: http://www.itu.int/rec/T-REC-X.1205-200804-I

[28] According to management guru, Peter Drucker, strategic objectives fall into eight classifications including market standing (share present and new markets); innovation (development of new goods and services) and productivity (efficient use of resources relative to the output). Reliably functioning critical information infrastructures supports these strategic objectives.

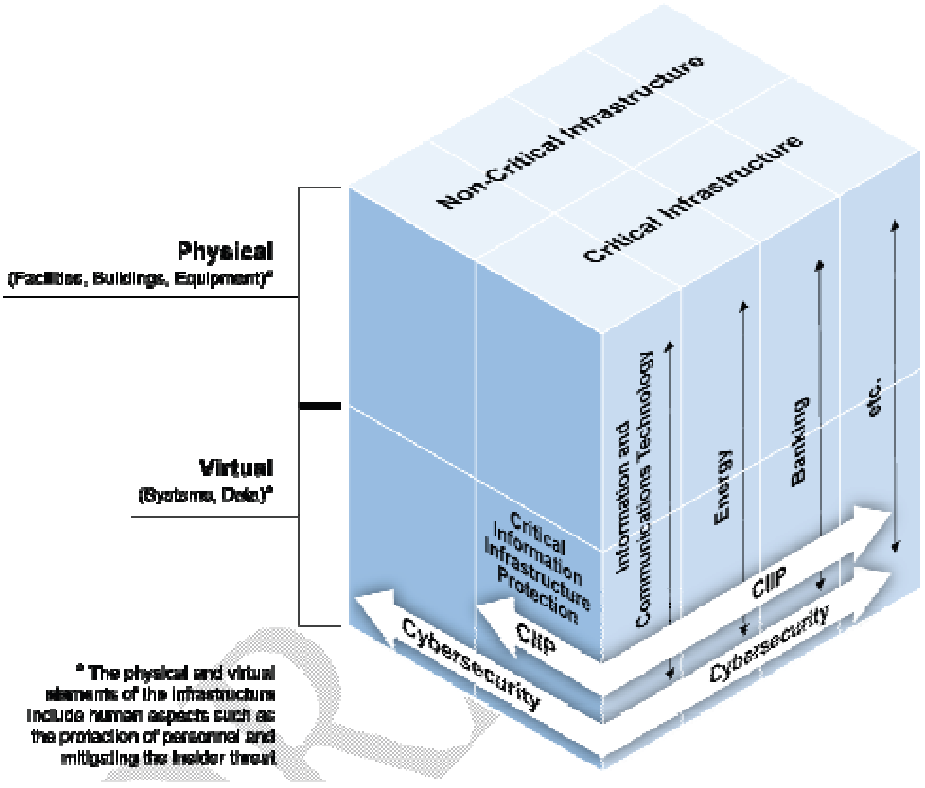

Non-Critical Infrastructure
Critical Infrastructure
Physical
(Facilities, Buildings, Equipment)*
Virtual
(Systems, Data)*
* The physical and virtual elements of the infrastructure include human aspects such as the protection of personnel and mitigating the insider threat
Information and Communications Technology
Energy
Banking
etc.
Critical Information Infrastructure Protection
CIIP
Cybersecurity
CIIP
Cybersecurity

Figure 4 – Critical Infrastructure Protection and Cybersecurity

5.2 PURPOSE OF A CYBERSECURITY STRATEGY

We now proffer ideas that could help national leaders convince other stakeholders of the importance of a national cybersecurity strategy and their roles and responsibilities. We begin with the premise that all relevant stakeholders understand the contribution that CII make to the delivery services essential to daily life, commerce and national security. Yet the stakeholders may lack knowledge about the steps required to enhance the security of systems under their ownership and/or use. The stakeholders would also require help in understanding their role in improving cybersecurity. We offer the suggestions below.

5.2.1 Focus of National Cybersecurity Strategy

Cybersecurity is a global challenge. Thus, a coordinated multi-sector response provides the only plausible route to building public confidence and trust in the use of ICTs. Since we do not have a world government, global efforts rely on national action. States are vital players in cybersecurity because they hold the legal, economic and diplomatic tools that determine the success of the Pillars of the Global Cybersecurity Agenda. Based on our experience of advising ITU Member States, we provide three main reasons for justifying strategies. However, feel free to come up with reasons most suited to your local setting.

5.2.1.1 Treats Cyberspace as a strategic domain

Promoters of a national cybersecurity strategy (hereafter "strategy") should consider highlighting the value of cyberspace to achieving strategic national objectives. One may note that States devise strategies for land, air, sea and space domains because of their criticality to achieving national interests. Similarly, one may point out that States require a strategy for securing cyberspace because of its growing contribution to the delivery of services essential to daily life, commerce, national security, innovation and the general free flow of information[29]. Therefore, strategies help mitigate the impact of cyber attacks.

5.2.1.2 Basis for a National Programme

Our work has also brought us in touch with parties sceptical of national programmes. For example, a national leader wondered why his country required a national cybersecurity strategy when the liberalisation of the telecommunications sector handed responsibility over to the private sector. Readers may consider answering similar concerns as follows. One may say that despite liberalisation, governments never cede accountability for facilitating commerce and protecting the lives and property of their citizens. As such, one may add that the strategy would help the Government perform its duties to citizens. To allay Government fears, consider stressing that the Government's primarily serves as a facilitator rather than a doer. However, the Government has to lead efforts to define national cybersecurity goals. The strategy helps initiate a systematic national programme to defend cyberspace from threat whatever their origin. Critically, the strategy prioritises cyber threats and risks as well as allocates responsibilities. The national programme ensures that all relevant stakeholders accept responsibility for and take steps to enhance cybersecurity. As a result, the strategy improves security as it provides all stakeholders awareness of relevant risks, preventive measures and effective responses.

5.2.1.3 Strategy Builds Capacity

Lastly, we recommend that promoters of strategies highlight the human and institutional capacity building impact of an inclusive national cybersecurity strategy. Our proposed national cybersecurity strategy model is a good example. The model defines ends (vision), ways (approaches) and means (resources). As we shall see later, cybersecurity goals could be economic, social and national security. Based on the goals, the ways identify priorities in terms of the five Pillars of the ITU Global Cybersecurity Agenda. For example, our strategy model calls for legal measures and organisational structures such as CIRT. The strategy also caters for information sharing and collaboration due to the global nature of threats. Therefore, a strategy could yield benefits beyond security.

5.3 WHO: CYBERSECURITY STAKEHOLDERS

We recommend that States involve as many stakeholders as possible in the elaboration of national cybersecurity strategies. This is because cyberspace increasingly touches all forms of social, economic and national security activity. Involving a wide group of players is important for the following practical reasons. First, it helps ensure stakeholder buy-in.

[29] Refer to United Nations Resolution 64/211

Stakeholders usually develop a sense of ownership for strategies they help form. The support is critical during the implementation phase of the strategy. Second, national governments may not be in a good position to dictate strategy because the stakeholders actually own and operate the infrastructure. Crucially, the other stakeholders normally possess skills outside the core competencies of most governments. Thus, the external players know what works in practice. We now consider the parties[30] that often shape national cybersecurity strategies. Naturally, the stakeholders may vary across countries.

5.3.1 Executive Branch of Government

Governments have a duty to ensure the prosperity and security of nations. Therefore, the Executive is accountable for setting the agenda for securing all national security domains including cyberspace. Ideally, the Executive performs the following roles:

- Definition of the role of cyberspace in achieving national development goals;
- Identification, analysis and mitigation of risks to achieving national interests;
- Sponsoring and resourcing national cybersecurity programmes;
- Developing cybercrime legislation that is globally applicable and interoperable;
- Encouraging the development of secure technologies such as cryptography;
- Managing human and institutional capacity building programmes;
- Signing cybersecurity related international treaties and conventions; and
- Formulating and defending cybersecurity positions at regional and global fora.

Governments draw on legislative powers and economic incentives to help ensure that all stakeholders accept responsibility and take steps to defend their part of cyberspace.

5.3.2 Legislative Branch of Government

Parliament plays a crucial role in providing the Executive the tools needed to ensure that cyberspace keeps a country secure and prosperous. As Section 5.4 shows, legislatures may trigger national cybersecurity strategies by passing legislation and treaties. The legislature may also ensure that cyber programmes have sufficient funding by approving budgets. Legislatures further review embryonic strategies to ensure that the defence of cyberspace does not infringe on national values such as freedom of expression.

5.3.3 Critical Infrastructure Owners and Operators

It is almost impossible to over-emphasise the importance of critical infrastructure owners and operators to the elaboration and implementation of national cybersecurity strategies. The organisations should contribute to the national strategy elaboration because of their direct economic interest in the success of national cybersecurity programmes. States may deploy legal and regulatory measures to compel the organisations' compliance with cybersecurity requirements. In our experience, the willing participation of the owners and

[30] The Carnegie Mellon document entitled "Best Practices for National Cybersecurity: Building a National Computer Security Incident Management Capability" presents a comprehensive list of national cybersecurity stakeholders. We adopt this list.

operators of critical infrastructure may serve the nation better in the long-term. Critical infrastructure owners and operators play the following roles in strategy elaboration:

- Providing insights into how given cyber threats and vulnerabilities affect their sectors;
- Offering information on how vulnerabilities affect proprietary systems and software;
- Sharing knowledge of what really works due their operational security experience;
- Sharing expertise on cyber assets, networks, systems, facilities and functions;
- Showing how to balance cybersecurity with efficiency and profitability; and
- Contributing to incident response expertise and experience.

We discuss public-private partnerships in strategy implementation in more detail later.

5.3.4 The Judiciary

The judiciary's main role is to ensure that the nascent cybersecurity strategy aligns with national law in areas such as privacy. The judiciary also works with global partners to close gaps in national legislation that may provide a safe haven to cyber criminals.

5.3.5 Law Enforcement

Law enforcement teams enforce cybercrime legislation. The teams should contribute to the elaboration of national cybersecurity strategy elaboration for the following reasons. First, law enforcement can validate the enforceability of proposed cybercrime framework. Second, the teams could advise on current and future national cybercrime investigatory requirements. Third, law enforcement may provide views on collaborative international arrangements against cybercrime. Law enforcement teams belong to organisations such as Interpol and the Virtual Global Taskforce (VGT) on child abuse material.

5.3.6 Intelligence Community

The ITU does not deal with national defence and national security matters. However, for completeness, we should note that intelligence agencies can play a distinctive role in the planning and execution of a national cybersecurity strategy. Intelligence agencies have enduring expertise in monitoring telecommunications networks. For example, agencies are experts in cryptography[31] and cryptanalysis[32]. Thus, the agencies may offer insights into the usefulness of technical countermeasures. We should stress that the involvement of intelligence agencies is often controversial. Many States segregate civilian and military networks. Therefore, involving the intelligence agencies in the planning of a strategy may blur the distinction and provoke civil liberties issues. That said the interconnected nature of cyberspace and potential attack spill over makes such segregation academic.

[31] Cryptography is the art and science of hiding information

[32] Cryptanalysis is the ability to break a code (cipher) and obtain plaintext from ciphertext. Cryptography and cryptanalysis are sub-domains of cryptology a branch of Mathematics that deals with the science of information secrecy

5.3.7 Vendors

Vendors should participate in the strategy elaboration process because they design the technical measures required to prevent, detect, deter and recover from cyber attacks. Leaving the vendors out of the process would deprive a nation of opinions of parties that could be a source or solution to cyber threats and vulnerabilities. Vendor roles include:

- Providing information on how vulnerabilities affect their systems and software;
- Offering insights into capacity to design, administer and maintain secure products;
- Shaping national cyber threat and vulnerability diagnostics capacity;
- Sharing experience on incident response activities;
- Defining information sharing processes with customers on major threats; and
- Building capacity to produce next generation cybersecurity solutions.

5.3.8 Academia

Academic institutions should play an active role in the elaboration of the strategy for the following reasons. First, academic institutions educate the technical, management and information assurance experts required to devise and execute cybersecurity strategies. Second, academia hosts Computer Incident Response Teams. Third, academia leads the research and development of secure cybersecurity solutions.

5.3.9 International Partners

As we illustrate in section 5.4, we propose that you consider asking your allies and other international partners to contribute to your national cybersecurity strategy. Collaboration is vital because we all rely on one cyberspace. Therefore, vulnerabilities in one country may affect other nations with established economic and national security links. However, there are obvious economic, political and national security concerns about collaborating with foreign governments in this strategic domain. The concerns may not be that allies may turn into adversaries. It may be that a country may not be sure about the adequacy of controls in place to protect the sensitive data shared with allies. States may assuage concerns by signing Memorandums of Understanding[33] to collaborate on specific areas such as legal measures, incident response, research and development.

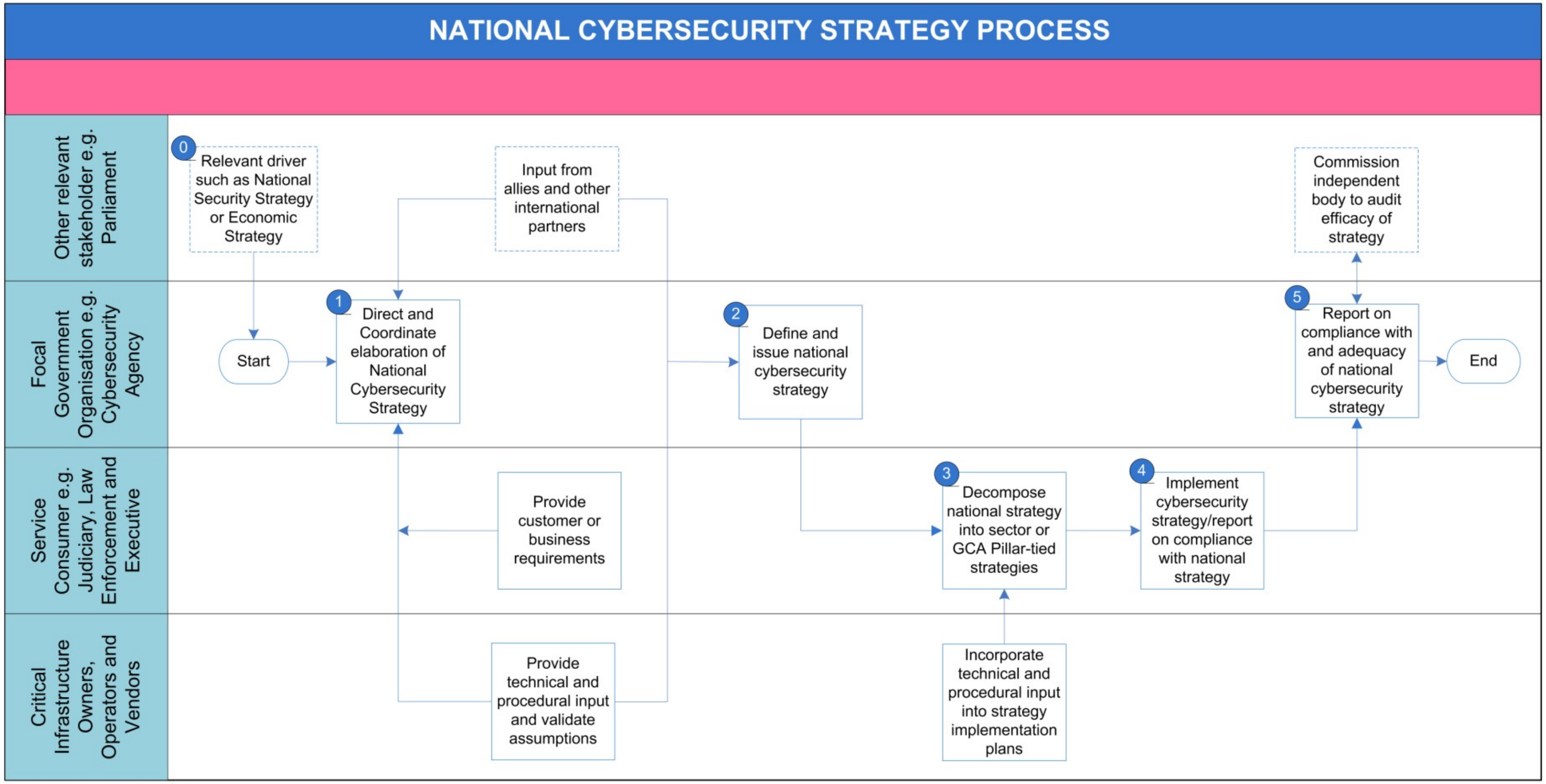
5.3.10 Citizens

Last, but not least by any means, the national cybersecurity strategy must accommodate the voice of its citizens. Cyberspace is essential to modern life. Individuals communicate, socialise, shop, pay bills and study over the Internet. Therefore, the citizens have a stake in a reliably functioning cyberspace that is free from fraud, child abuse material and other risks. However, citizens may not support the national cybersecurity strategy if it prizes security over fundamental rights such as privacy. It may not be possible to obtain input from citizens directly. Thus, Parliament and civil society may offer the views of citizens.

[33] Example - US-UK Communiqué: https://update.cabinetoffice.gov.uk/sites/default/files/resources/CyberCommunique-Final.pdf

5.4 HOW: STRATEGY ELABORATION PROCESS

Having identified the list of stakeholders above, we now present the strategy formulation process for your consideration.


NATIONAL CYBERSECURITY STRATEGY PROCESS
Other relevant stakeholder e.g. Parliament
Focal Government Organisation e.g. Cybersecurity Agency
Service Consumer e.g. Judiciary, Law Enforcement and Executive
Critical Infrastructure Owners, Operators and Vendors
0 Relevant driver such as National Security Strategy or Economic Strategy
Start
1 Direct and Coordinate elaboration of National Cybersecurity Strategy
Input from allies and other international partners
Provide customer or business requirements
Provide technical and procedural input and validate assumptions
2 Define and issue national cybersecurity strategy
3 Decompose national strategy into sector or GCA Pillar-tied strategies
Incorporate technical and procedural input into strategy implementation plans
4 Implement cybersecurity strategy/report on compliance with national strategy
5 Report on compliance with and adequacy of national cybersecurity strategy
Commission independent body to audit efficacy of strategy
End

Source: Dr Frederick Wamala

Figure 5 – National Cybersecurity Strategy Process Flowchart

5.4.1 Purpose of Strategy Process Flowchart

We depict the strategy process in the Figure 5 cross-functional flowchart. The flowchart provides a high-level view of the process including functions and activities. As national governance structures, capabilities and needs vary, the flowchart is illustrative only. We briefly discuss the five steps of the flowchart that we highlight.

5.4.2 Stage 0 – Cybersecurity Strategy Driver

A number of events may spur cybersecurity strategy activities. The actions include major data leakages and national policies. Data leakages include deliberate or accidental loss of government and/or personal data. Stakeholders such as the Executive, legislature and citizens groups may demand action in response to the leakage that later serves to spur the cybersecurity strategy process. In addition, policies such as national development plans[34] and national security[35] strategies spur cybersecurity strategy activity. The policies classify cyberspace as a domain vital to achieving national economic and security goals. Therefore, the national policies may require action to improve the country's ability to exploit cyberspace with confidence and trust. Whatever the spur of the action on the national cybersecurity strategy, we recommend that promoters of the strategy develop a case for action that shows all stakeholders the benefits of the coordinated approach.

5.4.3 Stage 1 – Direct and Coordinate Elaboration

The Executive is accountable for leading the elaboration of the cybersecurity strategy. Whilst the government may require stakeholder participation, our experience shows that a collaborative approach may offer more sustainable benefits. Government can win the support of other stakeholders by emphasising the mutual benefits of working together. Whilst every State has a right to choose the most efficacious approach, we recommend that Governments focus on setting the agenda and the conditions for all stakeholders to work together. The agreed strategy sets a stage for national and global cooperation.

5.4.4 Stage 2 – Define and Issue Strategy

This stage sees the publication of the cybersecurity strategy. The focal organisation for cybersecurity should highlight the roles and responsibilities of major stakeholders. Vitally, the publicity should stress that every government department, business, organisation, owner, and individual user of ICTs has a role to play in securing national cyberspace.

5.4.5 Stage 3 – Sector or GCA Pillar-specific Strategies

The national cybersecurity strategy sets a vision for cybersecurity action. The document does not focus on sector or GCA pillar-specific issues. For example, States may allocate

[34] For example, the Botswana National Development Plan (2010) sees improvement of the ICT infrastructure for all businesses as critical increase those service exports, which rely on improved access to the internet. Obtain a copy here: http://www.finance.gov.bw/index.php?option=com_content1&parent_id=334&id=338

[35] As we shall see later, many countries regard cyber attacks as a priority risk to achieving national security objectives.

sector-specific coordination roles to leading agencies[36]. The agencies focus on sector-specific cyber threats. Critically, the lead agencies have a duty to decompose the national vision into sector-relevant strategies[37] and action plans. The agencies may enter agreements[38] between each other to collaborate on areas of common interest.

5.4.6 Stage 4 – Implement Cybersecurity Strategy

This stage sees the lead agencies working with critical infrastructure operators and other stakeholders to implement the sector-specific action plans. As we see later, the ways of executing the strategy align with the five pillars of the ITU Global Cybersecurity Agenda.

5.4.7 Stage 5 – Report on Compliance and Efficacy

The cybersecurity focal organisation is accountable for monitoring the effectiveness of the national strategy. The body may delegate the responsibility to the lead agencies for every sector. The focal body may also commission periodic independent reviews.

[36] The US National Strategy to Secure Cyberspace nominates seven critical infrastructure lead agencies. These include the Department of Homeland Security (DHS) and Department of Defense (DoD). The agencies may in turn issue sector-specific strategies. Obtain a copy of the strategy here: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

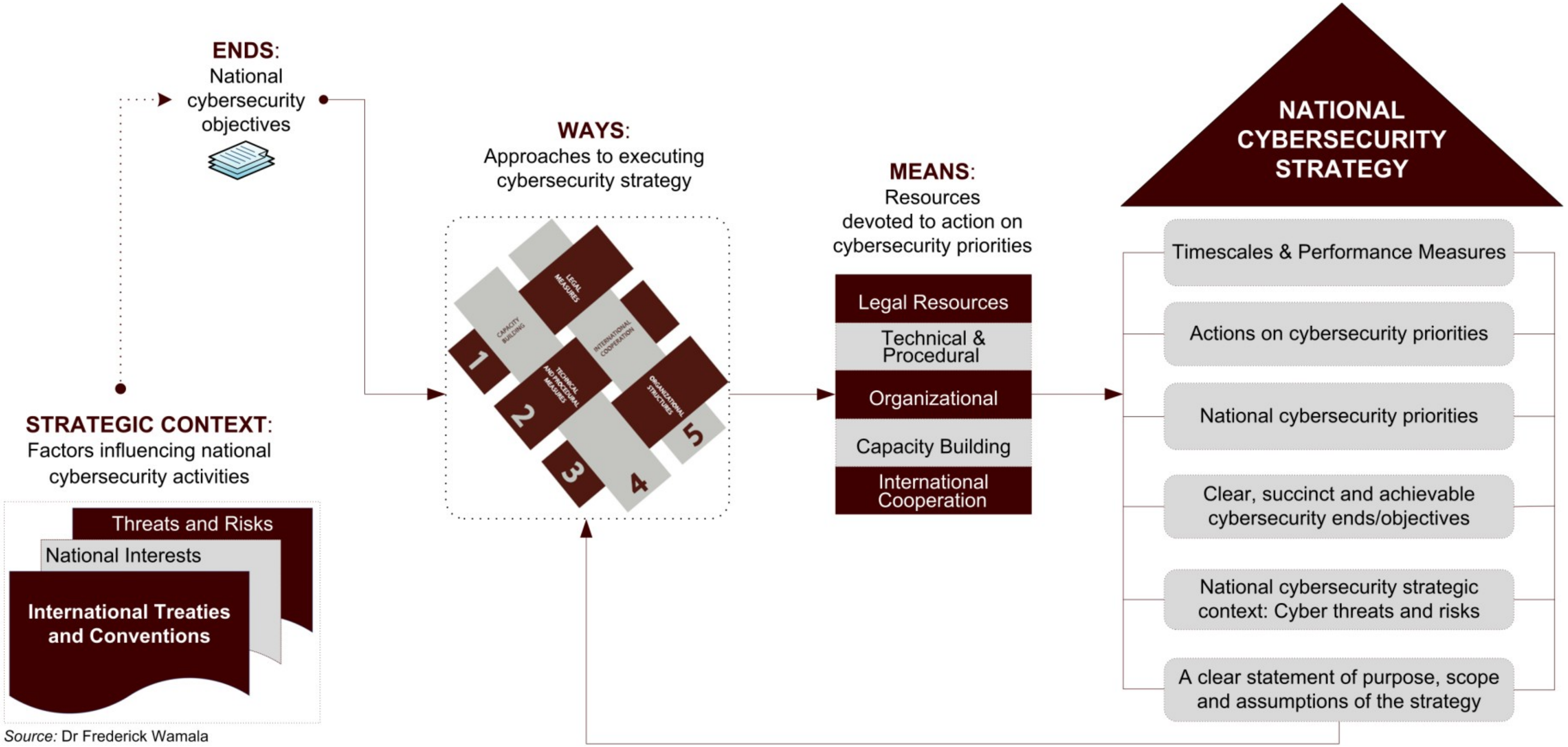
[37] In July 2011, the US DoD issued the "Department of Defense Strategy for Operating in Cyberspace."

[38] In late 2010, the DHS and the DoD's National Security Agency (NSA) entered a Memorandum of Agreement to work together to defend the United States against cyber attack.

IV. NATIONAL CYBERSECURITY STRATEGY MODEL

6 CYBERSECURITY STRATEGY MODEL

Below is a national cybersecurity strategy model that provides a holistic view of the cybersecurity domain.


ENDS:
National cybersecurity objectives
STRATEGIC CONTEXT:
Factors influencing national cybersecurity activities
Threats and Risks
National Interests
International Treaties and Conventions
WAYS:
Approaches to executing cybersecurity strategy
1
CAPACITY BUILDING
LEGAL MEASURES
2
TECHNICAL AND PROCEDURAL MEASURES
INTERNATIONAL COOPERATION
3
4
ORGANIZATIONAL STRUCTURES
5
MEANS:
Resources devoted to action on cybersecurity priorities
Legal Resources
Technical & Procedural
Organizational
Capacity Building
International Cooperation
NATIONAL CYBERSECURITY STRATEGY
Timescales & Performance Measures
Actions on cybersecurity priorities
National cybersecurity priorities
Clear, succinct and achievable cybersecurity ends/objectives
National cybersecurity strategic context: Cyber threats and risks
A clear statement of purpose, scope and assumptions of the strategy

Source: Dr Frederick Wamala

Figure 6 – National Cybersecurity Strategy Model

6.1 INTRODUCTION

Having identified the parties that usually contribute to national strategy development and proposed a process flowchart, we now present the strategy model. Our goal is to define a reference model for countries elaborating new or improving existing national strategies on cybersecurity. As Figure 6 shows, the Global Cybersecurity Agenda is at the heart of our model. We use the GCA along with the Ends-Ways-Means strategy paradigm. We see this is a vital combination as it sets the stage for collaboration between cybersecurity strategists and a diverse group of stakeholders responsible for national policy.

6.1.1 Assumption of Cybersecurity Strategy Model

Given that cybersecurity drivers and threats vary across countries, it is essential to state the assumptions behind our model. The model grew out of ITU Expert Missions that used the GCA as a guiding framework. The main themes of these efforts included:

- ICTs viewed as an engine for economic improvements that hold promise for citizens;
- There was a need to encourage private sector investment in the information and communications sector following liberalisation and de-monopolisation of the sector;
- A desire to promulgate a comprehensive set of cybercrime legislation to preserve the evidential weight and ensure admissibility of electronic data in Courts of Law;
- A need to protect critical infrastructure in sectors such as banking, transport, energy and utilities, communications and telecoms against major cyber attacks;
- Ambitious eGovernment projects aimed at fighting corruption and inefficiency in the public Administration system;
- Cybersecurity regarded as critical to major education projects;
- ICTs as tools for modernising inefficient governments that relied on insufficient and unreliable information; and
- National security concerns due to a weak classified information protection system and thus risk of unauthorised access, modification and destruction of state secrets.

6.2 NATIONAL STRATEGIC CONTEXT

Cybersecurity is not an end unto itself. Instead, we regard cybersecurity as a means to an end. The goal is to build confidence and trust that critical information infrastructure would work reliably and continue to support national interests even when under attack. Therefore, we deem it important that cybersecurity strategies focus on the threats most likely to disrupt important national activities. The first feature of our model is identification of the factors influencing national cybersecurity activities.

6.2.1 Global Treaties and Conventions

We have considered the factors influencing national cybersecurity activities. We trust readers agree that all stakeholders should support coordinated local, national and global multi-sector action. However, no international treaty and convention on cybersecurity is in place to guide the global response. Therefore, national cybersecurity activities are not as effective as they could be. Crucially, agreed norms could help avert actions that may reduce confidence and trust in the use of cyberspace. As a result, ITU Secretary-General Dr. Hamadoun I. Touré has called for a cybersecurity treaty requiring countries to undertake not to make the first cyber strike against other States (Toure 2010). He has championed the treaty out of fear that the next major war is just as likely to start in cyberspace as it is to start on the ground, or at sea, or in the air (Toure 2010c). Since treaties take years to agree and are difficult to enforce, there is growing consensus around agreeing acceptable norms. Thus, the World Telecommunication Development Conference in Resolution 45 (Hyderabad, 2010) and the Plenipotentiary Conference in Resolution 130 (Guadalajara, 2010) asked the ITU Secretary-General and Directors of the Bureaux to prepare a possible cybersecurity Memorandum of Understanding (MoU).

6.2.2 Guiding Principles

We aim to share best practices and solutions for creating a culture of cybersecurity. We now identify the principles that often form the basis for cybersecurity strategies.

6.2.2.1 Protecting National Values

Like individuals, countries feel they have a unique character. Public officials often define national character as “our way of life.” National values sum up the national character. The values are ideals that a country holds most dear. In some cases, they are the reason a country exists. The values determine a country’s worldview. In common with individuals, countries have a sovereign right to decide their national character. Examples of national values include freedom (choice; pursuit of happiness); rule of law (no one is above the law) and prosperity (economic policy based on transparent rules). Countries can commit treasure, time, energy and even blood to defend the values. We recommend that national cybersecurity strategies support national values. Strategies that support the values often obtain the support of major stakeholders such as the judiciary and citizens.

6.2.2.1.1 Example: Values guiding UK Cybersecurity Strategy

The UK Cyber Security Strategy[39] shows how national values may shape a cybersecurity approach. The UK strategy states that the cyber approach is consistent with overarching principles of the National Security Strategy. The national security approach itself relies on core values including: human rights, the rule of law, legitimate and accountable government, justice, freedom, tolerance and opportunity for all. Applied to cybersecurity, the document states, "The Government believes that the continuing openness of the Internet and cyber space is fundamental to our way of life, promoting the free flow of ideas to strengthen democratic ideals and deliver the economic benefits of globalisation." It continues that, "Our approach seeks to preserve and protect the rights to which we are accustomed (including privacy and civil liberties) because it is on these rights that our freedoms depend." The strategy recognises the fundamental challenge of balancing the measures intended to protect security and the right to life with the impact they have on other rights that the UK cherishes and form the basis of society (UK 2009).

6.2.2.2 Systematic National Leadership

This principle aims to ensure that national strategies tackle cybersecurity holistically and avoid the duplication of resources and efforts. Therefore, this principle sees it as a government responsibility to address cyber threats systematically and nationally in coordination with all relevant stakeholders.

6.2.2.3 Shared Responsibility

Cybersecurity strategies also work on the premise of shared responsibility. This principle implies that in a manner appropriate to their roles, Governments, business, organisations and individual owners and users of cyberspace should assume responsibility and take reasonable steps to enhance cybersecurity. The principle also requires all stakeholders to be aware of relevant risks, preventive measures and effective responses to threats.

6.2.2.4 A Multi-stakeholder Approach

Cybersecurity strategies further assume a multi-stakeholder approach. This is a belief that no country, company or individual can surmount the cybersecurity challenge alone. Thus, every stakeholder has a role to play in creating a safe environment for all.

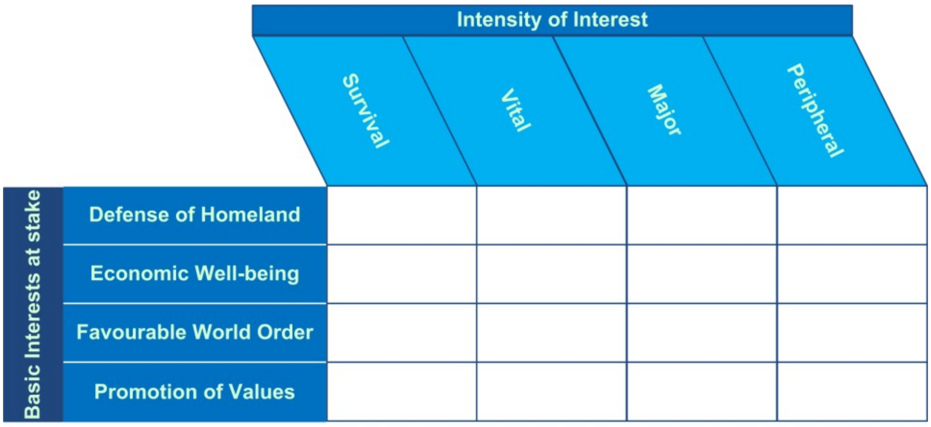
6.2.2.5 Risk Management

Cyberspace is never risk free. Therefore, the principle cautions against aiming to prevent all cyber threats and vulnerabilities from becoming cyber risks. It is costly and often not required. Instead, cybersecurity strategies should focus on tackling threats most likely to prevent government agencies and businesses from carrying out critical missions.

[39] Obtain a copy of the UK Cybersecurity Strategy here: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

6.3 NATIONAL INTERESTS, THREATS & RISKS

National interests flow from national values and guide political decisions. The realisation of national interests achieves goals such as economic prosperity, security and stability of the State, protection of individual freedoms and a good international order. Nations mobilise all tools of national power to realise their national interests. Failure to protect national interests endangers national values. As the figure below indicates, nations may justify the threat or use of military force to defend one of four national interests.



© Donald Neuchterlein

Figure 7 – National Interest Matrix

The vertical axis shows the four main national interests. “Defense of homeland” is the most important because countries must resist threats to their existence and territorial integrity at any cost. On the horizontal axis, “Survival” interests have the highest intensity as they too focus on direct national threats. As such, nations rely on military force to defend such interests. A country suffers serious harm if “vital” interests are unattainable. Thus, nations are unwilling to compromise these interests and deploy strong measures including force (Drew and Snow 2006, Sklenka 2007). “Major” interests do not require force to defend. Lastly, “peripheral” interests do not pose a threat to a nation as a whole.

6.3.1 Cybersecurity “Intensity of Interest”

We regard cybersecurity as a “Vital” interest to many nations. We follow the advice of the Plenipotentiary Conference Resolution 174 (Guadalajara, 2010) that warns that the illicit use of ICTs could have a detrimental impact on a State’s infrastructure, national security and economic development. This could be any State as attacks are borderless.

6.3.2 Strategic Context Considerations

We conclude this section with questions that could help States gather information for the strategic context section of the national cybersecurity strategy. We feel the questions in Figure 8 provide a practical way of linking the strategy with national values and interests.

# ITEM	STRATEGIC CONTEXT
1	**International Treaties and Conventions** Identify treaties under the interests below and their impact on values: (a) Defense of Homeland (b) Economic Well-being (c) Favourable World Order (d) Promotion of Values
2	**"Intensity of Interest"** Rate the intensity of each of the interests in 1(above) in terms of: (a) Survival (b) Vital (c) Major (d) Peripheral
3	**Identify cyber threats and risks and "Intensity of Interest"** Identify cyber threats and rate their impact on the "Intensity of Interest": (e) Defense of Homeland (f) Economic Well-being (g) Favourable World Order (h) Promotion of Values

Figure 8 – Considerations under Strategic Context

V. ENDS – CYBERSECURITY OBJECTIVES

7 CYBERSECURITY ENDS

Ends are the objectives that a national cybersecurity strategy seeks to accomplish. Just as national interests flow from national values, ends describe what a nation has to do to support national interests in cyberspace. Thus, cybersecurity strategies help focus efforts towards ensuring that cyberspace keeps a country secure and prosperous. As we see below, nations do not regard cybersecurity as an end unto itself. Instead, cybersecurity is a means to protecting the critical infrastructures that support core national interests.

7.1.1 Rationale for Ends Categories

Cybersecurity strategy documents often appear written by technical security specialists for fellow specialists. In our experience, good cybersecurity strategies appeal to a broad audience. In particular, the strategies help non-technical national policy makers visualise and create a strategic narrative for cybersecurity. The narrative outlines an overarching approach for advancing core national interests in cyberspace. To support this goal, we recommend that countries assign cybersecurity ends the same titles as the core national interest categories presented in Figure 7. We believe that that using common titles would help planners see how cyber attacks affect their capacity to deliver national policy goals.

7.2 NATIONAL SECURITY

We should state from the outset that the ITU does not specialise in national security and national defence[40] matters. The Union's core mandate and expertise are in the technical and development spheres. However, national security drives cybersecurity strategies because military activities may threaten national political systems and spill over into civilian computer systems dealing with economic, public health and safety matters. We previously noted ITU Secretary-General Dr Touré's concern that cyberspace is possible theatre of war. Figure 9 below provides examples of how nations view the matter.

# STATE	NATIONAL SECURITY END
Australia (2009)	**Cybersecurity Policy Supporting National Security** The aim of the Australian Government's cyber security policy is the maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security.
Canada (2010)	**Undermine National Security** Reliance on cyber technologies makes us more vulnerable to those who attack our digital infrastructure to undermine our national security.
Estonia (2008)	**Aspect of National Security** Vulnerability of a society's information systems is an aspect of national security in urgent need of serious appreciation.

Figure 9 – National Security Ends in Cybersecurity Strategies

[40] The ITU Plenipotentiary Conference in Resolution 130 (Rev. Guadalajara, 2010) resolved that ITU should focus resources and programmes on areas of cybersecurity within its core mandate and expertise, notably the technical and development spheres, and not national defence, national security. See http://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_130.pdf

Countries handle the national security aspects of cybersecurity strategy in different ways. First, cybersecurity strategies often flow from the national security strategy. For example, the national security strategies of Canada[41], the UK[42] and the USA[43] name cyber attacks as priority risks. Second, as Figure 9 above indicates, national cybersecurity strategies describe the impact that cyber attacks may inflict on national security. Lastly, States may issue a defence[44] cybersecurity strategy to enable military and intelligence operations.

7.3 ECONOMIC WELL-BEING

Cyberspace and the technologies that enable it support crucial economic activities. The economic well-being case for action stems from the growing concern that online attacks are causing nations severe but often unquantifiable economic harm. Earlier on, we noted research[45] pointing at major thefts of intellectual property from businesses and other organisations. The European Union also warned about the "spread of malicious software creating 'botnets'[46] – networks of infected computers that can be remotely controlled to stage large-scale, coordinated attacks (EU 2010)." As Figure 10 below shows, many States feel cyber threats threaten economic growth and national competitiveness.

# STATE	ECONOMIC WELL-BEING END
Australia (2009)	**High Risk to Economy** The risk to the Australian economy from computer intrusion and the spread of malicious code by organised crime has been assessed as high.
Czech Republic (2011)	**Sustainable Economic Growth** Safe, secure and reliable operation of ICTs is necessary for the functioning of government and public structures and is an indispensable prerequisite for prosperity and a sustainable economic growth.
Estonia (2008)	**Vital to Economy** The seamless operation of this (critical information) infrastructure is vital to the daily functioning of the Estonian economy.
Germany (2011)	**Promoting Economic Prosperity** The Federal Government aims at making a substantial contribution to a secure cyberspace, thus maintaining and promoting economic and social prosperity in Germany.
India (2011)	**Economic Security** The operational stability and security of critical information infrastructure is vital for economic security of the country.
Holland (2011)	**Sustainable Economic Growth** Safe and reliable ICT is of fundamental importance for our prosperity and well-being and forms a catalyst for (further) sustainable economic growth.
New Zealand (2011)	**Negative impact on Economy** A successful targeted cyber attack could disrupt our critical services, negatively impact our economy.

Figure 10 – Economic Ends in National Cybersecurity Strategies

[41] Canada security strategy: http://www.pco-bcp.gc.ca/docs/information/publications/natsec-secnat/natsec-secnat-eng.pdf
[42] UK National Security Strategy: http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf
[43] US National Security Strategy: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf
[44] Example is the US Department of Defense cybersecurity strategy: http://www.defense.gov/news/d20110714cyber.pdf
[45] The "Operation Shady RAT" report is here: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf
[46] European Union on Botnets: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/463

7.4 PROMOTION OF VALUES

Cybersecurity strategies may arise out the desire by countries to confront cyber threats without losing focus on national values. Some of the values are universal. For example, the ITU Child Online Protection is a success because most stakeholders agree on the need to protect children from information and material injurious to their well-being. Other values are country specific. For example, the US has issued an international strategy[47] to ensure that cyberspace reflects that country's "core commitments to fundamental freedoms, privacy, and the free flow of information." Other values include ensuring that cyberspace supports free trade, human rights and democracy. We would like to stress that the ITU does not have views on national values. It is every States' sovereign right to agree what constitutes national values. Figure 11 below indicates that States often struggle to balance cybersecurity and the openness of the Internet.

# STATE	PROMOTION OF VALUES END
Australia (2009)	**Australian Values** Australia must pursue cyber security policies that enhance individual and collective security while preserving Australians' right to privacy and other fundamental values and freedoms.
Czech Republic (2011)	**Respect Principles** The government of the Czech Republic will adopt necessary measures to protect and guarantee national cyber security. These measures will respect privacy, fundamental rights and liberties, free access to information and other democratic principles.
Holland (2011)	**Appropriate Balance** An appropriate balance must remain between, on the one hand, our desire for public and national security and, on the other, the safeguarding of our fundamental rights.
UK (2009)	**Balancing Security and Rights** A fundamental challenge for any government is to balance measures intended to protect security and the right to life with the impact they may have on the other rights that we cherish and which form the basis of our society.

Figure 11 – Promotion of Values in National Cybersecurity Strategies

7.5 FAVOURABLE WORLD ORDER

We see this as a macro-national interest category. The case for a favourable world order covers the economic, social and diplomatic policies that a State may deploy to ensure that cyberspace promote its values and safeguard its interests in the community of nations. For example, some States may seek to use cyberspace as a tool for promoting national values such as democracy and other universal rights. On the contrary, other States may prefer to ensure that cyberspace preserves stability and national unity. In common with the promotion of values, we stress that the ITU does not hold views on sovereign rights. Let us consider how the US seeks to promote a favourable order.

[47] US Strategy is at http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

# STATE	FAVOURABLE WORLD ORDER
USA (2011)	**Coordinated International Cyberspace Policy** This strategy is a roadmap allowing the United States Government's departments and agencies to better define and coordinate their role in our international cyberspace policy, to execute a specific way forward, and to plan for future implementation. It is a call to the private sector, civil society, and end-users to reinforce these efforts through partnership, awareness, and action. Most importantly, it is an invitation to other states and peoples to join us in realizing this vision of prosperity, security, and openness in our networked world. These ideals are central to preserving the cyberspace we know, and to creating, together, the future we seek.

Figure 12 – Favourable World Order in Cybersecurity Strategies

7.6 GOVERNANCE

This last case is not one of the four national interest categories we identified in section 6.5. The crosscutting case deals with building the confidence of citizens and business in government systems. This case is popular due to attempts to create effective, efficient and responsive ICT-enabled government operations. Electronic Government (eGovernment) enables governments to re-invent themselves and get closer to their citizenry within the context of national development agendas (Okot-Uma 2000)." ICTs support innovative, transparent and accountable service delivery to citizens and businesses. Governments also regard ICTs as crucial tools for fighting corruption and inefficiency in the public administration system. As the strategies in Figure 13 indicate, governance considerations prompt cybersecurity strategies as citizens and businesses shun eGovernment systems with confidentiality, integrity and availability issues.

# STATE	GOVERNANCE ENDS
Estonia (2008)	**Pioneer e-Government Practices** In Estonia we are accustomed to the availability of e-services in a wide range of private and public fields. This is reflected in our people's exceptionally high confidence in the use of information systems. ... Estonia has been recognised internationally as a pioneer in e-government and e-election practices.
New Zealand (2011)	**Government Services Online** Government agencies utilise the Internet, digital document management systems and shared online platforms in their day-to-day business. Increasingly, New Zealanders are accessing government services online, to complete tasks such as submitting tax returns and making applications for passport renewals and student loans.
UK (2009)	**Efficient Services** The Government itself is reliant on cyber space and, through programmes such as the *Transformational Government Strategy*, provides efficient services to the public whenever and wherever they want them. All of these activities rely on the Internet and exploit the benefits of cyber space – and more will follow.

Figure 13 – Governance End in National Cybersecurity Strategies

7.6.1 Cybersecurity Ends Considerations

Figure 14 presents questions to help in gathering of information on cybersecurity ends.

# ITEM	"CYBERSECURITY ENDS” STATEMENT
1	**Role of ICTs** Describe the role of ICTs in each of the following areas: (a) Economic well-being (b) National security (c) Promotion of values (d) Governance (e) Favourable world order
2	**Stakeholders and Roles** Identify the lead institutions for each sector and their interest in addressing cyber threats: (a) Identify critical sector that dependent on ICTs e.g. banking etc (b) Identify relevant stakeholders (c) Describe the stakeholder’s potential role in the development, implementation and maintenance of cybersecurity initiatives (d) Identify point of contact (preferably role rather than individual)
3	**International Cooperation** Consider international cooperation, dialogue and coordination by: (a) Identifying local and global cybersecurity-focused organisations (b) Identifying related international cybersecurity activities.

Figure 14 – Cybersecurity Ends Considerations

VI.
WAYS – PRIORITIES

8 WAYS – PRIORITIES

Our national cybersecurity strategy model chose the five pillars of the GCA as the forms through which States may pursue national cybersecurity strategies. Therefore, the ways identify the strategic activities to help countries govern the pillars. Governance defines how nations may use the resources in the five pillars to attain the outcomes that the ends envisage. In the multi-stakeholder domain of cybersecurity, the ways define how nations may allocate resources, coordinate and control the activities of all relevant stakeholders. Allocating roles and responsibilities clearly prevents overlapping and often contradictory mandates that paralyse many national cybersecurity programmes. Clear governance structures further confer legitimacy on stakeholders including government. Importantly, the ways define expectations for activities and thus are a basis for verifying performance.

9 PRIORITY 1 – LEGAL MEASURES

Gaps in national and regional legislation make cybercrime a low risk and lucrative undertaking. In keeping with the first GCA pillar, this priority aims to help devise strategies to govern the development of cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures. We align this priority with GCA strategic goals relevant to the Legal Measures pillar as follows:

GCA PILLAR: LEGAL MEASURES		
Corresponding GCA Goals	Goal 1	Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures.
	Goal 7	Proposals on a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

Figure 15 – Legal Measures Pillar and related GCA goal

We now propose the forms through which States may consider pursuing the national cybersecurity strategies under this pillar.

9.1 LEGAL MEASURES STRATEGY

Nations should strengthen their capacity to regulate cyberspace. Nations may adopt the strategy formulation process that we presented in Figure 5. In particular, stage 3 of the flowchart deals with sector or GCA-pillar specific strategies. The flowchart shows how the executive, law enforcement, the judiciary, the private sector, and other stakeholders could support of the legal strategy. Due to transnational nature of cyber threats, our strategy flowchart expects input from allies and other international partners. Global harmonisation is important because gaps in national legislation abet cybercrime. As we see under the international cooperation pillar, the strategy may visualise and support the adoption of cybercrime conventions at the United Nations. Naturally, every country should select an approach that best fits its local needs and conditions. We identify the main aspect of the strategy next.

9.1.1 Government Legal Authority

We have noted that national administrations are accountable for cybersecurity because cyber attacks threaten national interests in economic, diplomatic and national security spheres. However, national governments often lack the legal authority to run coherent national cybersecurity programmes for the following reasons. First, the commercial sector owns the majority of the critical information infrastructure. Second, cyberspace blurs the line between normal law enforcement and military operations. Third, global cooperation on cybercrime requires treaties on extradition and cross-border Internet searches that may not exist. Therefore, we advise that the legal measures strategy contains a governance structure to provide the Executive the legal mandate to mobilise all resources against cyber threats. Whilst local conditions differ, the mandate typically:

- Provides the Head of Government the legal authority to create and fund a national cybersecurity programme;
- Defines the legal basis for creating a national Computer Incident Response Team;
- Grants powers to shutdown a critical infrastructure asset if at risk of a cyber attack;
- Provides the basis for promoting cybersecurity skills, training and awareness;
- Defines the legal and operational basis for an integrated and fully coordinated public-private sector partnership on cybersecurity;
- Fosters innovation in cybersecurity to help develop long-term solutions; and
- Grants the government powers to participate in international cooperation, dialogue and coordination activities focused on cybersecurity such as mutual assistance

9.1.2 Parliamentary Cybersecurity Process

In sub-section 5.3.2, we noted that the legislature plays a crucial role in providing the Executive the tools to ensure that cyberspace keeps a country secure and prosperous. Parliament also maintains oversight over national cybersecurity programmes to ensure that efforts to secure critical information infrastructure do not infringe on national values such as civil liberties. Parliament further harmonises national legislation with international conventions and treaties on cybercrime. However, parliaments may lack the requisite governance structures to handle cybercrime legislation quickly because they typically work in committees. Thus, different committees have jurisdiction over economic, social, diplomatic and national security matters. Important cybersecurity committees[48] include information and communications; science; constitutional affairs; judiciary; homeland security; education and media. The approach often fragments cybersecurity legislative activities as no single committee may have the powers to provide the Executive the resources required to defend national cyberspace. We, thus, believe that streamlining

[48] Data from the "Fourth Parliamentary Forum on Shaping the Information Society: The Triple Challenge of Cyber-Security: Information, Citizens and Infrastructure." Obtain a list of participants at: http://www.ictparliament.org/parliamentaryforum2011

the parliamentary governance of cybersecurity matters should be a top priority of the legal measures strategy. For example, countries may consider forming joint-committees with a focus on cybersecurity matters. Thereafter, Parliament may pass a Cybersecurity Act to define the responsibilities of the joint cybersecurity committee.

9.1.3 Law Enforcement Governance Framework

The legal measures strategy should also consider creating a governance structure or strategic framework to coordinate law enforcement, investigatory, policy and regulatory activities against cybercrime. Efficient law enforcement helps prevent, deter, respond to and supports the prosecution of the illicit use of ICTs. The governance structure should:

- Define the roles of investigatory and law enforcement organisations;
- Link online and offline law enforcement action against all types of crime;
- Provide a solid and globally harmonised approach for law enforcement activities;
- Provide law enforcement agencies the requisite information and resources to gain and maintain the skills to combat cybercrime effectively; and
- Create a framework for dialogue and coordination of law enforcement agencies at local, regional and international levels.

9.1.4 Global Fight against Cybercrime

Nations should participate in efforts to develop and harmonise legal measures globally. The participation could be part of crosscutting international cooperation efforts. Countries may also consider incorporating legal measures into a cohesive international strategy for cyberspace. For example, the US strategy[49] provides a roadmap for coordinating all the international cyberspace policy activities of the government, private sector, civil society and end-users. To build confidence in the use of cyberspace, the US aims to:

- Participate fully in international cybercrime policy development;
- Improve cooperation through the harmonisation of cybercrime laws; and
- Focus cybercrime laws on combating illicit use rather than restricting access.

As ever, all nations have a sovereign right to choose the most efficacious approach.

[49] US Strategy is at http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

10 PRIORITY 2 – TECHNICAL AND PROCEDURAL MEASURES

All stakeholders have an interest in increasing the resiliency and reliability of critical information infrastructure. In keeping with the second GCA pillar, this priority focuses on the development of measures for addressing vulnerabilities in hardware and software products. The measures are critical because whereas threats and threat actors change, security vulnerabilities exist throughout the life of a system or protocol unless addressed. Therefore, global security standards offer the best defence against shared vulnerabilities.

10.1 PROCEDURAL MEASURES

Simply put, procedural measures are processes that help preserve the security around physical and information assets. Whilst this is a technical and procedural priority, we present the Procedural Measures first because they provide the operational context for technical measures. Security goals or context informs the selection of Procedural and Technical Measures. Without clear security goals, organisations typically fail to make effective use of security tools as it unclear what to check for and the restrictions to impose (IETF 1997). We align this priority with the strategic goals related to the Technical and Procedural Measures Pillar of the GCA as follows:

GCA PILLAR: TECHNICAL AND PROCEDURAL MEASURES		
Corresponding GCA Goal – Procedural Measures	Goal 3	Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for hardware and software applications and systems.
	Goal 5	Development of global strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organisational structures to ensure the recognition of digital credentials across geographical boundaries.

Figure 16 – Procedural Measures and related GCA goals

10.1.1 Cybersecurity Goals

We feel that cybersecurity goals should precede the adoption of technical and procedural measures. We hold this opinion because cybersecurity goals define the overall risk tolerance[50]. Without defining the goals, relevant stakeholders can never know when a system is sufficiently secure. We adopt the cybersecurity goals we use here from the

[50] Defined simply, risk tolerance means the degree of exposure to security risk acceptable to policy makers/business owners.

Internet Engineering Task Force (IETF) Site Security Handbook[51]. The cybersecurity goals provide an organisation's security philosophy. Additionally, the goals define security expectations, identify trade-offs and provide the basis for verifying performance. Below are the basic goals as per the Handbook.

10.1.1.1 Service offered versus Security

Each service offered to users carries its own security risks. For example, many e-Government projects are pushing government data online as additional services to citizens. However, the risk of services such as electronic voting currently outweighs the benefit. Thus, it might be better to eliminate the service rather than try to secure it.

10.1.1.2 Ease of Use versus Security

Security controls restrict freedom to move about, talk and write and require users to lock doors; cars and take precious time enter passwords into devices (Parker 1997). The easiest system to use would allow access to any user and require no passwords. However, whereas the controls make system use a little less convenient, the constraints add security. Yet, excessive security may be counterproductive. For example, whereas a complex 40-character password is secure, it difficult to remember and could instead reduce security by encouraging users to write it down to aid memory.

10.1.1.3 Cost of Security versus Risk of Loss

IETF (1997) identifies different security costs. These include: monetary i.e. the costs of purchasing security hardware and software such as firewalls and one-time password generators; performance i.e. the impact of security functions such as encryption on service levels; and ease of use i.e. secure systems are typically less convenient to use. The security risks include loss of privacy, loss of data and loss of service. You should weigh each cost against each type of loss. If the cost of security substantially outstrips the impact of loss, you should consider other options such as eliminating the service altogether rather than try to secure it i.e. avoid the risk.

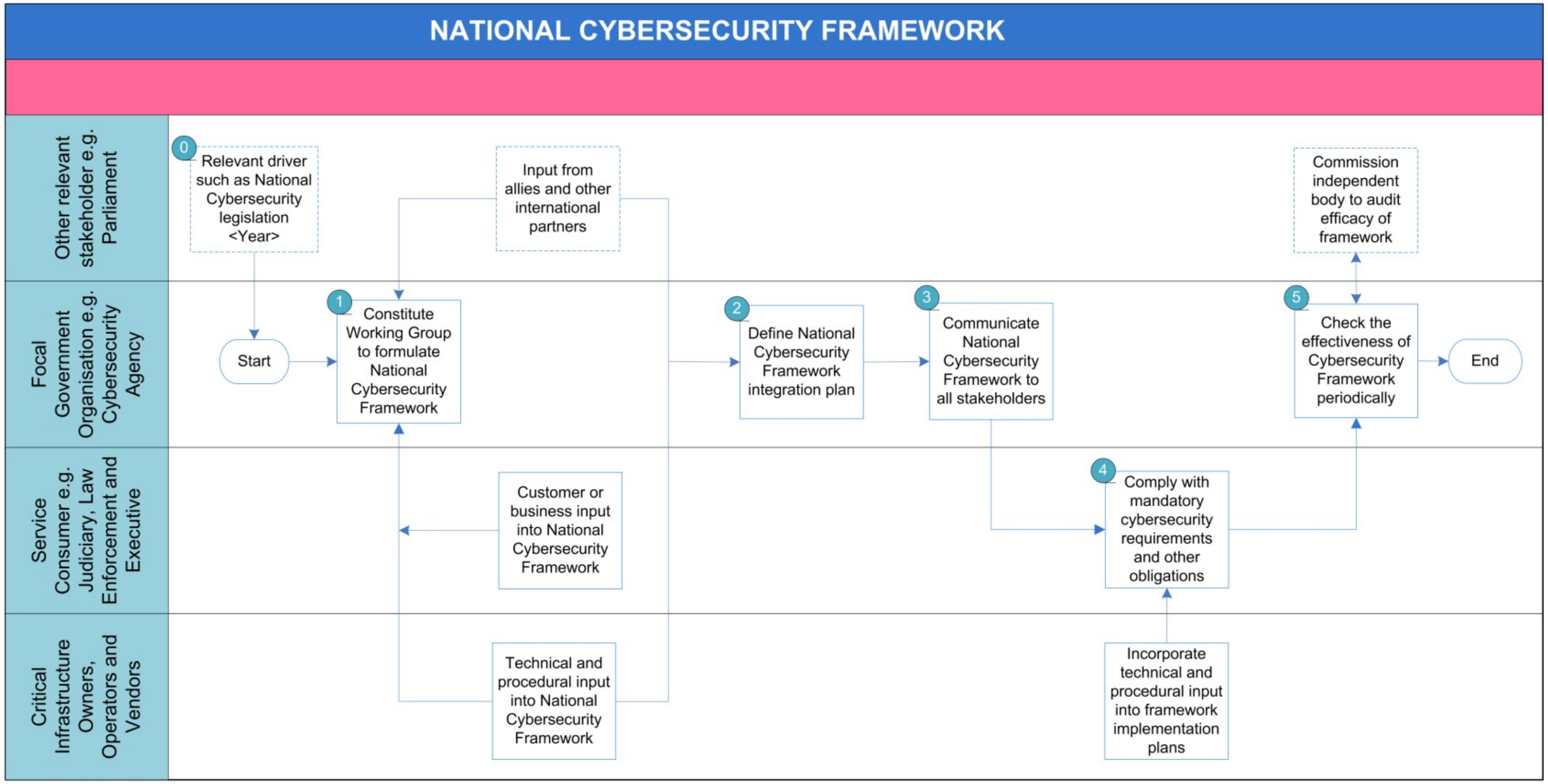
10.1.2 National Cybersecurity Framework

We recommended that countries adopt a legal strategy to coordinate activities aimed at enacting and enforcing cybercrime legislation. Likewise, we now call on States to adopt National Cybersecurity Frameworks. Cybersecurity Frameworks flow from cybersecurity goals and are the national cybersecurity governance structure. Frameworks define roles and responsibilities; allocate resources, coordinate and control activities nationally. The Frameworks define core security principles and standards that apply to a wide range of stakeholders and thus communicate the security goals. Figure 17 illustrates the process for generating national cybersecurity frameworks and indicative activities.

[51] Obtain a copy of the IETF Site Security Handbook at: http://www.ietf.org/rfc/rfc2196.txt

10.1.2.1 National Cybersecurity Framework Flowchart

The flowchart below shows how a nation may establish, implement, operate and monitor a national cybersecurity framework.


NATIONAL CYBERSECURITY FRAMEWORK
Other relevant stakeholder e.g. Parliament
Focal Government Organisation e.g. Cybersecurity Agency
Service Consumer e.g. Judiciary, Law Enforcement and Executive
Critical Infrastructure Owners, Operators and Vendors
0 Relevant driver such as National Cybersecurity legislation <Year>
Start
1 Constitute Working Group to formulate National Cybersecurity Framework
Input from allies and other international partners
Customer or business input into National Cybersecurity Framework
Technical and procedural input into National Cybersecurity Framework
2 Define National Cybersecurity Framework integration plan
3 Communicate National Cybersecurity Framework to all stakeholders
4 Comply with mandatory cybersecurity requirements and other obligations
Incorporate technical and procedural input into framework implementation plans
Commission independent body to audit efficacy of framework
5 Check the effectiveness of Cybersecurity Framework periodically
End

Source: Dr Frederick Wamala

Figure 17 – National Cybersecurity Framework

10.1.2.2 Purpose of National Cybersecurity Framework Flowchart

The flowchart is Figure 17 provides a high-level view of how a country may create an overall cybersecurity governance framework. The flowchart outlines minimum-security measures that all stakeholders must abide by. As we see under Means, the governance framework also serves as the basis for critical activities such as risk management.

10.1.2.3 Stage 0 – Relevant Driver

A number of events may drive the formulation of national cybersecurity frameworks. The adoption of national cybersecurity legislation is a typical example. Whatever the origin, national frameworks typically define core security principles and standards that apply to a wide range of stakeholders and thus communicate the security goals.

10.1.2.4 Stage 1 – National Cybersecurity Framework Working Group

We underscore the government's accountability for cybersecurity throughout this Guide. It is no surprise then that we would expect a focal government organisation to create and orchestrate the national cybersecurity framework working Group. We further expect the participation of all organisations that handle and/or use information critical to advancing national interests. Countries may choose to limit the list to organisations responsible for local and national government data including contractors. Working groups also typically enlist the input organisations with technical and information assurance competencies. Lastly, flowchart envisages a possible role for allies and other international partners.

10.1.2.5 Stage 2 – Define Framework Integration Plan

We noted in stage 1 that it might be practical to limit the working group's membership to organisations that handle and process government information. Whatever approach a nation chooses, it is crucial to ensure that all stakeholders have a governance structure similar to the national cybersecurity framework. For example, a State would have major gaps in the implementation of its strategy if the private sector, which owns and operates the critical infrastructure, does not follow any sort of framework. Therefore, this stage ensures that all frameworks coherently support the national cybersecurity strategy goals.

10.1.2.6 Stage 3 – Communicate Cybersecurity Framework

This stage calls for the creation of an efficient mechanism for ensuring all stakeholders know about the cybersecurity framework as well as any changes to it.

10.1.2.7 Stage 4 – Cybersecurity Framework Implementation

At this stage, all relevant stakeholders must demonstrate compliance with the minimum-security requirements. The stage also requires stakeholders to demonstrate compliance with security obligations that apply to specific risk profiles as required by national bodies.

10.1.2.8 Stage 5 – Periodic Compliance Reporting

The cybersecurity focal organisation is accountable for monitoring the effectiveness of the national cybersecurity framework. Focal organisations often take three approaches to gathering compliance data. First, the organisation may rely on self-assessment reports from the relevant stakeholders. Second, the focal organisation may undertake the audits itself. Lastly, the organisation may require reporting as part of external audits. As ever all States should choose the approaches that fits local circumstances. The compliance data may form the basis for an annual national cybersecurity report.

10.2 TECHNICAL MEASURES

We advise States to pursue a united approach to tackling vulnerabilities in hardware and software products. The ever-increasing sophistication of malware requires that nations devise coherent strategies for sourcing trusted software and hardware tools to prevent, detect, deter and recover from cyber attacks. The measures satisfy these GCA Goals:

GCA PILLAR: TECHNICAL AND PROCEDURAL MEASURES		
Corresponding GCA Goal – Technical Measures	Goal 5	Development of global strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organisational structures to ensure the recognition of digital credentials across geographical boundaries.
	Goal 7	Proposals on a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

Figure 18 – Technical Measures and related GCA goals

10.2.1 Network Protection Strategy Principles

The technical solutions required depend on the application of cyberspace and the threats and risks to those activities. Therefore, it is unhelpful to require nations to acquire given solutions without knowing the local confidentiality, integrity and availability requirements. Requirements emanate from the system's operational environment and user needs. Therefore, we feel providing technology-neutral principles would be more beneficial. The principles would guide stakeholders in their formulation of technology strategies as well as during the selection of technical solutions. The principles are as follows:

10.2.1.1 Uniform Access Management

According to Recommendation ITU-T X.1205[52], the term "access management" defines systems that may make use of both authentication and authorisation services in order to control the use of a resource. Authentication is the process in which a user or entity requests the establishment of an identifier to a network. On the other hand, authorisation determines the level of allowed privileges for that entity based on access control. Access privileges depend on the control policy definition and its enforcement. The figure below depicts the ITU-T X.1205 reference model for secure authentication and authorisation.

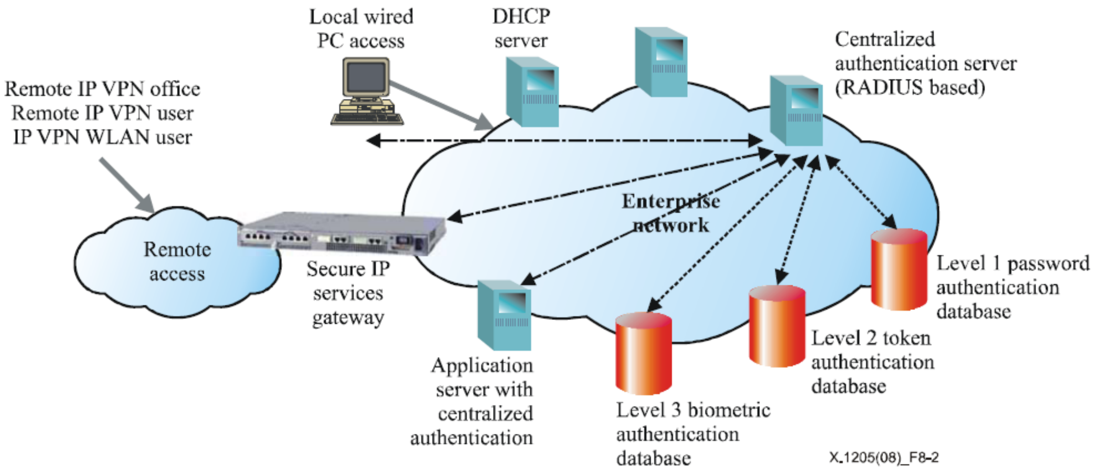


Figure 19 – Secure Authentication and Authorisation reference model

In line with Reference Model, nations should obtain solutions that meet the goals below:

- Centralised Authentication – The mechanism facilitates administration and removes the need for local or host-based storage of credentials (passwords or certificates);
- Centralised Authorisation – In common with authentication, this approach ensures that access to system resources is managed in a transparent and auditable way;
- Enforcement of strong (complex) passwords rules for all passwords;
- Secure storage of all passwords in a one-way encrypted (hashed) format;
- Simplicity – The principle focuses on enabling ease of use and administration; and
- Secure logging of all events with respect to authentication and authorisation.

10.2.1.2 Secure Communications

This principle recognises the convergence of voice, data and video packets on unified networks. Thus, countries should ensure that the technical solutions provide the different packets types the protection appropriate to their security needs. In addition, appropriately strong cryptographic ciphers should secure data, voice and mobile networks.

[52] Obtain a copy of Recommendation ITU-T X.1205 at: http://www.itu.int/rec/T-REC-X.1205-200804-I

10.2.1.3 Variable Depth Security or Zoning

This security principle requires that cybersecurity solutions enforce sufficient separation between networks handling data of different protective marking levels. Security layering results in the ability to offer variable depth security. Each additional security level builds upon the capabilities of the layer below. As such, this principle requires the creation and the enforcement of zones for different levels of trust. For example, IT systems should require a Demilitarised Zone (DMZ) between zones to provide additional protection from untrusted services. Additionally, untrusted data should only enter the system in low risk zones. Untrusted data requires verification before elevation to a higher classification.

10.2.1.4 Defence in Depth

To ensure that critical data receives sufficient protection even in face of increasingly sophisticated attacks, this principle requires the use of multiple controls and different security products to mitigate security threats collectively. For example, a network may implement firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), content checkers and anti-virus software. If malicious code escaped the firewall rules and IDS/IPS controls, probably the content checker or anti-virus software may trap it. The principle also requires the sourcing of Security Enforcing Functions and devices from different manufacturers. Thus, this principle creates secure IT solutions because diversity means that there is more than one device in place and each is different.

10.2.1.5 Network Survivability Even Under Attack

Recommendation ITU-T X.1205 defines a survivable network as one that continues to fulfil a minimum set of essential functionality in a timely manner in the presence of attacks. Survivable networks are able to deliver essential functionality in a timely manner even if parts of the network are unreachable or have failed due to an attack. Survivability is a feature that network designers can build into the infrastructure. The concept relies on the existence of a data classification scheme. Network segments reflect the Protective Marking Levels such as Not Protectively Marked, Restricted and Confidential. Thereafter, the engineers should define a strategy for dealing and recovering from attacks.

10.2.1.6 Independently Evaluated and Tested Products

Another principle deals with the adequacy of security testing. We recommend that selectors of cybersecurity technologies aim to acquire assured products for Security Enforcing Functions throughout critical infrastructure. While the products that have Evaluation Assurance Level (EAL) are not automatically secure, they undergo rigorous testing and are likely to provide a solid foundation for security functions. Assured products are particularly vital in the enforcing of zone segregation. Additionally, Commercial off-the-Shelf (COTS) products are preferable to be-spoke solution as large vendors are more likely to have the resources and incentive to go through EAL testing.

10.2.1.7 IT System Configuration

We would like to emphasise that EAL is not a security panacea. EAL markings only help if product configuration and use conforms to the Target of Evaluation (ToE) criteria.

Thus, this principle emphasises the need to configure systems according to installation and configuration guides. Common configuration mistakes include failure to remove known default passwords leaving a system trivially exploitable. Thus, EAL Certification without good configuration may provide a false sense of security. ISO/IEC 27001 and Common Criteria (CCRA 2009) require an assessment after a major upgrade or installation to verify that the changes have not weakened the system's security controls.

10.2.1.8 Staff training

Staff training closely links to configuration. Technical teams are more likely to make poor configuration choices if they lack training to enable them to understand security threats, risks and the need for mitigating controls. As recommended elsewhere, countries should train skilled professionals to manage assured products. The technical teams should have a business understanding of risk and expertise to deploy technological and network security technologies. As outlined under the Cybersecurity Skills and Training section, your organisation should have a clear plan to ensure that the security team maintains the requisite security skills.

10.2.1.9 Security Baselines

Service minimisation is an example of good configuration. This principle requires that your IT teams create "Security Baselines" or "Builds" under which devices provide only the services required for business. Thus, as part of the compliance-checking framework, relevant stakeholders should validate that devices such as servers and end user computers run official services only and disable anything extra. Additionally, the service minimisation principle discourages the use of multi-purpose devices, where practical, as this increases system vulnerability and the impact of cyber attacks. For example, running web server, e-mail and file storage applications on a single device may appear cheap but this practice increases the security impacts of a successful cyber attack.

10.2.1.10 Aggregation

This principle aims to prevent data aggregation risks. Data aggregation occurs when data that individually is of low classification obtains a higher Impact Level when combined with a large number of other data items. Aggregation occurs in two ways. Accumulation is a situation where increasingly large amounts of information stored together increases the overall Impact Level of compromise. Conversely, association is where the linking of different information assets, which individually have no or low Impact Level when compromised, but associated have a higher impact level of compromise.

10.2.2 Global Cooperation on Technical Measures

Nations should participate in international efforts to develop secure network solutions. The technical measures work area may form part of a broader international cooperation strategy. Whatever the approach of choice, nations should, devise a roadmap for having a say in the evolution of technical standards a multilateral forums. For example, the ITU Standardisation Sector (ITU-T) Study Group 17 would be an excellent international forum to attend[53]. Study Group 17 is accountable for devising telecom security, identity management, languages and description techniques recommendations. In addition, an increasing number of countries are striking bi-lateral agreements to collaborate on the development of next generation secure international technologies.

[53] Evaluate ITU-T Study Group 17 activities at http://www.itu.int/ITU-T/studygroups/com17/index.asp

11 PRIORITY 3 – ORGANISATIONAL STRUCTURES

We stress the need for coordinated action throughout this Guide. Effective coordination requires strong local, national and global public and private organisational structures. For this reason, we present ideas on how to build organisational structures and strategies to help prevent, detect and respond to attacks against critical infrastructure. We align the GCA Organisational Structures Pillar with the relevant strategic goals.

GCA PILLAR: ORGANISATIONAL STRUCTURES		
Corresponding GCA Goal	Goal 2	Elaboration of global strategies for the creation of appropriate national and regional organisational structures and policies on cybercrime.
	Goal 4	Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.
	Goal 6	Development of a global strategy to facilitate human and institutional capacity building to enhance knowledge and know-how across sectors and in all the above-mentioned areas.

Figure 20 – Organisational Structures Pillar and related GCA goals

11.1 GOVERNMENTAL ORGANISATIONAL STRUCTURES

Cybersecurity is everyone's responsibility because countermeasures only work well if all stakeholders we identified in section 5.3 perform their roles. As we have said repeatedly, national administrations have overall accountability for cybersecurity. We now explore what we consider the most relevant governmental organisational structures.

11.1.1 Head of Government Accountability

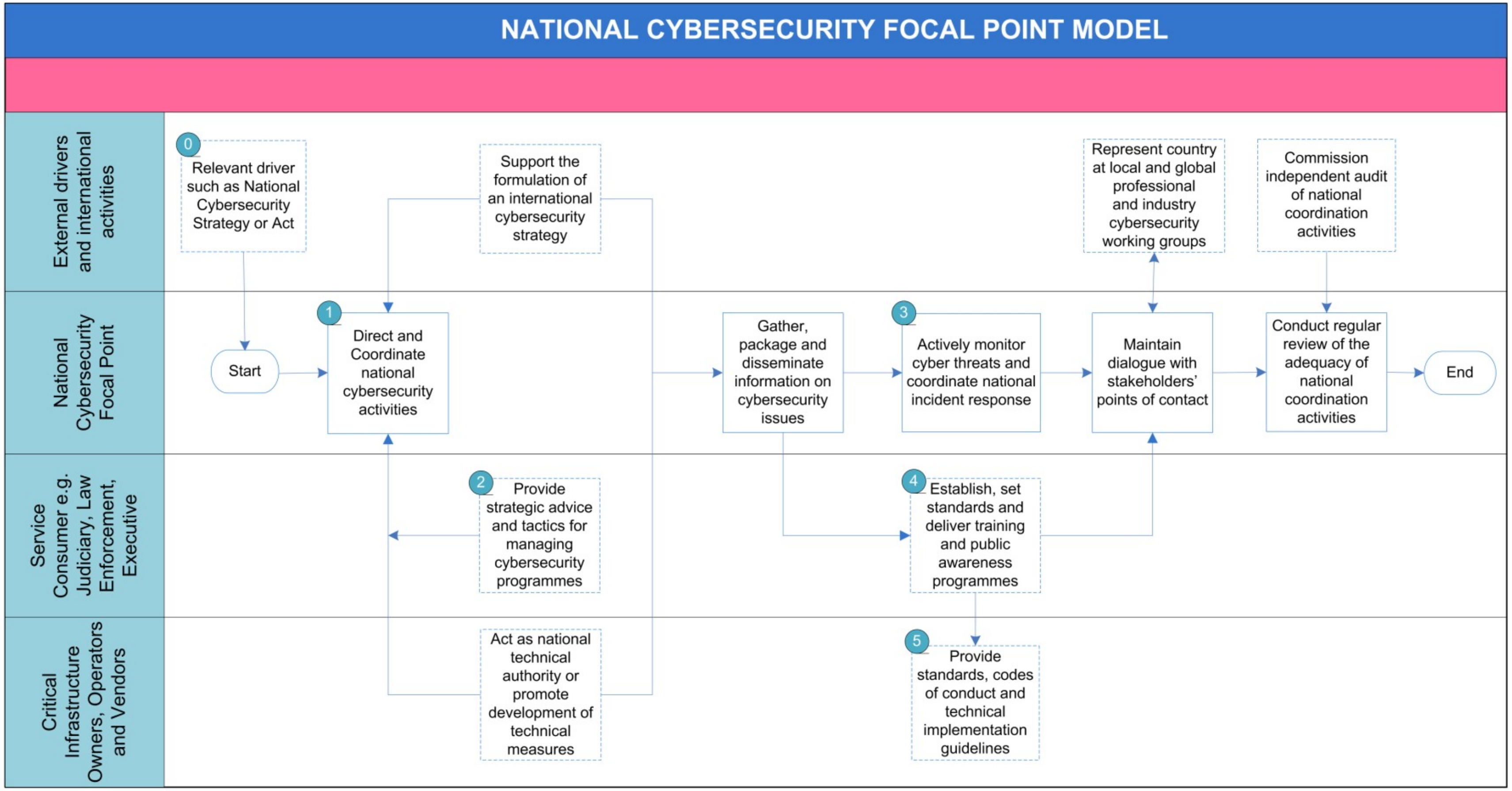
Cybersecurity requires all tools of national power. Therefore, we recommend that Heads of Government or State assume overall accountability for cybersecurity. Top government leadership stresses the vitality of cybersecurity to the advancement of national interests.

11.1.1.1 National Cybersecurity Coordinator

Heads of Government often delegate cybersecurity duties to a national cybersecurity coordinator. The coordinator (an individual or an office) directs all cybersecurity activities in government. If an individual, the coordinator should understand cybersecurity issues, be able to direct and coordinate the efforts of governmental institutions, and effectively collaborate with industry (ITU 2008a).

11.2 NATIONAL CYBERSECURITY FOCAL POINT

Cybersecurity programmes often contain a multi-agency body to serve as a focal point for all cybersecurity matters. We illustrate below.


NATIONAL CYBERSECURITY FOCAL POINT MODEL
External drivers and international activities
National Cybersecurity Focal Point
Service Consumer e.g. Judiciary, Law Enforcement, Executive
Critical Infrastructure Owners, Operators and Vendors
0
Relevant driver such as National Cybersecurity Strategy or Act
Start
1
Direct and Coordinate national cybersecurity activities
Support the formulation of an international cybersecurity strategy
2
Provide strategic advice and tactics for managing cybersecurity programmes
Act as national technical authority or promote development of technical measures
Gather, package and disseminate information on cybersecurity issues
3
Actively monitor cyber threats and coordinate national incident response
4
Establish, set standards and deliver training and public awareness programmes
5
Provide standards, codes of conduct and technical implementation guidelines
Represent country at local and global professional and industry cybersecurity working groups
Maintain dialogue with stakeholders' points of contact
Commission independent audit of national coordination activities
Conduct regular review of the adequacy of national coordination activities
End

Source: Dr Frederick Wamala

Figure 21 – National Cybersecurity Focal Point

Figure 21 provides a high-level view of the national cybersecurity focal point roles. Let us briefly explore the numbered processes within the flowchart.

11.2.1 Stage 0 – Relevant Driver

Focal points often grow out of national cybersecurity strategies and similar legislation. The focal organisation may take several forms. First, the law may create a brand new organisation to perform the role. Second, the law may designate an existing ministry as the focal point. Third, the functions in the model may reside with different government ministries. Lastly, an existing body such as ICT regulator may assume the role.

11.2.2 Stage 1 – Direct and Coordinate Cybersecurity

The focal point coordinates the activities of all cybersecurity stakeholders. Directing and coordinating ensures that right actions occur at the right time on the right cybersecurity priorities. The focal point also participates in international cybersecurity activities.

11.2.3 Stage 2 – Strategic and Tactical Cybersecurity Advice

The focal point helps with the strategic and tactical aspects of operating cybersecurity programmes. First, the organisation explains the purpose of the national cybersecurity as well as the obligations it places on individual stakeholders. Second, the focal point may help shape cybersecurity programmes of major stakeholders in public and private sectors. Third, the focal point may use its influence to promote the adoption of good practice models. Fourth, focal point may advise on operational aspects of cybersecurity.

11.2.4 Stage 3 – Coordinate Incident Response

The focal point may not have overall technical responsibility for incident management. However, the focal point often ensures united local and global incident response. It may also have overall strategic ownership of major incidents. In addition, its strategic and tactical advice role helps organisations prevent, detect and recover from incidents.

11.2.5 Stage 4 – Training and Public Awareness

The focal point ensures that all stakeholders understand the relevant cyber risks, trends and effective countermeasures. In terms of training, the focal point could encourage the development of cybersecurity as follows. First, the organisation may set and/or review technical training courses for professionals. Second, the focal point may require the inclusion of given technical security features for example, parent controls. In terms of public awareness, focal points often lead campaigns to build a culture of cybersecurity. The campaigns take the form of television, radio and internet advertisements. In addition, the focal point may evaluate training programmes, prepare materials and train trainers.

11.2.6 Stage 5 – Standards and Implementation Guides

National focal points also help critical infrastructure owners, providers and vendors build capacity to defend systems and information. The organisation may issue technical implementation guides and best practice guides. The focal point may either perform this role or work with the national technical and information assurance organisations.

11.3 NATIONAL COMPUTER INCIDENT RESPONSE TEAM (CIRT)

The growing sophistication, frequency and gravity of cyber threats necessitate formal frameworks for watch, warning and incident response. Resolution 58[54] of the ITU World Telecommunication Standardization Assembly (WTSA) 2008 and WTDC-10 Resolution 69[55] encourage ITU Member States to create national CIRTs (ITU 2008). Typically, a national CIRT is responsible for:

- Providing incident response support to all relevant stakeholders via established, trusted, authorised and centrally coordinated initiatives at the national level;
- Dissemination of critical information such as early warnings and alert notifications, security advisory, and upholding security best practices;
- Acting as a single point of contact for cyber incident reporting and coordination;
- Detecting and identifying anomalous activity;
- Analysing cyber threats and disseminating cyber threat warning information;
- Analysing and synthesizing incident and vulnerability information disseminated by others such as vendors to provide an assessment for interested stakeholders;
- Establishing trusted communications mechanisms and facilitating communications among stakeholders to share information and address cyber security issues;
- Developing mitigation and response strategies and coordinating incident response;
- Sharing data and information about the incident and corresponding responses;
- Determining trends and long-term remediation strategies;
- Publicising best practices in incident response and prevention advice;
- Coordinating international cooperation on cyber incidents; and
- Building capacity in all the above areas using advanced technology and techniques, establishing methods, and researching threat analyses and mitigations.

11.3.1 Protection Principles

ISO/IEC 27002:2005 regards incident management as about ensuring the effective and timely communication of security events and weaknesses associated with information systems. All employees, contractors and third party users must understand the

[54] Obtain a copy of WTSA-08 Resolution 58 at http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.58-2008-PDF-E.pdf
[55] Obtain a copy of WTDC-10 Resolution 69 at http://www.itu.int/osg/csd/intgov/resoultions_2010/resolution69.pdf

procedures for reporting the different types of events and weaknesses that might have an impact on the security of organisational assets. A formal process requires the timely reporting of any security events and weaknesses to a designated point of contact. Thus, we recommend that incident management participants consider adopting the ITU-T E.409 terminology (ITU 2004). Whereas the requirements differ across nations, ITU-T E.409 sees incident handling as typically aiming to support these requirements:

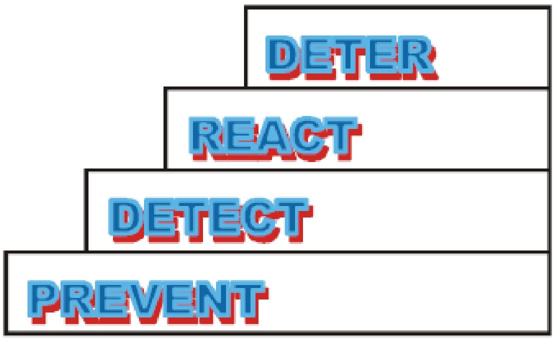


Figure 22 – Protection principles

11.3.1.1 Prevent

The *preventive* protection mechanisms come first. When adequate preventive protection mechanisms are in place, implemented via physical or logical protection, it is possible to identify and activate the *detecting* protection mechanisms. Physical controls could include barriers such as fences, lighting and gates. As discussed under cybersecurity technologies, logical preventive tools include tools that correlate logs from Security Enforcing Functions. The tools correlate logs in real time, establish whether an attack has occurred and either respond or alert an incident response module or team.

11.3.1.2 Detect

The *detection* protection mechanisms could, in the simplest form be the checking of log files, logical or physical alarms, i.e., burglar alarms, fire alarms or other surveillance functions. One form of detection mechanism is the Intrusion Detection System (IDS). The section on cybersecurity tools discusses IDS including network and host-based types.

11.3.1.3 React

Once an incident is detected and validated, action should follow. Actions include: (a) stopping an ongoing incident; (b) identifying scope/scale of incident; (c) limiting damage; (d) taking measures in order to investigate the course of events and (e) preventing the incident from recurring.

11.3.1.4 Deter

Deterrence involves active steps to beat off attacks. As discussed under cybersecurity technologies, Intrusion Prevention Systems (IPSs) can react, in real-time, to block or prevent intrusions. IPSs drop offending packets on detecting malicious activity but allow all other traffic to pass through. Modern IPSs combine firewall, intrusion detection, anti-virus and vulnerability assessment capabilities.

11.4 CYBERSECURITY PARTNERSHIPS

Whilst the national government has ultimate responsibility for leading systematic national cybersecurity programmes, securing cyberspace is a collective responsibility. Therefore, policy development and the elaboration of a national strategy should take into account the views and interest of all participants. The partnerships are local and international.

11.4.1 Public-Private Partnerships

Government Departments and Agencies at all levels should form meaningful partnership with the private sector on cybersecurity because government alone cannot secure cyberspace. Public-private partnerships are vital as they:

- Facilitate the exchange information on the development of new legislation and regulation between stakeholders;
- Enable collaborative work and sharing of training courses that could help alleviate the severe shortage of skilled cybersecurity professionals; and
- Enable real time exchange of information about cyber threats and vulnerabilities. The communication channel is valuable for the national CIRT as the exchange complements the stretched national incident detection and warning resources.

The ITU has identified that successful government-industry collaboration requires three important elements (ITU 2008a). These are:

11.4.1.1 A Clear Value Proposition

Leaders of a cybersecurity programme should describe the programme's benefits to government and the commercial sectors. For example, government requires industry to take steps to secure cyberspace because infrastructure vendors and operators provide capabilities that typically fall outside government's core competencies, such as:

- Expert knowledge of cyber assets, networks, systems, facilities, functions, and other capabilities;
- Incident response expertise and experience;
- Ability to innovate and provide products, services, and technologies to quickly focus on requirements; and
- Design, deployment, operation, administration and maintenance of the Internet

Conversely, the private sector benefits from the collaboration because:

- Governments have the resources to offer owners and operators timely, analytical, accurate, aggregated, and useful information on critical infrastructure threats;
- Governments have the legal tools to create an environment that encourages all companies to invest in cybersecurity practices and hence boost collective security;
- The government can more easily focus on issues of interest to private sector;
- Government may provide incentives for research in enhancing cybersecurity; and

- It enables time-sensitive information sharing as well as restoration and recovery support to priority infrastructure facilities and services during an incident.

11.4.1.2 Clearly delineated Roles and Responsibilities

Governments and the commercial sector have different cybersecurity objectives. Thus, it is vital for all parties to understand each other's roles and responsibilities. Typically, governments have the responsibility and resources to perform overall coordination and leadership on cybersecurity. Conversely, industry has the expertise and the motivation to improve security processes and tools. Therefore, governments normally play the role of facilitators while industry implements the cyber defences.

11.4.1.3 Trust

Due to the different agendas, public-private partnerships only work if each party trust the other's motives and ability to discharge their duties. Trust is important at all stages of the collaboration. For example, private companies may not fully participate in information exchange activities if the government lacks the skills to protect company private details.

11.5 NATIONAL CYBERCRIME UNITS

Countries should consider building cybercrime investigation capability in line with the Legal Measures (1) and Capacity Building (4) Pillars. Typically, Cybercrime Units build on the capacity of Criminal Police departments. However, many countries' Police units lack adequate capacity to undertake cybercrime investigations. Therefore, countries should launch either their own forensic investigation learning programmes or work in partnership with established international organisations. For example, the IMPACT Training and Skills Development Centre conducts such cybercrime investigatory courses in collaboration with companies and institutions such as the ITU, SANS Institute, E-Commerce Consultants (EC-Council), (ISC)^2 and the Honeynet Project. In line with the International Cooperation Pillar, the Unit should have working relationships with global organisations such as the Interpol Cybercrime Unit and regional and national partners.

12 PRIORITY 4 – CAPACITY BUILDING

This pillar cuts across all the other pillars of the Global Cybersecurity Agenda. However, let us consider some that we feel nations should pay special attention to under this pillar.

12.1 CYBERSECURITY SKILLS AND TRAINING

Resolution 130 of the ITU Plenipotentiary Conference 2010 invites Member States to promote the development of educational and training programmes to enhance user awareness of risks in cyberspace. The Resolution also instructs the BDT[56] Director to continue collaboration and exchange of best practices with relevant organisations. This could be through workshops and training sessions. This Guide supports this agenda.

12.1.1 Typical Cybersecurity Skills

To ensure secure and prosperous societies, countries require a skilled cybersecurity workforce. The skills and training requirement addresses the sixth GCA goal, which calls for the development of a strategy to facilitate human and institutional capacity building to enhance knowledge across sectors. To illustrate the matter, we group cybersecurity skills in managerial, information assurance and technical categories as follows:

Management	Information Assurance	Technical
• Cybersecurity Strategy • Legal and Regulatory • Cybersecurity business case formulation • IT Base skills • Staff Management skills/ Leadership skills • Personnel Security • Multi-Disciplinary skills (technology, people etc) • Communication skills • Cyber-Criminal Psychology • Cyber-Ethics Skills	• Cybersecurity Policies, Standards and Procedures • Risk Management • System Accreditation • Compliance Checking • Audit and Monitoring • User Rights and Responsibilities • Incident Management Process Design • Assurance, trust and confidence mechanisms	• IT technical skills (security management) • IT technical skills (Security deployment) • Security Design Principles e.g. zoning • Resilient Infrastructure • Data Protection/ System administration • Cryptographic and Applied Crypto Skills • Data custodianship • Operational Security • Incident Management

Figure 23 – Typical Cybersecurity skills

[56] The ITU Telecommunication Development Bureau (BDT)

12.2 JUDICIAL CAPACITY

The judiciary enforces cybersecurity legal measures. However, the judiciary often lacks the skills required to prosecute criminal electronic investigations. Thus, we recommend that the cybersecurity strategy addresses the need to improve judicial capacity against cybercrime. Strategists should build capacity to enable judges and prosecutors to gain a reasonable understanding of computers, software, networks and electronic evidence. In the short-term, countries may consider instituting training courses. In the long-term, it is important to modify curricula to ensure that lawyers and prosecutors obtain grounding in computer-enabled crime. The judiciary requires training in methods of handling electronic evidence to ensure that it preserves its evidential weight and thus admissibility in Court.

12.3 NATIONAL CULTURE OF CYBERSECURITY

National governments have ultimate responsibility for leading a systematic effort to bring about a cybersecurity culture in collaboration with other relevant stakeholders. A culture of security aligns with the sixth GCA Strategic goal that deals with capacity building mechanisms to raise awareness, transfer knowledge and boost cybersecurity on the national policy agenda. The United Nations General Assembly (UNGA) has also encouraged the promotion, development and implementation of a robust global culture of cybersecurity because confidence and security in the use of ICTs are among the main pillars of the information society (UN 2010).

12.4 CYBERSECURITY INNOVATION

Cyberspace will underpin the prosperity of the global economy, government services and national security for many years to come. To build capability to secure cyberspace from attacks as well as exploit its potential in an internationally compatible way, countries should develop long-term strategies for enhancing knowledge and fostering innovation across sectors. For example, PP-10 Resolution 130 identifies the need for continual evolution in new technologies to support the early detection of, and coordinated and timely response to, events or incidents compromising computer security.

13 PRIORITY 5 – INTERNATIONAL COOPERATION

This is the second pillar that cuts across all the other pillars of the GCA. We feel nations should pay special attention to the following:

13.1 COOPERATIVE INTERNATIONAL EFFORTS

The ITU Global Cybersecurity Agenda is an international cooperation tool. A growing coalition of nations regards the GCA as critical to engaging all relevant stakeholders in a concerted effort to build confidence and security in the information society. As we discussed in section 4.5, the ITU has struck significant partnerships under the GCA. We also noted that cybersecurity has concerned the United Nations for many years. The United Nations Chief Executives Board (CEB) recently resolved to elaborate a UN-wide strategy for cybersecurity. The CEB nominated the ITU and UNODC as the lead UN agencies for cybersecurity and cybercrime respectively. We earlier noted that the ITU and UNODC signed a MoU to mitigate the risks posed by cybercrime. In the long-term, the United Nations to reduce further duplication of effort by using the expertise of existing bodies such as OSCE[57]. It is also important to involve other groups at the global level such as INTERPOL, NATO[58], OECD[59], IPU[60] and UNDESA[61].

[57] Organization for Security and Co-operation in Europe (OSCE)
[58] North Atlantic Treaty Organization (NATO)
[59] Organisation for Economic Co-operation and Development (OECD)
[60] Inter-Parliamentary Union (IPU)
[61] United Nations Department of Economic and Social Affairs (UNDESA)

VII. MEANS – ACTIONS

14 MEANS – ACTIONS

The Means flow from the Ways. The means describe the resources available to achieve the stated ends. The actions we present are not prescriptive. Local conditions should determine the type and order of actions you choose from this list. One should feel free to create new actions. The only condition, of course, is that one does not lose track of the GCA association. National administrations may also use the section to review or improve existing institutions, policies, and relationships addressing cybersecurity issues.

15 PRIORITY 1 – LEGAL MEASURES

Actions under this priority focus on the establishment and modernisation of criminal law, procedures, and policy to prevent, deter, respond to, and prosecute cybercrime.

15.1 ACTION 1: LEGAL MEASURES STRATEGY

We advise that nations adopt a legal measures strategy to provide common direction and obtain the commitment of all stakeholders. The strategy would allocate resources, coordinate and control all activities aimed at enacting and enforcing a comprehensive set of laws relating to cybersecurity. The strategy also identifies the roles and responsibilities in the creation and modernisation of criminal law, procedures, and policy to prevent, deter, respond to, and prosecute cybercrime.

15.2 ACTION 2: REVIEW ADEQUACY OF LEGISLATION

Statutes define roles of parties that fight cybercrime. Thus, countries should establish whether national statutes related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption are adequate. The review should involve as many stakeholders as possible. Typical participants include government departments, intelligence and law enforcement, private firms, civil society, academics and citizens. We recommend that you involve regional and international partners, where practical, because international cooperation is pivotal to confronting the global issue:

15.2.1 Model Cybercrime Legislation

If relevant experts and stakeholders determine no sufficient legislation exists, then the country should draft and/or adopt cybercrime legislation. We recommend that you adopt harmonised legislation that is compatible with regional and cybercrime legislation. For example, the ITU Toolkit for Cybercrime Legislation contains sample language that countries may use to elaborate their own cybercrime legislation and thus facilitate international cooperation against cybercrime

15.2.1.1 Cybercrime Toolkit for Developing Countries

The “Understanding Cybercrime: A Guide for Developing Countries” is the second major ITU cybercrime resource. The Guide aims to help developing countries:

- Understand the national and international implications of cyber threats;
- Assess the requirements of existing national regional and global instruments; and
- Establish sound legal foundations.

The Guide provides a comprehensive overview of the most relevant topics linked to the legal aspects of cybercrime. Furthermore, the Guide identifies international approaches as well as good practice examples from national solutions.

15.2.1.2 ITU Toolkit for Cybercrime Legislation

ITU has collaborated with the American Bar Association’s (ABA) Privacy and Computer Crime Committee (PACC) and more than a hundred legal and cybersecurity specialists to create a document entitled the “ITU Toolkit for Cybercrime Legislation.” The Toolkit analyses cybercrime legislation of Australia, Canada, the European Union, the Council of Europe, Germany, Japan, Mexico, Singapore, India, China, the United Kingdom and the USA. Therefore, this Guide recommends that ITU Member States consider aligning their national cybercrime laws with the ITU Toolkit because:

- The Toolkit incorporates salient points from legislation of major countries (developed and developing) as well as influential regional bodies; and
- The Toolkit helps address gaps in country and regional cyber legislation.

Countries may customise the Toolkit’s Sample Language to form local cybercrime laws. Countries that model legislation on the Toolkit’s Sample Language would facilitate global cooperation as the Toolkit’s Clauses help resolve jurisdictional and evidentiary issues.

15.3 ACTION 2: GOVERNMENT LEGAL AUTHORITY

The second action deals with providing the government the legal power it requires to undertake activities to ensure that cyberspace keeps a country secure and prosperous. As we saw earlier, depending on national conditions, priorities and needs, you should focus on providing the national administration the requisite legal authority to:

- Create regionally and globally compatible cybersecurity organisational structures;
- Designate a system as critical national information infrastructure;
- Mandate government and critical infrastructure operators and owners to prepare and test emergency plans in the event of a nationwide cyber attack;
- Define the legal basis for creating a national CIRT;

- Provide the basis for promoting cybersecurity skills, training and awareness;
- Foster innovation in cybersecurity to help develop long-term solutions; and

Grant the government powers to participate in international cooperation, dialogue and coordination activities focuses on cybersecurity such as mutual assistance.

15.3.1 Legal Measures Actions

Below are the actions you should consider under the Legal Measures Priority/Way.

# ITEM	LEGAL MEASURES
1	**Cybercrime Legislation** Establish whether: (a) Your country has cybercrime laws in areas such as computer misuse, electronic signatures, data protection, intellectual property, liability and dispute resolution; (b) Relevant stakeholders believe your country's criminal code adequately addresses current (and future) cybercrime issues; and (c) Your country's cybercrime laws comply with the ITU Toolkit for Cybercrime Legislation country worksheet
2	**Cybersecurity Legal Authority** Establish whether national government has legal powers to: (a) Constitute a national cybersecurity programme; (b) Allocate roles and responsibilities; (c) Designate systems as critical national information infrastructure; (d) Require stakeholders to secure critical systems under their control; (e) Participate in collaborative international activities on cybercrime
3	**Cybercrime Capacity** Establish whether: (a) Police has capacity to detect, deter and prosecute cybercrime; (b) Cooperative relationships exist with other elements of the national cybersecurity infrastructure and the private sector; (c) Judicial and legislative branches have awareness of cybercrime risks, preventive measures and remedies; and (d) The curriculum of the legal profession covers cybercrime.
4	**International Cooperation** On international cooperation and investigative assistance assess if: (a) National cybercrime laws are globally applicable and interoperable with existing regional and global legislative measures; and (b) National cybercrime legislation allows global cooperation on cybercrime investigations and prosecution.

Figure 24 – Legal Measures Action Items

16 PRIORITY 2 – TECHNICAL AND PROCEDURAL MEASURES

Actions under this priority address help create a generic and universal digital identity system and the necessary organisational structures to recognise digital credentials across jurisdictions through the following actions:

16.1 PROCEDURAL MEASURES

Countries should consider the following actions under this priority/pillar:

16.1.1 Action 1: National Cybersecurity Framework

A Cybersecurity Framework implements the vision outlined in the Cybersecurity strategy. The Framework is a standards-based but flexible model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving Cybersecurity Programmes. The Framework outlines minimum-security measures that stakeholders must abide by to claim compliance with national cybersecurity requirements. Cognisant that cybersecurity is a global issue, this Guide defines a Framework modelled on ISO/IEC 27000 Series, the most widely recognised Information Security Management System (ISMS).

16.1.2 Cybersecurity Goals

The eleven ISO/IEC 27002 security control clauses are a natural model for security goals because organisations that implement these clauses are on the way to meeting ISO/IEC 27001 requirements. This Guide adapts the control clauses to define four model security goals for the consideration of national administrations. The goals are not security policies for direct application by departments and agencies. Instead, the security goals define the minimum or mandatory security requirements. We provide an example below:

16.1.2.1 Goal 1: Governance and Risk Management

Objective: Effective security results from a good governance structure as well as the selection of security controls based on sound risk management principles.

16.1.2.1.1 Governance

This sub-goal coincides with the ISO/IEC 27002 "Organising Information Security" security control clause. The clause calls for the creation of a management framework to initiate and control the implementation of security within an organisation. This Guide recommends that the organisation serves as the focal point for all activities dealing with protecting that organisation’s part of cyberspace against threats. The team should approve security goals, policy, assign security roles and co-ordinate and review the implementation of cybersecurity across the organisation. The head of the team is accountable for its success. The executive may delegate this responsibility to heads of department, contractors and individual employees. The multi-disciplinary cybersecurity team coordinates action on shared risks and sets mandatory requirements for all stakeholders. Departmental heads are responsible for determining the additional level of compliance required and convincing the central body that the interpretation is competent. The organisation should have access to specialist cybersecurity advice. The team should develop contacts with external cybersecurity specialists or groups including relevant national authorities and, where appropriate, regional and global organisations.

16.1.2.1.2 Risk Management

Every organisation faces internal and external factors that bring a degree of uncertainty to whether or not they will achieve its objectives. ISO 31000 regards this uncertainty as risk. Organisations manage risk by identifying it, analysing it, evaluating the likelihood of occurrence, determining the potential impacts of the risk materialisation and designing countermeasures. Organisations should decide whether to modify the risk by treatment to satisfy the risk criteria (ISO 2009). Similarly, ITU-T regards risk management as about assessing and quantifying risk and taking action to ensure that residual risk is below predetermined acceptable levels (ITU 2009f). Recommendation ITU-T X.1055 describes and recommends the processes, techniques and functional profiles for telecommunication information security risk management (ITU 2008c). Among other aspects, the risk management process provides guidance on how to:

- Identify risks;
- Analyse and evaluate the risks;
- Identify and evaluate options for the treatment of risks; and
- Select control objectives and controls for the treatment of risks.

This Guide recommends that all organisations adopt solid risk management processes. Risk management process helps organisations determine what assets need protection, the threats they require protection against and the controls. The evaluation helps categorise risks by severity and involves making cost-effective decisions on what needs protection. The process helps organisations ensure that the efforts and money spent on security yield cost effective benefits (IETF 1997).

Good risk management processes are not prescriptive. Instead, the processes recognise that organisations have different business requirements, structures and operational environments. The process defines broad requirements allowing organisations to decide the most cost effective and efficient risk management approaches (ISO/IEC 2008). A full treatment of risk management is outside the scope of this document. ISO/IEC 27005 is the definitive standard on the topic as it covers concepts such as context establishment, risk assessment, risk treatment, risk acceptance, risk communication and risk monitoring and review. ISO/IEC 27005 adopts the PDCA model.

16.1.2.1.2.1 Risk Assessment Model

A risk assessment exercise helps your organisation to produce a list of risks that assets are facing or is likely to face (ITU 2008c). Thereafter, you should prioritise the risks to ensure that the more serious one get first attention. Serious risks are the type where the cost of recovery from their impacts exceeds the cost of instituting countermeasures. A simplified risk assessment model appears as follows:

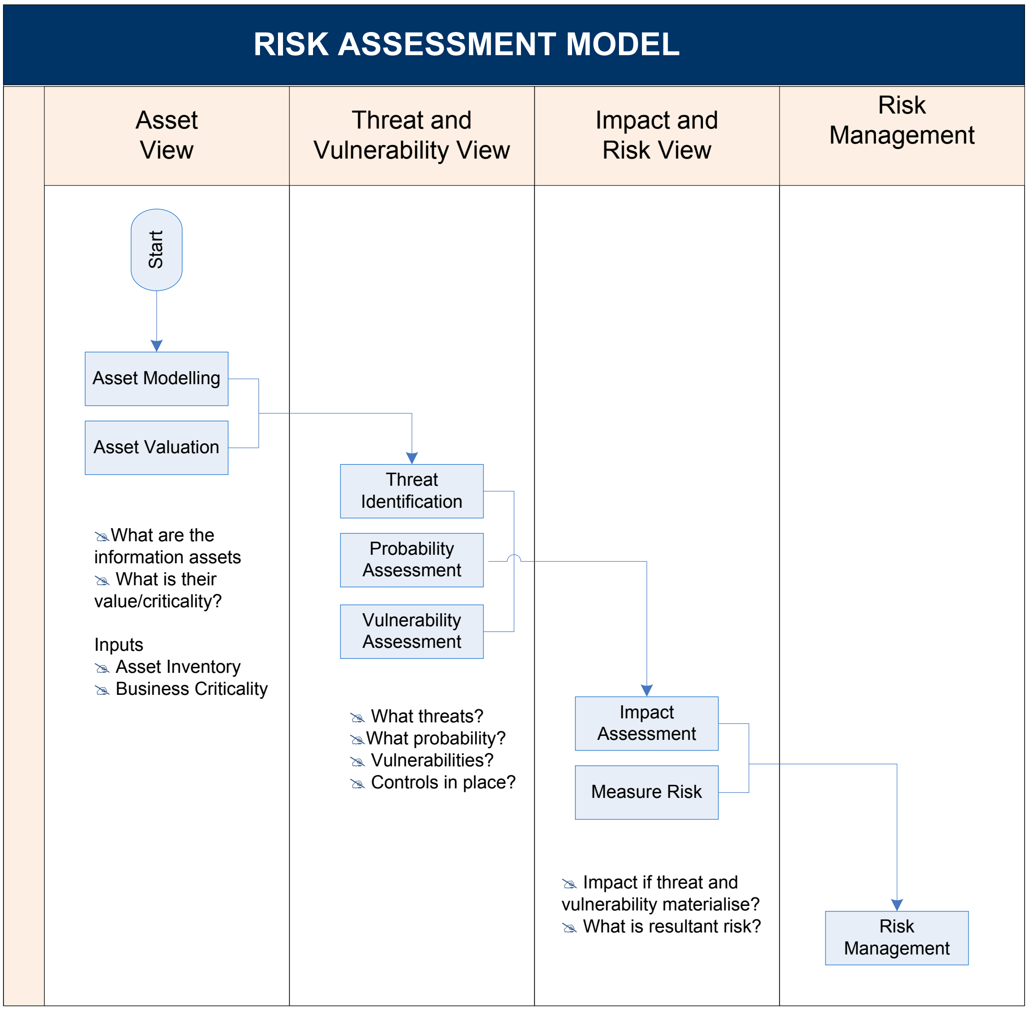


Figure 25 – Risk Assessment Model

16.1.2.1.3 Risk Management Model

The overall objective of the risk management process is to ensure that an organisation and its assets have suitable protection against risks identified under the risk assessment process. The Risk management process involves:

- The selection of controls to mitigate the risks identified in the risk assessment view;
- Formalisation of the risks identified during the risk assessment view;
- Management's acceptance of the controls identified;
- The acceptance of residual risk; and
- The preparation of a Risk Treatment Plan

The risk management process appears as follows:

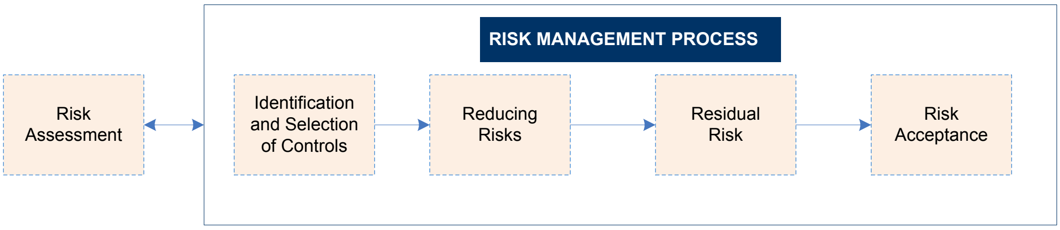


Figure 26 – ISO/IEC Risk Management Process

16.1.2.1.4 Example: Risk Management and Accreditation Document Set

This Guide recommends that countries explore the benefits of a Risk Management and Accreditation Document Set (RMADS). As stated in the title, an RMADS supports risk management and accreditation. The RMADS is a common tool for managing the risk to complex United Kingdom (UK) public sector Information Systems.

We recommend that you consider using the RMADS to manage risks to your systems as it complies with international standards. An RMADS brings together the procedures, processes, instructions and plans required to maintain security of a complex IT system as defined in Her Majesty's Government (HMG) Information Assurance Standard No. 2 (IS2). IS2 acknowledges the ISO/IEC 27000 Series standards and provides a framework consistent with the ISO/IEC 27002 Code of Practice (UK 2008). Compliance with IS2 thus put your organisation on track to certification to ISO/IEC 27001.

An RMADS identifies security management roles and provides evidence to support risk management and accreditation. Furthermore, the RMADS defines timescales and the content of regular compliance checking activities, including audit and security reviews in accordance with recognised best practice. Consequently, an RMADS helps adopters justify and account for risk management decisions, the basis for risk management in service and a compliance monitoring reference. An advantage of the RMADS is that it varies in size according to the complexity of the system as well as the existence of other supporting documents. For example, an RMADS may be a brief document if the other documents such as Corporate Information Assurance cover the accreditation criteria.

16.1.3 Procedural Measures Actions

We summarise the typical Procedural Measures as follows:

# ITEM	PROCEDURAL MEASURES
1	**Cybersecurity Accountability** Review procedural measures to establish whether they define: (a) Top Leadership accountability for cybersecurity; (b) Collective accountability of all staff and contractors; (c) Individual accountability for security for every employee; and (d) Requirements for employing trustworthy individuals
2	**Risk Management** Assess whether: (a) An agreed view on risk exists; (b) Stakeholders follow sound risk management principles.
3	**Security Policies** Assess whether: (a) Minimum security requirements are in place for all stakeholders; (b) Detailed technical standards supplement minimum requirements
4	**Compliance and Assurance** Assess whether: (a) Compliance and assurance framework are in place; (b) Principles such as self-assessment, internal and external audit apply; (c) Clear compliance timetables are in place; (d) Transparency exists in reporting of compliance; (e) Non-compliance carries consequences e.g. disconnection from shared services and systems.

Figure 27 – Procedural Measures Action Items

16.2 TECHNICAL MEASURES

Technical measures form the second part of the Technical and Procedural Measures Pillar. We believe the actions below are important:

16.2.1 Action 1: Deploy Technical Solutions

The ITU Cybercrime Guide for Developing Countries discusses a technical approach to cybersecurity and explores security technologies (ITU 2009c). We cover similar ideas but with an emphasis on the broader security principles to guide cybersecurity strategy formulation. We present a table based on categories developed by the United States General Accounting Office (GAO 2004) as well as Recommendation ITU-T X.1025 (ITU 2008d). Refer to Annex 2 for the technological solutions.

16.2.2 Action 2: Secure Applications

ITU-T Study Group 17 Question 7/17 on secure application services and Question 8/17 Service oriented architecture security address the issues around services that do not necessarily obey perimeter security. The result has been the development of Service Oriented Architectures (SOA) to support operations such as service discovery, externalisation, composition and re-use within communication enabled workflows. As a result, a new security paradigm applies in the SOA era. Rather than assuming trusted users in a secure internal network, SOA aim to help distrusting parties to conduct business transactions securely. SOA security requires the ability to manage trust across separate security domains since the adversary is not an intruder but a fraudulent insider.

Question 8/17 emphasises that cybersecurity involves more than securing the perimeter. The technologies discussed above such as IDS traditionally helped defend the perimeter that separates the internal from external network. Perimeter technologies are extremely important. However, your organisation should understand that perimeter security offers limited protection in the era of SOA and ubiquitous services that span different wire-line, wireless, mobile networks, devices and users. Therefore, countries should implement a coherent strategy for securing your applications.

16.2.3 Action 3: Secure Government Infrastructure

Whilst national governments own and operate only a minority of critical infrastructure, government systems require protection against threats from State and non-State actors. Therefore, we recommend that you consider measures to secure government systems. This action is important because government must lead other stakeholders in systematic efforts to secure national infrastructure. A national administration will have limited credibility unless it fixes its leads by example. As the Guide indicates, critical steps in securing government systems include definition of Protective Marking Schemes, Staff Vetting and Clearance and an overall accreditation regime.

16.2.4 Technical Measures Actions

Below are the typical considerations around Technical Measures.

# ITEM	TECHNICAL AND PROCEDURAL MEASURES
1	**Business Objectives** Establish: (a) Business objectives; (b) Business risk environment, (c) Risk appetite – level of risk acceptable in pursuit of business goals (d) Organisational ownership of the asset (e) High level business aims and objectives served by the asset (f) Business functions supported by the asset (g) Information processes carried out by the asset
2	**Cyber Threats** Establish: (a) Threat sources and actors the system faces (b) The kind of protection is needed against the threats (ITU-T X.805) (c) Vulnerabilities (d) The likelihood that threats will materialise (e) The impact if threats materialised
3	**Risk Management** Assess: (a) Controls and reporting mechanisms are in place to support the wider IA governance requirements; (b) Detailed technical standards supplement minimum requirements
4	**Technical Measures** Identify: (a) Specific business goals that technical solutions support; (b) Core security principles that the technical solutions support; (c) The distinct type of network equipment and facility grouping that need protection (ITU-T X.805) (d) The distinct network activities that need protection (ITU-T X.805)

5	**Accreditation Maintenance**
	Assess how the Accreditation will occur:
	(a) Documentation inspections;
	(b) IT Health Check;
	(c) Technical audit;

Figure 28 – Technical Measures Action Items

17 PRIORITY 3 – ORGANISATIONAL STRUCTURES

We believe the actions below are important.

17.1 ACTION 1: ROLE OF GOVERNMENT

This Action requires Governments to put in place appropriate national structures to protect infrastructure, classified data and all assets required to deliver essential services to the public. The Government is also responsible for communicating national priorities to the commercial sector to ensure that infrastructure in private hands in sectors such as banking, transport and telecommunications receives sufficient protection. The Head of Government may appoint a National Cybersecurity Coordinator. Typically, National cybersecurity coordinators establish a pan-government programme to address the priority areas of this Strategy. The official provides strategic leadership and ensures the coherence of cybersecurity activities across government.

17.1.1 National Cybersecurity Coordinator

Heads of Government often delegate cybersecurity duties to a National Cybersecurity Coordinator. The Coordinator (an individual or an office) directs all cybersecurity activities in Government. If an individual, the Coordinator should understand cybersecurity issues and be able to direct and coordinate the efforts of governmental institutions and effectively collaborate with industry (ITU 2008a). The Coordinator should with and through Permanent Secretaries or chief executives to ensure that Departments and Agencies manage cybersecurity risks in line with national policy. The Coordinator should ensure that national and regional organisational structures and policies on cybercrime are in place in accordance with Goal 2 of the GCA. To ensure that cybersecurity programmes keep countries secure and prosperous, national coordinators typically serve as members of national security and economic bodies.

17.1.1.1 Example: National Cybersecurity Coordinator

17.1.1.1.1 US National Cybersecurity Coordinator

In the US, the White House-based Cybersecurity Coordinator directs all cybersecurity activities across Government. He leads on the Comprehensive National Cybersecurity Initiative (CNCI), a plan for securing government and private industry networks. CNCI consists of twelve initiatives including deployment of intrusion detection and prevention system sensors across the Federal enterprise network; development a comprehensive approach for global supply chain risk management; expanded cyber education; research and development. The mutually reinforcing initiatives aim to help secure the United

States in cyberspace. The CNCI and its linked activities are key elements of the National Strategy to Secure Cyberspace. The Coordinator has regular access to the President and serves as key member of the National Security Council (NSC) staff.

17.2 ACTION 2: NATIONAL FOCAL POINT

Given the scope of the cybersecurity challenge, countries require an accountable organisation to serve as a focal point for coordinating cybersecurity activities. This multi-agency body should unite operational cybersecurity efforts of government institutions and leads collaboration with industry. Public-private partnership coordination is critical to protecting critical infrastructure because it enhances information sharing and cooperation on cyber threat identification, incident response and recovery. Poor coordination may lead to misuse of resources and may thus leave countries less secure.

17.2.1 Examples: Cybersecurity Focal Points

17.2.1.1 US Department of Homeland Security

In the United States of America, the Department of Homeland Security (DHS) is the focal point for cybersecurity. DHS roles include developing a comprehensive national plan for Critical Infrastructure Protection including cybersecurity (Powner 2009). Other DHS duties include identifying, assessing and supporting efforts to reduce cyber threats and vulnerabilities, including those associated with infrastructure control systems.

17.2.1.2 UK Office of Cyber Security & Information Assurance (OCSIA)

The OCSIA supports the UK Security Minister and the National Security Council in determining priorities in relation to securing cyberspace. The unit provides strategic direction and coordinates action relating to enhancing cyber security and information assurance in the UK. OCSIA duties include:

- Overall ownership of the UK Cybersecurity Strategy;
- Provision of cybersecurity strategic leadership across government; and
- Driving delivery of the strategy through a cross-government programme that adopts elements already underway, for example in the field of Information Assurance.

The OCSIA works alongside the Cyber Security Operations Centre (OCS) in driving forward the cyber security programme for UK government and give the UK the balance of advantage in cyberspace. The major government departments involved include the Home Office, Ministry of Defence, Government Communications Headquarters (GCHQ), Communications-Electronics Security Group (CESG), the Centre for the Protection of National Infrastructure (CPNI) and the Department for Business, Innovation and Skills.

17.2.1.3 Singapore Infocomm Technology Security Authority (SITSA)

The Singapore Infocomm Technology Security Authority (SITSA) is the national specialist authority for operational security. SITSA deals with threats to Singapore’s national security especially external threats such as cybercrime and cyber-espionage.

SITSA focuses on capacity-building and engaging regulators and industry players in Singapore (Shanmugam 2009) in the short-term.

17.2.1.4 National Leadership Actions

Below are the typical considerations under the cybersecurity national leadership.

# ITEM	NATIONAL CYBERSECURITY LEADERSHIP
1	**Government Accountability** Establish whether: (a) Political leadership understands what is at stake; (b) National government has assumed responsibility for leading a systematic national cybersecurity programme; (c) The Head of Government has ultimate cybersecurity accountability (d) Top Government official coordinates daily cybersecurity tasks (e) Cybersecurity Accountability is delegated to all Government levels (f) Incentives in place to encourage Government departments to consider cybersecurity in procurement and investment decisions
2	**National Cybersecurity Coordination** Establish whether: (a) An accountable multi-agency body serves as a focal point for cybersecurity (b) Nominated organisations lead sector cybersecurity activities
3	**International Cooperation** Assess whether: (a) Cybersecurity considerations form part of foreign policy (b) Country participates in inter-governmental cybersecurity activities

Figure 29 – National Cybersecurity Leadership Action Items

17.3 ACTION 3: NATIONAL CIRT

The government should create legal and regulatory incentives to encourage critical infrastructure owners and operators to ensure that their systems are resilient to attacks. Countries may also consider participating in global efforts such as IMPACT.

17.3.1 Examples: National CIRTs

The following are examples of national CIRTs with national responsibility presented in alphabetical order. The acronym CERT is synonymous with ITU's CIRT terminology.

17.3.1.1 Malaysian Computer Emergency Response Team (MyCERT)

MyCERT[62] is responsible for addressing the computer security concerns of Malaysian Internet users. MyCERT's vision is to reduce the probability of successful cyber attacks and lower the risk of consequential damage. Launched in 1997, MyCERT helps handle incidents such as intrusion, identity theft, malware infection, cyber harassment and other computer security related incidents. MyCERT works closely with law enforcement agencies such as the Royal Malaysian Police, Securities Commission and the Central Bank of Malaysia. MyCERT maintains close working relationships with ISPs and is a member of global incident management initiatives such as FIRST[63].

17.3.1.2 Qatar CERT (Q-CERT)

Q-CERT[64] is the national Computer Emergency Response Team (CERT) for Qatar. The government-sponsored Q-CERT works under the auspices of ictQATAR. Launched in 2004, ictQATAR's main mandate is to transform Qatar into an information-based society. IctQATAR also serves as a telecommunications regulator and technology champion. Q-CERT's main activities are cybersecurity intelligence and cyber incident management and coordination. Q-CERT's constituency includes all organisations authorised to use the .QA URL domain extension as well as Qatar Internet users. Cognisant of the global nature of the cyber threat, Q-CERT participates in collaborative international efforts against cyber threats such as being a full member of FIRST.

17.3.1.3 United Arab Emirates CERT (aeCERT)

The Ministerial Council for Services has designated aeCERT[65] as the national CIRT for the United Arab Emirates (UAE). The UAE Telecommunications Regulatory Authority (TRA) established aeCERT as an initiative to facilitate the detection, prevention and response to cyber incidents. In May 2009, the TRA and the IMPACT Alliance signed an agreement of partnership and cooperation. The agreement made UAE the first country in the region to be one of IMPACT Alliances affiliates and partners. The agreement with IMPACT gives aeCERT access to resources and information of a global network. The agreement also helps build human and institutional capacity in the UAE with IMPACT training facilities and resources. aeCERT promotes cybersecurity through its Security@Work and Security@Home programmes. aeCERT is a full member of FIRST.

[62] The MyCERT website is at: http://www.mycert.org.my/en/

[63] Forum of Incident Response and Security Teams (FIRST) is a global forum of incident response and security teams.

[64] The Q-CERT website is at: http://www.qcert.org/EN/Pages/default.aspx

[65] The aeCERT website is at: http://www.aecert.ae/index-en.php

17.3.1.4 CIRT Actions

The considerations below present an abridged and modified version of the ITU-IMPACT CIRT Readiness Assessment questionnaire as follows:

# ITEM	CIRT – READINESS ASSESSMENT QUESTIONNAIRE
1	**National CIRT Capacity** Identify: (a) Government Agencies involved in CIRT activities (b) Points of contact for incident response in the CIRT (c) Internal or external organisations interfacing with CIRT Project (d) Relevant Agencies / ministries /sectors involved in CII (e) Internet Service Providers
2	**Mission and Target** For operational or planned CIRT establish: (a) Objectives of the CIRT (b) Short-term and long-term goals
3	**CIRT Initiatives within the Country** Record: (a) Current or past Government or private sector CIRT initiatives (b) Systems protected by each CIRT initiative (c) Initiatives focused on recording cybercrime (d) History of cyber incidents (e) Cybersecurity research initiatives
4	**CIRT Service Model** For every CIRT identify: (a) CIRT service model i.e. Unbounded, Bounded and Hybrid (b) Criteria for selecting CIRT service model (c) Operational Framework e.g. advertisement of membership/services (d) Level of CIRT authority i.e. Full, Shared and None (e) Whether CIRT owns its premises and technical infrastructure (f) Manpower planning i.e. Staffing levels and Cybersecurity skills (g) Incident Response and Performance evaluation model (h) Participation in international information sharing activities
5	**CIRT Reporting Structure** Identify: (a) Whether CIRT is an independent or Subsidiary organisation (b) Its relationship with other CIRTs (c) Financial model i.e. source of funding and revenue

Figure 30 – CIRT Leadership Action Items

18 PRIORITY 4 – CAPACITY BUILDING

We recommend that countries consider the following actions.

18.1 ACTION 1: CYBERSECURITY SKILLS AND TRAINING

This action focuses on the creation of programmes to increase the cadre of cybersecurity professionals in Managerial, Technical and Information Assurance areas rather than general user awareness and education. Therefore, countries should re-organise their educational priorities to address cyberspace challenges and opportunities.

18.1.1 Cybersecurity Skills Framework Assumptions

Knowing that cybersecurity needs are situation-dependent, we propose that countries adopt framework for planning and implementing a training programme. The framework may follow the structure of the strategy elaboration flowchart in Figure 5. We make the following assumptions about the Skills Framework:

18.1.1.1 Working Group

Typically, representatives from different stakeholder groups for example Government Departments and Agencies constitute a Working Group to define cybersecurity skills needs. Working Group participants should represent stakeholder groups in managerial, technical and information assurance areas. The business teams, represented under the heading “Government Ministry or Private Sector” in the Framework, provide the contextual factors for the skills i.e. assets protected and why. The technical teams should define the technical skills required to meet protection needs.

18.1.1.2 Job Descriptions

The constituted Working Group should define a continuum of management, information assurance and technical job descriptions. The job descriptions help standardise the understanding of skills and training needs for a cybersecurity programme.

18.1.1.3 Certification

GCA strategic goal six calls for the development of a global strategy to facilitate human and institutional capacity building to enhance knowledge and know-how sharing. As such, this skills framework assumes that leaders of cybersecurity programmes will consider sponsoring their staff to pursue commercial information security certifications. The logic is follows. The private sector designs most of the critical infrastructure around the world. Indeed, the private sector engineers the security enforcing functions in critical infrastructure such as firewalls, IDS, IPS and anti-virus software. Therefore, commercial certifications would facilitate global cybersecurity knowledge sharing on common issues. Besides, commercial certifications are most likely to keep pace with the increasingly sophisticated, frequent and severe cyber threats.

18.1.1.4 Training Coordination

The skills framework assumes that, at least in the initial stages, some training should be coordinated centrally. Centralised training helps create common understanding of the cybersecurity challenge. This Guide assumes that a National Cybersecurity Agency or similar multi-agency organisation should either deliver the training itself or coordinate courses provided on its behalf. The Agency should request stakeholder organisations to validate the courses and obtain commitment for funding from their local budgets.

18.1.1.5 Periodic Review

This framework assumes that a competent organisation would periodically evaluate cybersecurity skills and awareness levels. The audit aims to ensure that a country retains sufficient expertise to secure its cyberspace. Relevant stakeholders may appoint an independent auditor to perform the skills compliance and effectiveness audit.

18.1.1.6 Example: Scholarship-For-Cyber-Service Programme

Countries seeking to recruit and train the next generation of information technology workers and security managers for the Government should consider adopting ideas from the US Scholarship-For-Cyber-Service Programme. The Programme provides full tuition, fees, and a stipend, for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field (Lipinski *et al.* 2010, Rockefeller *et al.* 2009). Scholarship recipients work for the Government agency for a period equal to the length of the scholarship after graduation if offered employment in cybersecurity.

18.2 ACTION 2: CULTURE OF CYBERSECURITY

Many cyber threats materialise due to insecure user activities. Given the increased vulnerability of computer networks around the world to cyber threats, it is important to promote a strong security culture. A strong culture of security could reduce the likelihood and impact of attacks on infrastructure vital for the delivery of essential services. We recommend that countries consider the steps below:

18.2.1 National Awareness Programme

Governments should organise a national awareness programme so that all participants – government, business, the workforce, and the public – understand what is at stake and how they can help secure their parts of cyberspace. Awareness aims to share information about risks, preventative measures and responses. The programme:

- Emphasises that while cybersecurity is a collective responsibility, every stakeholder has a duty to take steps to secure their own systems;
- Facilitates communication on cybersecurity within government as well as with other local and international stakeholders; and
- Helps standardise approaches to cybersecurity. For example, the programme may emphasise the need to conduct user education before granting new employees access to critical information infrastructures.

The programme should undergo periodic review to measure progress and identify areas of improvement. Ideally, independent parties should perform the audits on annual basis. The programme should also contain collaborative user training activities. Cybersecurity awareness courses should not restrict themselves to contents of the security policies and procedures. Instead, trainers should consider the continued relevance of cybersecurity controls in light of rapidly changing threats and information risks.

18.2.1.1 National Awareness Functional Components

ITU-D Study Group 1 Question 22/1 identifies three functional components of a national awareness programme (ITU 2008a). These are:

- Stakeholder outreach and engagement to build and maintain trusted relationships among and between industry, government, and academia to raise cyber security awareness and effectively secure cyberspace;
- Coordination, which works to ensure collaboration on cybersecurity events and activities across the government; and
- Communications and messaging, which focuses on development of internal (within the government agency responsible for programme) and external communications (other government agencies, industry, academia, home users, and general public).

18.2.2 Cybersecurity Culture in Government

Governments own and operate only a minority of information infrastructure around the world. However, governments have ambitious Electronic Government (eGovernment) projects. Governments also have law enforcement and counter-terrorism responsibilities. Yet, networks supporting government activities face a growing threat from hostile nations seeking classified data as well as hackers and cyber criminals. Therefore, governments require stringent data handling procedures to maintain integrity and confidentiality of sensitive and classified information. Governments have spent substantial amounts of money on building technological defences. However, the safeguards do not work well unless all government employees, contractors and third party users have the right knowledge and skills to reduce cyber threats. However, incidents of lost government data, even in developed countries, indicate an underdeveloped culture of cybersecurity. Therefore, governments can boost the culture of security through awareness training. The training should emphasise that:

- Senior management is accountable for cybersecurity;
- All staff and contractors have personal responsibility for security;
- All staff and contractors have collective responsibility to maintain security; and
- Untrustworthy people and companies will not be allowed to handle government data.

The activities above would help reduce the risk of theft, fraud or misuse of classified and/or sensitive government information and facilities.

18.2.3 Cybersecurity in business enterprises

The private sector owns and operates the majority of critical information infrastructure. Therefore, businesses should understand the relevant risks, preventive measures and effective responses. Whereas large companies own the bigger systems, it is important to address the cybersecurity risks at small and medium sized companies as they often lack the human and institutional capacity to address the threats. Governments should work with industry associations to develop and implement cybersecurity education and training programmes. It is useful to produce cybersecurity booklets, manuals, handbooks and model policies for business enterprises. Where feasible, governments should produce security self-assessment tools dedicated to companies. Countries may also consider using tax incentives and financial assistance to foster secure systems development.

18.2.4 Children and Vulnerable individuals

Cyberspace plays an important role in children’s education and entertainment. However, it is important to provide children and young people guidance on safe online behaviour. Providing training and increasing the children’s awareness of cybersecurity issues has a big multiplier potential as they are bound to share this information with their parents and grandparents. We saw earlier that the Child Online Protection Initiative has issued four guidelines for children; parents, guardians and educators, industry and policy makers.

18.3 ACTION 3: CYBERSECURITY INNOVATION

We previously recommended that nations devise a technology strategy to ensure that they have the required solutions to prevent, deter, detect and recover from attacks. In particular, countries should consider the following actions:

18.3.1.1 Cybersecurity Research and Development

Cyberspace is changing. Gone are the days when the Internet meant web browsing and electronic mail. Cyberspace combines data, voice and video applications. The Internet has also moved beyond the confines of the computer to all manner of devices. The new cyberspace provides opportunities for innovation and commerce. However, convergence of media has stretched the security underpinning the Internet. Therefore, a worldwide race is on to develop the next generation of secure Internet technologies. At the same time, cyber threats continue to evolve in complexity and gravity. Therefore, countries should direct some of the science and technology budgets towards the development of secure information infrastructures. Countries may also consider adopting secure open platforms where they exist. As discussed earlier, the ITU-T Recommendation X.805 defines security-related architectural elements that when appropriately applied, can provide end-to-end network security (ITU 2003).

18.3.1.1.1 Academic-Industry Collaboration

Academic institutions created the current security enforcing technologies for cyberspace. Therefore, this Guide recommends that countries encourage industry and academic collaboration to avoid duplication of effort and leverage complementary capabilities. Countries should further create a cybersecurity R&D framework to define a process for transitioning from current Internet infrastructure to more resilient and secure platforms.

19 PILLAR 5 – INTERNATIONAL COOPERATION

We recommend that countries consider taking the following action.

19.1 ACTION 1: INTERNATIONAL CYBERSECURITY STRATEGY

The global nature of cyberspace and threats to its reliable functioning make international cooperation indispensable. The ITU regards a coordinated international response as the only answer and possible solution. In common with the US, countries may consider promulgating an international strategy for cyberspace to coordinate all activities under the five pillars. We also noted bi-lateral agreements[66] aimed at building capacity in all the priority areas. Nations may use a combination of international cooperation models.

[66] Example - US-UK Communiqué: https://update.cabinetoffice.gov.uk/sites/default/files/resources/CyberCommunique-Final.pdf

VIII. ASSURANCE AND MONITORING

20 ASSURANCE & MONITORING

Assurance constitutes activities to monitor cybersecurity programmes to ensure that they meet business requirements. In particular, cybersecurity programmes require realistic and achievable timescales to deliver on the Action on Priorities. Delayed cybersecurity programmes often run the risk of termination. Of course, what constitutes a realistic timescale will depend on the national priorities and needs. All that matters is delivery on timescales. Since cybersecurity is a global challenge, it is prudent to re-use the ISO/IEC 27001-based Plan-Do-Check-Act (PDCA) model. The model helps structure Information Security Management Systems (ISMSs). The PDCA model also reflects the OECD guidelines towards building a culture of security (OECD 2002). Therefore, the use of the PDCA model supports the GCA notably international cooperation.

20.1 PLAN-DO-CHECK-ACT (PDCA)

The PDCA model dovetails with national cybersecurity strategies because it focuses on specific requirements such as economic or national security. For example, countries may apply the model to ensure that security breaches do not disrupt or destroy essential services in named sectors. This Guide presents a modified PDCA model as follows:

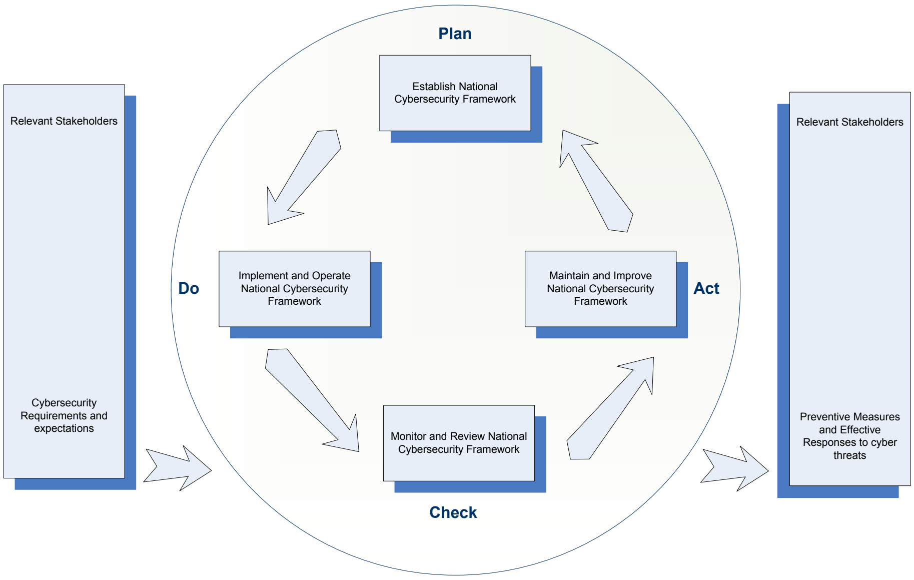

Plan
Establish National Cybersecurity Framework
Relevant Stakeholders
Cybersecurity Requirements and expectations
Do
Implement and Operate National Cybersecurity Framework
Act
Maintain and Improve National Cybersecurity Framework
Monitor and Review National Cybersecurity Framework
Check
Relevant Stakeholders
Preventive Measures and Effective Responses to cyber threats

Figure 31 – PDCA Model applied to National Cybersecurity Framework

20.1.1 Plan (Establish Framework)

The planning phase involves establishing overall objectives, processes and procedures relevant to managing risk and improving cybersecurity.

20.1.2 Do (Implement and Operate Framework)

This phase involves the implementation and operation of the Framework, policies, controls, processes and procedures. This phase requires realistic timescales and resources to deliver on the Action on Priorities. Countries should view this phase as a process not a mere event as the activities involved typically require time and patience. For example, training a talented and innovative pool of citizens to protect critical infrastructure requires patience. Additionally, the creation of national cyber incident response capacity is not a trivial task. Countries also require a lot of time to ensure that public and private sector organisations have the skills to participate in emergency response exercises. Exercises that are rushed give countries little knowledge about readiness for major cyber incidents. Therefore, it is better to set the sights low and do small-scale exercises first, learn the lessons from that and assess the problems and issues that arise before moving to national activities.

20.1.3 Check (Monitor and Review Framework)

It is important to assess and, where applicable, measure process performance against the Cybersecurity Framework, policies, objectives and practical experience and report the results to relevant stakeholders for review. This Guide discusses the principles for creating performance metrics in a separate section later.

20.1.4 Act (Maintain and Improve Framework)

This phase involves taking corrective and preventive actions, based on the results of the Cybersecurity Framework audit and management review or other relevant information, to achieve continual improvement of the Framework.

20.2 PERFORMANCE METRICS

As noted above, performance metrics may form part of the Check phase of the PDCA. Metrics allow all relevant stakeholders to determine the success of the cybersecurity programme and thus make informed purchasing and deployment decisions. We use the terms metrics, measures and measurements interchangeably.

20.2.1 EXAMPLE 1: ISO/IEC 27004 MEASUREMENTS

20.2.1.1 ISO/IEC 27001 Requirements

ISO/IEC 27001 requires organisations to:

- Undertake regular reviews of the effectiveness of the ISMS taking into account results from effectiveness measurement;
- Measure effectiveness of controls to verify that security requirements have been met
- Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measures are to be used to assess control effectiveness to produce comparable and reproducible results.

20.2.1.2 Factors Determining Measurements Requirements

The approach an organisation takes to measuring effectiveness of ISMS depends on:

- Information security risks that the organisation faces;
- Organisational size;
- Resources available; and
- Applicable legal, regulatory and contractual requirements.

Therefore, the resources allocated to security measurement activities should be in line with the factors above. Ideally, measurement activities should be part of business-as-usual activities to minimise additional requirements (ISO/IEC 2009).

20.2.1.3 ISO/IEC 27004

This International Standard guides the development and use of measurement to assess the effectiveness of an implemented ISMS and controls or groups of controls, as specified in ISO/IEC 27001. The standard covers:

- Policy;
- Information security risk management;
- Control objectives;
- Controls; and
- Processes and Procedures.

ISO/IEC 27004 helps determine whether each of the ISMS processes or controls require modification and improvement. The assessment activities result into an Information Security Measurement Programme. The Programme assists management in identifying and evaluating noncompliant and/or ineffective ISMS processes and controls. Additionally, management obtains guidance on priority actions linked with improvement or changing these processes and/or controls (ISO/IEC 2009). The Programme may further demonstrate ISO/IEC 27001 compliance and provide additional evidence for management review and information security risk management processes.

20.2.1.4 Information Security Measurement Programme

An Information Security Measurement Programme encourages organisations to provide reliable information to relevant stakeholders concerning information security risks and the status of the ISMS implemented to manage the risks. Effectively implemented, the Programme improves stakeholder confidence in the metrics and enables stakeholders to use the measures to effect continual improvement of security and the ISMS. The accumulated metrics allow comparison of progress towards meeting security goals as part of an organisation’s ISMS continual improvement process (ISO/IEC 2009).

20.2.1.5 ISO/IEC 27004 Recommendations

ISO/IEC 27004 provides recommendations on the activities below to help organisations fulfil measurement requirements specified in ISO/IEC 27001. The activities include:

- Developing measures (i.e. base measures, derived measures and indicators);
- Implementing and operating an Information Security Measurement Programme;
- Collecting and analysing data;
- Developing measurement results;
- Communicating developed measurement results to the relevant stakeholders;
- Using measurement results as contributing factors to ISMS-related decisions;
- Using measurement results to identify needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures; and
- Facilitating continual improvement of the Security Measurement Programme.

The size, complexity of an organisation and the importance of security to business affect the required measurements in terms of both numbers and frequency. For example, large organisations typically require multiple Security Measurement Programmes.

20.2.2 EXAMPLE 2: NIST PERFORMANCE METRICS

According to the US National Institute of Standards and Technology (NIST), security measures facilitate decision-making, boost performance and increase accountability through the collection, analysis, and reporting of relevant performance-related data. Thus, the measures link implementation, efficiency and effectiveness of security controls to success in achieving a cybersecurity mission (Chew *et al.* 2008).

20.2.2.1 NIST Guide Principles

NIST believes that the development and implementation of a measurement programme for information security should consider the following factors:

- Measures must yield quantifiable information (percentages, averages and numbers);
- Data that supports the measures needs to be readily obtainable;
- Only repeatable security processes should be considered for measurement; and
- Measures must be useful for tracking performance and directing resources.

NIST process aims to identify causes of poor performance and identify corrective action. Therefore, NIST focuses on readily obtainable measures notably:

- Security policy implementation;
- Security service deliver effectiveness/efficiency; and
- The business consequences of security incidents.

NIST advises that security practitioners may use many measurements simultaneously. Indeed, the focus of measures tends to shift as implemented security controls mature. The NIST performance metrics document is freely available on the Internet.

IX. ANNEXES

21 ANNEX 1: DRAFT NATIONAL CYBERSECURITY STRATEGY

21.1 INTRODUCTION

This section is a culmination of the work of the Guide. We present a reference model for national administrations seeking to elaborate new or improve existing National Strategies on Cybersecurity. We use the GCA as the multi-stakeholder framework for international cooperation. We align the GCA Pillars with the Ends-Ways-Means strategy process model. Therefore, we infuse the daily language of strategy into the GCA. We believe this is an important combination as it sets a stage for collaboration between cybersecurity strategists and a diverse group of stakeholders responsible for national security strategy.

21.2 EXECUTIVE SUMMARY

Objective: The Executive Summary previews the main points of the cybersecurity strategy template. Therefore, it contains enough information to allow a reader to understand the main cybersecurity issues and drivers discussed in detail in later sections. The section should have as little technical information as practical. The Executive Summary may contain the following sections.

21.3 STATEMENT OF PURPOSE

Objective: The preface outlines the purpose of the National Cybersecurity Strategy. Depending on the purpose of the "end", the preface should underline the role of ICTs in areas such as daily life, commerce, governance and national security. Since the template utilises the GCA as the guiding framework, the preface places national cybersecurity efforts in the context of other regional and international activities.

Sample Text:

<COUNTRY> requires reliable physical and information communication technologies (ICTs). The two types of infrastructure jointly support essential services in sectors such as communications, emergency services, energy, finance, food, government, health, transport and water. Therefore, to achieve our economic, security and democratic objectives, we require reliable physical and digital infrastructure. Physical assets increasingly depend upon the reliable functioning of the digital infrastructure or critical information infrastructure (CII) to deliver services and to conduct business. Consequently, significant disruption to CII could have an immediate and debilitating impact that reaches far beyond the ICT sector and affects the ability of a nation to perform its essential missions in multiple sectors. Therefore, critical information infrastructure protection (CIIP) is everyone's responsibility.

This document is "*The National Cybersecurity Strategy of <COUNTRY>*". It is one of the long-term measures for protecting our country against security threats, risks and challenges to national security. The Strategy addresses the "<COUNTRY> <national security strategy>. The purpose of this document is to create a coherent vision for keeping <COUNTRY> secure and prosperous by coordinating government, private sector, citizens and international cyberspace defence efforts.

This *National Cybersecurity Strategy* outlines a framework for organising and prioritising efforts to manage risks to our cyberspace or critical information infrastructure. To achieve the goals above, this Strategy significantly raises the profile of cybersecurity within our national and regional governments and defines clear roles and responsibilities.

Cognisant of the shared nature of cyber vulnerabilities, this Strategy also requires a public-private partnership to fix the potential vulnerability of private sector-owned critical infrastructures in banking, utilities and telecommunications sectors against cyber attacks.

In addition, we recognise that cybersecurity is a global challenge that demands truly international solutions. Therefore, we commit ourselves to joining regional and international partnerships creating solutions for addressing the cybersecurity challenge regardless of threat. We, therefore, present this *Strategy* in terms of the Pillars of the International Telecommunication Union's Global Cybersecurity Agenda (GCA). The GCA contains five strategic pillars and seven goals for building collaboration between relevant parties in the fight against cyber threats. We aim to help the GCA become the key framework for creating a secure and safe information society.

21.4 STRATEGIC CONTEXT

Objective: This section relies on the findings of the "Introduction" Chapter of this Guide. The section identifies context-specific cyber threats and vulnerabilities. A good section helps build a "Case for Action" statement.

Sample Text:

<COUNTRY> needs to building confidence and security in the use of ICTs because of the growing sophistication, frequency and gravity of cyber threats. Cyber threats are a concern because the disruption or destruction of critical information infrastructure could potentially have severe economic, public safety, social and national security impacts. Therefore, the lack of confidence that risks to information systems are under control undermines the Information Society.

Our cyberspace faces a range of threats. Cyber threats range from <EXAMPLES> espionage directed towards obtaining political intelligence to phishing to facilitate credit card fraud. In addition to Government information, espionage now targets the intellectual property of commercial enterprises in areas such as communication technologies, genetics, optics, electronics and genetics </EXAMPLES>. The design of the Internet infrastructure facilitates some of the cyber threats due to it borderless, anonymous and cross-border nature. Yet, the same insecure Internet serves as a basis for critical government and private sector services in <COUNTRY>.

We attach great value to the protection of <EXAMPLES>. Indeed, cyberspace is swiftly becoming critical to the control of <EXAMPLES> devices linked to the energy and transportation sectors such as electronic transformers and pipeline pumps. New smart grid technologies deliver intelligent monitoring, control, communication and self-healing technologies. However, smart meters are susceptible to unauthorised modification, distributed denial of service and disruption during patching </EXAMPLES>.

We are also concerned about <EXAMPLES> an increasing number of cyber attacks that resemble political conflict rather than traditional crime. For example, a growing number of cyber attacks aim to steal official government documents detailing negotiating positions. Disclosure of such details would seriously harm our national security and interests.

Worryingly, cyber espionage and other cybercrimes are very low cost activities. Attack tools and methodologies for activities such as phishing or malware distribution are freely available on the Internet even to amateurs. Besides, perpetrators face little risk of conviction due to incompatible legal frameworks and the lack of organisational structures to aid international cooperation, dialogue and coordination in dealing with cyber threats.

Silent surveillance enables hostile nations to map the structure and defences around key government and private sector infrastructures, plant backdoors, create and test attacks. During a crisis, enemies may launch attacks against our critical infrastructure to disrupt essential services and weaken public confidence. Indeed, we previously witnessed cyber incidents in which attackers targeted communication infrastructures leading to denial of access to governmental, news and banking websites. The incidents led to the closure of governmental, news, online banking and automatic teller machine services (ATMs) </EXAMPLES>.

21.5 CYBERSECURITY ENDS

Objective: This section outlines the objectives/ends/goals a country seeks to achieve. Whereas in this Guide, we have separated the ends – national economy, national security, social (promotion of values) and governance – in practice national cybersecurity strategy cover all at once. As we outlined earlier, this is because in practice all ends serve to promote national values and defend national interest

21.5.1.1 Example of a Generic End

The example below reflect a possible cybersecurity end.

- “Working collaboratively at home and abroad, we shall manage all major cyber risks that affect us directly whatever their origin and type thereby creating a safe, secure and resilient critical national information infrastructure for (e.g. our economy, national security, our society, our values etc).”

Sample Text:

<PURPOSE OF STRATEGY> This Strategy recognises the impact of cyber threats, risks and challenges to our national values and interests. The Strategy underlines the need for concerted effort to countering these fast evolving threats. This fully integrated approach leverages the resources of the Government, organisations across all sectors, individual private citizens and international partners in mitigating threats to our cyberspace. The Strategy defines the organisational structures required to address this embryonic risk to our prosperity and national security </PURPOSE OF STRATEGY>.

21.6 WAYS – PRIORITIES

Objective: In line with the GCA, this section focuses on the Strategic Pillars that typically help a country create coherent national and globally compatible programmes for protecting critical infrastructure against cyber threats.

This *National Cybersecurity Strategy* is aligned with our <*National Security or Economic Strategy* >*.* The Strategy is the basis for a coordinated national and globally compatible approach to protecting our critical infrastructure against cyber threats. In line with the Global Cybersecurity Agenda (GCA), our strategic Areas are:

- The development of a comprehensive set of national cybercrime legislation that is regionally and globally applicable and harmonised
- The implementation of measures to reduce vulnerabilities in software products through the deployment of accreditation schemes, protocols and standards;
- The definition of strategies for capacity building mechanisms to raise awareness, transfer know-how and boost cybersecurity on the national policy agenda; and
- The development of a unified national multi-stakeholder strategy for international cooperation, dialogue and coordination in dealing with cyber threats.

21.6.1 Cybersecurity Priorities

Objective: This section focuses on the concrete steps typically taken to implement the Actions and Initiatives identified under each Critical Cybersecurity Priority. The Priorities correspond to the GCA Pillars. Inevitably, the actions will depend on national conditions, local needs and cybersecurity priorities.

NOTE – We only articulate priorities under the first three pillars. As we demonstrated in the body of the Guide, countries should feel free to use examples we provided.

Our *National Cybersecurity Strategy* articulates three national priorities:

- Legal Measures;
- Technical and Procedural Measures; and
- Organisational Structures

The first priority focuses on strategies for the development of cybercrime legislation that is harmonised and applicable globally. The second priority deals with organisational structures and policies on cybercrime, watch, warning and incident response as well as the creation of a generic and universal digital identity system. Priority three, focuses on a national framework of security protocols, standards and software accreditation schemes.

The Strategy does not articulate priorities under the Capacity Building and International Cooperation pillars of the GCA as they cut across the three selected Priorities.

21.6.2 Priority 1: Legal Measures

Objective: This Priority deals with the establishment of laws to deter and prosecute cybercrime. Inevitably, the actions will depend on national conditions and local needs.

<*PURPOSE*> The establishment and modernisation of criminal law, procedures, and policy to prevent, deter, respond to, and prosecute cybercrime is an integral component

of the *National Cybersecurity Strategy of <COUNTRY>*. Since cybersecurity is a global challenge, the lack of harmonised national and regional cybercrime legislation weakens *<COUNTRY's>* and worldwide ability to detect, prosecute and deter cybercrime. The *National Cybersecurity Strategy* identifies the actions below as necessary for creating suitable cybercrime legal measures *</PURPOSE>*:

21.6.2.1 Action 1: Cybercrime Legislation

Objective: This Action involves creation of laws that are interoperable and applicable globally. For example, a country may consider aligning national laws with the ITU Toolkit for Cybercrime Legislation. Inevitably, the required legal authorities will depend on national conditions, existing capacities and cybersecurity priorities.

Our cybercrime legislation shall be harmonised with global conventions. Therefore, we shall align our cybercrime legislation with the ITU Toolkit for Cybercrime Legislation. The alignment of our cybercrime legislation with the ITU Toolkit for Cybercrime helps international cooperation and addresses jurisdictional and evidentiary issues. Additionally, internationally harmonised legislation strengthens cybersecurity, as it helps our country build capacity for preventing, deterring and prosecuting cybercrime.

21.6.2.2 Action 2: Government Legal Authority

Objective: This Action aims to ensure that governments have sufficient legal authority to secure cyberspace in public interest.

The <APPROPRIATE LAW> governs cyberspace defence activities in <COUNTRY>. The <APPROPRIATE LAW>:

- Provides the <APPROPRIATE HEAD OF GOVERNMENT i.e. President or Prime Minister> the requisite legal authority to create cybersecurity organisation structures including the <Example: National Cybersecurity Agency> etc;
- Defines the legal basis for creating a national CIRT. For example, the Act defines the powers to shutdown a critical infrastructure if at risk of a cyber attack;
- Provides the basis for promoting cybersecurity skills, training and awareness;
- Defines the legal and operational basis for an integrated and fully coordinated public-private sector partnership on cybersecurity;
- Fosters innovation in cybersecurity to help develop long-term solutions; and
- Grants the government powers to participate in international cooperation, dialogue and coordination activities focuses on cybersecurity such as mutual assistance.

21.6.3 Priority 2: Technical and Procedural Measures

Objective: This Priority focuses on the facilitation of communication, information exchange and recognition of digital credentials across jurisdictions. The actions coincide with the section of the Guide dealing with this GCA Pillar.

<PURPOSE> The This Priority addresses the need to create organisational structures at national and regional levels to facilitate communication, information exchange and the recognition of digital credentials across jurisdictions. The structures would help create a generic and universal digital identity system and the necessary organisational structures to recognise digital credentials across jurisdictions through the following actions </PURPOSE>.

21.6.3.1 Action 1: National Cybersecurity Framework

Objective: This Action aims to create a Framework that defines mandatory security standards and offers guidance on issues such as risk management, compliance and assurance. As ever, the contents depend on the local conditions and priorities.

The <COUNTRY> <APPROPRIATE> Framework outlines minimum-security measures that stakeholders must abide by to claim compliance with national cybersecurity requirements. The Framework contains core security values and minimum standards that apply to a wide range of stakeholders. Stakeholders select the applicable standards based on their risk profile and information protection needs. The stakeholders may use an internal audit or external auditor to demonstrate compliance with the minimum-security standards to a central organisation. However, the Framework does not provide detailed technical instructions on specific ICT systems.

Cognisant that cybersecurity is a global challenge, this Strategy adopts the ISO/IEC 27000 Series of standards. The *National Cybersecurity Strategy* identifies the following Policy Goals as vital components of the National Cybersecurity Framework:

- Governance and Risk Management
- Information Security and Assurance
- Protective Marking and Asset Management
- Staff Vetting and Clearance
- Physical and Environmental Security

We shall work with international partners such as ITU and IMPACT to ensure that the selected Cybersecurity Framework Policy goals respond properly to the five GCA Pillars. The cybersecurity framework undergoes an annual assess its effectiveness.

21.6.3.2 Action 2: Secure Government Infrastructure

Objective: This Action deals with spreading awareness of relevant risks, preventive measures and effective responses to government Departments and Agencies. The goal is to ensure that the Government leads by example on cybersecurity.

The Government of <COUNTRY> owns and operates only a minority of critical information infrastructure. However, <COUNTRY> attributes considerable importance to the protection of critical information infrastructure. Therefore, the Government will lead by example in cyberspace security. For example, the Government's procurement process will mandate the inclusion of security clauses in service contracts to encourage development of secure cyberspace technologies. The *National Cybersecurity Strategy* identifies the following actions as vital for securing government's cyberspace:

- Create and enforce a staff vetting and clearance scheme;
- Create and enforce a formal information or data classification for sensitive data;
- Create and enforce a cybersecurity risk management process across government ministries and agencies;
- Define and enforce a robust government Authentication Framework;
- Improve security in government outsourcing and procurement through vetting of suppliers, incorporation and enforcement of security clauses in contracts;
- Make cybersecurity a national, local and regional government accountability;
- Create a vulnerability management process for all government cyber systems;
- Secure government local area networks.

21.6.3.3 Action 3: Critical Information Infrastructure Protection

Objective: This Action focuses on defining a process for tracking and fixing vulnerabilities; improving attack attribution and prevention capabilities.

<PURPOSE> Vulnerabilities are weaknesses that allow a threat or attacker to breach a system's confidentiality, integrity and availability defences. Most of cyber attacks result from poor technical designs or the exploitation of known but unfixed vulnerabilities. The impact of the exploitation of a vulnerability depends on the value and criticality of information. Critical information infrastructures inevitably store valuable information.

The *National Cybersecurity Strategy* identifies the following major actions and initiatives to reduce threats and related vulnerabilities in <COUNTRY>:

- Create a process for national vulnerability assessments to help understand the potential consequences of threats and vulnerabilities;
- Designate important systems as critical information infrastructure and enforce an accreditation regime around them. For example, no system will connect to critical infrastructure without a penetration test and other assurance activities;
- Enhance law enforcement capabilities in the investigation, prevention and prosecution of cybercrimes;
- Require the use of evaluated software products;
- Prioritise national cybersecurity research and development activities;

- Assess and secure emerging systems; and
- Participate in international efforts to improve the security of Internet protocols and routing technologies.

21.6.4 Priority 3: Organisational Structures

Objective: This Priority focuses on the organisational structures required to detect and respond to cyber threats.

This Priority Area requires the building of organisational structures and strategies to help prevent, detect and respond to attacks against critical infrastructure. The *National Cybersecurity Strategy* identifies the actions below as essential to creating appropriate national and regional organisational structures and policies on cybercrime:

21.6.4.1 Action 1: Government's Cybersecurity Role

Objective: The Action emphasises Governments' responsibility to address cyber threats systematically in collaboration with relevant stakeholders.

Cybersecurity is everyone's responsibility because countermeasures only work well if all relevant stakeholders play their part. The stakeholders include government, business, infrastructure owners and users. Collaboration is vital because neither government nor the private sector can independently control and protect information infrastructure.

Ultimately, however, the Government of <COUNTRY> has overall responsibility for securing the infrastructure in public interest. National governments play a central role in cybersecurity because they are responsible for facilitating commerce and protecting the lives and property of their citizens.

To improve cybersecurity in <COUNTRY>, it is vital that the Government puts in place appropriate national structures to protect its own infrastructure and all assets required to deliver essential services to the public. The national, regional and globally compatible organisational structures aim to protect classified data and networks against cyber attacks. The Government is also responsible for communicating national priorities to the private sector to help ensure that critical infrastructure under private hands in sectors such as banking, transport and telecommunications receives sufficient protection.

To address the cybersecurity challenge, the <APPROPRIATE Head of Government> of <COUNTRY> has appointed a senior aide as the National Cybersecurity Coordinator. The official has established a cross-government programme to address the priority areas of this Strategy. The official provides strategic leadership and ensures the coherence of cybersecurity activities across government. The role cuts across government agencies and the official reports to the <RELEVANT NATIONAL BODIES e.g. National Security Council, National Economic Council>. The Coordinator has direct access to the APPROPRIATE Head of Government> as well as sufficient staff and financial resources to coordinate inter-government activities at a strategic level.

21.6.4.2 Action 2: National Cybersecurity Agency

Objective: The Action deals with the creation of a multi-agency body should serve as a focal point for activities dealing with protecting a nation's cyberspace against threats.

The National Cybersecurity Agency is the focal point for coordinating efforts to protect our cyberspace. This multi-agency body unites operational cybersecurity efforts of government institutions and leads collaboration with industry. Public-private partnership coordination is critical to protecting our critical infrastructure because it enhances information sharing and cooperation on cyber threat identification, incident response and recovery. The *Cybersecurity Strategy* mandates the Agency to perform the roles below:

- Developing a comprehensive national plan for securing critical infrastructure and services whether in government or private sector;
- Providing national major incident response capacity in an event of significant attacks on critical infrastructure;
- Providing government and private sector organisations strategic advice and processes for managing cybersecurity Programmes;
- Providing integrated security advice (combining information, personnel and physical) to the government agencies and businesses owning or operating critical information infrastructure to reduce its vulnerability to cyber and other threats;
- Acting as the National Technical Authority for Information Assurance for private sector organisations and government agencies in all aspects of cybersecurity;
- Working with other government agencies including intelligence agencies to review threat and vulnerability information and distribute advice on the countermeasures to regional and local governmental organisations, private sector, academia and the general public;
- Engage in international schemes such as the International Multilateral Partnership Against Cyber Threats (IMPACT) for alerts, early warning and cooperation;
- Perform and fund research and development with other agencies to create a new generation of secure cyber technologies.

An annual review assesses the effectiveness of the Agency's cybersecurity activities.

21.6.4.3 Action 3: National Incident Management Capacity

Objective: The Action deals with the need to create a national point-of-contact for 24x7 cyberspace analysis, information sharing, major incident response etc.

Timely identification, communication and recovery from major cybersecurity events and weaknesses affecting critical information infrastructure can often mitigate the damage resulting from malicious cyberspace activity. Best practice indicates that these efforts are most effective at national level because they provide wider participation in analysis, warning, information gathering, vulnerability reduction, mitigation and recovery. Inevitably, the government needs to work with the private sector to coordinate a national response because private firms own the infrastructure and often have better skills. The government creates legal and regulatory incentives to encourage critical infrastructure owners and operators to ensure that their systems are resilient to attacks. This Strategy identifies the following actions regarding cyber incident response:

- Build National Computer Incident Response Team (N-CIRT) at the National Cybersecurity Agency;
- Establish a public-private framework for responding to major cyber incidents;
- Encourage development of business continuity and disaster recovery capacity;
- Develop strategic and tactical cyber attack and vulnerability assessment capacity;
- Encourage the development of private sector capacity to share status information about the health of cyberspace;
- Coordinate processes for voluntary participation in the development of national public-private continuity and contingency plans;
- Create a Cyber Warning and Information Network at Cybersecurity Agency; and
- Develop mechanism to share information about cyber attacks, threats and vulnerabilities with the public and non-governmental bodies locally and globally.

21.6.4.4 Action 4: Public-Private Partnerships

Objective: The Action focuses on the need to raise awareness about cyber threats and the role all relevant stakeholders must play to secure their part of cyberspace.

The commercial sector owns and operates most of the critical infrastructure that <COUNTRY> relies on at home and abroad. Clearly, the Government alone cannot secure cyberspace since it does not own or operate the infrastructure. Therefore, the Government of <COUNTRY> has formed meaningful partnership with the private sector on cybersecurity. The *National Cybersecurity Strategy* requires the Government of <COUNTRY> and its agents to consult the private sector in the development, implementation and maintenance of regulation, cybersecurity initiatives and policies. Cooperative relationships with the private sector are vital because they:

- Facilitate the exchange information on the development of new legislation and regulation between stakeholders;
- Enable collaborative work and sharing of training courses that could help alleviate the severe shortage of skilled cybersecurity professionals; and
- Enable real time exchange of information about cyber threats and vulnerabilities. The communication channel is valuable for the national CIRT as the exchange complements the stretched national incident detection and warning resources

With private sector input, the Government shall also develop a coordinated national strategy for participating in major international discussions that shape policy in areas such as territorial jurisdiction, sovereign responsibility and the use of cyberspace for war.

Additionally, the Cybersecurity Coordinator or an equally empowered party works with government departments and agencies, the private sector and academia to formulate and coordinate <COUNTRY’s> international cybersecurity positions. Thereafter, the ministries of Foreign Affairs should work on improving international cooperation.

21.6.4.5 Action 5: Cybersecurity Skills and Training

Objective: The Action focuses on the creation of programmes to increase the cadre of cybersecurity professionals in Managerial, Technical and Information Assurance areas.

This Action requires the initiation of a programme to train a cadre of citizens to secure information flows. This Action focuses on the training of professionals not creating general awareness. This *Cybersecurity Strategy* identifies the following major activities:

- Adopt a national Cybersecurity Skills Framework;
- Create a continuum of cybersecurity job descriptions;
- Identify commercially available cybersecurity certifications;
- Deliver or manage commercial delivery of training or certification examinations;
- Periodically measure Cybersecurity skills and training levels;
- Invest in mainstream cybersecurity education and research;
- Build cybersecurity capacity of national companies; and
- Work with global partners such as IMPACT to coordinate cybersecurity training.

21.6.4.6 Action 6: National Culture of Cybersecurity

Objective: The Action focuses on the need to raise awareness about cyber threats and the role all relevant stakeholders must play to secure their part of cyberspace.

Many cyber threats materialise due to insecure user activities. The users could be end users or system administrators. A lack of awareness coupled with a general lack of skilled cybersecurity professionals increases the likelihood that attackers would trick users into performing insecure activities. On the contrary, user awareness helps create a cybersecurity culture that in turn reduces the likelihood and impact of cyber attacks. This *Cybersecurity Strategy* identifies the following major activities:

- Promotion of a national awareness programme to empower end users – at home or general workforce – to secure their own cyberspace-linked systems;
- Implementation of a cybersecurity awareness programme for government systems that contain classified data;
- Encouraging cybersecurity culture development in business enterprises;
- Adding cybersecurity awareness to the national education curriculum as a way of spreading knowledge to pupils and their relatives;
- Engaging civil society in outreach to children and individual users;
- Promotion of private-sector support for professional cybersecurity certifications;
- Work with global partners such as IMPACT to improve cyber threat awareness.

21.7 MEANS – ACTIONS

Objective: These are the technical, organisational and human resources devoted or required to execute the national cybersecurity strategy.

For security reasons, strategies typically do not contain details of resources deployed. The resources are instead part of classified implementation plans. However, some countries publish minimum standards especially the procedural measures.

22 ANNEX 2: TECHNICAL SOLUTIONS

The table below outlines common cybersecurity technologies.

SECURITY GOAL	TECHNOLOGY	ROLE
Access Control		
Boundary or Perimeter Protection	Firewalls	Aim to prevent unauthorised access to or from a private network.
	Content Management	Monitor web, messaging and other traffic for inappropriate content such as spam, banned file types and sensitive or classified information.
Authentication	Biometrics	Biometric systems rely on human body parts such as fingerprints, iris and voice to identify authorised users
	Smart tokens	Devices such as smart cards with integrated circuit chips (ICC) to store and process authentication details
Authorisation	User Rights and Privileges	Systems that rely on organisational rules and/or roles to manage access
System Integrity		
	Antivirus and anti-spyware	A collection of applications that fight malicious software (malware) such as viruses, worms, Trojan Horses etc
	Integrity Checkers	Applications such as Tripwire that monitor and/or report on changes to critical information assets
Cryptography		
	Digital Certificates	Rely on Public Key Infrastructure (PKI) to deliver services such as confidentiality, authentication, integrity and non-repudiation
	Virtual Private Networks	Enable segregation of a physical network in several ‘virtual’ networks
Audit and Monitoring		
	Intrusion Detection Systems (IDS)	Detect inappropriate, incorrect or abnormal activity on a network

SECURITY GOAL	TECHNOLOGY	ROLE
	Intrusion Prevention Systems (IPS)	Use IDS data to build intelligence to detect and prevent cyber attacks
	Security Events Correlation Tools	Monitor, record, categorise and alert about abnormal events on network
	Computer Forensics tools	Identify, preserve and disseminate computer-based evidence
Configuration Management and Assurance		
	Policy Enforcement Applications	Systems that allow centralised monitoring and enforcement of an organisation's security policies
	Network Management	Solutions for the control and monitoring of network issues such as security, capacity and performance
	Continuity of Operations tools	Backup systems that helps maintain operations after a failure or disaster
	Scanners	Tools for identifying, analysing and reporting on security vulnerabilities
	Patch Management	Tools for acquiring, testing and deploying updates or bug fixes

Figure 32 – Cybersecurity Technologies and their roles

Next, we discuss the technologies identified in Figure 32 and cybersecurity role.

22.1.1.1 Access Control Technologies

Access Control technologies prevent unauthorised parties from accessing, viewing or modifying sensitive information. Common access control technologies fall into three broad categories:

22.1.1.1.1 Boundary Protection Technologies

Boundary technologies enforce the "Zoning principle" discussed early by creating logical or physical boundaries between protected information and untrusted users and networks. Firewalls are the most prominent boundary technology. Network or host-based firewalls help prevent the accidental or deliberate leakage of sensitive information. Content management systems also protect boundaries. The content-checking software typically monitors web, messaging and other traffic for inappropriate content such as spam, banned file types and sensitive or classified information.

22.1.1.1.2 Authentication Technologies

Authentication technologies tie an individual to an identity. Identification is through three means namely: *what someone knows* (e.g. password), *what someone has* (e.g. smart card or token) and *what someone is* (e.g. biometric data such as voice). Secure systems often combine two methods to create “two-factor” authentication.

22.1.1.1.3 Authorisation Technologies

After authentication, authorisation systems take over to determine whether to grant or deny a user access to particular information or resources. Authorisation modules enforce principles such as least privilege, separation of duties and legitimate use. Usernames and passwords are the most popular authentication techniques.

22.1.1.1.4 System Integrity

As identified in Policy Goal 1 of the Cybersecurity Framework, countries should develop and implement policies to manage the malicious code scourge. The following technical solutions typically support the implementation of malicious code policy:

22.1.1.1.5 Antivirus and Anti-spyware systems

These technologies protect systems and data therein against unauthorised modification, destruction and corruption by malicious software. The malicious software (malware) includes viruses, Trojan horses, worms, spyware, adware and worms. Antivirus and integrity checkers help maintain system integrity by identifying, blocking and eliminating malware. Antivirus or anti-spyware software can reside on computers or gateways to detect incoming malware, eliminate resident malware and repair damaged files.

22.1.1.1.6 Integrity Checkers

Integrity checkers also help fight unauthorised tampering with information and assets. Integrity checkers are security tools that monitor and alert on specific file changes on a range of systems. Integrity checkers create a base integrity file and routinely compare that snapshot file with current system files to detect unauthorised changes.

22.1.1.2 Cryptography

22.1.1.2.1 Digital Signatures and Certificates

Cryptography is the basis for transactional security through support for confidentiality, integrity, authentication and non-repudiation services. Therefore, cryptographic solutions are vital for protecting sensitive data both at rest (on computer or storage) and during transit. Large cyber systems rely on Public Key Infrastructure (PKI) to deliver the above named security services due to its low infrastructure overload. The older crypto systems rely on shared secrets (symmetric keys) that are impractical in real time transactions. The ITU-T X.509 Recommendation is the definitive PKI standard (ITU 2005).

22.1.1.2.2 Virtual Private Network (VPN)

VPN technology is vital in cybersecurity as it securely extends a private network over insecure public networks such as the Internet. VPNs allow government departments to extend their private network to several physical locations without requiring expensive leased lines. VPNs use end-to-end cryptographic protocols to secure communications over public networks. VPN protocols include IPSec, Secure Sockets Layer (SSL) or Transport Layer Security (TLS[67]) and Point-to-Point Tunnelling Protocol (PPTP).

22.1.1.3 Audit and Monitoring

Audit and monitoring systems record user and system activities to support monitoring, incident response and investigations. The technologies help administrators to evaluate the security status of devices, perform investigations during and after attacks and identify ongoing attacks. Audit and monitoring tools include IDS, IPS, Security Event Correlation Tools and Computer Forensic tools.

22.1.1.3.1 Intrusion Detection System (IDS)

An ID detects inappropriate or irregular activities that have potential to affect a system's confidentiality, integrity and availability status. IDSs are Network or Host-based:

22.1.1.3.1.1 Network Intrusion Detection System (NIDS)

NIDS monitor network traffic with an aim of detecting potentially malicious activity such as denial of service attacks, port scans or attempts to infiltrate computers by monitoring network traffic. NIDS can monitor traffic as it enters or leaves the network. NIDSs inspect network packets to identify anomalies such as unusual requests patterns or unexpected protocols. NIDS monitor traffic by comparing it with a signature file that provides a list of potentially malicious activities. NIDS normally obtain the original signature file from a vendor. It is critical to keep the signature file updated as this helps keep track of new malicious activities or attacks. Newer NIDSs use behaviour-based threat detection methods instead of signatures. The behaviour-based threat detection technology makes it easier to identify the so-called zero-day attacks for which no signatures exist.

22.1.1.3.1.2 Host-based Intrusion Detection System (HIDS)

HIDS do not monitor networks. Instead, HIDS focus on potentially malicious dynamic activity on specific components of a computer system. HIDS focus on the state of system components, for example, stored data, system logs and configuration files and check whether they appear as expected. HIDS monitor the state of components on a live system and compare the results to either the expected values for static objects or pre-determined rules such as excessive variation in size, non-scheduled jobs or attempted deletion of read-only files. The HIDS comparison database requires strong protection to prevent attackers modifying entries and enabling their attacks to go undetected.

[67] TLS and its predecessor SSL encrypt segments of network connections at the Transport Layer end-to-end.

22.1.1.3.2 Intrusion Prevention System (IPS)

An IPS is an active response IDS. Rather than merely raising an alert to administrators as its passive counterparts, an IPS monitors network and/or system activities for malicious or unwanted behaviour and can react, in real-time, to block or prevent intrusions. IPSs drop offending packets on detecting a malicious activity but allow all other traffic to pass through. Modern IPSs have firewall, intrusion detection, antivirus and vulnerability assessment capabilities. Indeed, IPS may act as intelligent firewalls as they can base access control decisions on content rather than IP address or ports only as older firewalls. IPSs use destination ports as their signature format. In common with IDSs, IPSs are also Host-based IPS (HIPS) or Network-based IPS (NIPS).

22.1.1.3.3 Security Event Correlation Tools

Correlation tools collect logs from Security Enforcing Functions in operating systems, firewalls, applications, IDSs, IPSs and network devices. Thereafter, the correlation tools analyse the logs in real time, establish whether an attack has occurred, respond or alert an incident response module or team. Correlation tools may respond to attacks passively or actively. A tool takes no action to stop the attack under passive mode. On the contrary, an active response involves automated action to mitigate the risk, for example, by blocking the attack through firewall interfaces.

22.1.1.3.4 Computer Forensics Tools

Computer forensics tools automate the evidence handling processes. The forensics tools can identify data modification, file deletions, link a computer crime to an offender and individuate attack methods. The effective use of computer forensics tools should start from the development of policies and procedures to ensure that the collection and maintenance of electronic evidence is in accordance with all relevant legislation.

22.1.1.4 Configuration Management and Assurance Tools

Configuration and assurance tools help administrators to create, view or modify security settings on computer systems and devices as well as confirm whether the implemented settings are correct. Before purchasing the configuration management tools, countries should define controls around the updating or modifications of software to prevent unauthorised and uncontrolled updating of critical system software. The most common configuration and management assurance technologies include the following:

22.1.1.4.1 Policy Enforcement Tools

These are tools for defining and enforcing compliance with set rules and configurations such as password policy and maintenance of server and desktop builds. For example, in Windows Operating Systems, Group Policy (GP) controls the working environment of user and computer accounts. GP provides centralised management and configuration of operating systems, applications and user settings in an Active Directory environment.

22.1.1.4.2 Network Management Tools

These tools maintain networks and systems. For example, many network management tools utilise Simple Network Management Protocol (SNMP) to monitor network-attached devices and flag problems to system administrators. SNMP provides information on issues such as memory usage and the number of running processes. SNMP also allows active management tasks such as modifying and applying new configurations.

22.1.1.4.3 Continuity of Operations Tools

Backup tools help restore system functionality and data in the event of a computer failure due to power outage or cyberattack as well as during a natural disaster. Continuity of operations tools include high-availability systems, journaling file systems and Redundant Array of Independent Disk (RAID). However, the Guide stress that continuity tools should only be acquired after risk assessment and the adoption of business continuity policies.

22.1.1.4.4 Scanners

Vulnerability scanners help conduct network reconnaissance to identify gaps in system configuration that may enable an unauthorised intrusion. Relevant stakeholders should develop a formal process to require periodic formal IT Health Checks (ITHC).

22.1.1.4.4.1 Patch management

Cyber attacks often thrive on un-patched systems. Therefore, this Guide recommends the acquisition of patch management tools to help administrators to test and apply updates and bug fixes to firmware and software applications

23 REFERENCES

Alperovitch, D. (2011) "Revealed: Operation Shady RAT" *McAfee Corporation* Santa Clara, CA.

CCRA (2009) *Common Criteria for Information Technology Security Evaluation,* Common Criteria Recognition Agreement (CCRA), CCMB-2009-07-001.

Chew, E.*, et al.* (2008) *Performance Measurement Guide for Information Security,* National Institute of Standards and Technology (NIST), Gaithersburg, Maryland.

Drew, D. M. and D. M. Snow (2006) *Making Twenty-First-Century Strategy: An Introduction to Modern National Security Processes and Problems,* Air University Press, Maxwell AFB, Alabama.

EU (2010) *MEMO/10/463: Proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA,* European Union (EU), Brussels.

GAO (2004) *Information Security: Technologies to Secure Federal Systems,* United States General Accounting Office, Report to Congressional Requesters, Washington, DC.

IETF (Ed.) (1997) *RFC 2196: Site Security Handbook,* Internet Engineering Task Force (IETF).

IETF (Ed.) (2007) *RFC 4949: Internet Security Glossary, Version 2,* Internet Engineering Task Force (IETF).

ISO (2009) *ISO 31000: Risk Management - Principles and Guidelines,* International Organization for Standardization (ISO), Geneva, Switzerland.

ISO/IEC (2008) *ISO/IEC 27005: Information Technology — Security Techniques — Information Security Risk Management,* International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), Geneva, Switzerland.

ISO/IEC (2009) *ISO/IEC 27004: Information technology — Security techniques — Information Security Management — Measurement,* International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), Geneva, Switzerland.

ITU (2003) "ITU-T X.805 - Security Architecture for Systems Providing End-to-End Communications". in *Series X: Data Networks and Open System Communications - Security,* Geneva, Switzerland, Telecommunication Standardization Sector of ITU (ITU-T).

ITU (2004) "ITU-T E.409 - Incident organization and security incident handling: Guidelines for Telecommunication Organizations". in *Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors - Network management – International Network Management,* Geneva, Switzerland, Telecommunication Standardization Sector of ITU (ITU-T).

ITU (2005) *ITU-T Recommendation X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks,* International Telecommunication Union, Geneva, Switzerland.

ITU (2008) "WTSA-08 Resolution 58 - Encourage the creation of national Computer Incident Response Teams, particularly for developing countries". in *World Telecommunication Standardization Assembly,* Johannesburg, Telecommunication Standardization Sector of ITU (ITU-T).

ITU (2008a) *ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts,* ITU-D Secretariat, Geneva.

ITU (2008c) "ITU-T X.1055 - Risk Management and Risk Profile Guidelines for Telecommunications Organizations". in *Series X: Data Networks, Open System Communications and Security - Telecommunication Security,* Geneva, Switzerland, Telecommunication Standardization Sector of ITU (ITU-T).

ITU (2008d) "ITU-T X.1205 - Overview of Cybersecurity". in *Series X: Data Networks, Open System Communications and Security - Telecommunication Security,* Geneva, Switzerland, Telecommunication Standardization Sector of ITU (ITU-T).

ITU (2009c) *Understanding Cybercrime: A Guide for Developing Countries,* ICT Applications and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Development Sector, Geneva, Switzerland.

ITU (2009f) *Security in Telecommunications and Information Technology: An Overview of Issues and the Deployment of Existing ITU-T Recommendations for Secure Telecommunications,* Telecommunication Standardization Sector of ITU (ITU-T), Geneva, Switzerland.

ITU (2010f) "Resolution 174 (WGPL/1) - ITU's role with regard to International Public Policy Issues Relating to the Risk of Illicit Use of Information and Communication Technologies". in *ITU Plenipotentiary Conference 2010 (PP-10), 4-22 October 2010,* Guadalajara, Mexico, International Telecommunication Union (ITU).

Lipinski, D.*, et al.* (2010) "H.R. 4061: Cybersecurity Enhancement Act of 2010". in *111th Congress 2009-2010,* Washington, DC, United States House of Representatives.

OECD (2002) "OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security" *Organisation for Economic Co-operation and Development (OECD)* Paris, France.

Okot-Uma, R. W. (2000) *Electronic Governance: Re-Inventing Good Governance,* Commonwealth Secretariat, London.

Parker, D. B. (1997) "The strategic value of information security in business", *Computers & Security,* **16 (7),** pp. 572-582.

Powner, D. (2009) "National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture". in *Testimony Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives,* Washington, United States Government Accounting Office (GAO).

Rockefeller, J., E. Bayh, B. Nelson and O. Snowe (2009) "S. 773: Cybersecurity Act of 2009". in *111th Congress 2009-2010,* Washington, DC, United States Senate Committee on Commerce, Science & Transportation.

Shanmugam, K. (2009) "Cooperating for Infocomm Security: Singapore Infocomm Technology Security Authority (or SITSA)". in *The 18th Governmentware Seminar,* The Suntec Singapore International Convention and Exhibition Centre, Minister for Law and 2nd Minister for Home Affairs.

Sinks, M. A. (2008) *Cyber Warfare and International Law,* Air University, Alabama.

Sklenka, S. D. (2007) *Strategy, National Interests, And Means to An End,* Strategic Studies Institute, U.S. Army War College, Carlisle, PA.

Toure, H. (2010) "Securing Cyberspace". in *Annual Meeting 2010 of the World Economic Forum,* Davos, Switzerland, World Economic Forum.

Toure, H. (2010c) "Building Confidence and Security in the Use of ICTs". in *Interactive Facilitation Meeting on WSIS Action Line C5: Cybersecurity (12 May 2010) - Speech by ITU Secretary-General, Dr. Hamadoun I. Toure,* Geneva, Switzerland, International Telecommunication Union (ITU).

UK (2008) *HMG IA Standard No. 2: Risk Management & Accreditation of Information Systems,* Communications-Electronics Security Group (CESG), London.

UK (2009) *Cyber Security Strategy of the United Kingdom - Safety, Security and Resilience in Cyber Space,* Cabinet Office, London.

UN (2010) "A/RES/64/211: Creation of a Global Culture of Cybersecurity and taking stock of national efforts to protect Critical Information Infrastructures". in *Sixty-Fourth Session of the United Nations (UN) General Assembly - Resolution adopted by the General Assembly,* New York, United Nations.

Printed in Switzerland
Geneva, 2012

Photo credit: © Shutterstock