"Cybersecurity Capacity Building & International Collaboration "

Dr David E. Probert

Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

ITU AND CITEL REGIONAL CYBERSECURITY CAPACITY BUILDING WORKSHOP FOR THE AMERICAS
Monday 1st November 2010, Salta City, Argentina

International Telecommunication Union
Committed to connecting the world

Capacity Building & International Collaboration

1–Aim:Capacity Development	**2 – Cyber Skill Requirements**	**3 – Critical Sector Cyber Skills**
4– Cyber Culture & Awareness	**5 –ITU Academy & Workshops**	**6 – ITU Standards & Toolkits**
7 – IMPACT Cyber Training	**8 – International Partnerships**	**9 – Next Suggested Steps**

ITU: Cybersecurity Capacity Development

- Call for Action: Migration from 20thC Physical Security to 21stC Cyber Security for all National ICT Networks, & across Critical Service Sectors
- Global Shortage: Practically ALL countries & regions, including UK and USA, have significant shortage of qualified cybersecurity professionals
- Cybercrime : The growth in cybercrime & cyber terrorism means that countries need to quickly build capacity to defend critical services
- National CIRTs : The Computer Incident Response Teams can be focused upon capacity building across the Key Cybersecurity Actions
- Partnerships: Global organisations such as the ITU are working intensively to develop & communicate cybersecurity training resources, as well as guidelines and standards for "best practice"

…..In this presentation I review the major skill requirements, professional qualifications, the role of CIRTs & supporting ITU Training Programmes

National Cybersecurity: Cyber Skills Strategy

- **National CIRT:** Each country needs to build cybersecurity skills within the context of its national cybersecurity plan, led by the National CIRT

- **Stakeholders:** The skills development programme will be an on-going multi-year programme and should be undertaken by the government in partnership with key public & private security stakeholders including:

  - Academic & Research Institutions such as major Universities & Colleges
  - Awareness Programmes with High Schools through games & competitions such as the UK and US Government "Cyber Challenge" Programmes
  - ICT Market Sector, including the major Telecomms, ISP & Mobile Players
  - Critical Service Sector Businesses including Energy, Financial & Transportation

- **Support:** The Government should provide some financial support to "kick-start" the programme which should initially run for 3 to 5 years, with the aim to train-up professionally certified cybersecurity specialists

Capacity Building & International Collaboration

1–Aim:Capacity Development	2 – Cyber Skill Requirements	3 – Critical Sector Cyber Skills
4– Cyber Culture & Awareness	5 –ITU Academy & Workshops	6 – ITU Standards & Toolkits
7 – IMPACT Cyber Training	8 – International Partnerships	9 – Next Suggested Steps

Cybersecurity Skills Needs

Management	Information Assurance	Technical
• 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 • Data ownership	• 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 (IT defences deployment) • Security Design Principles e.g. zoning • Resilient Infrastructure • Data Protection/ System administration • Cryptographic and Applied Crypto Skills • Data custodianship • Operational Security • Incident Management

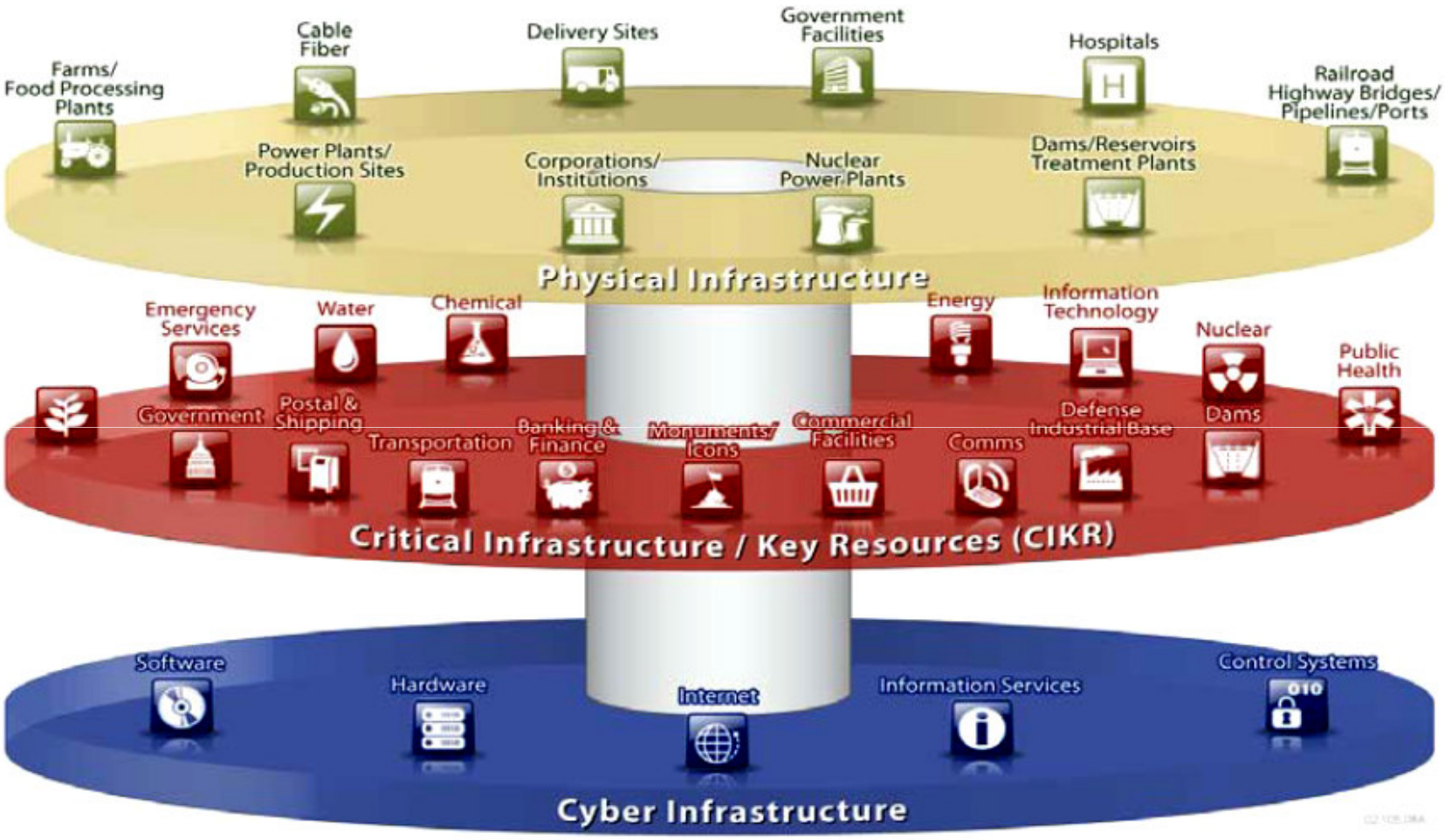
Professional Cybersecurity Roles

1) Chief Information Security Officer (CSO/CISO)
2) Systems Operations & Maintenance Personnel
3) Network Security Specialists
4) Digital Forensics & Incident Response Analysts
5) Information Security Assessor
6) Information Systems Security Officer
7) Security Architect
8) Vulnerability Analyst
9) Information Security Systems & Software Development

Capacity Building & International Collaboration

1–Aim:Capacity Development	2 – Cyber Skill Requirements	3 – Critical Sector Cyber Skills
4– Cyber Culture & Awareness	5 –ITU Academy & Workshops	6 – ITU Standards & Toolkits
7 – IMPACT Cyber Training	8 – International Partnerships	9 – Next Suggested Steps

Infrastructure Relationships in Cyberspace



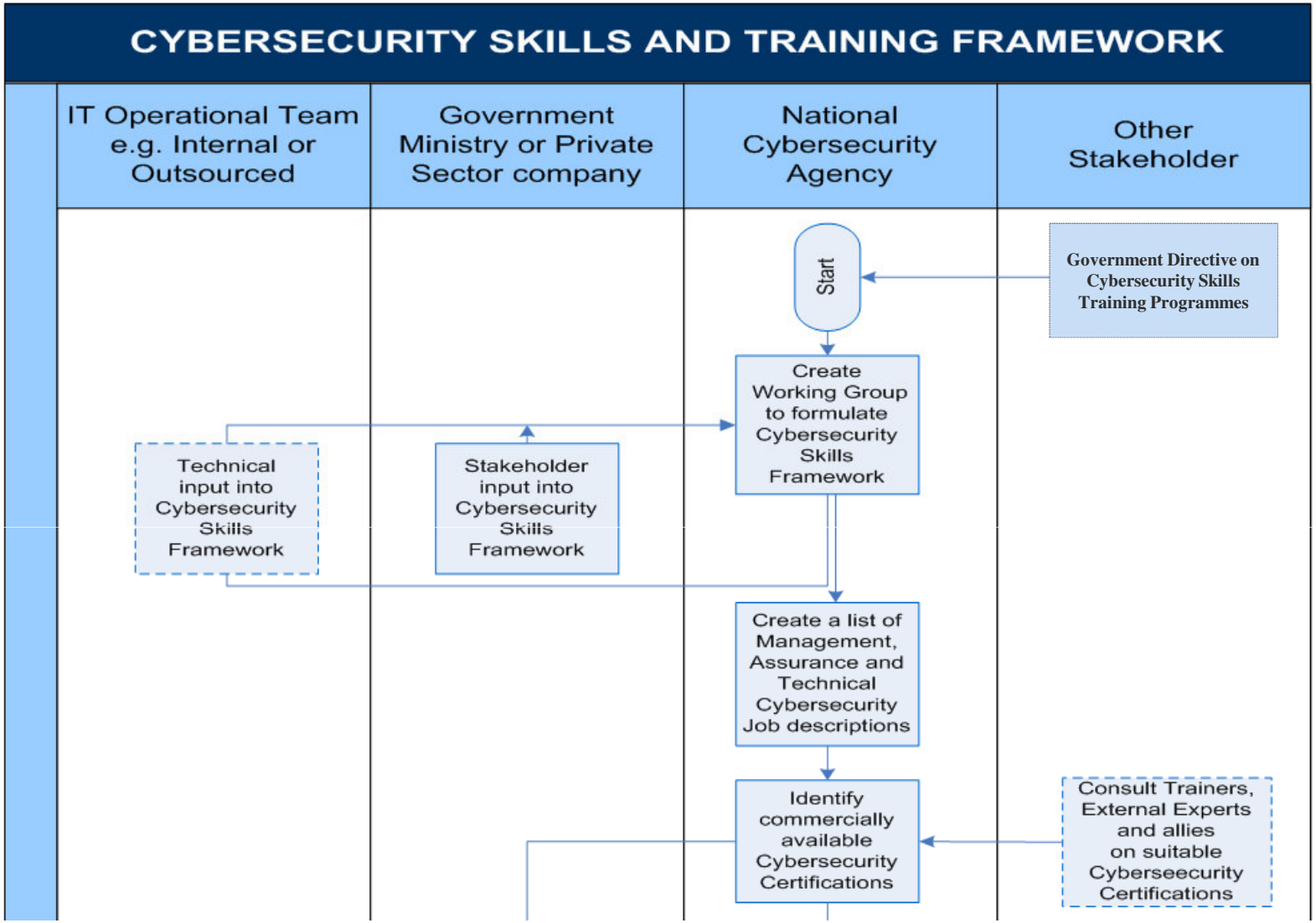
Critical Sector Cybersecurity Skills

- Every critical service sector will require some professional level of both general and sector specific cybersecurity expertise in the future:

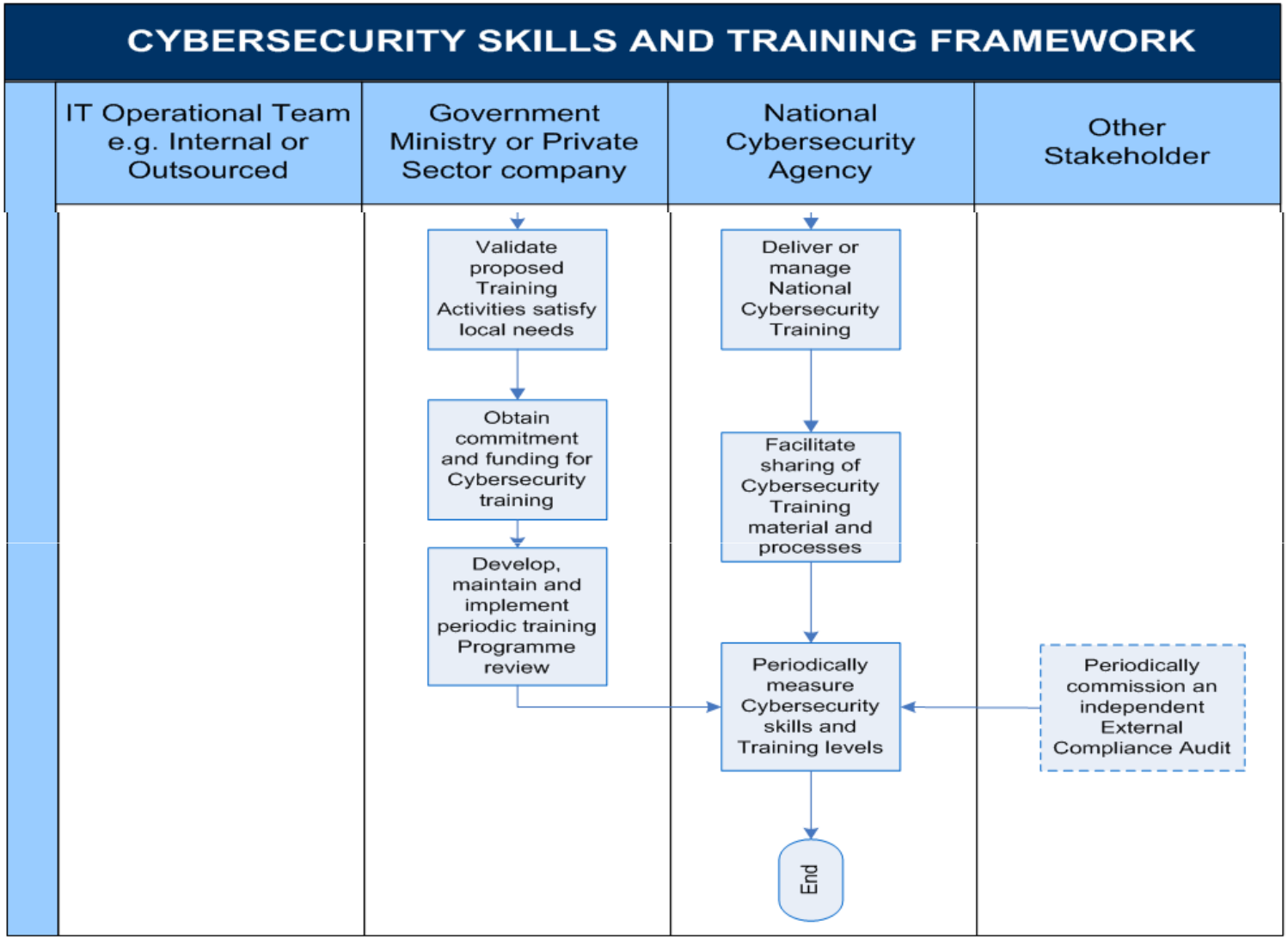
  - Telecommunications: End-to-End Network & Systems Security for Servers, Routers, Switches, Transmission and all ICT Comms Hubs & Facilities
  - Banking/Finance: Defences against financial cybercrime and ID Theft
  - Civil/Military Forces: Digital Forensics and e-Crime Investigation Units
  - Transportation/Airports: Integrated security for airports & Transport Hubs
  - Energy/Water Utilities: Protection for the National Electrical Power Grids, and Operational Control Networks for Pipelines for Oil, Gas and Water
  - Industry/Manufacturing: Integrated physical-cyber security including Process Control Systems (SCADA) against targeted *Stuxnet* type threats
  - Emergency Services: Secure real-time communications and applications
  - Healthcare: Integrated security for hospitals, medical systems & facilities
  - Education: Professional training courses, and advanced cybersecurity R&D

  ……Provision of these sector specific skills will require the National CIRT to establish partnerships "best practice" public & private sector organisations.

ITU: Flow-Chart for Cyber Skills Capacity Building(1)



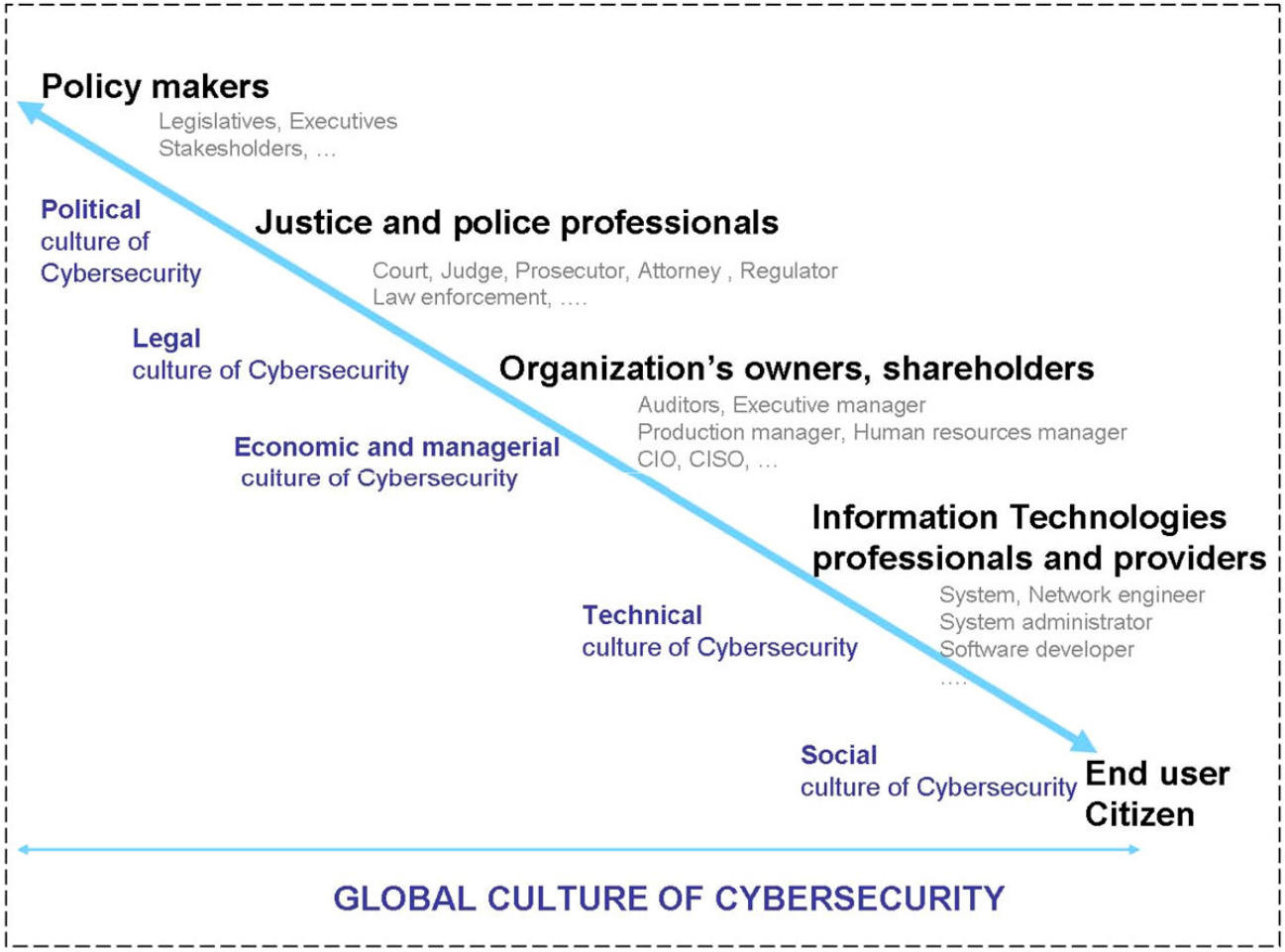
ITU: Flow-Chart for Cyber Skills Capacity Building(2)



Capacity Building & International Collaboration

1–Aim:Capacity Development	2 – Cyber Skill Requirements	3 – Critical Sector Cyber Skills
4– Cyber Culture & Awareness	5 –ITU Academy & Workshops	6 – ITU Standards & Guidelines
7 – IMPACT Cyber Training	8 – International Partnerships	9 – Next Suggested Steps

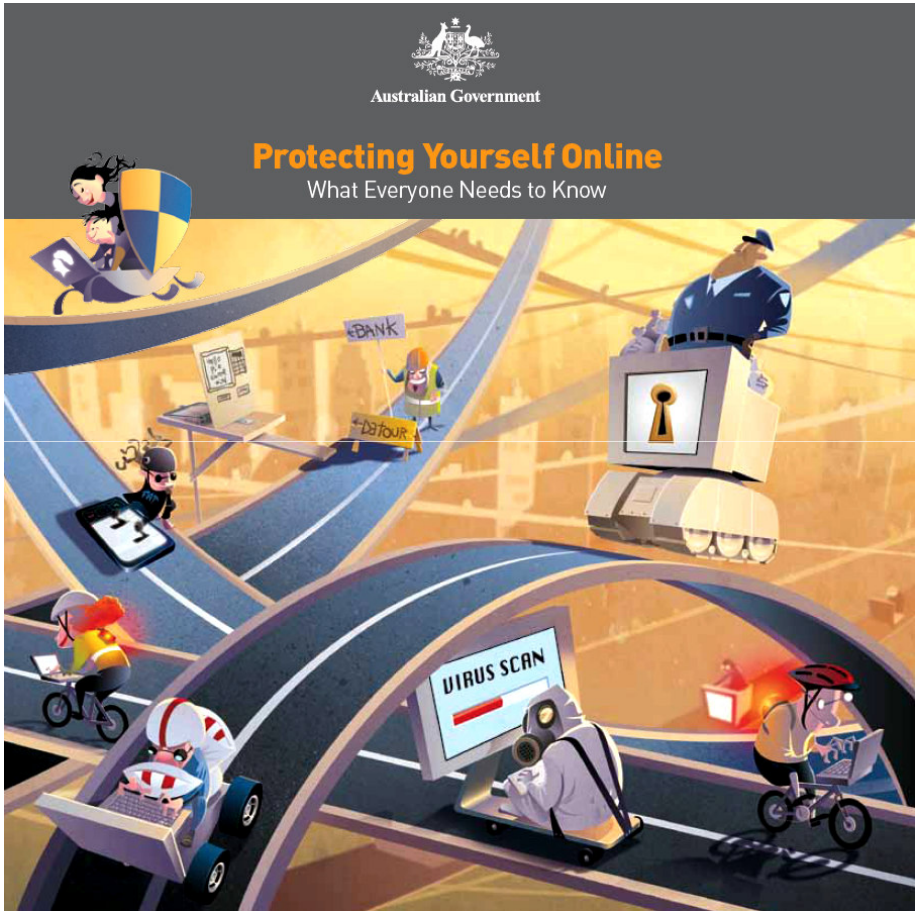
ITU: Promoting a Culture of Cybersecurity



Cybersecurity Training and Awareness

- Cybersecurity training and awareness will need to be tackled as a *multi-sector* and multi-stakeholder programme.
- Ultimately *every* business and *every* citizen will need to become cyber aware if they are to remain safe in the virtual world of cyberspace.
- Public awareness programmes will need strong central government support in order that all citizen segments from children to the elderly become conversant with *cyber risks* & how to protect oneself on-line.
- Awareness Campaigns may target the client sectors through:
  - Brochures, Newsletters and Video Materials
  - Local Discussions Groups held in Schools
  - Employee Handbooks for Staff Awareness
  - Short Training & Awareness Courses
  - Interactive Cybersecurity Website
  - Viral Marketing Campaign through Social Media Sites
- Every media awareness channel is important if the country is to promote & achieve a cybersecurity culture during the coming 3 to 5 years!...

Australian Government: CSPC – Cybersecurity Awareness Campaign



"Cybersecurity Awareness: Malaysia"

- *Cyber Awareness:* Excellent example of Awareness Campaign targeting End-users with regards to 10 Major Cybersecurity & Cybercrime Threats:

1) Phishing Scam
2) Identify Theft
3) Safety of Internet Chat
4) Spam Emails
5) Safe On-Line Shopping
6) Safe On-Line Banking
7) Security Checklists
8) Malware
9) Spyware
10) Password Protection

- *Campaign* is promoted by the Malaysian Government Cybersecurity Agency under MOSTi – Ministry of Science, Technology and Innovation

UK Government : Office of Cybersecurity (OCS)

The UK Government Office of Cybersecurity (OCS) has eight well defined work streams as follows:

1) Safe, Secure and Resilient Systems
2) Policy, Legal and Regulatory Issues
3) Awareness and Culture Change
4) Cybersecurity Skills and Education
5) Technical Capabilities and R&D
6) Exploitation of UK Capabilities
7) International Engagement & Partnership
8) Governance, Roles and Responsibilities

…these include the further development of Digital Forensics Skills & the UK Cybercrime response through the National eCrime Unit.

The Government will…

"Secure the UK's advantage in cyber space …

…by **reducing risk from the UK's use of cyber space…**

- Reduce the threat of cyber operations by reducing an adversary's motivation and capability;
- Reduce the vulnerability of UK interests to cyber operations;
- Reduce the impact of cyber operations on UK interests;

…and **exploiting opportunities in cyber space…**

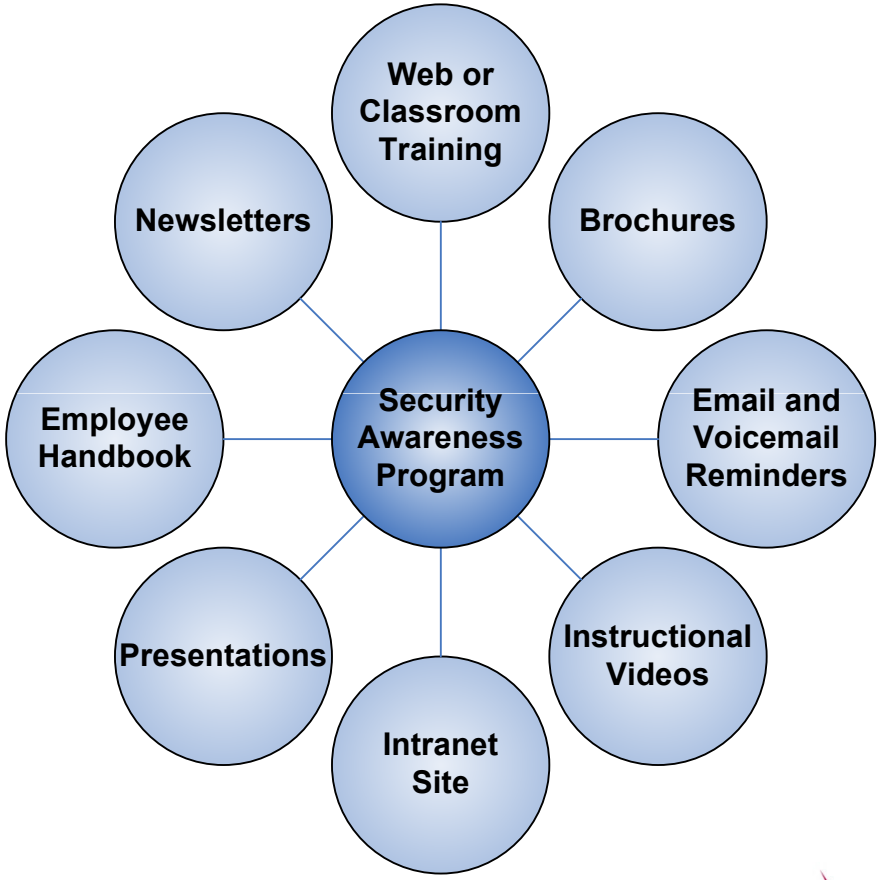
- Gather intelligence on threat actors;
- Promote support for UK policies; and
- Intervene against adversaries;

…through **improving knowledge, capabilities and decision-making.**

- Improve knowledge and awareness;
- Develop doctrine and policy;
- Develop governance and decision making;
- Enhance technical and human capabilities.

….. Significant focus in the UK Office of Cybersecurity (OCS) is also focused upon "Cybersecurity Capacity Building" and the Development of a "Cybersecurity Culture"

Cybersecurity Awareness & Education Techniques



ITU: Child On-Line Protection (COP)

Guidelines for Children, Policy Makers, Industry and Educators

Cyber Skills & Capacity Building

- Professional Cybersecurity Skills are currently in extremely short supply even in developed countries & regions such as USA, UK and Europe!

- The US Centre for Strategic and International Studies published a report in July 2010 recommending ways to overcome the skills crisis

- The UK Government launched the Cybersecurity Challenge – July 2010
- The US-led DC3 Digital Forensics Challenge finishes *today* – 1st Nov 2010

ITU: National Cybersecurity Culture & Awareness

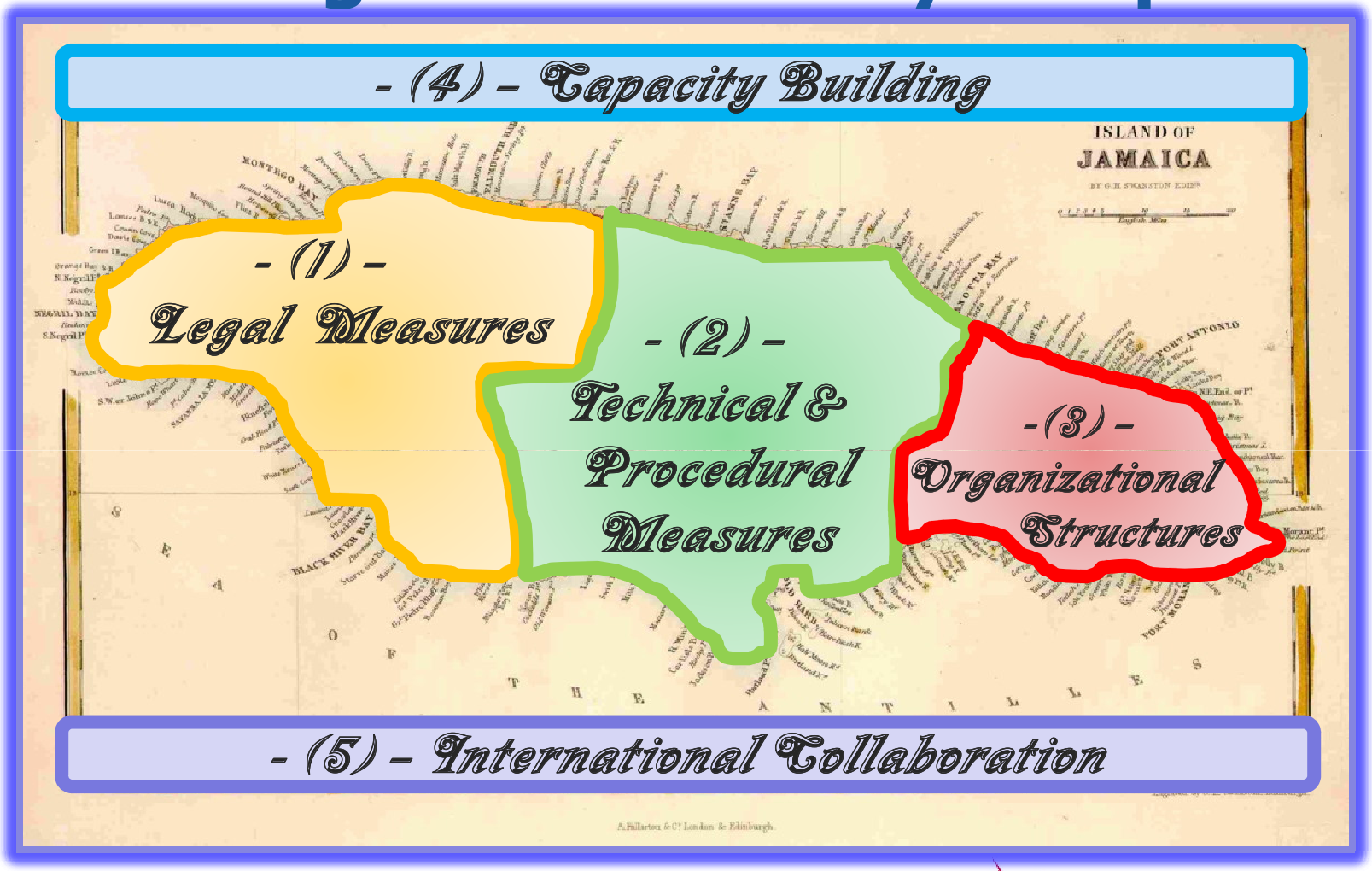
Task 1:	**Government** Assess whether: (a) A comprehensive national awareness programme exists to encourage all participants—businesses, the general workforce, and the general population— to secure their own parts of cyberspace (b) Government has allocated resources to build cybersecurity culture (c) Government has led by example and required all staff, contractors and third parties to demonstrate good cybersecurity practices (d) Government has invested in Research and Development (R&D) activities to develop solutions to cyber risks.
Task 2:	**Business** Establish whether: (a) Business understand their responsibility to secure their cyberspace (b) Incentives exist to encourage the development of a culture of cybersecurity in business enterprises (c) Penalties exist against poor security practices
Task 3:	**End users** Assess whether: (a) End users are aware of risks to business from their use of ICTs (b) Users understand their individual responsibility and accountability for actions on ICTs (c) Users have received adequate training (d) Security Operating Procedures clearly state user responsibility and accountability for security (e) A programme exists to educate and protect children and other vulnerable groups against cyber threats

Capacity Building & International Collaboration

1–Aim:Capacity Development	2 – Cyber Skill Requirements	3 – Critical Sector Cyber Skills
4–Cyber Culture & Awareness	5 –ITU Academy & Workshops	6 – ITU Standards & Toolkits
7 – IMPACT Cyber Training	8 – International Partnerships	9 – Next Suggested Steps

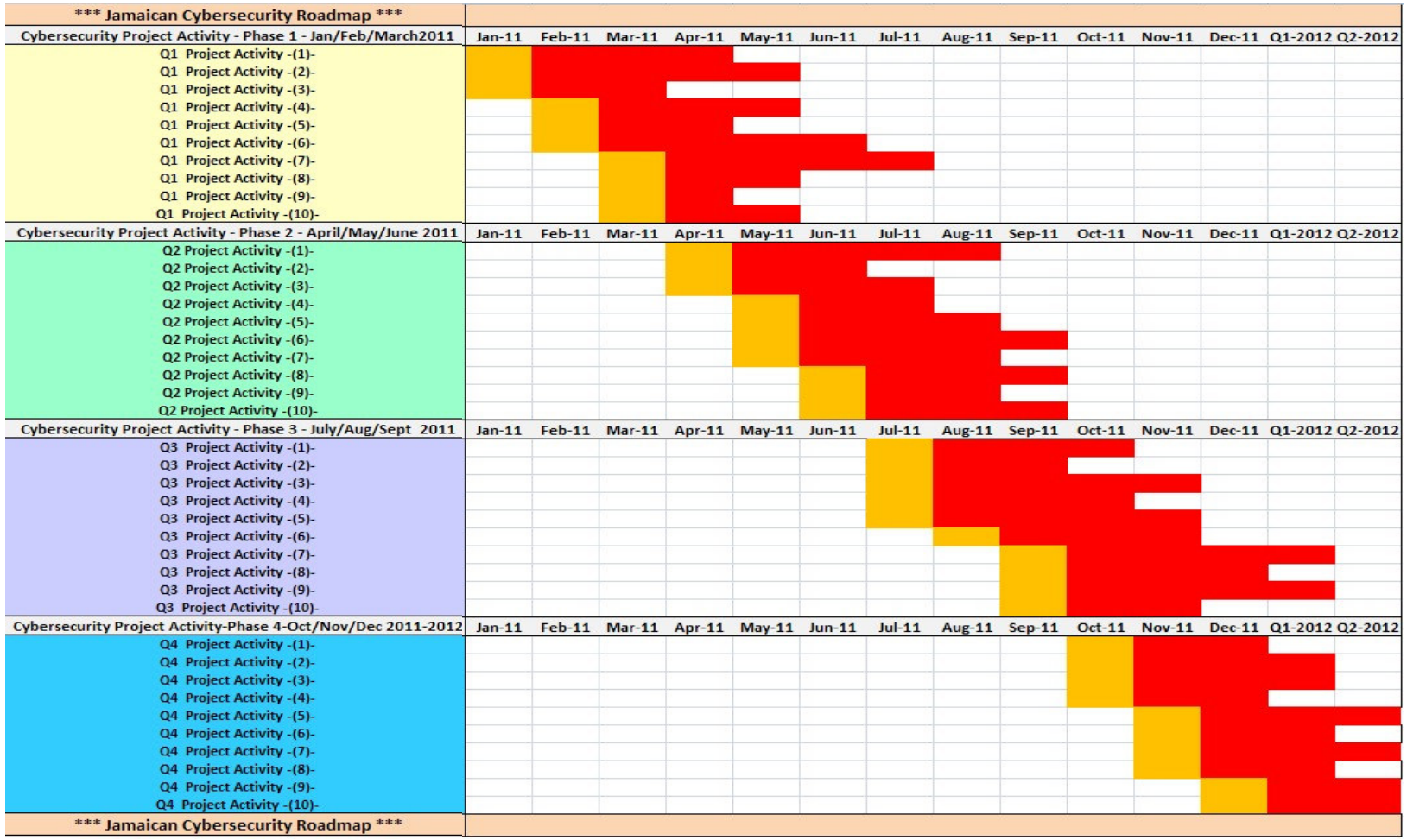
ITU Academy Centres of Excellence

Securing Jamaica in Cyberspace!



ITU: 5-day Cybersecurity Workshop - Jamaica 2010

Jamaican Cybersecurity RoadMap:
- *Project Activities for Critical Sectors* -



ITU Cybersecurity Mission to Georgia

Georgian Cyber Mission Objectives & Outcomes

- Stakeholders: Interview the key stakeholders including the Government Ministries, Georgian CERT (GRENA) & Critical Infrastructure Sectors (Telecommunications, ISPs, National & Commercial Banks)

- ITU GCA: Follow the 5 GCA Pillars: Legal, Technology, Organisation, Capacity Building & Partnerships and develop detailed recommended *Action Plan* & *Rolling Project Road-Map* for the Georgian Government

- General Outcomes:
  - National Cybersecurity Agency(NCA) : Recommendation to establish an NCA with authority and budget to manage the national cybersecurity strategy & programmes
  - Georgian CERT: Key player with professional skills that can be leveraged to build up capacity across both the Public and Private Sector working with International Partners
  - Critical Infrastructure: Recommendation to Review, Audit and then Upgrade Critical Infrastructure to International Technical & Operational Security Standards (ITU/ISO)

……Long-Term Success will be dependant upon developing professional cybersecurity skills through public-private partnerships that leverage existing CERT skills & also international organisations.

CERT Georgia: "GRENA" – Educational Sector

The primary mission of GRENA is creation of a unique information infrastructure connected to Internet for Georgian research and educational institutions, libraries, academic hospitals, international organizations and their programs working in education.
It was founded on 26 July 1999.

GRENA

Georgian Research and Educational Networking Association

ქართული English

Georgian Research and Educational Networking Association (GRENA)
10 Chovelidze St.,
0108 Tbilisi, Georgia
Tel: +995 32 250590
+995 32 250591
Fax: +995 32 912952
E-mail: contact[at]grena.ge
Web-site: www.grena.ge

- About GRENA
- News
- Service
- Cooperation
- Education

We offer guaranteed high speed internet service (ADSL) to the organizations working in scientific, educational and informational spheres using following telephone stations:
22, 23, 25, 29, 31, 32, 33, 36, 37, 38, 39, 91, 92, 93, 94, 95, 96, 97, 98,

(832)25 14 40
CALL
(890)25 14 40

The Georgian educational informational-communication network operation center is responsible for the internet connectivity to the schools provided by the Educational and Scientific Infrastructure Development Agency. Hot-line will support you in solving Internet connectivity problems.

Dear Customers,

For the purposes of improving our service and its transparency, we have created an online system for monitoring internet speed used by you. You have an opportunity to control your internet speed during 24 hours.

CERT Georgia and Association GRENA provide technical support in terms of computer and network security to the Georgian higher education institutions using GRENA internet network.

CERT GEORGIA

Association GRENA possesses the newest conference equipment, which will enable you to carry out high-speed video conferences using internet. GRENA is the member of EyeNetwork world video conference network.

RESEARCHERS IN BLACK SEA COUNTRIES TO GET ONLINE

The Black Sea Interconnection (BSI) project launched and will build a regional research and education network among South Caucasus countries and link them to GÉANT2, the high bandwidth, pan-European research network. This flagship project is the largest of its kind in the region and will allow Caucasian research communities to participate effectively in joint research and educational activities with the rest of Europe.

BSI

Association GRENA is a member of following International organizations

NCET RIPE

Association GRENA collaborate with NATO Science Programme

NATO OTAN Science for Peace and Security (SPS) North Atlantic Treaty Organisation

Georgia: Risk Assessment & Compliance Review

- A priority action for every National Government and major Business will be to assess the current levels of risks & security of computing installations, networks, systems and applications.

- During the ITU Georgian Mission, the following topics were considered during each stakeholder interview such as Government, Telco & Banking:
  1) ICT Management Organization
  2) Personnel Security – Vetting & Access Controls
  3) Software & Applications Security
  4) Device and Hardware Security
  5) Network Communications – Access, Encryption, Fail-over
  6) Business Continuity and Disaster Recovery (BCP/DR)
  7) Personal & Business Data Protection
  8) Cybersecurity Standards and Frameworks
  9) Physical Building & Facilities Security

……Following the initial audit and upgrades for each designated critical computing facility there typically be annual audits to check upon standards compliance

ITU: Regional CIRT Training Workshops

- ITU Cybersecurity Team has established CIRT Workshop and Training Programme rolling-out during 2010/2011 across geographical regions

- CIRT Development is at the *core* of the ITU Global Cybersecurity Agenda

- The ITU Workshops promote *CIRT* creation and evolution under a practical 3 Phase Model & proceeds through the traditional Project Methodology of - "Plan" – "Design" – "Implement" and "Operations":

  - *Phase 1* – 6 Months – Training & Awareness, Alerts, Incident Management
  - *Phase 2* – 12 Months – Vulnerability Handling & Management, Technology Watch
  - *Phase 3* - 18 to 24 Months – Risk Analysis & Consulting, Forensics & Audits

…ITU CIRT Workshops have already been held in the regions of West & East Africa, and a further workshop will be held this month for Central & Eastern Europe…

ITU: CIRT Organisational Development Phases

ITU-IMPACT: CIRT READINESS ASSESSMENT QUESTIONNAIRE

Task: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
Task:2	**Mission and Target** For operational or planned CIRT establish: (a) Objectives of the CIRT (b) Short-term and long-term goals
Task: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
Task: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
Task: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

ITU Regional Workshop on National CIRT Readiness Assessment and Capacity Building

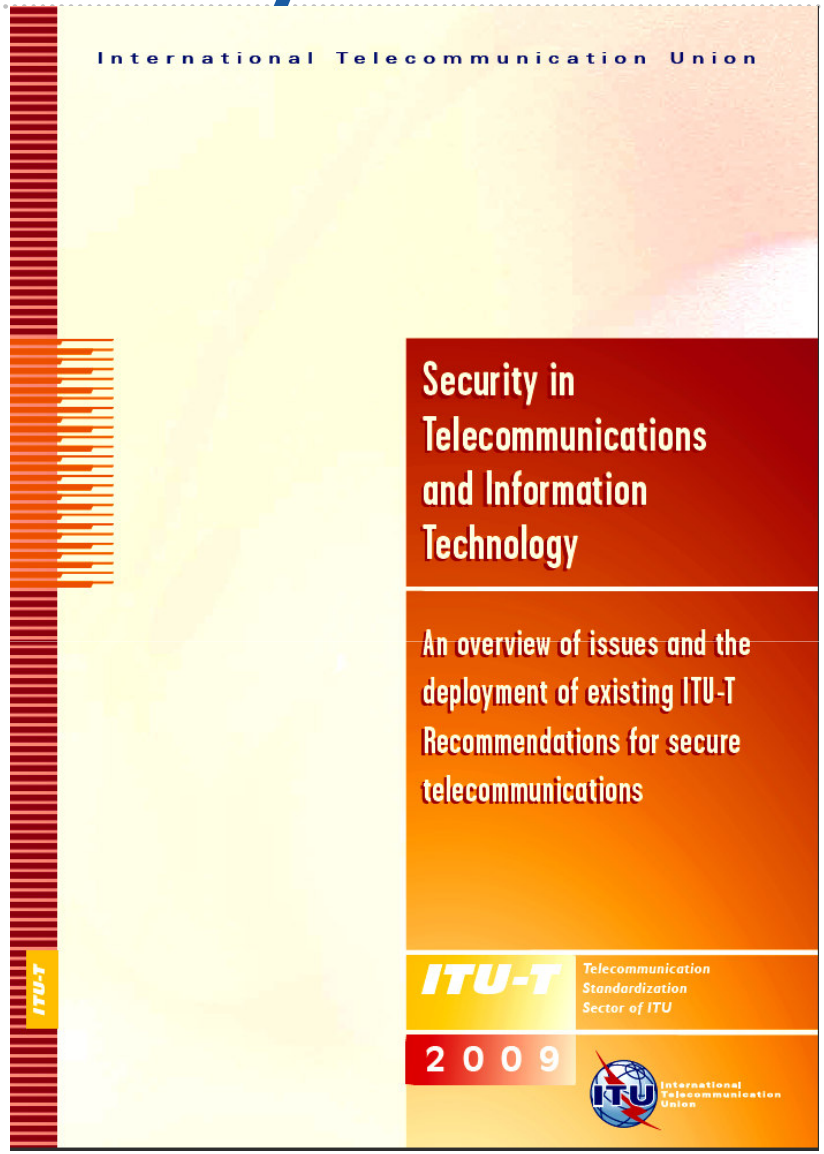
- West-Africa Workshop – 4 Member States attended (May 2010)
- East-Africa Workshop - 4 Member States attended (June 2010)
- South-East Asia – assessment in 5 Member States
- Central Eastern Europe Workshop – expected 6 Member States (November 2010) to attend
- Central Africa Workshop – expected 5 Member States (December 2010) to attend

ITU Regional CIRT Workshop Programme

Capacity Building & International Collaboration

1–Aim:Capacity Development	2 – Cyber Skill Requirements	3 – Critical Sector Cyber Skills
4– Cyber Culture & Awareness	5 – ITU Academy & Workshops	6 – ITU Standards & Toolkits
7 – IMPACT Cyber Training	8 – International Partnerships	9 – Next Suggested Steps

ITU Security Handbook for ICT



ITU-X Technical Security Standards

- The ITU Technical Families of Telecommunications Security Standards are extremely comprehensive and span practically all technical aspects of government and enterprise cybersecurity systems and architectures.

- *The ITU-X Series Standards are extremely useful in providing structures, architectures and project guidelines during capacity building programmes.*

- The standards are also being continuously developed and upgraded by professional specialists from the ICT Industry, Government & Academia

  - *X.805* – Security Architecture for End-to-End Communications
  - X.1056 – CIRTs: Incident Response Management Structures
  - *X.1121* – Security Technologies for Mobile Data Communications
  - *X.1191* – Functional Requirements for IPTV Security Agents
  - *X.1205* – Overview of Cybersecurity and General Guidelines (Technologies)
  - *X.1250* – Security Standards for Identity Management (IdM)
  - *X.509* – Public Key Infrastructure & Certificate Frameworks (PKI)

……The ITU-X security standards can be freely downloaded from "ITU.int"

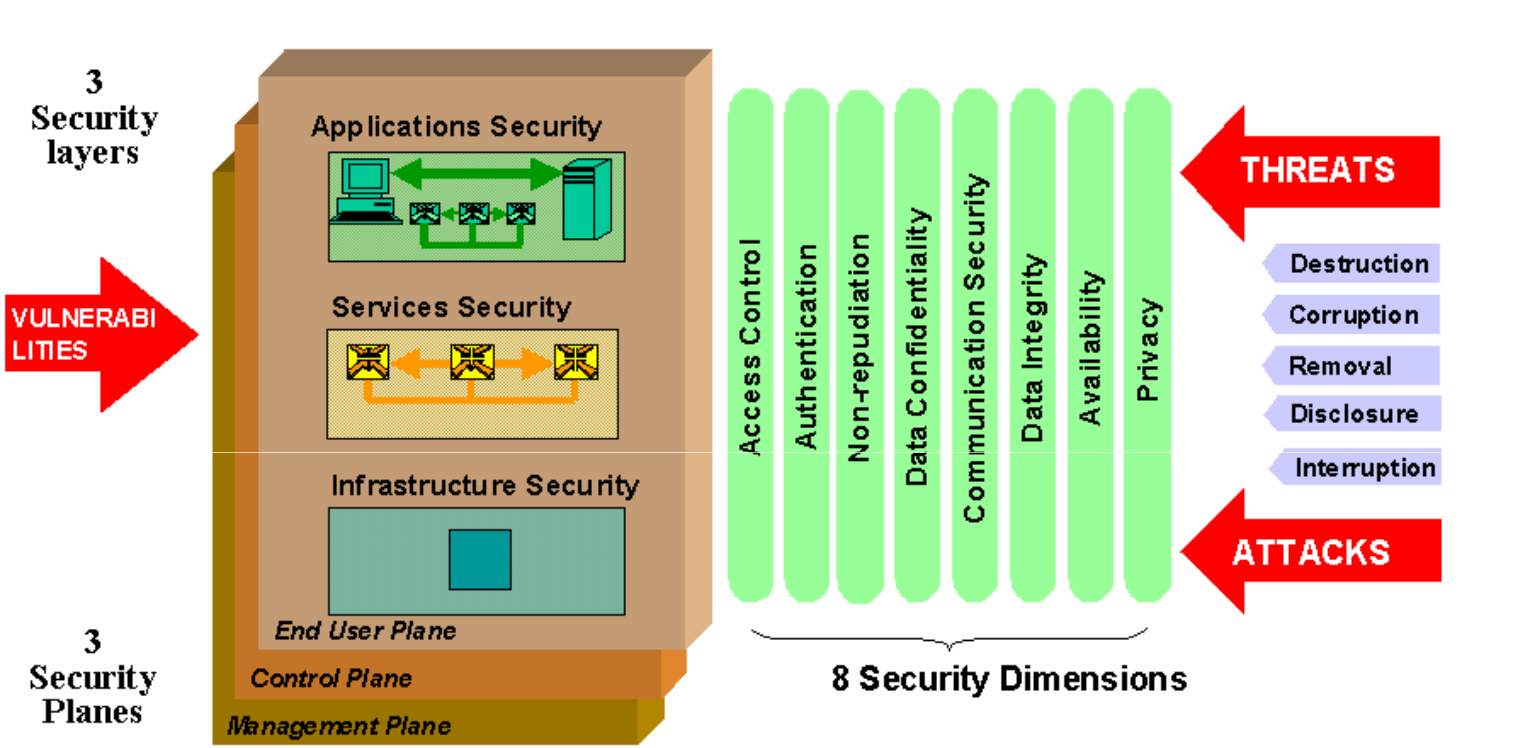
Cybersecurity in Telecomms & ICT (1)

Topic	Sub-topics	Examples of relevant Recommendations & publications
3. Security requirements	3.2 Threats, risks and vulnerabilities 3.3 Security objectives 3.4 Rationale for security standards 3.6 Personnel and physical security requirements	X.1205: Overview of cybersecurity E.408: Telecommunication networks security requirements X.1051: Information security management guidelines for telecommunications organizations Outside plant technologies for public networks Application of computers and microprocessors to the construction, installation and protection of telecommunication cables
4. Security architectures	4.1 Open systems security architecture 4.2 Security services 4.3 Security architecture for systems providing end-to-end communications 4.3.2 Availability of the network and its components 4.4 Implementation guidance 4.5 Application-specific architectures	X.800: Open systems security architecture X.805: Security architecture for systems providing end-to-end communications X.810: Security framework overview X.Sup3: ITU-T X.800-X.849 series - Supplement on guidelines for implementing system and network security X.1162: Security architecture and operations for peer-to-peer networks X.1161: Framework for secure peer-to-peer communications X.1143: Security architecture for message security in mobile web services.
5. Security management	5.1 Information security management 5.2 Risk management 5.3 Incident handling	X.1051: Information security management guidelines for telecommunications organizations X.1055: Risk management and risk profile guidelines for telecommunication organizations E.409: Incident organization and security incident handling
6. The Directory, authentication and Identity management	6.1 Protection of Directory information 6.1.4 Privacy protection 6.2 Public-key security mechanisms 6.2.3 Public-key infrastructures 6.4 Identity management 6.5 Telebiometrics	X.500: Overview of concepts, models and services X.509: The Directory: Public-Key and attribute certificate frameworks X.1171: Threats and requirements for protection of personally-identifiable information in applications using tag-based identification Y.2720: An NGN identity management framework X.1081: A framework for the specification of security and safety aspects of telebiometrics, X.1089: Telebiometrics authentication infrastructure

Cybersecurity in Telecomms & ICT (2)

7. Securing the network infrastructure	7.1 The telecommunications management network 7.2 Network management architecture 7.4 Securing monitoring and control activities 7.5 Securing network-based applications 7.6 Common security management services 7.6.4 CORBA-based security services	M.3010: Principles for a telecommunications management network X.790: Trouble management function for ITU-T applications X.711: Common Management Information Protocol X.736: Security alarm reporting function X.740: Security audit trail function X.780: TMN Guidelines for defining CORBA managed objects
8. Some specific approaches to network security	8.1 Next Generation Network (NGN) security 8.2 Mobile communications security 8.3 Security for home networks 8.4 Security requirements for IPCablecom 8.6 Security for Ubiquitous Sensor Networks	Y.2001: General overview of NGN Y.2701: Security requirements for NGN release 1 X.1121: Framework of security technologies for mobile end-to-end data communications X.1111: Framework for security technologies for home network J.170: IPCablecom security specification
9. Application security	9.1 Voice over IP (VoIP) and multimedia 9.2 IPTV 9.3 Secure fax 9.4 Web services 9.5 Tag-based services	H.235: Framework for security in H-series multimedia systems X.1191: Functional requirements and architecture for IPTV security aspects T.36: Security capabilities for use with Group 3 facsimile terminals X.1141: Security Assertion Markup Language (SAML 2.0)
10. Countering common network threats	10.1 Countering spam 10.2 Malicious code, spyware and deceptive software 10.3 Notification and dissemination of software updates	X.1231: Technical strategies on countering spam X.1240: Technologies involved in countering email spam X.1244: Overall aspects of countering spam in IP-based multimedia applications X.1207: Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software X.1206: A vendor-neutral framework for automatic notification of security related information and dissemination of updates
For a complete set of ITU-T security Recommendations see http://www.itu.int/ITU-T/recommendations/		

ITU – X.805 Security Architecture



….The ITU-X.805 Cybersecurity Architecture coupled with ITU-X.1205 Standards together provide an excellent framework for in-depth Professional Technical Training

X.1205 Cybersecurity Technologies (1)

Techniques	Category	Technology	Purpose
Cryptography	Certificate and public key architecture	Digital signatures	Used to enable the issuance and maintenance of certificates to be used in digital communications
		Encryption	Used encryption of data during transmission or storage
		Key exchange	Establish either a session key or a transaction key to be used to secure a connection
	Assurance	Encryption	Insures data authenticity
Access control	Perimeter protection	Firewalls	Control access to and from a network
		Content management	Monitors traffic for non-compliant information
	Authentication	Single factor	A system that uses user ID/password combinations to verify an identifier
		Two factor	A system that requires two components in order to grant a user system access, such as the possession of a physical token plus the knowledge of a secret
		Three factor	Adds another identification factor such as a biometric or measurement of a human body characteristic
		Smart tokens	Establish trusted identifiers for users through a specific circuitry in a device, such as a smart-card
	Authorization	Role based	Authorization mechanisms that control user access to appropriate system resources based on its assigned role
		Rule based	Authorization mechanisms that control user access to appropriate system resources based on specific rules associated with each user independent of their role within an organization

X.1205 Cybersecurity Technologies (2)

Techniques	Category	Technology	Purpose
System integrity	Antivirus	Signature methods	Protect against malicious computer code, such as viruses, worms, and Trojan horses using their code signatures
		Behaviour methods	Checks running programs for unauthorized behaviour
	Integrity	Intrusion detection	Can be used to warn network administrators of the possibility of a security incident, such as files on a server are compromised
Audit and Monitoring	Detection	Intrusion detection	Compare network traffic and host log entries to match data signatures that are indicative of hackers
	Prevention	Intrusion prevention	Detect attacks on a network and take actions as specified by the organization to mitigate the attacks. Suspicious activities trigger administrator alarms and other configurable responses
	Logging	Logging tools	Monitor and compare network traffic and host log entries to match data signatures and host address profiles indicative of hackers
Management	Network management	Configuration management	Allows for the control and configuration of networks, and fault management
		Patch management	Install latest updates, fixes to network devices
	Policy	Enforcement	Allow administrators to monitoring and enforce security policies

On-Line Cybersecurity Resources: ITU

All the ITU Publications can be found & downloaded from: www.itu.int
(use the titles below as search terms on the ITU Website Home Page)

1) ITU – Global Cybersecurity Agenda – HLEG Strategic Report – 2008
2) ITU – Cybersecurity Guide for Developing Countries – 2009
3) ITU – "BotNet" Mitigation Toolkit Guide – 2008
4) ITU – National Cybersecurity/CIIP Self-Assessment Tool – 2009
5) ITU – Toolkit for Cybersecurity Legislation – 2010
6) ITU – Understanding Cybercrime: A Guide for Developing Countries-2009
7) ITU – Technical Security Standards & Recommendations – "X-Series" – including X.509 (PKI), X.805 (Architecture), X.1205 (Threats & Solutions)
8) ITU – GCA: Global Cybersecurity Agenda: Summary Brochure – 2010

……..ITU GCA Home Page: www.itu.int/osg/csd/cybersecurity/gca/

ITU Cybersecurity Guides & Toolkits

ITU National Cybersecurity/CIIP Self-Assessment Tool

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

April 2009 Revised Draft

For further information, please contact the ITU-D ICT Applications and Cybersecurity Division at <cybmail@itu.int>

Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1205
(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Overview of cybersecurity

Recommendation ITU-T X.1205

ITU AND CITEL REGIONAL CYBERSECURITY CAPACITY BUILDING WORKSHOP FOR THE AMERICAS

Monday 1st November 2010, Salta City, Argentina

ITU Botnet Mitigation Toolkit

Background Information

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

January 2008

International Telecommunication Union

Committed to connecting the world

Cybercrime & Legislation:
- Definition & Scope -

- *Cybercrime:* Criminal activities that specifically target a *computer* or *network* for malicious damage, infiltration, extortion, theft & fraud.

- *Cyberterrorism:* Used for those cybercriminal acts that are deliberately targeted to create large-scale disruption of critical information instructure such as government, banking, energy & telecommunications networks

- *Cyberattacks:* Typical terms used to designate cyberattacks include: spamming, phishing, spoofing, pharming, denial of service, trojans, viruses, worms, malware, spyware and botnets.

Upgraded National Laws & Regulations are required to enable the civil & military enforcement agencies to investigate & prosecute cybercriminal & cyberterrorist activities that are illegal & disruptive against citizens, businesses and the state.

ITU Toolkits: Cybercrime Legislation and a Cybercrime Guide for Developing Countries

International Telecommunication Union

Cybercrime Legislation Resources

ITU TOOLKIT FOR CYBERCRIME LEGISLATION

Developed through the
American Bar Association's Privacy & Computer Crime Committee
Section of Science & Technology Law
With Global Participation

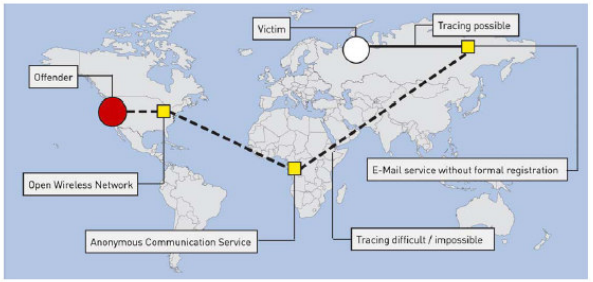
ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

Draft Rev. February 2010

For further information, please contact the
ITU-D ICT Applications and Cybersecurity Division at cybmail@itu.int

International Telecommunication Union

Cybercrime Legislation Resources



UNDERSTANDING CYBERCRIME:
A GUIDE FOR DEVELOPING COUNTRIES

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

Draft April 2009

For further information, please contact the
ITU-D ICT Applications and Cybersecurity Division at cybmail@itu.int

Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

ITU AND CITEL REGIONAL CYBERSECURITY CAPACITY BUILDING WORKSHOP FOR THE AMERICAS
Monday 1st November 2010, Salta City, Argentina

International Telecommunication Union
Committed to connecting the world

ITU Guidelines for Government Legislation Agencies

ITU CYBERCRIME TOOLKIT LEGISLATIVE REQUIREMENTS	Jurisdictional Provisions
	Section 21: Jurisdiction
Acts Against Computers, Computer Systems, Networks, Computer Data, Content Data, and Traffic Data	**International Cooperation**
Section 1: Definition of Terms	Section 22: International Cooperation: General Principles
Section 2: Unauthorized Access to Computers, Computer Systems, and Networks	Section 23: Extradition Principles
Section 3: Unauthorized Access to or Acquisition of Computer Data, Content Data, Traffic Data	Section 24: Mutual Assistance: General Principles
Section 4: Interference and Disruption	Section 25: Unsolicited Information
Section 5: Interception	Section 26: Procedures for Mutual Assistance
Section 6: Misuse and Malware	Section 27: Expedited Preservation of Stored Computer Data, Content Data, or Traffic Data
Section 7: Digital Forgery	Section 28: Expedited Disclosure of Preserved Content Data, Computer Data or Traffic
Section 8: Digital Fraud, Procure Economic Benefit	Section 29: Mutual Assistance Regarding Access to Stored Computer Data, Content Data, or Traffic Data
Section 9: Extortion	Section 30: Trans Border Access to Stored Computer Data, Content Data, or Traffic Data
Section 10: Aiding, Abetting, and Attempting	Section 31: Mutual Assistance In Real Time Collection of Traffic Data
Section 11: Corporate Liability	Section 32: Mutual Assistance Regarding Interception of Content Data or Computer Data
Provisions for Criminal Investigations and Proceedings for Offenses within this Law	
Section 12: Scope of Procedural Provisions	
Section 13: Conditions and Safeguards	
Section 15: Expedited Preservation and Partial Disclosure of Traffic Data	
Section 17: Production Order	
Section 18: Search and Seizure of Stored Data	
Section 19: Interception (Real Time Collection) of Traffic Data	
Section 20: Interception (Real Time Collection) of Content Data	

ITU: Cybersecurity Project Gateway

CYBERSECURITY GATEWAY

HOME | About the Cybersecurity Gateway | Stakeholders | Work Areas | ITU Initiatives

About the Cybersecurity Gateway

Links

IMPACT

GCA

WSIS

Child Online Protection

Welcome to the ITU Cybersecurity Gateway

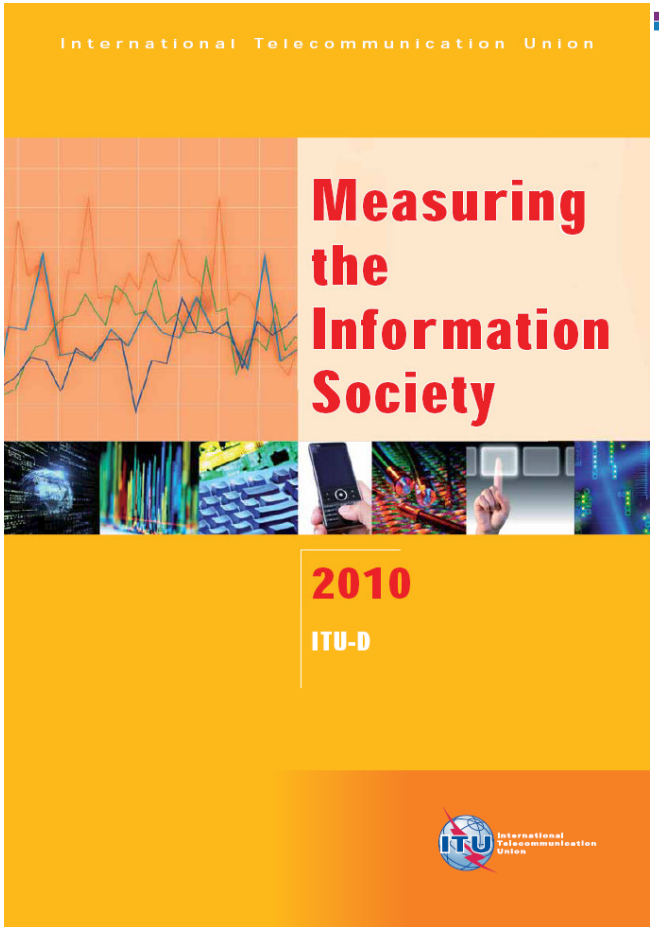
About the Cybersecurity Gateway

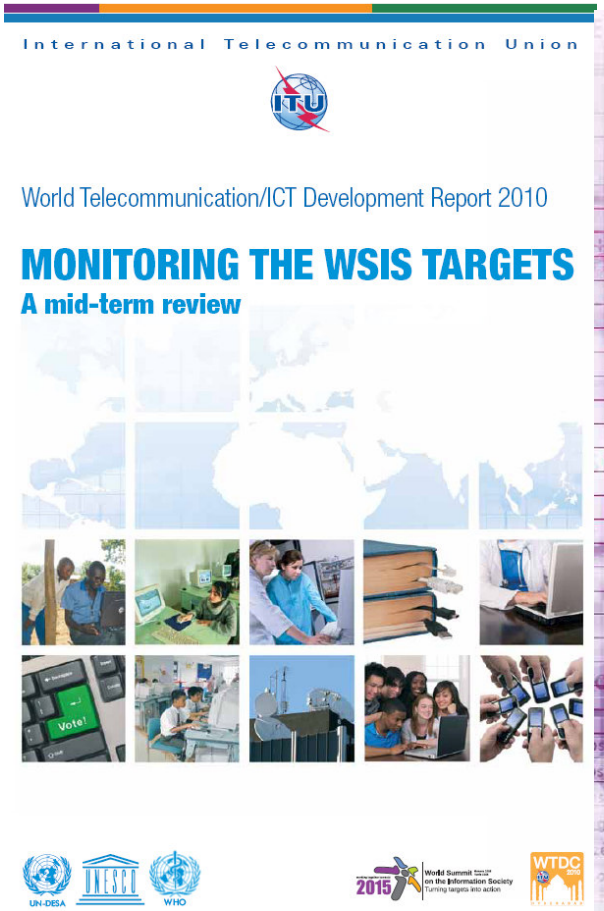
The purpose of the Cybersecurity Gateway is to provide an easy-to-use and interactive information resource on national and international Cybersecurity related initiatives worldwide.
The Cybersecurity Gateway aims to be a collaborative platform, providing and sharing information between partners in civil society, private sector, governmental and international organizations working in different work areas of Cybersecurity. All of these stake holders are invited to provide information about their activities and initiatives be they related to Legal Measure, Technical and Procedural Measures, Organizational Structures, Capacity Building or International Cooperation or any other work area relevant to Cybersecurity.

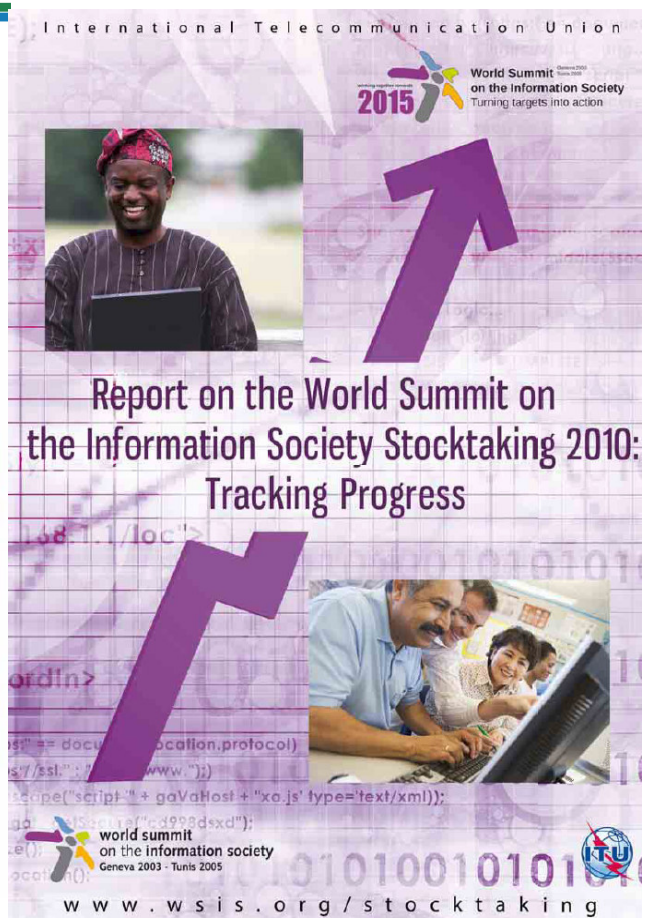
The new release of Cybersecurity Gateway is to make the information sharing process simpler, more dynamic and more collaborative. The ITU wish you good luck with all your initiatives and look forward to learn more about your initiatives!

….Currently **141** ITU Project Initiatives in partnership with **51** Organisations

WSIS = World Summit on the Information Society







…The ITU took the global lead for WSIS in Cybersecurity & "Securing the Information Society"

ITU: Cybersecurity Programmes

….Multiple ITU Programmes that all contribute to National Cybersecurity Capacity Building!

Capacity Building & International Collaboration

1–Aim:Capacity Development	2 – Cyber Skill Requirements	3 – Critical Sector Cyber Skills
4– Cyber Culture & Awareness	5 –ITU Academy & Workshops	6 – ITU Standards & Toolkits
7 – IMPACT Cyber Training	8 – International Partnerships	9 – Next Suggested Steps

IMPACT Global Headquarters: Cyberjaya, Malaysia

IMPACT Global Headquarters

IMPACT's Global HQ was launched on 20th May 2009 by the 5th Prime Minister of Malaysia, The Honourable Dato' Seri Abdullah Ahmad Badawi, witnessed by the current Prime Minister of Malaysia, The Honourable Dato' Sri Najib Tun Razak and the Secretary-General of the ITU, Dr. Hamadoun Touré.

The IMPACT's Global HQ is located on a seven acre estate near Kuala Lumpur with a current infrastructure of over 58,000 square feet. Its extensive infrastructure includes the Global Response Centre (GRC) – a state of the art centre for cyber threats detection, analysis and response – alongside well-equipped training rooms, research labs, an auditorium, meeting facilities and administrative offices. IMPACT is staffed by a global workforce.

IMPACT's Global HQ is also the physical and operational home of the Global Cybersecurity Agenda (GCA), a framework for international cooperation initiated by the International Telecommunication Union (ITU). The GCA is aimed at finding strategic solutions to boost confidence and security in an increasingly networked information society.

Besides the GRC, the facility is purpose built to house IMPACT's four Centres, which were formed around the four key functions of IMPACT.

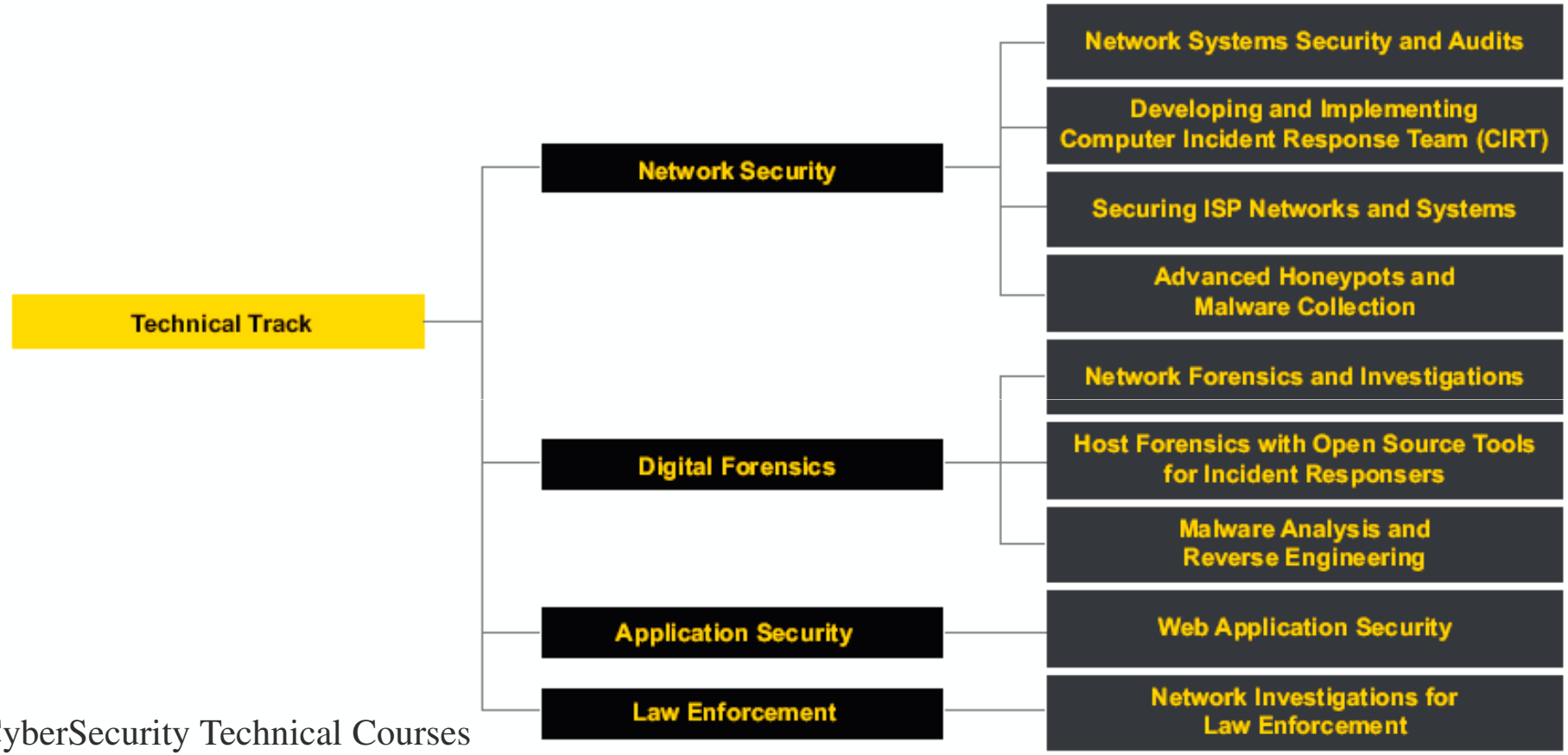
IMPACT = International Multilateral Partnerships Against Cyber Threats

IMPACT: Cyber Training Roadmap

IMPACT Training Roadmap

	Management Track			Technical Track			
	Security Management	Security Audit	Legal & Policy Framework	Network Security	Digital Forensics	Application Security	Law Enforcement
Target Audience	CIO, CISO, IT Security Manager, IT Security Executive, Compliance Manager, Dept. Head, Manager, Executive	Internal Auditor, External Auditor, Risk Manager, Compliance Manager, IT Security Manager	Law Students & Practitioners, IT Students & Professionals, Police & Law Enforcement Officers, Management Students & Professionals	Network Administrator/ Support, Incident Handlers, Network Managers, IT Support/ Administrators, CIRT Analyst	Forensics Analyst, Forensics Investigators, Incident Handlers, Malware Analyst	Web Application Developer, Webmasters, Application Support Executive	Police Officers, Law Enforcement Officers, Legal Officers, Lawyers
Foundation	**IMPACT SecurityCore** - Information Security Fundamentals + Security Awareness for Everyone/ Managers/IT Administrators						
Intermediate	Developing Security Policies & Procedures ISO 27001 Information Security Management (ISMS) Concepts and Awareness ISO 27001 Information Security Management (ISMS) Implementation	ISO 27001 Information Security Management System Lead Auditor (ISMS)	Cyber Crime: Domestic and International Models of Cooperation Legal Responses to Emerging Cyber Crimes	Network Systems Security and Audits Developing and Implementing Computer Incident Response Team (CIRT) Securing ISP Networks and Systems Advanced Honeypots and Malware Collection	Network Forensics and Investigations Host Forensics with Open Source Tools for Incident Responders Malware Analysis and Reverse Engineering	Web Application Security	Network Investigations for Law Enforcement
Advanced	$(ISC)^2$ CISSP CBK Review Seminar	$(ISC)^2$ CISSP CBK Review Seminar	$(ISC)^2$ CISSP CBK Review Seminar	$(ISC)^2$ CISSP CBK Review Seminar	$(ISC)^2$ CISSP CBK Review Seminar	$(ISC)^2$ CISSP CBK Review Seminar	$(ISC)^2$ CISSP CBK Review Seminar

ITU-IMPACT: Cybersecurity Technical Training



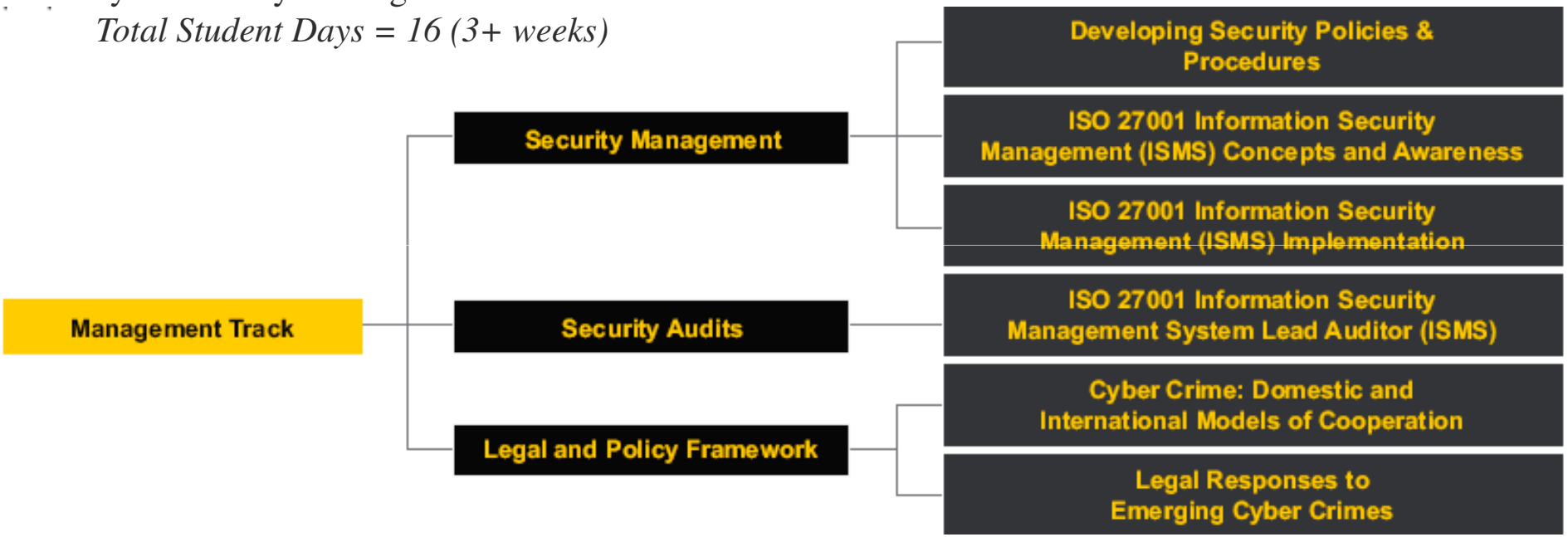
CyberSecurity Technical Courses

Total Student Days = 41 (8+ Weeks)

ITU-IMPACT: Cyber Management Training

CyberSecurity Management Courses

Total Student Days = 16 (3+ weeks)



Capacity Building & International Collaboration

1–Aim:Capacity Development	2 – Cyber Skill Requirements	3 – Critical Sector Cyber Skills
4– Cyber Culture & Awareness	5 –ITU Academy & Workshops	6 – ITU Standards & Toolkits
7 – IMPACT Cyber Training	8 – International Partnerships	9 – Next Suggested Steps

International Cybersecurity Collaboration

- Cybersecurity is a global trans-border issue. Cybercrime investigations and forensics can only be managed through strong international collaboration and partnerships

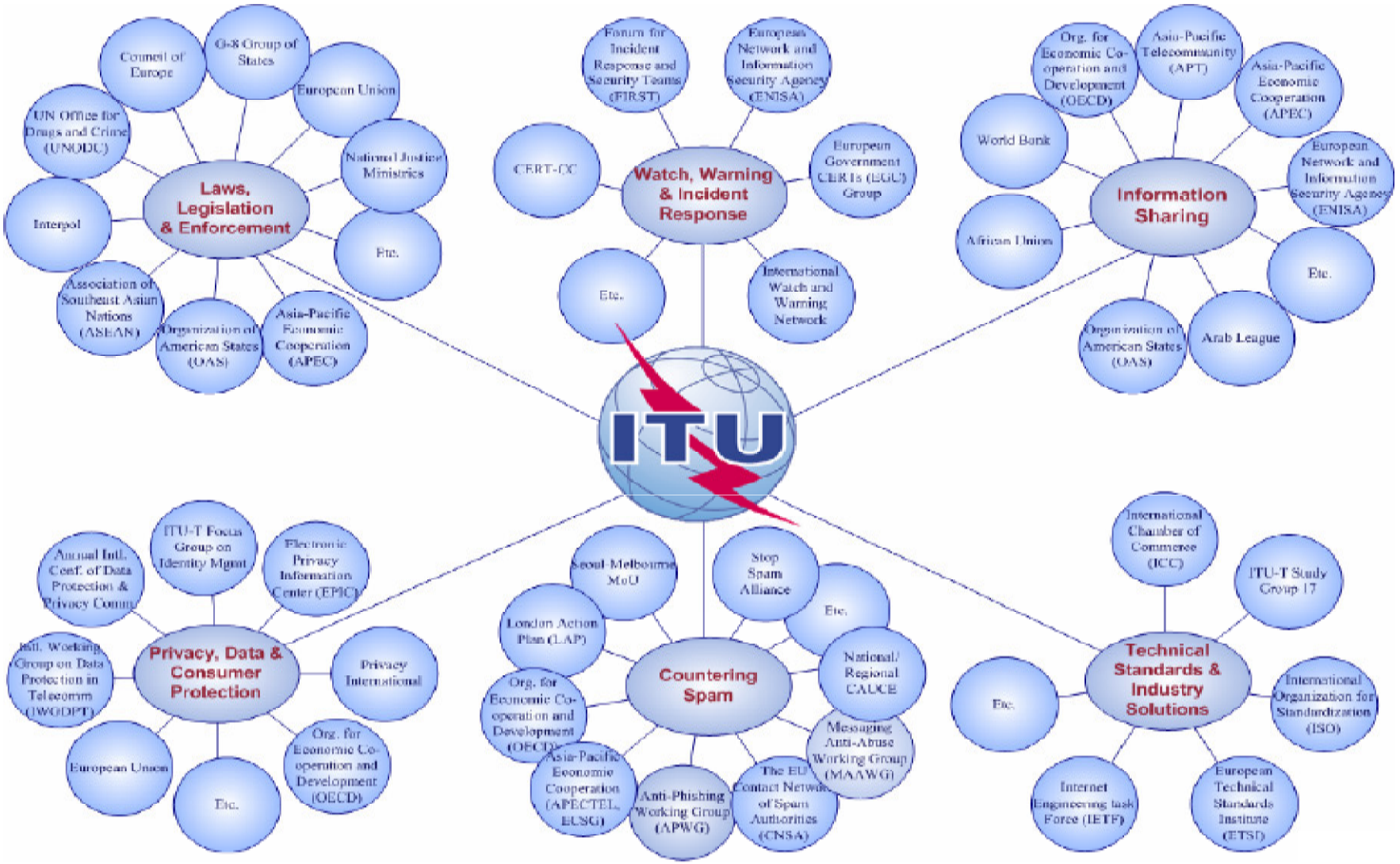
- The ITU Global Cybersecurity Agenda tackles this through multiple partnerships including its role within the IMPACT Alliance, and its NEWS and ESCAPE Programmes, as well as in-depth skills training, and the development of the CIRT-LITE Programme

- INTERPOL is also a critically important partner for law enforcement authorities in many countries for the investigation of international cybercrime "rings" & cyberterrorist "cells"

- CERTs/CSIRTS also have well connected international communities that enable member countries to support each other during cyber attacks:
  - *FIRST* – Forum for Incident Response & Security Teams : 226 Teams in 48 Countries (FIRST.org)
  - *CMU* – Carnegie Mellon University pioneered the concept of CERTs during the early 1990s and now runs the commercial CERT.ORG and provides global network support (CERT.org)
  - *US-CERT* – United States Computer Emergency Readiness Team (US-CERT.gov)
  - *ENISA* – European Network & Information Security Agency – (ENISA.europa.eu)

…The ITU currently has active working partnerships with all these international cybersecurity organisations & many more as in the following graphical slide!

Stakeholders for the ITU Cybersecurity Ecosystem



Capacity Building & International Collaboration

1–Aim:Capacity Development	2 – Cyber Skill Requirements	3 – Critical Sector Cyber Skills
4– Cyber Culture & Awareness	5 –ITU Academy & Workshops	6 – ITU Standards & Toolkits
7 – IMPACT Cyber Training	8 – International Partnerships	9 – Resources & Next Steps

Next Steps for CITEL/OAS Members

- During this intensive One Day Cybersecurity workshop we've covered all the Five Pillars of ITU's comprehensive Global Cybersecurity Agenda (GCA)

- Some key actions for ITU & CITEL Members to consider during the next year are:

  - *CIRT:* Build or Upgrade your National CIRT and use this resource as a *Catalyst* for Capacity Building
  - *NCA:* Develop a National Cybersecurity Agency (or Council) within your Government Administration
  - *Laws:* Review the Legislation and Regulations, and ways in which your nation can implement New Legislation to further secure the nation in Cyberspace, against Cybercrimes & Terrorism
  - *Culture:* Promote a culture of cybersecurity understanding and awareness across business & citizens
  - *Training:* Work with your National CIRT to facilitate professional training within educational institutions
  - *CIIP:* Ensure that the Government and Critical Sectors are fully supported by your National CIRT
  - *Forensics:* Upgrade the professional experience & skills of the Cybercrime Teams in Digital Forensics
  - *PPP:* Implement PPP Agreements to outsource Government Cybersecurity Programmes to Business
  - *Collaboration:* Promote Cybersecurity Collaboration through Regional and Global partnerships

……the ITU looks forward to supporting your actions through its global Cybersecurity Agenda of Guidelines, Workshops & Partnerships!

ITU & CITEL Regional Cybersecurity Workshop

- Capacity Building & International Collaboration -

ITU & CITEL Regional Cybersecurity Workshop:
- Capacity Building & International Collaboration -

BACK-UP SLIDES

ITU Cybersecurity Guide for Developing Countries

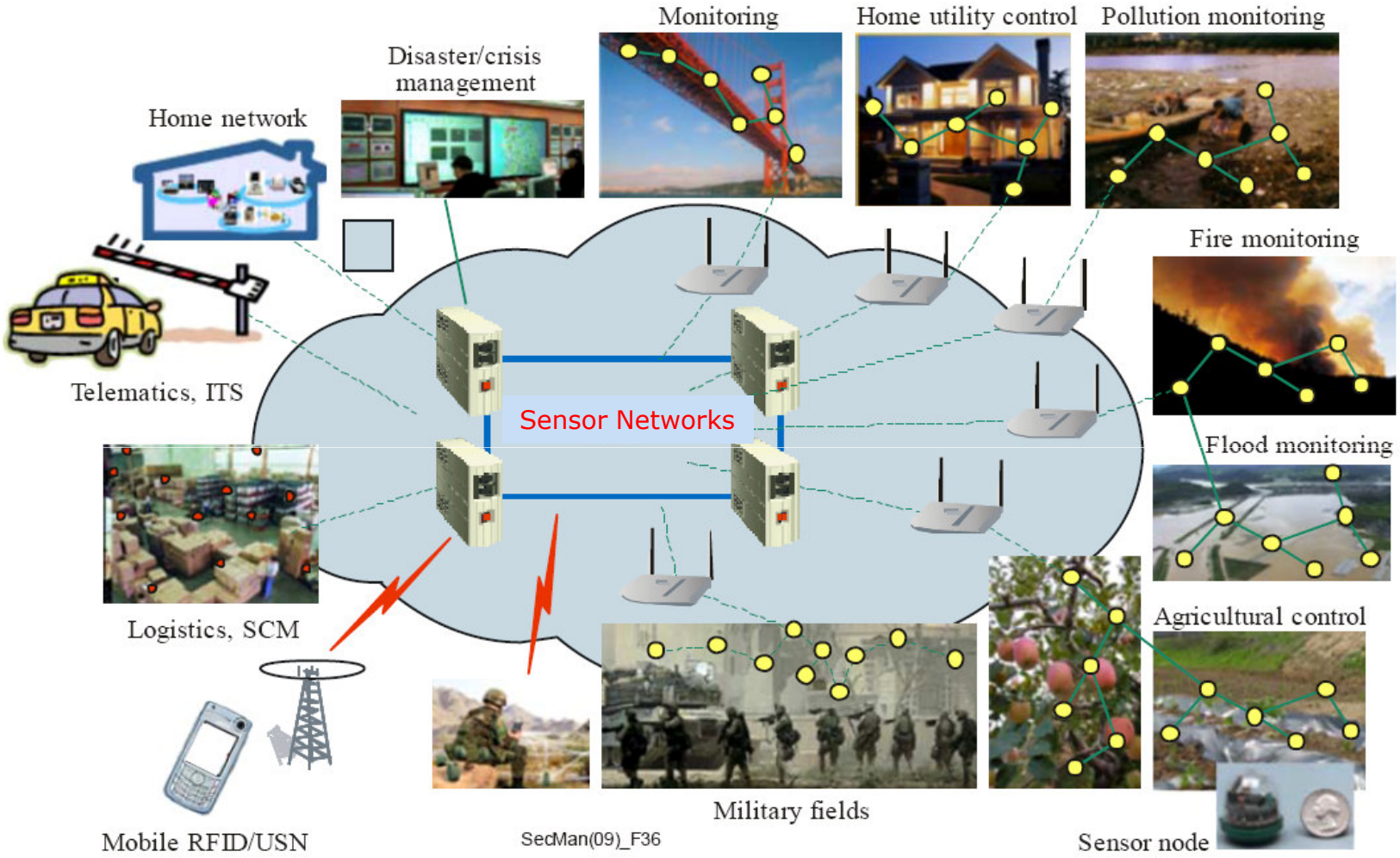
Table of Contents

Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

ITU AND CITEL REGIONAL CYBERSECURITY CAPACITY BUILDING WORKSHOP FOR THE AMERICAS
Monday 1st November 2010, Salta City, Argentina

International Telecommunication Union
Committed to connecting the world

Cybersecurity for Critical Sector "Sensor Networks"



StuxNet Worm: Targets Industrial SCADA Systems

User accesses an infected removable drive; his/her system is then infected by **WORM_STUXNET.A**

Stuxnet Worm : 1st Discovered June 2010

WORM_STUXNET.A drops files onto the *Windows* folder, creates registry entries, and injects codes into processes to stay memory-resident; it also drops **RTKT_STUXNET.A** to hide its malicious routines

WORM_STUXNET.A targets SCADA WinCC systems, which are used to manage industrial operations such as power plants and energy refineries.

It is also interesting to note that it attempts to access sites related to an online football-betting site. Though this does not pose threats, it may be a diversion tactic to confuse security analysts, causing them to fail to immediately realize the worm's main functionalities.

WORM_STUXNET.A drops copies of itself, a .LNK file detected as **LNK_STUXNET.A,** onto all removable drives connected to an affected system, allowing it to propagate

SCADA = Supervisory Control & Data Acquisition
- Mainly for Power Stations & Industrial Plants -

Special Cybersecurity Technical Organisations

- Effective national and enterprise cybersecurity requires the implementation of professionally staffed technical organisations
- In this session we'll consider the cybersecurity organisations and associated technical skills for:

  - CERT/CSIRT: Computer Emergency Response Team – *We'll explore the steps required to establish and manage a National or Enterprise CERT. We will use the CMU (Carnegie Mellon University), and ENISA (European Network & Information Security Agency) Guidelines as the foundations for our technical and management analysis*

  - NCU/eCrime Unit: National Cybercrime Unit – *We'll use the UK National eCrime Unit as an example of "Best Practice" for the organisation, including the process for cybercrime investigation, evidence collection and the skills for Digital Forensics*

  - Global IMPACT Centre: International Multi-Lateral Partnership against Cyber Threats - *This is a unique organisation is an alliance with several major global players including the ITU and Interpol. We'll present some of the programmes that may be relevant to National Government, major Institutions and Commercial Enterprises*

Cyber Technologies and Standards

- *Architectures & Standards:* The protection of critical national infrastructure requires systems & services to be implemented to internationally agreed architectures & technical standards

- *ITU Standards:* Standards Groups supported by the ITU have defined and published an extensive set of standards based around X.805 and X.1205b that cover practically all aspect of cybersecurity systems

- *Integrated Security:* The implementation of complete cybersecurity security solutions for critical sectors requires the integration of cybersecurity technologies within those for physical security

- *Open Wireless World:* The open world of mobile gadgets & social networking means that cybersecurity professionals have to continually design new technical solutions to maintain comprehensive security

CyberCrimes against Critical Sectors

- *Government:*
  - Theft of secret intelligence, manipulation of documents, and illegal access to confidential citizen databases & national records
- *Banking/Finance:*
  - Denial of Service attacks against clearing bank network, phishing attacks against bank account & credit cards, money laundering
- *Telecomms/Mobile:*
  - Interception of wired & wireless communications, and penetration of secure government & military communications networks
- *Transport/Tourism:*
  - Cyberterrorism against airports, hotels and resorts, malicious penetration of on-line booking & reservations networks
- *Energy/Water:*
  - Manipulation and disruption of the national energy grid & water utilities through interference of the process control network

CISSP Certification Domains

- The CISSP – Certified Information Systems Security Professional is one of the highest international qualifications from the (ISC)² , and is based upon the core tenets of *Confidentiality, Integrity & Availability:*

1) Access Control
2) Application Security
3) Business Continuity and Disaster Recovery
4) Cryptography
5) Information Security and Risk Management
6) Legal, Regulations, Compliance and Investigations
7) Operations Security
8) Physical (Environmental) Security
9) Security Architecture and Design
10) Telecommunications and Network Security

- *An in-depth study of all these security domains would easily fill an intensive 3 month training schedule, but it is possible to provide an overview of the essential features during an intensive 5-day workshop!*