"National Cybersecurity Strategy Roadmap and Action Plan"

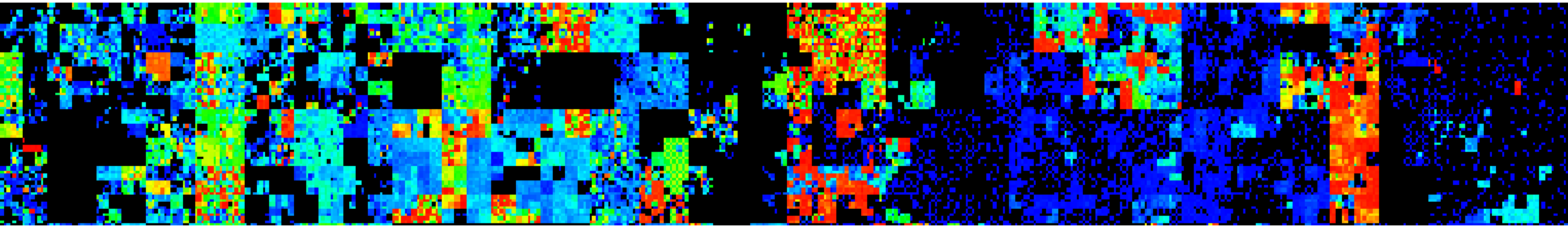
Dr David E. Probert

VAZA International

Dedicated to the Memory of Herbert Elijah Probert

National Cybersecurity Strategy, Roadmap & Actions

1 – Our Global Cybersecurity Challenge	2 – Developing the UN Cyber Framework	3 – National Cybersecurity Case Studies
4 – Dimensions of National Cybersecurity	5 – The UN Global Cyber Agenda (GCA)	6 - Technology, Standards & Operations
7 – New Legislation, Training and Partners	8 – National Roadmap - “Shopping List”	9 – Implementing YOUR Action Plan!



UN/ITU: High-Level Expert Group

– *Global Cybersecurity Agenda* -

International Telecommunication Union

ITU Global Cybersecurity Agenda (GCA)
High-Level Experts Group (HLEG)
Global Strategic Report

GLOBAL CYBERSECURITY AGENDA
A FIVE-PART PLATFORM

ITU Secretary-General

HLEG

HLEG MEMBERS[1]

The High-Level Experts Group (HLEG) of the Global Cybersecurity Agenda (GCA) comprises multi-stakeholder specialists in cybersecurity from a broad range of backgrounds: administrations of ITU Member States, industry, regional and international organizations, and research and academic institutions, as follows:

Argentine Republic • Brazil (Federal Republic of) • Cameroon (Republic of) • Canada • China (People's Republic of) • Costa Rica (Republic of) • Egypt (Arab Republic of) • Estonia (Republic of) • France • Germany (Federal Republic of) • India • Indonesia (Republic of) • Italy • Japan • Lithuania (Republic of) • Malaysia • Morocco (Kingdom of) • Portugal • Russian Federation • Saudi Arabia (Kingdom of), South Africa (Republic of) • Syrian Arab Republic • Switzerland (Confederation of) • United States of America • AT&T • Authentrus • BITEK International Inc. • BT Counterpane • Cisco • Cybex • eWorldwide Group • Gaztik • Intel Corporation • Microsoft Corporation • [illegible] • UMTS Forum • VeriSign • Asia Pacific Economic Telecommunication and Information Working Group (ApecTel) • African Telecommunication Union (ATU) • Computer Emergency Response Team (CERT) • Commonwealth Telecommunications Organization (CTO) • Council of Europe • European Network and Information Security Agency (ENISA) • Forum of Incident Response and Security Teams (FIRST) • International Criminal Police Organization (Interpol) • Organisation for Economic Cooperation and Development (OECD) • Organisation Internationale de la Francophonie (OIF) • United Nations Institute for Training and Research (UNITAR) • United Nations Office on Drugs and Crime (UNODC) • Carnegie Mellon CyLab (USA) • Ecole Polytechnique Fédérale de Lausanne (EPFL) (Switzerland) • Geneva Security Forum (Switzerland) • Georgia Institute of Technology (USA) • HEC-Université de Lausanne (Switzerland) • Information Security Institute (Australia) • Max-Planck Institute for Foreign and International Criminal Law University (Germany) • Moscow Technical University of Communications (Russian Federation) • Moss Tingrett Court (Norway) • Policyb (Canada) • Queensland University of Technology (Australia) • University of Cologne (Germany).

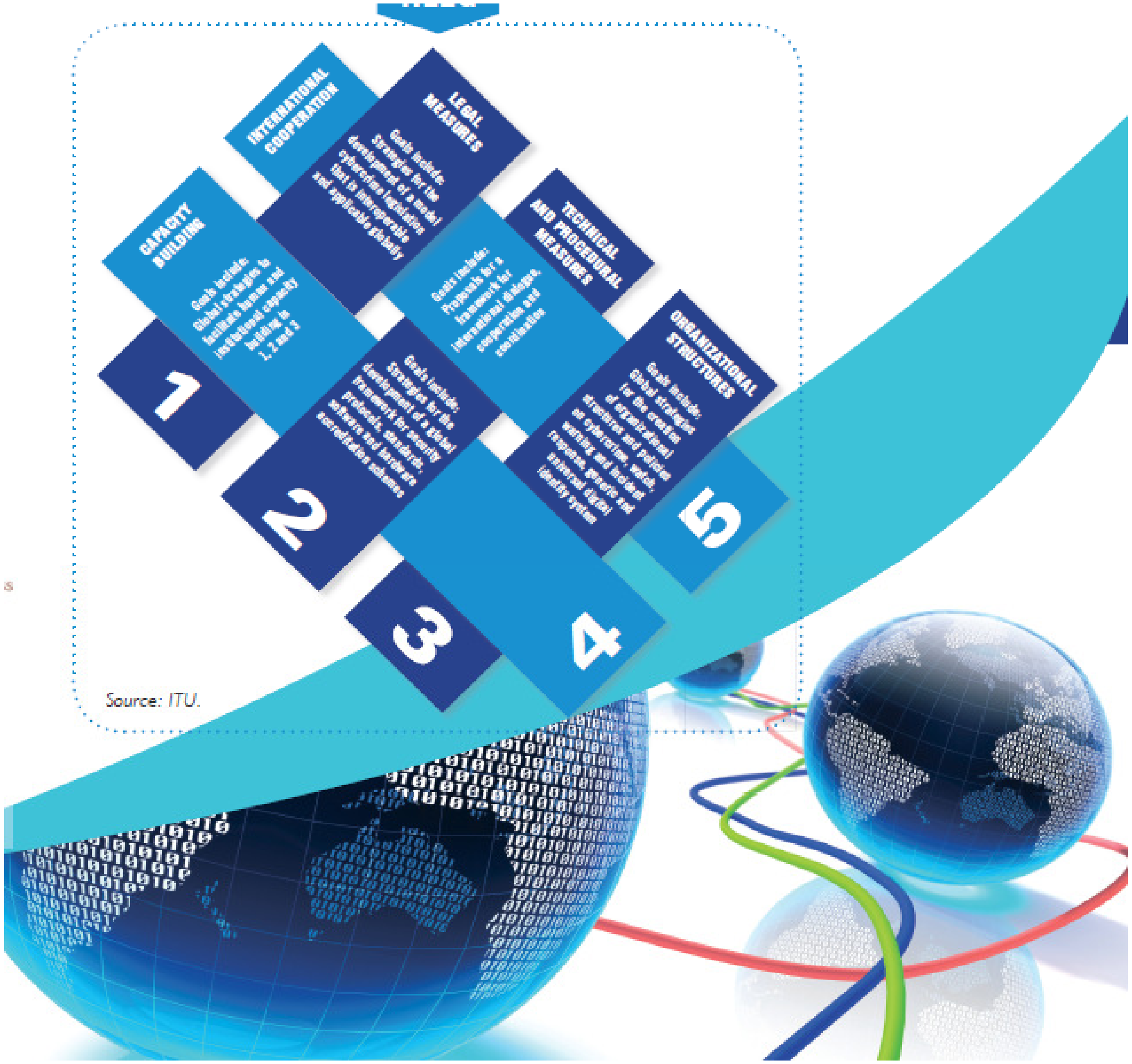
The experts have been invited to join the HLEG because of their world-renowned expertise in the work areas of the GCA and they participate in a personal capacity.

[1] [illegible]

ITU: Committed to connecting the world

e-mail: gca@itu.int — www.itu.int/cybersecurity/gca

International Telecommunication Union



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

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

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

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

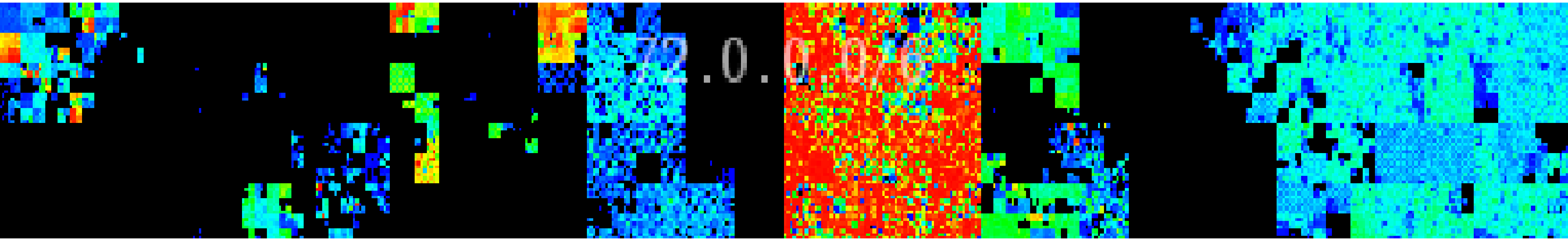
ORGANIZATIONAL STRUCTURES
Goals include: Global strategies for the creation of organizational structures and policies on cybercrime, watch, warning and incident response, generic and universal digital identity system

Source: ITU.

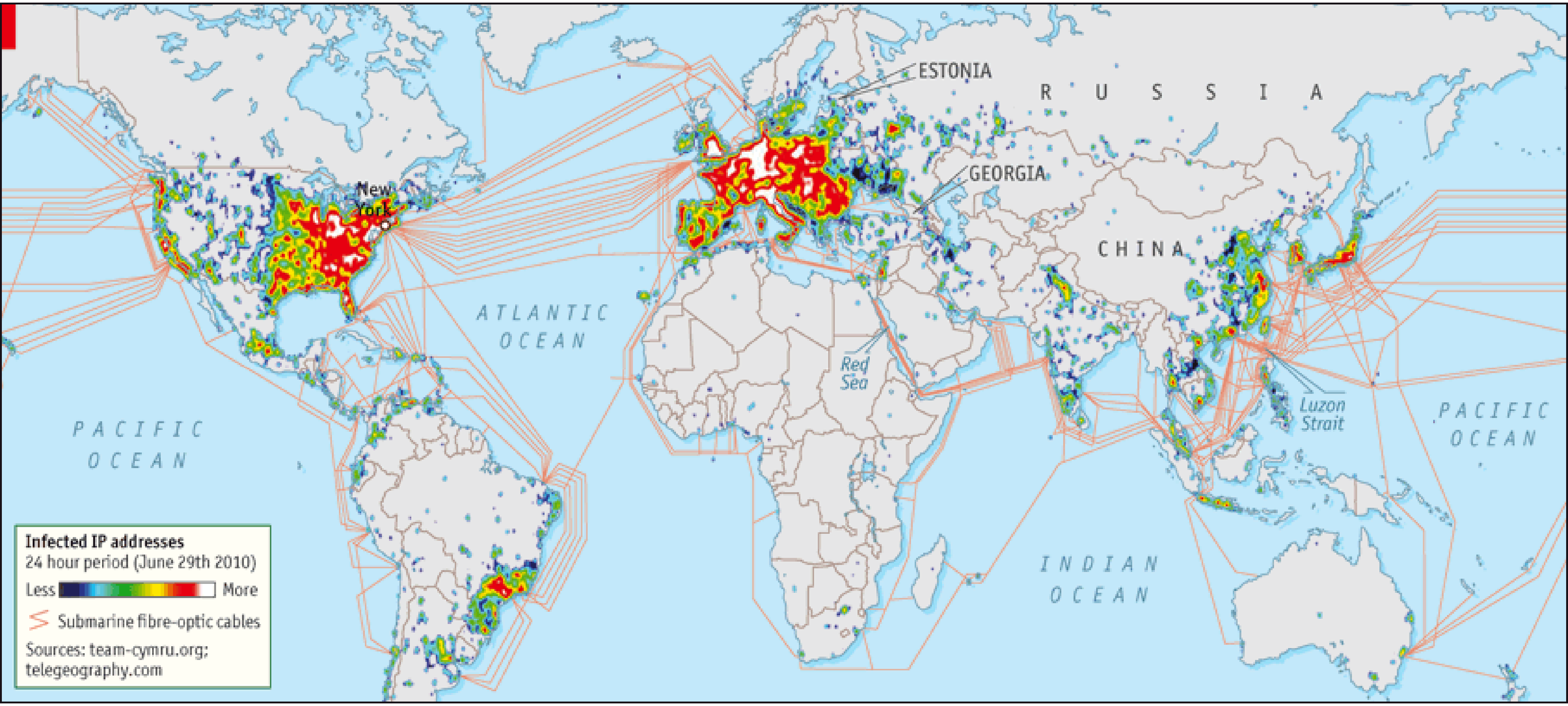
…..The UN/ITU Secretary General established "Cybersecurity" as a TOP priority!

National Cybersecurity Strategy, Roadmap & Actions

1 – Our Global Cybersecurity Challenge	**2 – Developing the UN Cyber Framework**	3 – National Cybersecurity Case Studies
4 – Dimensions of National Cybersecurity	5 – The UN Global Cyber Agenda (GCA)	6 – Technology, Standards & Operations
7 – New Legislation, Training and Partners	8 – National Roadmap - "Shopping List"	9 – Implementing YOUR Action Plan!

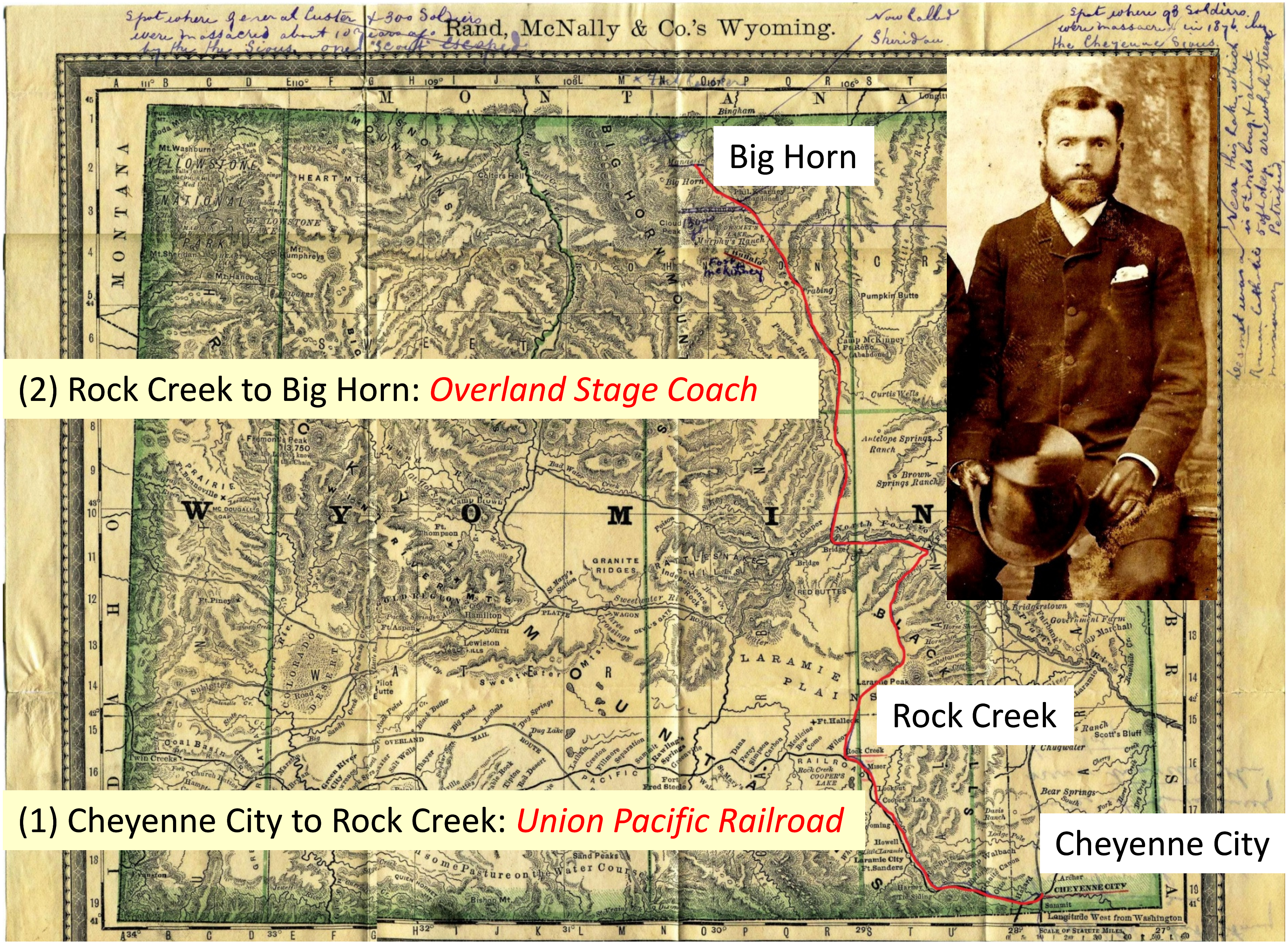


Global IP Connectivity: *Real-Time Infection*



"Visualisation of Cyberspace": *Global IP "WHOIS" Addresses*

...From 19thC Physical World To 21stC Intelligent World


Rand, McNally & Co.'s Wyoming.
Spot where General Custer & 300 Soldiers were massacred about 10 years ago by the the Sioux. one "Scout" Escaped.
Now called Sheridan.
Spot where 98 Soldiers were massacred in 1876. by the Cheyenne Sioux.
Near this lake which is 6½ mls long & about 50ft deep, are whole trees Petrified.
Lees met a Roman Catholic missionary
Fort McKinney
MONTANA
IDAHO
WYOMING
BRASKA
YELLOWSTONE NATIONAL PARK
BIG HORN MOUNTAINS
LARAMIE PLAINS
BLACK HILLS
CHEYENNE CITY
Longitude West from Washington

Big Horn

(2) Rock Creek to Big Horn: *Overland Stage Coach*

Rock Creek

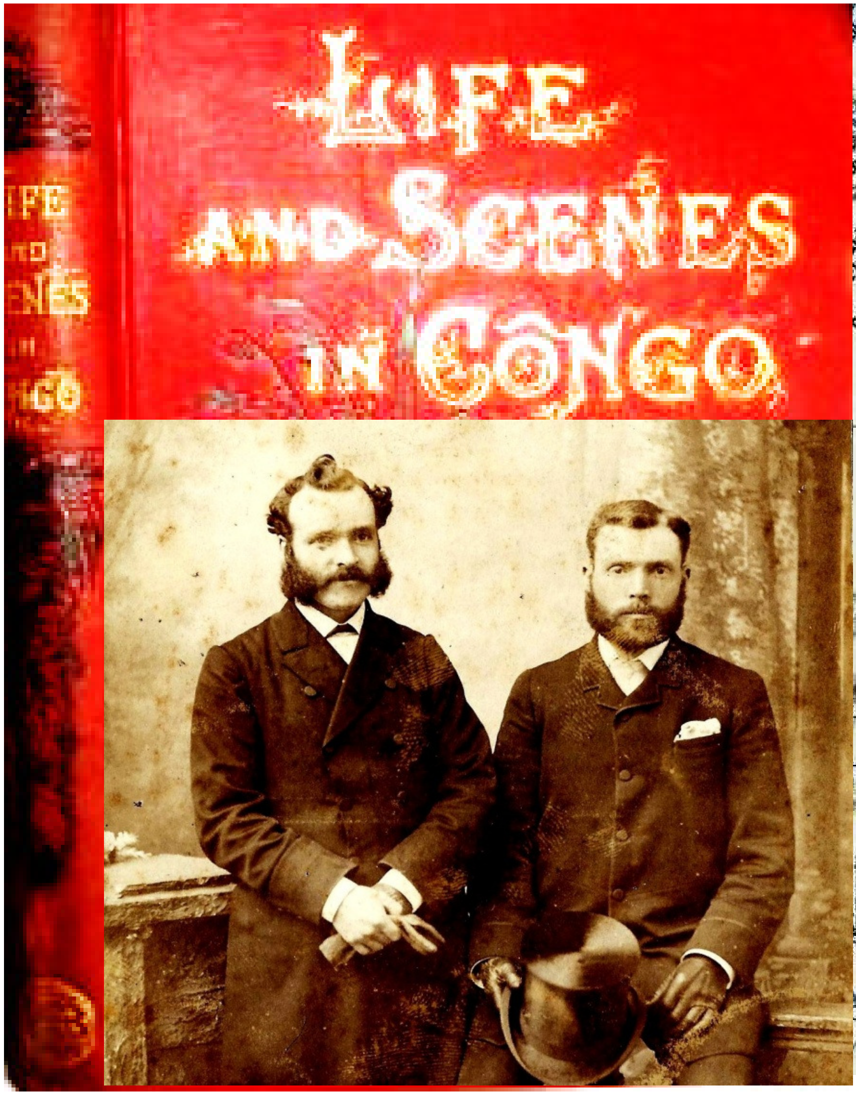
(1) Cheyenne City to Rock Creek: *Union Pacific Railroad*

Cheyenne City

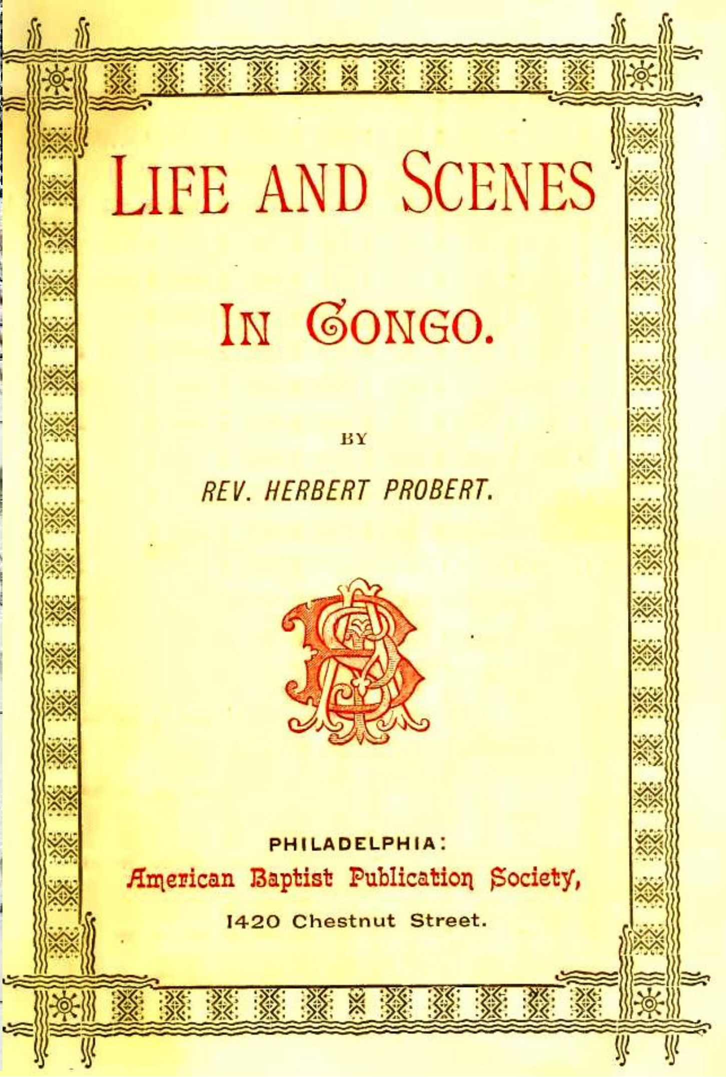
19th C Road-Map – *Rev Herbert E. Probert* – Cheyenne City to Big Horn, Wyoming – 1884

Physical Exploration - 1885 – 1887 : *Rev Herbert E. Probert*

- Travelling from Big Horn, Wyoming, USA to Equatorville, Congo, Central AFRICA -



MARUTU
BAKONGO
KAKONGO
NGOYO
SONYO
Kabinda
LIVINGSTONE R.
Thick Forest
Banana Pt
Padrão Pt



LIFE AND SCENES

IN CONGO.

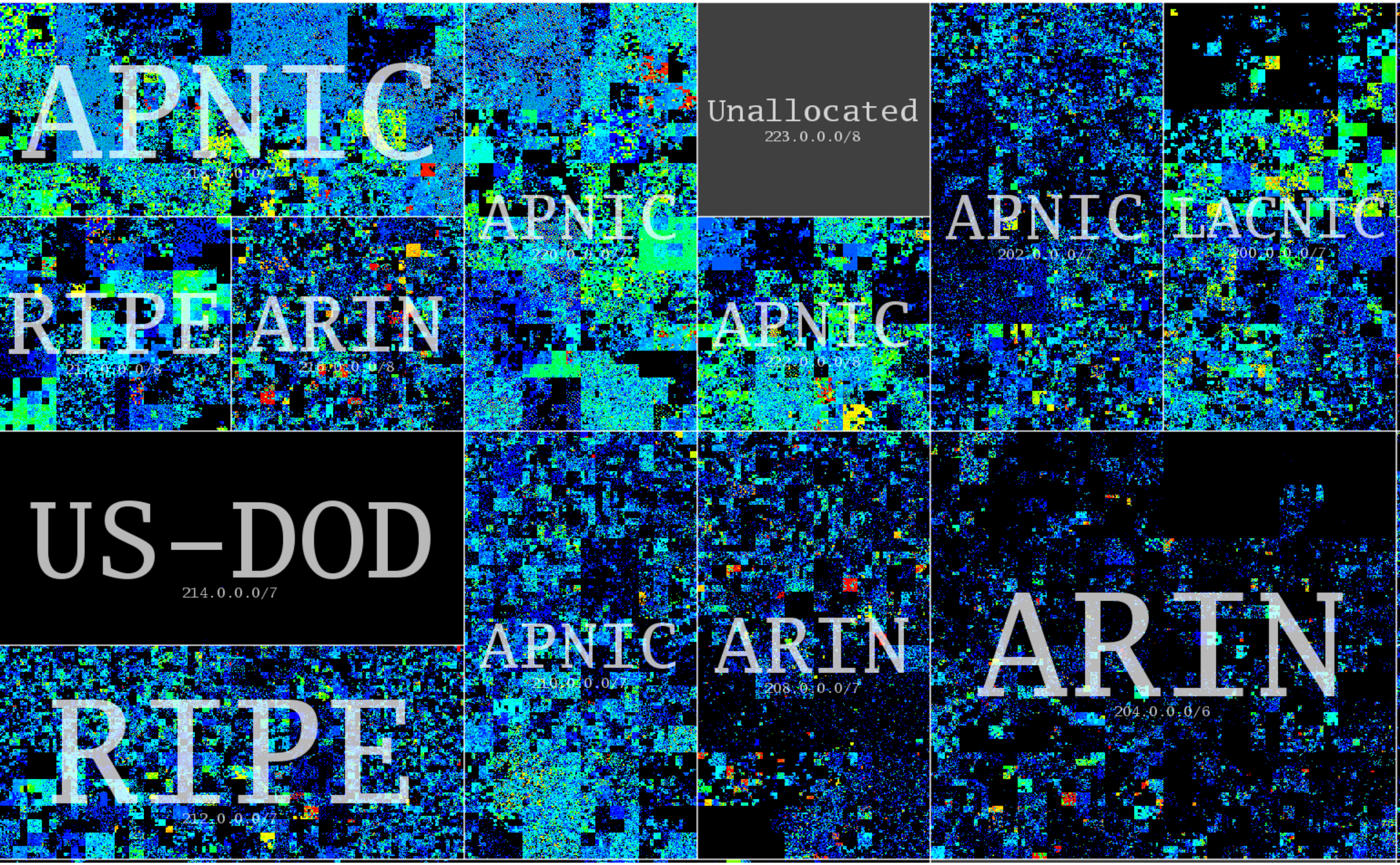
BY

REV. HERBERT PROBERT.

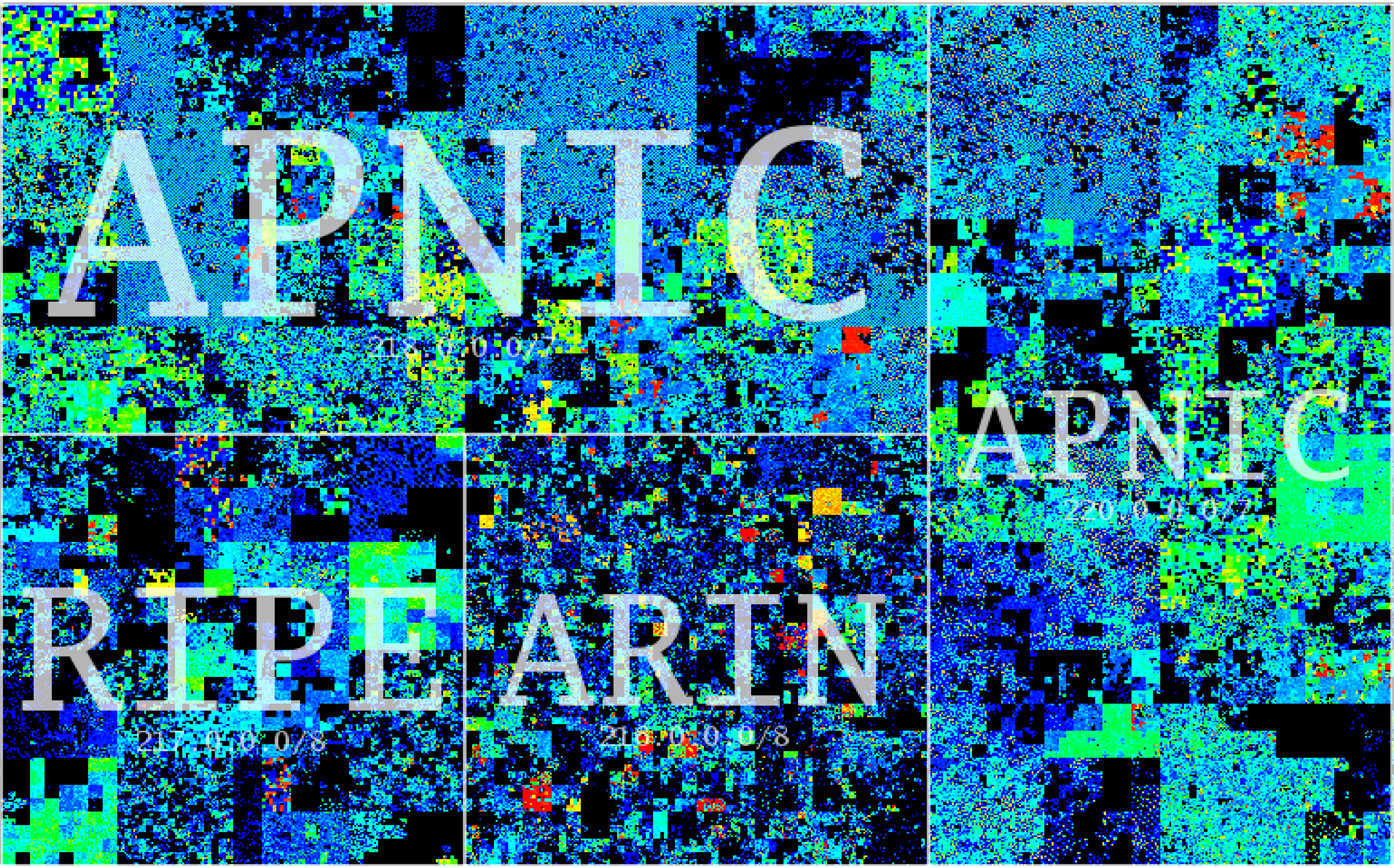
PHILADELPHIA:
American Baptist Publication Society,
1420 Chestnut Street.

"Life and Scenes in Congo" – Published 1889 – Free *eBook* download from: www.archive.org

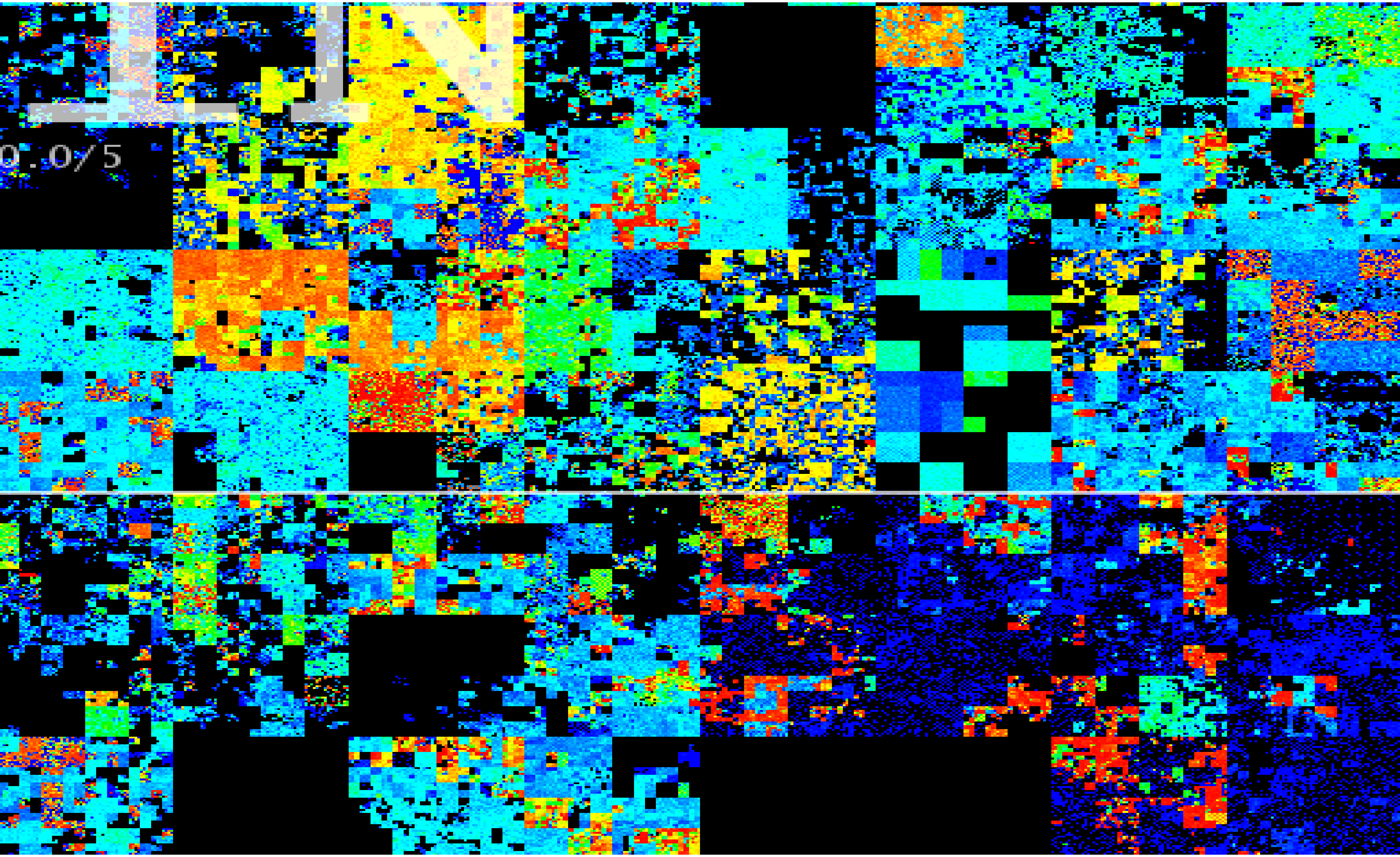
Densely Populated Regions of IP *Cyberspace*



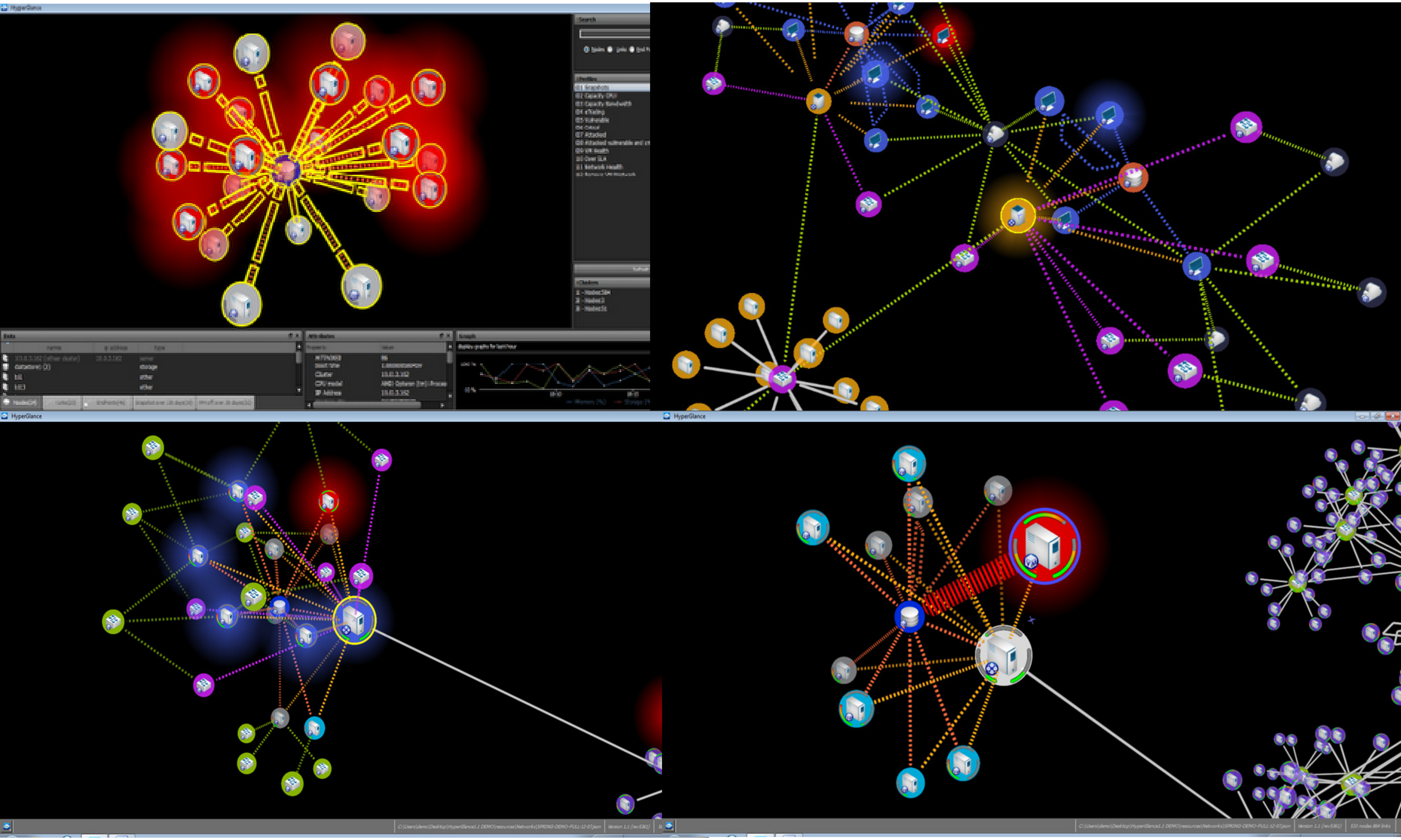
Visual IP Cyberspace: Asia-Pacific, Europe & America



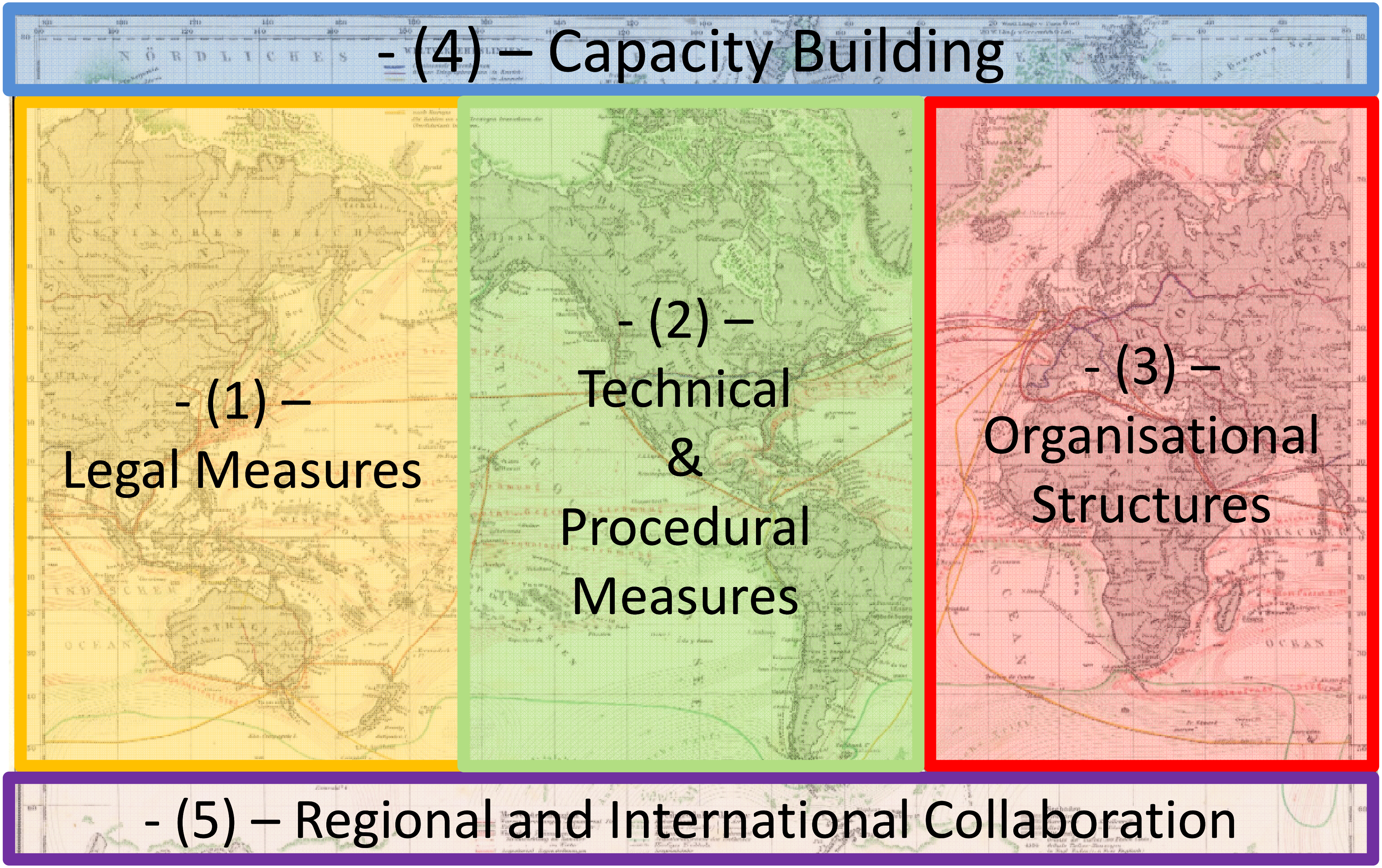
The Challenging Complexity of *Securing IP Cyberspace*



Smart 3D Network Cyber Simulation: *Hyperglance*



Worldwide Security in *Cyberspace*!



- (4) – Capacity Building

- (1) – Legal Measures

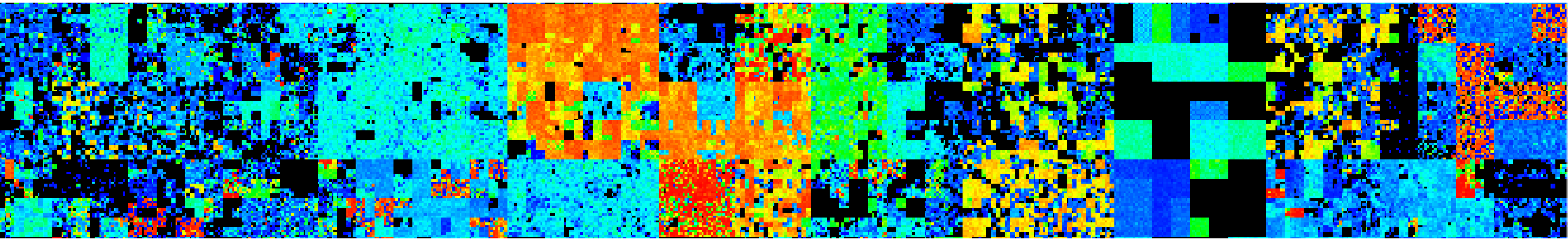
- (2) – Technical & Procedural Measures

- (3) – Organisational Structures

- (5) – Regional and International Collaboration

National Cybersecurity Strategy, Roadmap & Actions

1 – Our Global Cybersecurity Challenge	2 – Developing the UN Cyber Framework	**3 – National Cybersecurity Case Studies**
4 – Dimensions of National Cybersecurity	5 – The UN Global Cyber Agenda (GCA)	6 – Technology, Standards & Operations
7 – New Legislation, Training and Partners	8 –National Roadmap - “Shopping List”	9 – Implementing YOUR Action Plan!



“Smart Security”: *National Cybersecurity Case Studies*

- ***UK Government:*** Cybersecurity Strategy for the UK – Safety, Security & Resilience in Cyberspace (UK Office of Cybersecurity – June 2009)
- ***US Government:*** Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure – May 2009
- ***Canada:*** Canadian Cyber Incident Response Centre (CCIRC) – Integrated within the Strategic Government Operations Centre (GOC)
- ***Australia:*** Australian Cybersecurity Policy and Co-ordination Committee (CSPC – Nov 2009), within the Attorney-General’s Government Dept
- ***Malaysia:*** “Cybersecurity Malaysia” – Mosti : Ministry of Science, Technology & Innovation, and includes the MyCERT & Training Centre
- ***Singapore:*** Cybersecurity Awareness Alliance & the IDA Security Masterplan (Sept 2009) -Singapore Infocomm Technology Security Authority - SITSA
- ***South Korea:*** Korea Internet and Security Agency (KISA – July 2009)
- ***Latin America :*** CITEL/OAS has developed regional cybersecurity strategy
- ***European Union:*** ENISA – European Network and Information Security Agency (September 2005) tackles all aspects of cybersecurity & cybercrime for the EU & Beyond

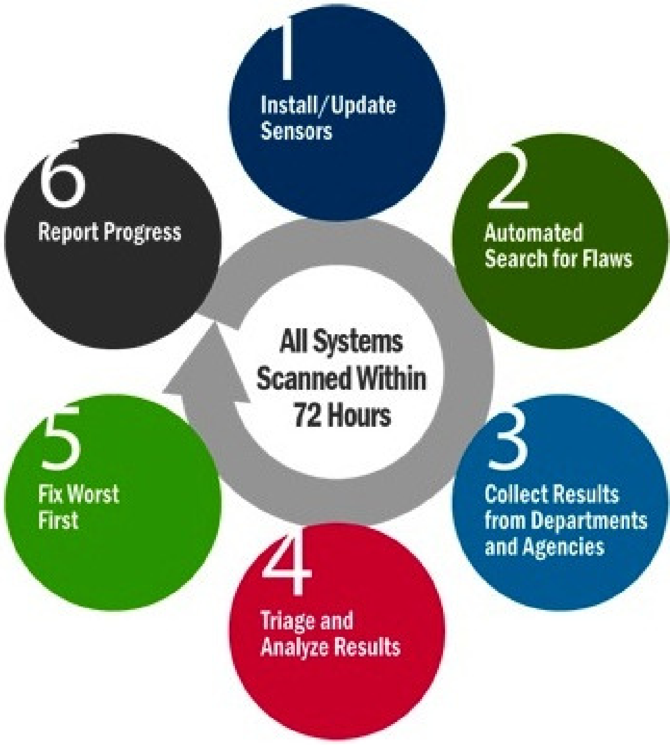
US Government : *Office of Cybersecurity* (CS&C)

- Following the June 2009, US Government Policy Review, the Department of Homeland Security (DHS) has responsibility for hosting the *"Office of Cybersecurity and Communications" (CS&C)*. Within this large organisation is the "*National Cyber Security Division" (NCSD):*

  – *National Cyberspace Response System*
    - National Cyber Alert System
    - US-CERT Operations
    - National Cyber Response Co-ordination Group
    - Cyber Cop Portal (for investigation & prosecution of cyber attacks)

  – *Federal Network Security*
    - Ensuring maximum security of executive civilian offices & agencies
    - National *CDM* Cyber Program – Continuous Diagnostics & Mitigation

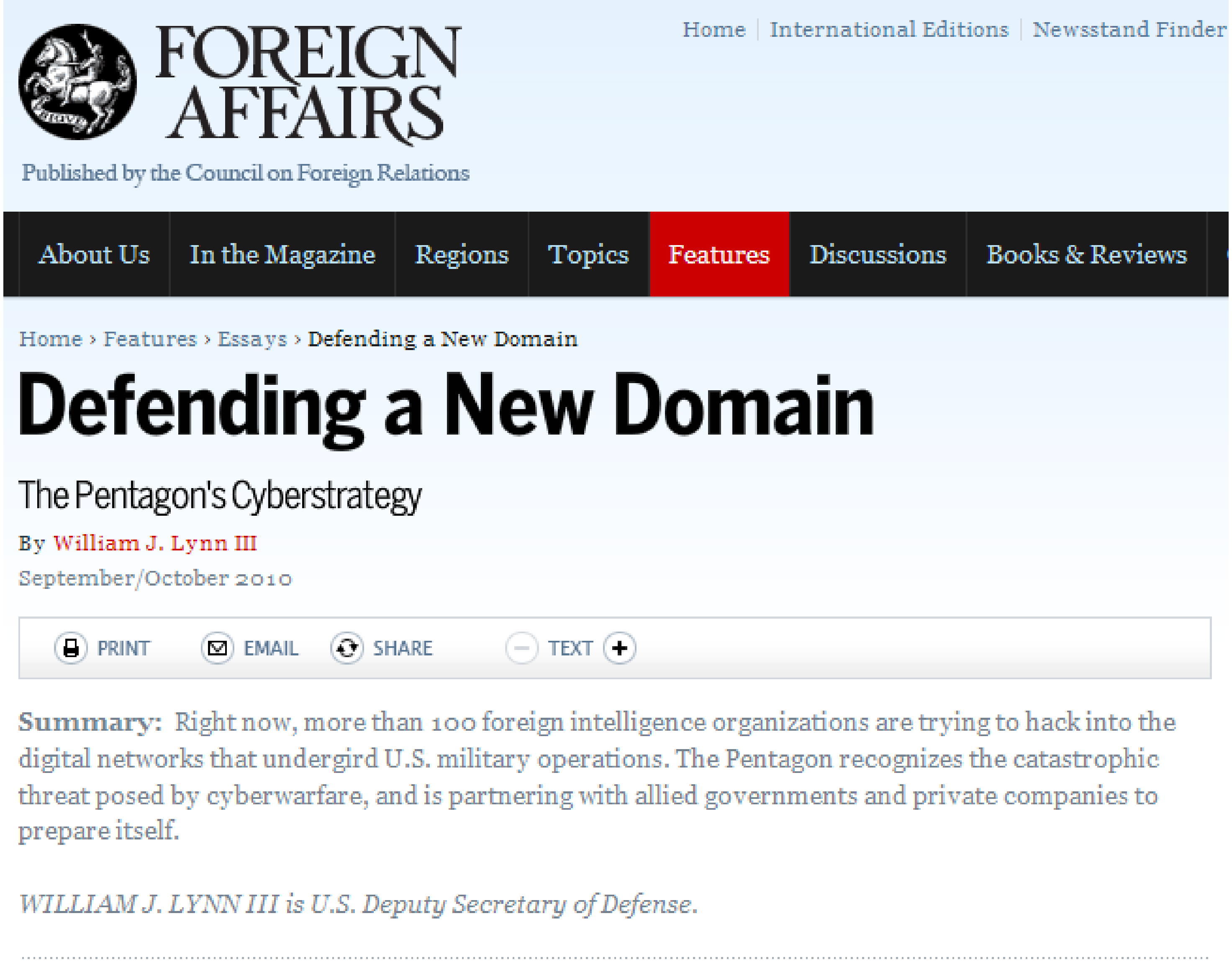
  – *Cyber-Risk Management Programmes*
    - Cyber Exercises: Cyber Storm
    - National Outreach Awareness
    - Software Assurance Program


1 Install/Update Sensors
2 Automated Search for Flaws
3 Collect Results from Departments and Agencies
4 Triage and Analyze Results
5 Fix Worst First
6 Report Progress
All Systems Scanned Within 72 Hours

....The US Government DHS also has a National Cyber Security Center (NCSC) with the mission to protect the US Government's Communications Networks

Evolving Cybersecurity for US Defence:

“The Pentagon’s Cyberstrategy”


FOREIGN AFFAIRS
Published by the Council on Foreign Relations
Home | International Editions | Newsstand Finder
About Us
In the Magazine
Regions
Topics
Features
Discussions
Books & Reviews
Home › Features › Essays › Defending a New Domain
PRINT
EMAIL
SHARE
TEXT

Defending a New Domain

The Pentagon's Cyberstrategy

By William J. Lynn III

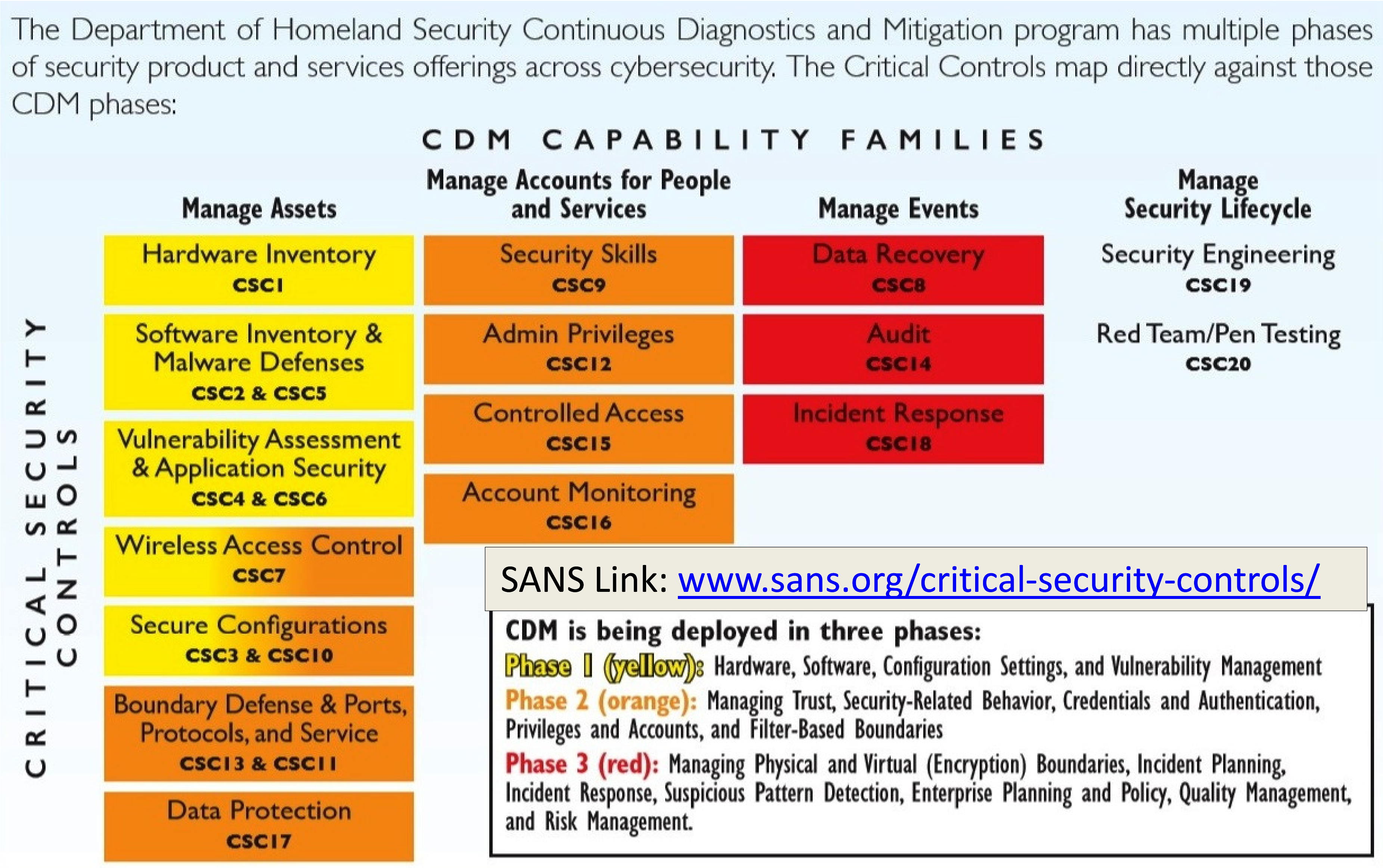
September/October 2010

Summary: Right now, more than 100 foreign intelligence organizations are trying to hack into the digital networks that undergird U.S. military operations. The Pentagon recognizes the catastrophic threat posed by cyberwarfare, and is partnering with allied governments and private companies to prepare itself.

WILLIAM J. LYNN III is U.S. Deputy Secretary of Defense.

Mapping the *SANS* Critical Security Controls:

US Govt – Dept of Homeland Security CDM Program -



The Department of Homeland Security Continuous Diagnostics and Mitigation program has multiple phases of security product and services offerings across cybersecurity. The Critical Controls map directly against those CDM phases:

CDM CAPABILITY FAMILIES

CRITICAL SECURITY CONTROLS

Manage Assets	Manage Accounts for People and Services	Manage Events	Manage Security Lifecycle
Hardware Inventory **CSC1**	Security Skills **CSC9**	Data Recovery **CSC8**	Security Engineering **CSC19**
Software Inventory & Malware Defenses **CSC2 & CSC5**	Admin Privileges **CSC12**	Audit **CSC14**	Red Team/Pen Testing **CSC20**
Vulnerability Assessment & Application Security **CSC4 & CSC6**	Controlled Access **CSC15**	Incident Response **CSC18**	
Wireless Access Control **CSC7**	Account Monitoring **CSC16**		
Secure Configurations **CSC3 & CSC10**			
Boundary Defense & Ports, Protocols, and Service **CSC13 & CSC11**			
Data Protection **CSC17**			

SANS Link: www.sans.org/critical-security-controls/

CDM is being deployed in three phases:

Phase I (yellow): Hardware, Software, Configuration Settings, and Vulnerability Management

Phase 2 (orange): Managing Trust, Security-Related Behavior, Credentials and Authentication, Privileges and Accounts, and Filter-Based Boundaries

Phase 3 (red): Managing Physical and Virtual (Encryption) Boundaries, Incident Planning, Incident Response, Suspicious Pattern Detection, Enterprise Planning and Policy, Quality Management, and Risk Management.

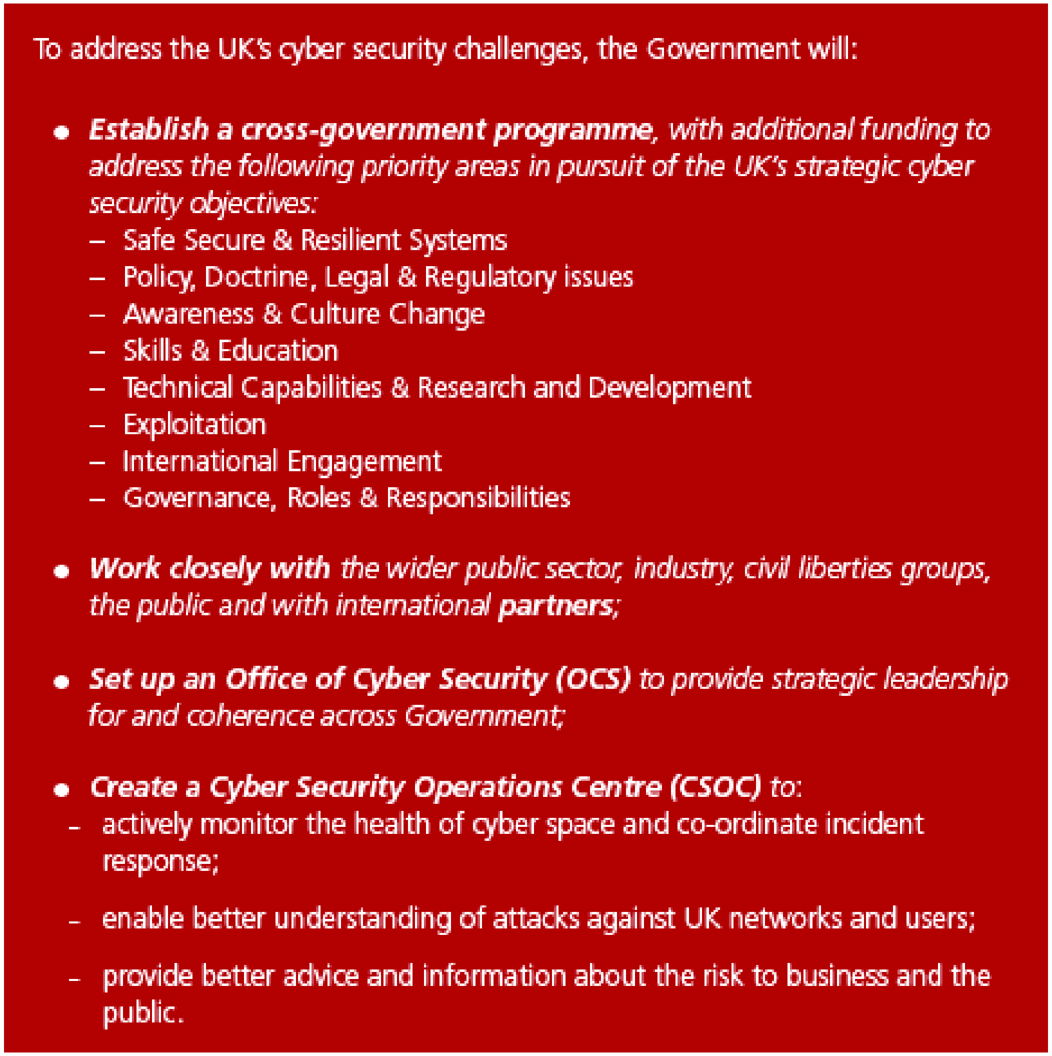
Canadian Government : *CCIRC*

- *The Canadian Cyber Incident Response Centre (CCIRC)* monitors the cyber threat environment around the clock and is responsible for coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber incidents. The Centre is a part of the Government Operations Centre and a key component of the government's all-hazards approach to national security and emergency preparedness.

- *Critical Infrastructure Role:* CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals and managers of critical infrastructure and other related industries.

UK Office of Cybersecurity – OCS & CSOC

Cyber Security Strategy of the United Kingdom
safety, security and resilience in cyber space
OCS
UK Office of Cyber Security
CSOC
UK Cyber Security Operations Centre



To address the UK's cyber security challenges, the Government will:

- ***Establish a cross-government programme**, with additional funding to address the following priority areas in pursuit of the UK's strategic cyber security objectives:*
  - Safe Secure & Resilient Systems
  - Policy, Doctrine, Legal & Regulatory issues
  - Awareness & Culture Change
  - Skills & Education
  - Technical Capabilities & Research and Development
  - Exploitation
  - International Engagement
  - Governance, Roles & Responsibilities
- ***Work closely with** the wider public sector, industry, civil liberties groups, the public and with international **partners**;*
- ***Set up an Office of Cyber Security (OCS)** to provide strategic leadership for and coherence across Government;*
- ***Create a Cyber Security Operations Centre (CSOC)** to:*
  - actively monitor the health of cyber space and co-ordinate incident response;
  - enable better understanding of attacks against UK networks and users;
  - provide better advice and information about the risk to business and the public.

Australian Government : *CSPC*

- *The **Cyber Security Policy and Coordination (CSPC) Committee*** is the Australian Government committee that coordinates the development of cyber security policy for the Australian Government. The CSPC Committee:
  - Provides whole of government strategic leadership on cyber security
  - Determines priorities for the Australian Government
  - Coordinates the response to cyber security events
  - Coordinates Australian Government cyber security policy internationally.

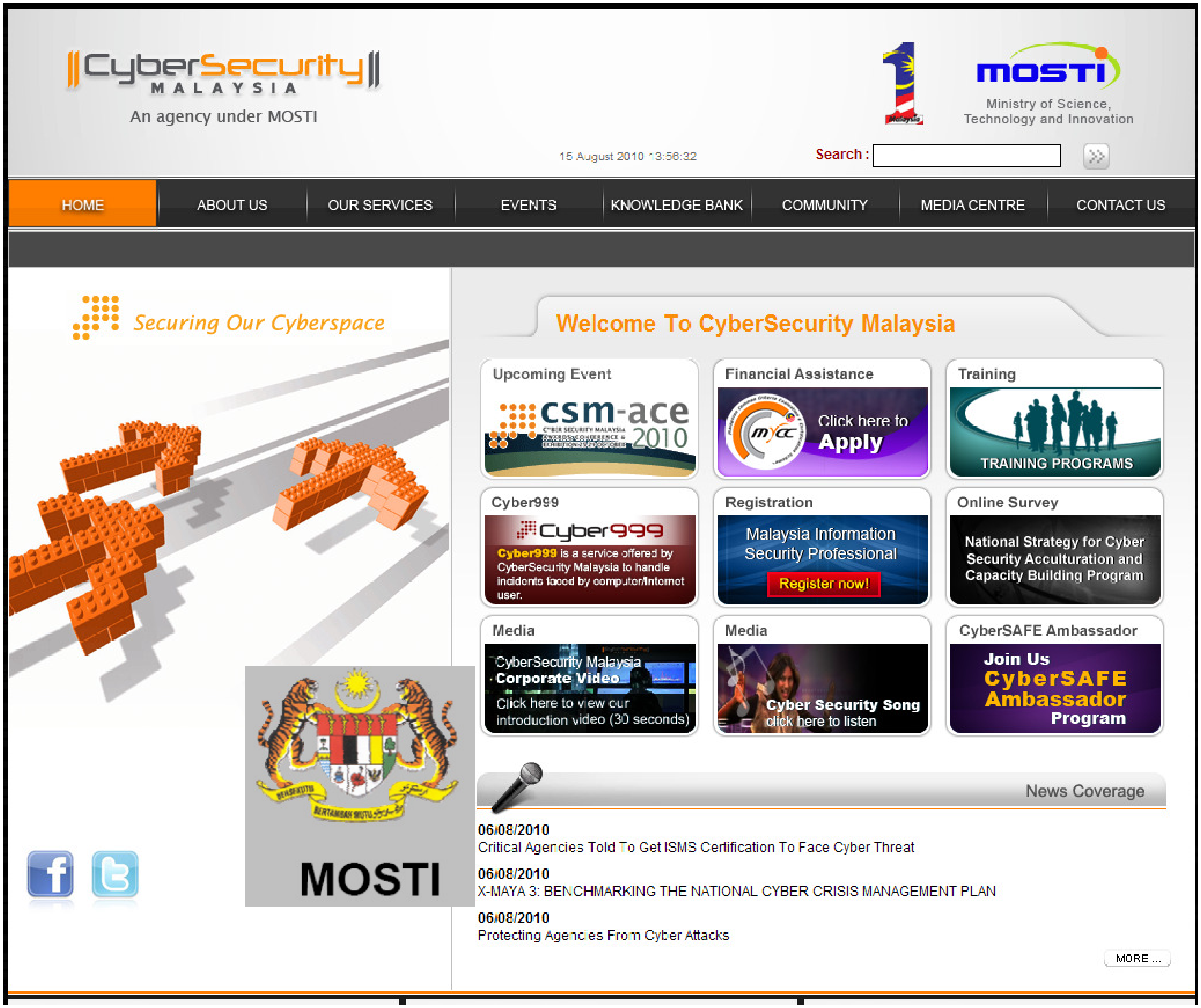
Cyber Security Operations Centre (CSOC)

Australian Government

CERT Australia

AUSTRALIA'S NATIONAL
COMPUTER EMERGENCY RESPONSE TEAM

Malaysian Government: *MOSTi*



CyberSecurity MALAYSIA

An agency under MOSTI

MOSTI Ministry of Science, Technology and Innovation

15 August 2010 13:56:32

Search :

HOME | ABOUT US | OUR SERVICES | EVENTS | KNOWLEDGE BANK | COMMUNITY | MEDIA CENTRE | CONTACT US

Securing Our Cyberspace

Welcome To CyberSecurity Malaysia

Upcoming Event: csm-ace 2010

Financial Assistance: Click here to Apply

Training: TRAINING PROGRAMS

Cyber999: Cyber999 is a service offered by CyberSecurity Malaysia to handle incidents faced by computer/Internet user.

Registration: Malaysia Information Security Professional — Register now!

Online Survey: National Strategy for Cyber Security Acculturation and Capacity Building Program

Media: CyberSecurity Malaysia Corporate Video — Click here to view our introduction video (30 seconds)

Media: Cyber Security Song — click here to listen

CyberSAFE Ambassador: Join Us CyberSAFE Ambassador Program

MOSTI

News Coverage

06/08/2010
Critical Agencies Told To Get ISMS Certification To Face Cyber Threat

06/08/2010
X-MAYA 3: BENCHMARKING THE NATIONAL CYBER CRISIS MANAGEMENT PLAN

06/08/2010
Protecting Agencies From Cyber Attacks

MORE ...

Phishing and Identity Theft

PHISHING SCAM

PHISHING SPAM is an act of getting someone into providing private information such as credit card numbers, bank account information, etc. through email, pop-up messages and websites that appear to be legitimate.

HOW TO PROTECT YOURSELF?

- Don't reply to emails asking for personal or financial information
- Use an antivirus and firewall software
- Don't email personal or financial information
- Be careful of downloading any attachments or files from emails
- Don't follow links in emails

Let's Make The Internet A Safer Place
www.esecurity.org.my

CyberSecurity MALAYSIA

ISMS

An agency under
MOSTI

CyberSecurity Malaysia

Level 7, Sapura @ Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan
Tel: +6 03 89926888 Fax: +6 03 89453205 | www.cybersecurity.my |

IDENTITY THEFT

HOW TO PROTECT YOURSELF?

- Do not send personal information to unknown websites
- Do not respond to unknown emails
- If shopping online, know your sources
- Read website's privacy statement carefully
- Post your resumes only on prominent jobsites
- Always LOG OFF your computer when not in use!

Let's Make The Internet A Safer Place
www.esecurity.org.my

CyberSecurity MALAYSIA

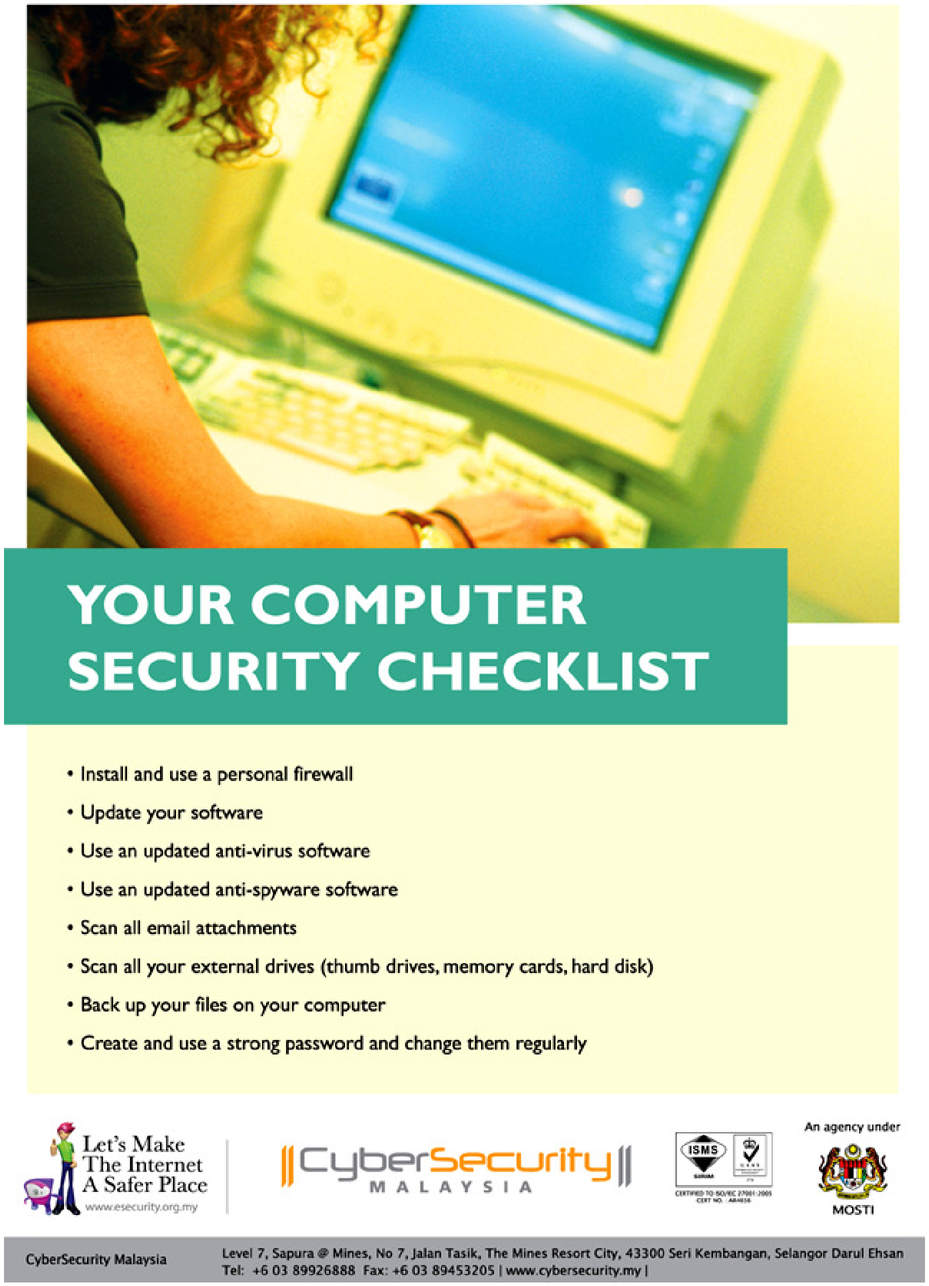
ISMS

An agency under
MOSTI

CyberSecurity Malaysia

Level 7, Sapura @ Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan
Tel: +6 03 89926888 Fax: +6 03 89453205 | www.cybersecurity.my |

Security Checklist & Malware



YOUR COMPUTER SECURITY CHECKLIST

- Install and use a personal firewall
- Update your software
- Use an updated anti-virus software
- Use an updated anti-spyware software
- Scan all email attachments
- Scan all your external drives (thumb drives, memory cards, hard disk)
- Back up your files on your computer
- Create and use a strong password and change them regularly

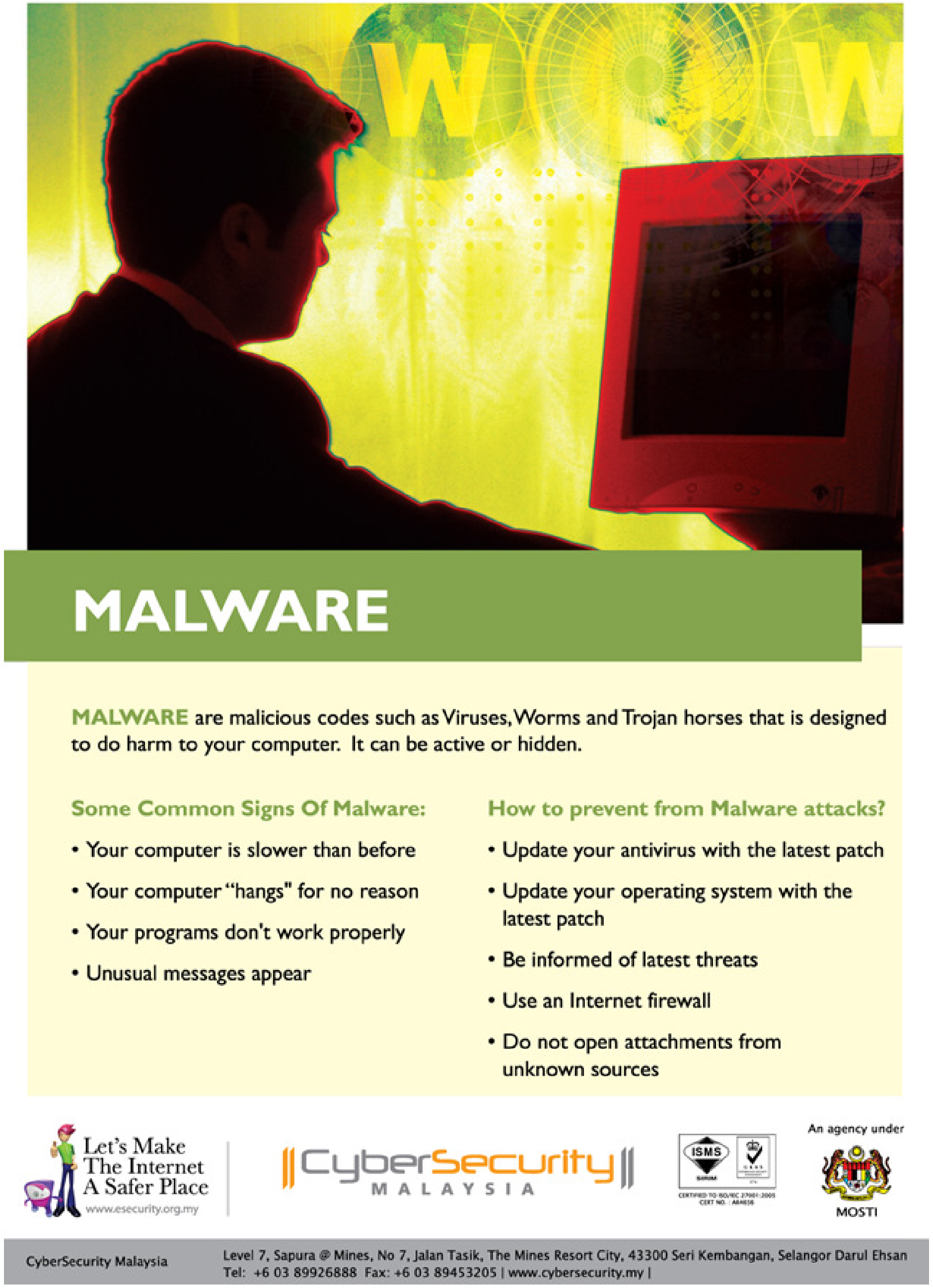
Let's Make The Internet A Safer Place
www.esecurity.org.my

CyberSecurity MALAYSIA

ISMS

An agency under MOSTI

CyberSecurity Malaysia
Level 7, Sapura @ Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan
Tel: +6 03 89926888 Fax: +6 03 89453205 | www.cybersecurity.my |



MALWARE

MALWARE are malicious codes such as Viruses, Worms and Trojan horses that is designed to do harm to your computer. It can be active or hidden.

Some Common Signs Of Malware:

- Your computer is slower than before
- Your computer "hangs" for no reason
- Your programs don't work properly
- Unusual messages appear

How to prevent from Malware attacks?

- Update your antivirus with the latest patch
- Update your operating system with the latest patch
- Be informed of latest threats
- Use an Internet firewall
- Do not open attachments from unknown sources

Let's Make The Internet A Safer Place
www.esecurity.org.my

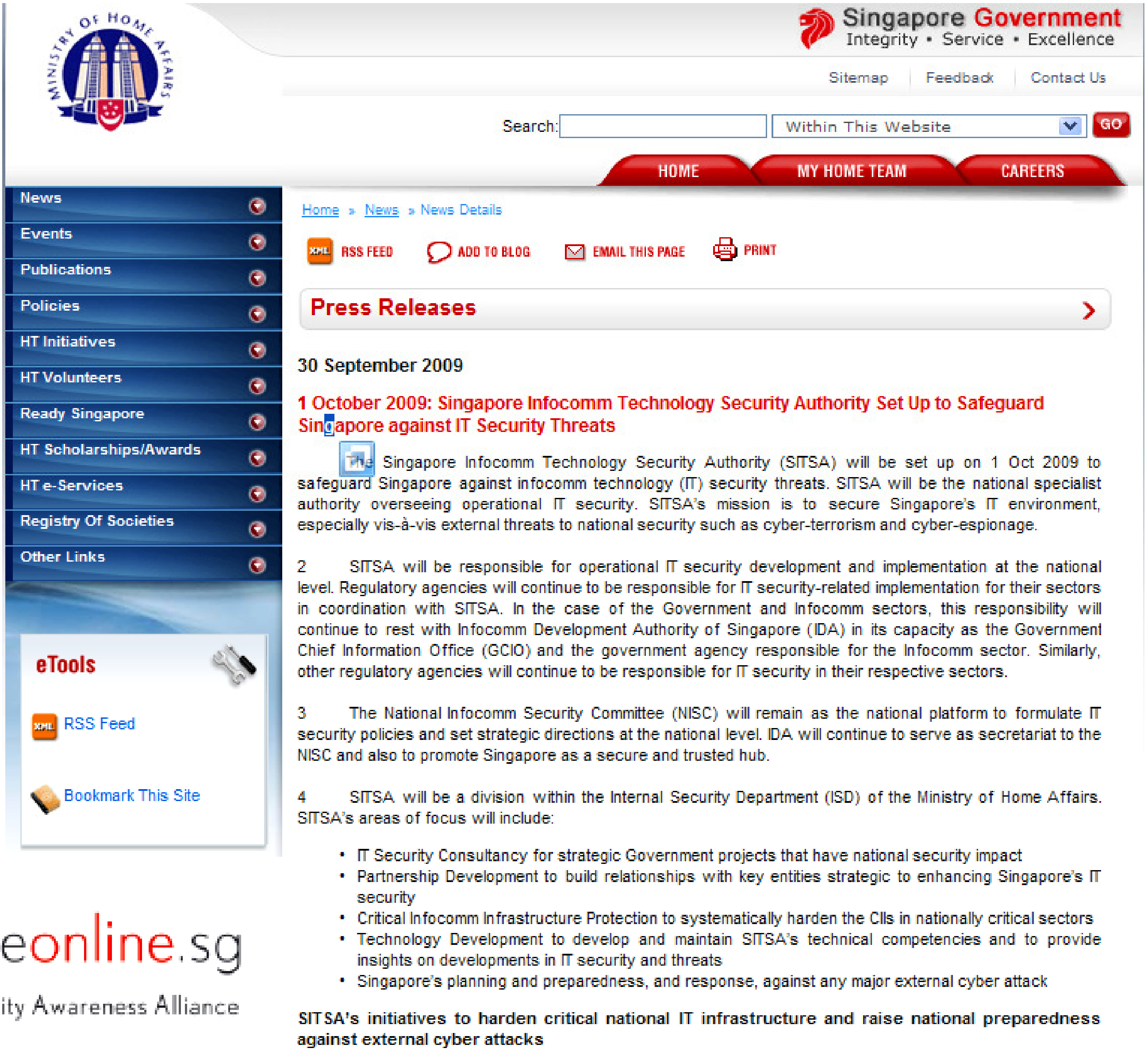
CyberSecurity MALAYSIA

ISMS

An agency under MOSTI

CyberSecurity Malaysia
Level 7, Sapura @ Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan
Tel: +6 03 89926888 Fax: +6 03 89453205 | www.cybersecurity.my |

Singapore Government : *SITSA*



Press Releases

30 September 2009

1 October 2009: Singapore Infocomm Technology Security Authority Set Up to Safeguard Singapore against IT Security Threats

The Singapore Infocomm Technology Security Authority (SITSA) will be set up on 1 Oct 2009 to safeguard Singapore against infocomm technology (IT) security threats. SITSA will be the national specialist authority overseeing operational IT security. SITSA's mission is to secure Singapore's IT environment, especially vis-à-vis external threats to national security such as cyber-terrorism and cyber-espionage.

2 SITSA will be responsible for operational IT security development and implementation at the national level. Regulatory agencies will continue to be responsible for IT security-related implementation for their sectors in coordination with SITSA. In the case of the Government and Infocomm sectors, this responsibility will continue to rest with Infocomm Development Authority of Singapore (IDA) in its capacity as the Government Chief Information Office (GCIO) and the government agency responsible for the Infocomm sector. Similarly, other regulatory agencies will continue to be responsible for IT security in their respective sectors.

3 The National Infocomm Security Committee (NISC) will remain as the national platform to formulate IT security policies and set strategic directions at the national level. IDA will continue to serve as secretariat to the NISC and also to promote Singapore as a secure and trusted hub.

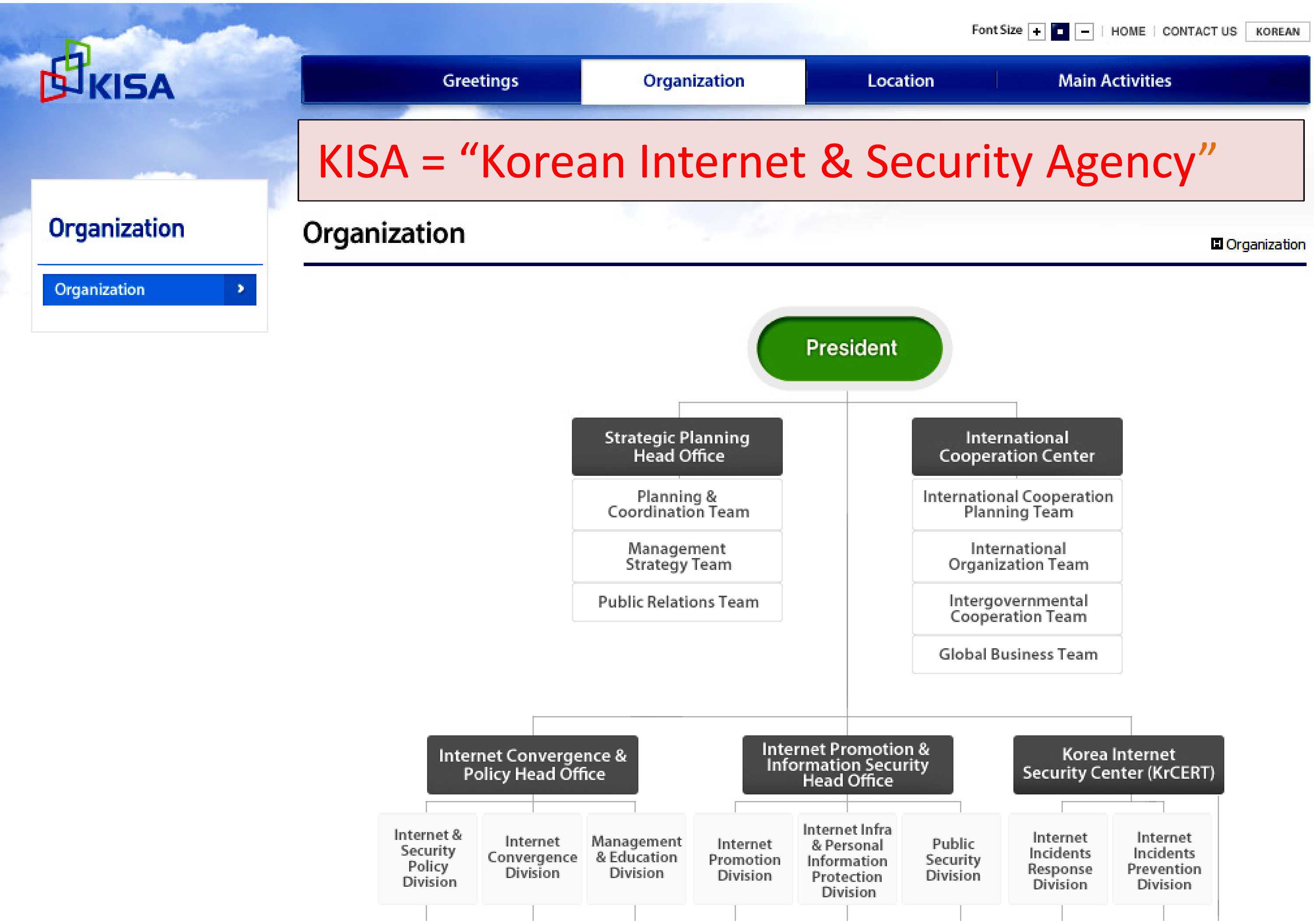
4 SITSA will be a division within the Internal Security Department (ISD) of the Ministry of Home Affairs. SITSA's areas of focus will include:

- IT Security Consultancy for strategic Government projects that have national security impact
- Partnership Development to build relationships with key entities strategic to enhancing Singapore's IT security
- Critical Infocomm Infrastructure Protection to systematically harden the CIIs in nationally critical sectors
- Technology Development to develop and maintain SITSA's technical competencies and to provide insights on developments in IT security and threats
- Singapore's planning and preparedness, and response, against any major external cyber attack

SITSA's initiatives to harden critical national IT infrastructure and raise national preparedness against external cyber attacks

GOsafeonline.sg
Cyber Security Awareness Alliance

South Korea Government: *KISA*



KISA = "Korean Internet & Security Agency"

President

Strategic Planning Head Office

- Planning & Coordination Team
- Management Strategy Team
- Public Relations Team

International Cooperation Center

- International Cooperation Planning Team
- International Organization Team
- Intergovernmental Cooperation Team
- Global Business Team

Internet Convergence & Policy Head Office

- Internet & Security Policy Division
- Internet Convergence Division
- Management & Education Division

Internet Promotion & Information Security Head Office

- Internet Promotion Division
- Internet Infra & Personal Information Protection Division
- Public Security Division

Korea Internet Security Center (KrCERT)

- Internet Incidents Response Division
- Internet Incidents Prevention Division

- Spam Response Team
- Web Security Team
- PC Security Team

- Network Monitoring Team
- Hacking Response Team
- Code Analysis Team
- Response & Security Planning Team

- Knowledge & Information Security Industry Team
- Electronic Signature & Authentication Team
- Security Evaluation Team
- Public Security Service Team
- Public Security Planning Team

- Internet User Right Protection Team
- Internet Service Protection Team
- Enterprise Information Security Management Team
- Personal Information Protection Technology Team
- Personal Information Protection Planning Team

- System Management Team (KRNIC)
- Internet Name Policy Team (KRNIC)
- IP Policy & Management Team (KRNIC)
- Internet Ethics Team
- Internet Planning Team

- KISA Academy Team
- General Administration Team
- Human Resource Management Team

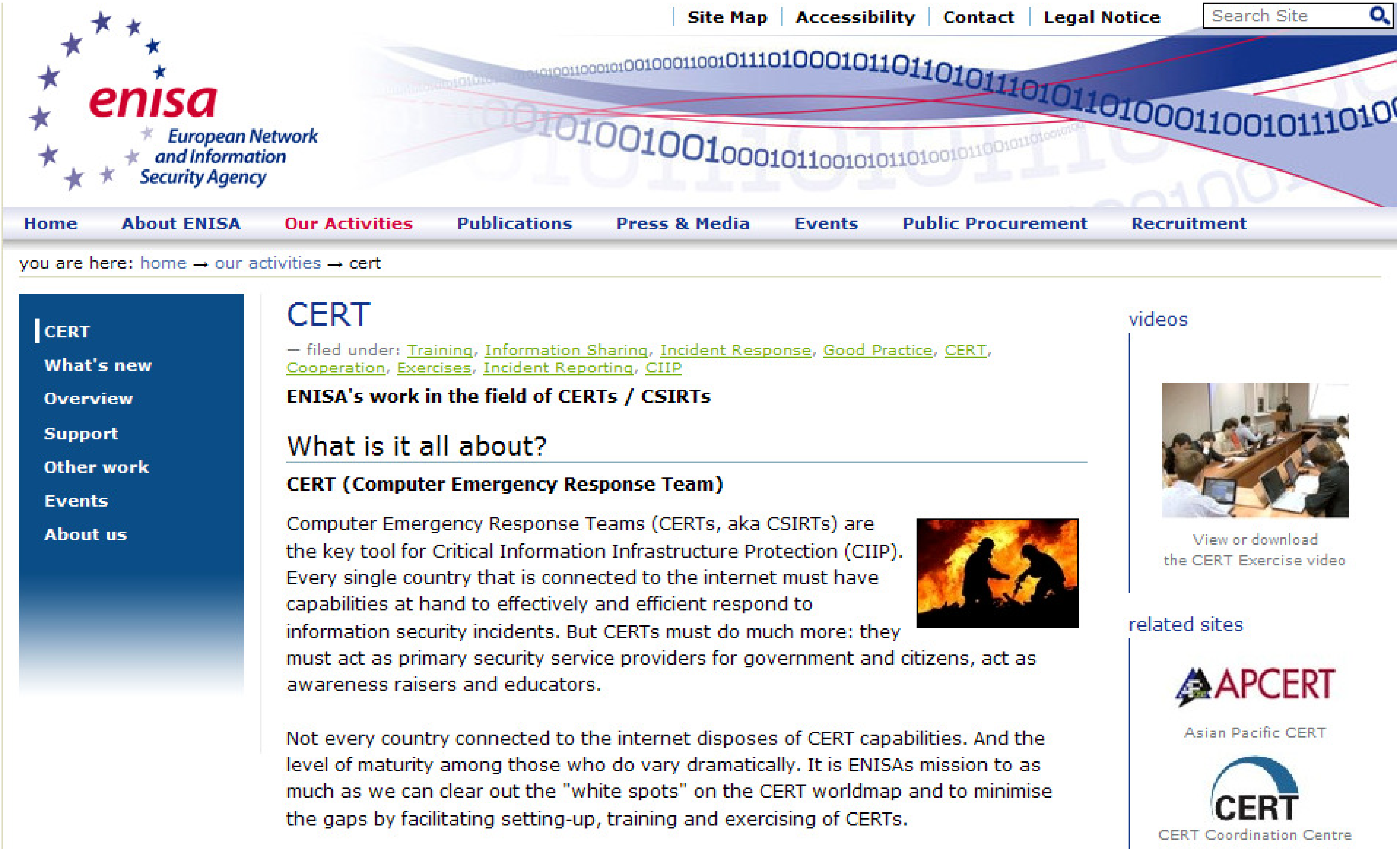
- Convergence Security R&D Team
- Wireless Internet Team
- New Business Contents Team
- Future Internet Team

- Legal Research Team
- Research & Analysis Team
- Policy Development Team

KISA : Korea Internet & Security Agency

- KISA(Korea Internet & Security Agency) was established as the public corporation responsible for managing the Internet of Korea on July 23th, 2009, by merging three institutes NIDA, KISA, and KIICA.
  - NIDA(National Internet Development Agency of Korea)
  - KISA(Korean Information Security Agency)
  - KIICA(Korea IT International Cooperation Agency)
- KISA has the following roles:
  - Protects Internet infrastructure from hacking cyber-terror, spam and other malicious activities
  - Operates krCERT CC (Korea Computer Emergency Response Team Coordination Center) to improve Internet security in Korea
  - Supporting international organizations such as ITU and OECD and assisting Korean IT companies
  - Specifically, KISA manages the Internet address resources such as IP address and .kr domain name as the national NIC (Network Information Center), and also researches for the next generation Internet address resources of Korea.

European Network and Information Security Agency: *enisa*



you are here: home → our activities → cert

CERT

— filed under: Training, Information Sharing, Incident Response, Good Practice, CERT, Cooperation, Exercises, Incident Reporting, CIIP

ENISA's work in the field of CERTs / CSIRTs

What is it all about?

CERT (Computer Emergency Response Team)

Computer Emergency Response Teams (CERTs, aka CSIRTs) are the key tool for Critical Information Infrastructure Protection (CIIP). Every single country that is connected to the internet must have capabilities at hand to effectively and efficient respond to information security incidents. But CERTs must do much more: they must act as primary security service providers for government and citizens, act as awareness raisers and educators.

Not every country connected to the internet disposes of CERT capabilities. And the level of maturity among those who do vary dramatically. It is ENISAs mission to as much as we can clear out the "white spots" on the CERT worldmap and to minimise the gaps by facilitating setting-up, training and exercising of CERTs.

View or download the CERT Exercise video

Asian Pacific CERT

CERT Coordination Centre

National Cybersecurity for Latin America & Caribbean:
- CITEL/CICTE/OAS -

- Within Latin America & Caribbean, CITEL, CICTE and the OAS are working together on Regional Cybersecurity Strategy, Plans & Programmes with UN/ITU support:
- CITEL = Inter-American Telecomms Commission
- CICTE = Inter-American Committee against Terrorism
- OAS = Organisation of American States

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

- Antigua and Barbuda
- Argentina
- Barbados
- Belize
- Bolivia
- Brazil
- Canada
- Chile
- Colombia
- Costa Rica
- Cuba [1]
- Dominica (Commonwealth of)
- Dominican Republic
- Ecuador
- El Salvador
- Grenada
- Guatemala
- Guyana
- Haiti
- Honduras [2]
- Jamaica
- Mexico
- Nicaragua
- Panama
- Paraguay
- Peru
- Saint Kitts and Nevis
- Saint Lucia
- Saint Vincent and the Grenadines
- Suriname
- The Bahamas (Commonwealth of)
- Trinidad and Tobago
- United States of America
- Uruguay
- Venezuela (Bolivarian Republic of)

Organización de los Estados Americanos
CITEL
Comisión Interamericana de Telecomunicaciones
CITEL
Portal » CITEL

National Cybersecurity Agencies: Common Roles

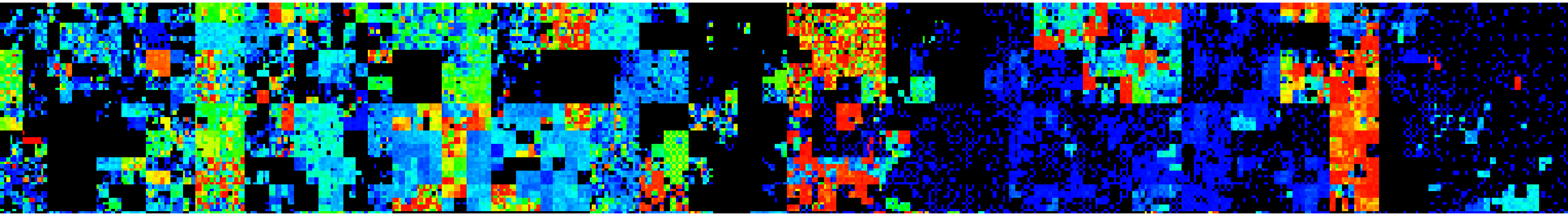
- Common roles and responsibilities for all these national cyber agencies:

  - *Cyber Alerts:* Management of the National Response to Cyber Alerts, and Attacks
  - *Education:* Co-ordination of the National Awareness and Skills Training Programmes
  - *Laws:* Leadership role in the development and approval of new cyber legislation
  - *Cybercrime:* Facilitation for building a National Cybercrime of e-Crime Unit
  - *Standards:* Setting the national cybersecurity standards and auditing compliance
  - *International:* Leadership in the promotion of international partnerships for
  - *Research:* Support for research & development into cybersecurity technologies
  - *Critical Sectors:* Co-ordination of National Programmes for Critical Infrastructure
  - *Integration* with National Physical Defence Resources – both Civilian and Military

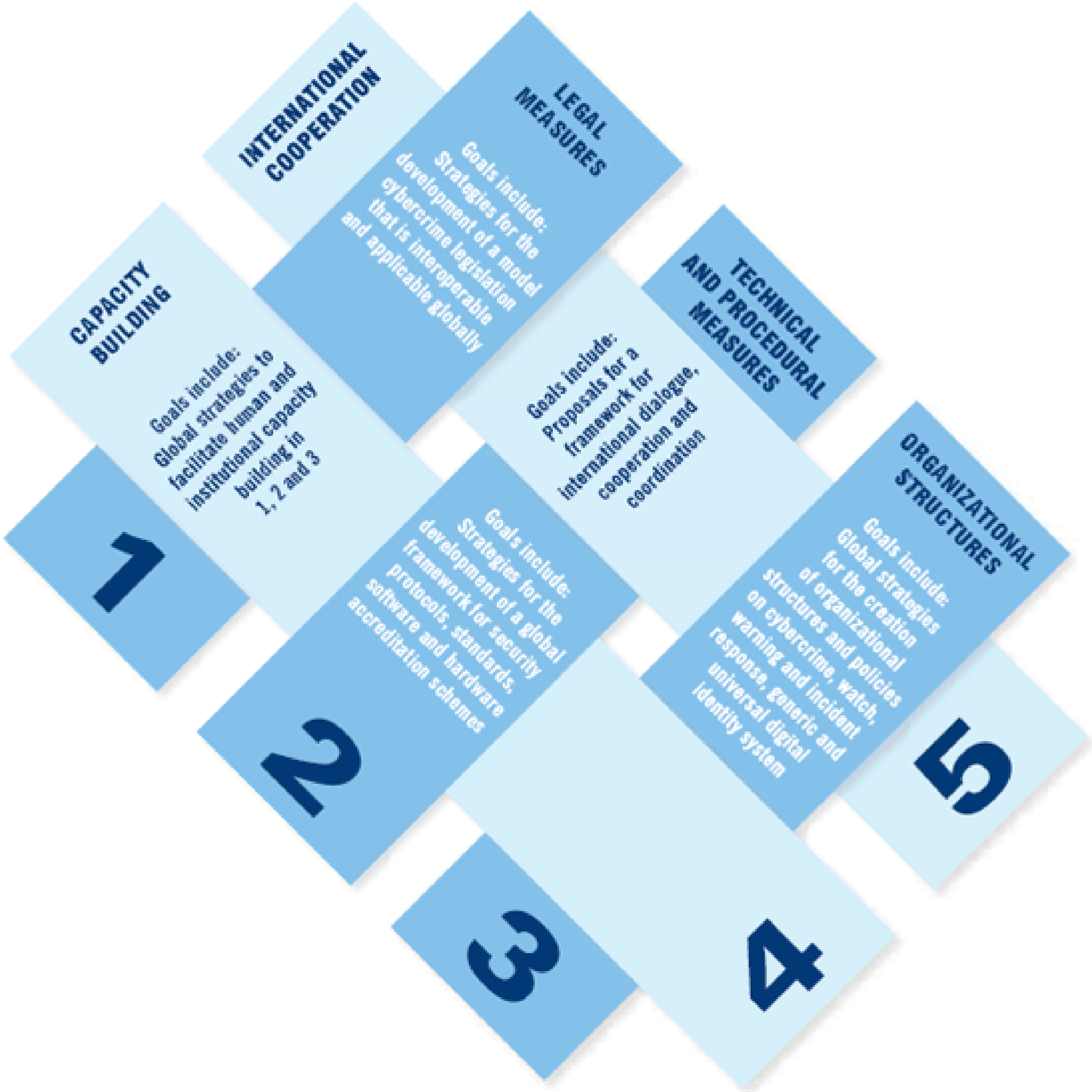
...Next we consider the major benefits from Integrated Physical Security and Cybersecurity = "Smart Security"!.....

National Cybersecurity Strategy, Roadmap & Actions

1 – Our Global Cybersecurity Challenge	2 – Developing the UN Cyber Framework	3 – National Cybersecurity Case Studies
4 – Dimensions of National Cybersecurity	5 – The UN Global Cyber Agenda (GCA)	6 – Technology, Standards & Operations
7 – New Legislation, Training and Partners	8 – National Roadmap - "Shopping List"	9 – Implementing YOUR Action Plan!



UN/ITU:– *Global Cybersecurity Agenda (GCA)*



INTERNATIONAL COOPERATION
LEGAL MEASURES
Goals include: Strategies for the development of a model cybercrime legislation that is interoperable and applicable globally
CAPACITY BUILDING
Goals include: Global strategies to facilitate human and institutional capacity building in 1, 2 and 3
TECHNICAL AND PROCEDURAL MEASURES
Goals include: Proposals for a framework for international dialogue, cooperation and coordination
1
Goals include: Strategies for the development of a global framework for security protocols, standards, software and hardware accreditation schemes
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
2
5
3
4

The UN/ITU GCA - Global Cybersecurity Agenda:

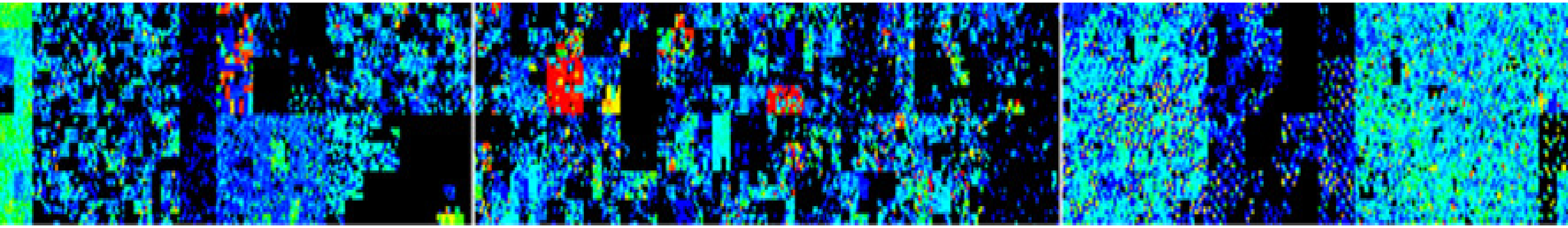
----

1 – Legal Measures
2 – Technical Measures
3 – Organisational Measures
4 – Capacity Building
5 – International Cooperation

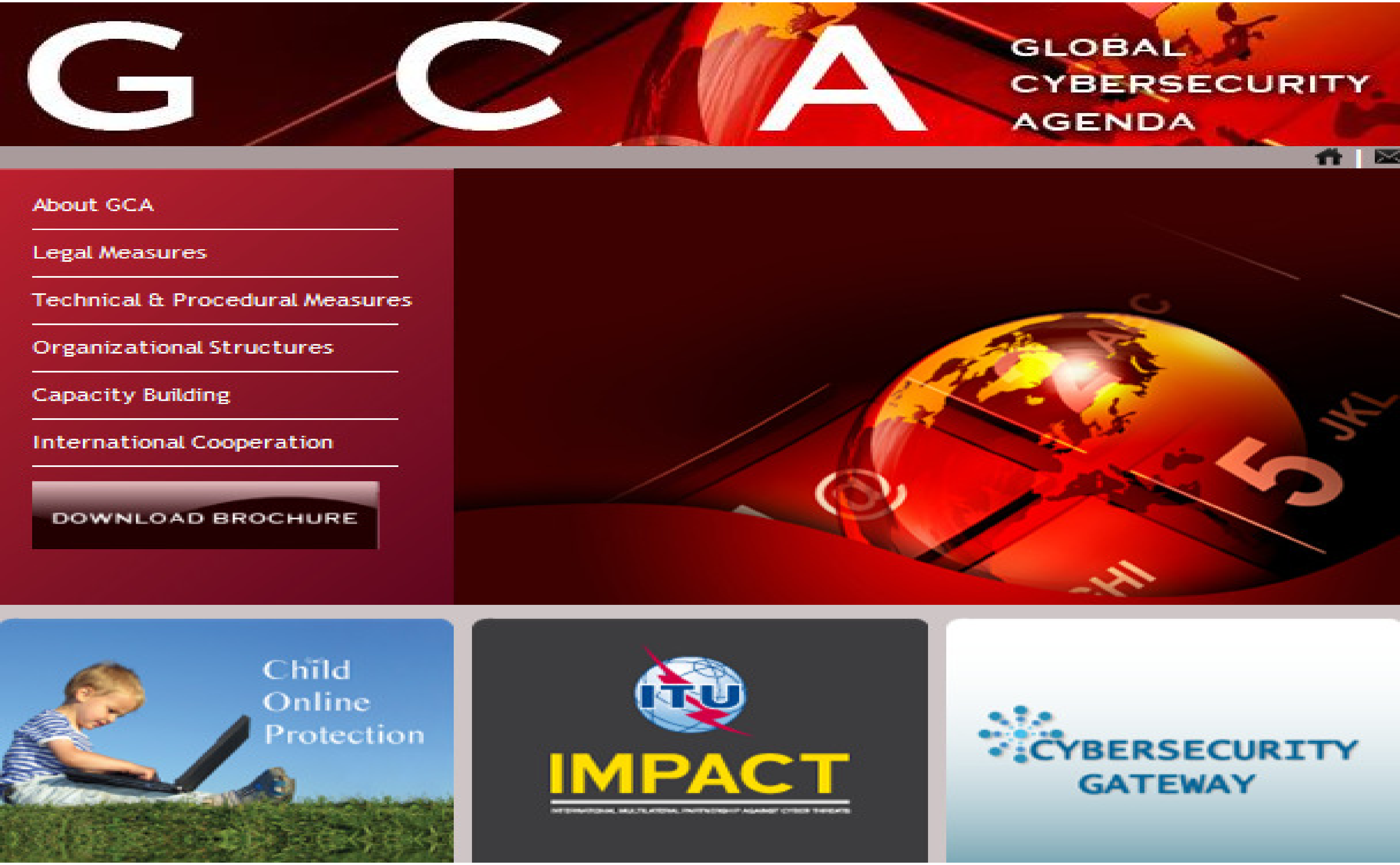
...The UN/**ITU** constitutes a unique global forum for partnership and the discussion of cybersecurity.

National Cybersecurity Strategy, Roadmap & Actions

1 – Our Global Cybersecurity Challenge	2 – Developing the UN Cyber Framework	3 – National Cybersecurity Case Studies
4 – Dimensions of National Cybersecurity	5 – The UN Global Cyber Agenda (GCA)	6 – Technology, Standards & Operations
7 – New Legislation, Training and Partners	8 – National Roadmap - “Shopping List”	9 – Implementing YOUR Action Plan!

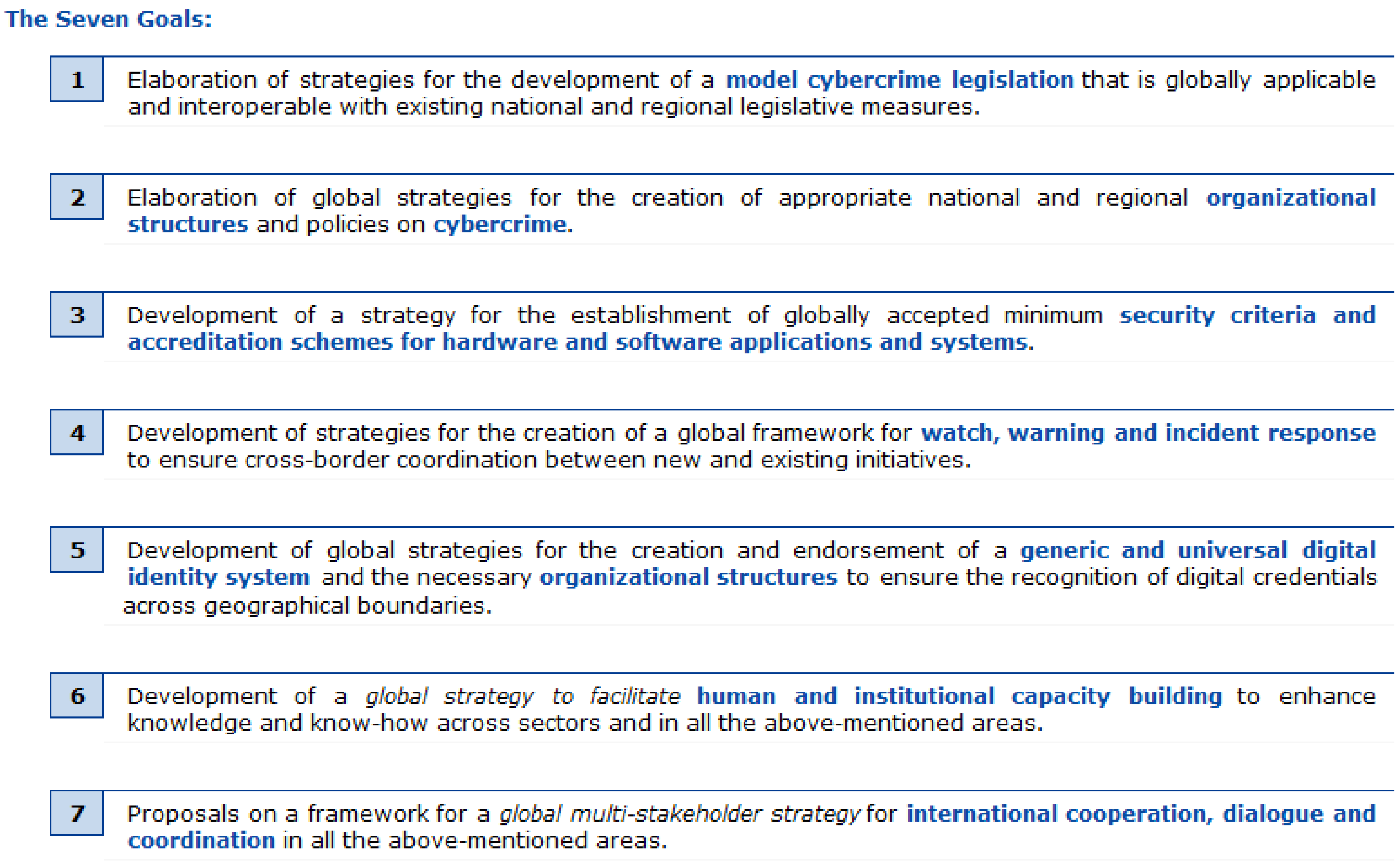


ITU: Global Cybersecurity Agenda – *On-Line*


G C A
GLOBAL CYBERSECURITY AGENDA
About GCA
Legal Measures
Technical & Procedural Measures
Organizational Structures
Capacity Building
International Cooperation
DOWNLOAD BROCHURE
Child Online Protection
ITU
IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS
CYBERSECURITY GATEWAY

UN/ITU : GCA – The Seven Strategic Goals

- *for National & International Cybersecurity* -



The Seven Goals:

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 **organizational structures** and policies on **cybercrime.**

3 Development of a strategy for the establishment of globally accepted minimum **security criteria and accreditation schemes for hardware and software applications and systems.**

4 Development of strategies for the creation of a global framework for **watch, warning and incident response** to ensure cross-border coordination between new and existing initiatives.

5 Development of global strategies for the creation and endorsement of a **generic and universal digital identity system** and the necessary **organizational structures** to ensure the recognition of digital credentials across geographical boundaries.

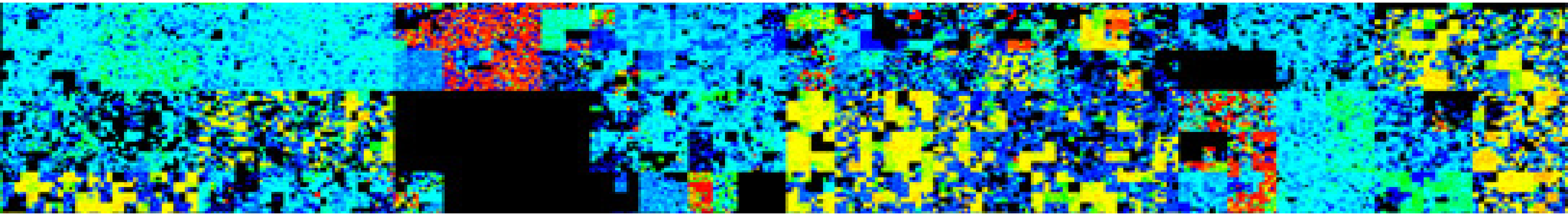
6 Development of a *global strategy to facilitate* **human and institutional capacity building** to enhance knowledge and know-how across sectors and in all the above-mentioned areas.

7 Proposals on a framework for a *global multi-stakeholder strategy* for **international cooperation, dialogue and coordination** in all the above-mentioned areas.

….These 7 goals can be achieved through the implementation of National CERTs!

National Cybersecurity Strategy, Roadmap & Actions

1 – Our Global Cybersecurity Challenge	2 – Developing the UN Cyber Framework	3 – National Cybersecurity Case Studies
4 – Dimensions of National Cybersecurity	5 – The UN Global Cyber Agenda (GCA)	6 – Technology, Standards & Operations
7 – New Legislation, Training and Partners	8 – National Roadmap - “Shopping List”	9 – Implementing YOUR Action Plan!



Practical International *Cybersecurity* Standards

- *Benefits:* Cybersecurity Standards and Technological Solutions are of great benefit in the establishment of organisations & operational policies, through reducing both costs & risks

- *Business Case:* The use of security standards, guidelines and ITU Recommendations should be driven by the organisation's economic business case, including a full evaluation of the short, medium and longer term risks & rewards

- *Start with Standards:* It is always *much* better to engineer new ICT systems and operations to standards, rather than to add them later!

- *Open Mobile Cloud World:* The open world of mobile devices, social networking and cloud computing means that cybersecurity professionals have to continually design new technical solutions to maintain comprehensive security

- *The ITU X800/X1200 Series* of Recommendations provide excellent ICT security frameworks for Government and Enterprises, whilst the ISO/IEC 27001/27002 are accepted worldwide for ISMS operations. *Other standards may also be deployed.*

…….Engineering and Managing ICT Operations to International Standards will place a major deterrence upon cybercriminals, hackers & attackers.

UN/ITU Technical *Security* Standards

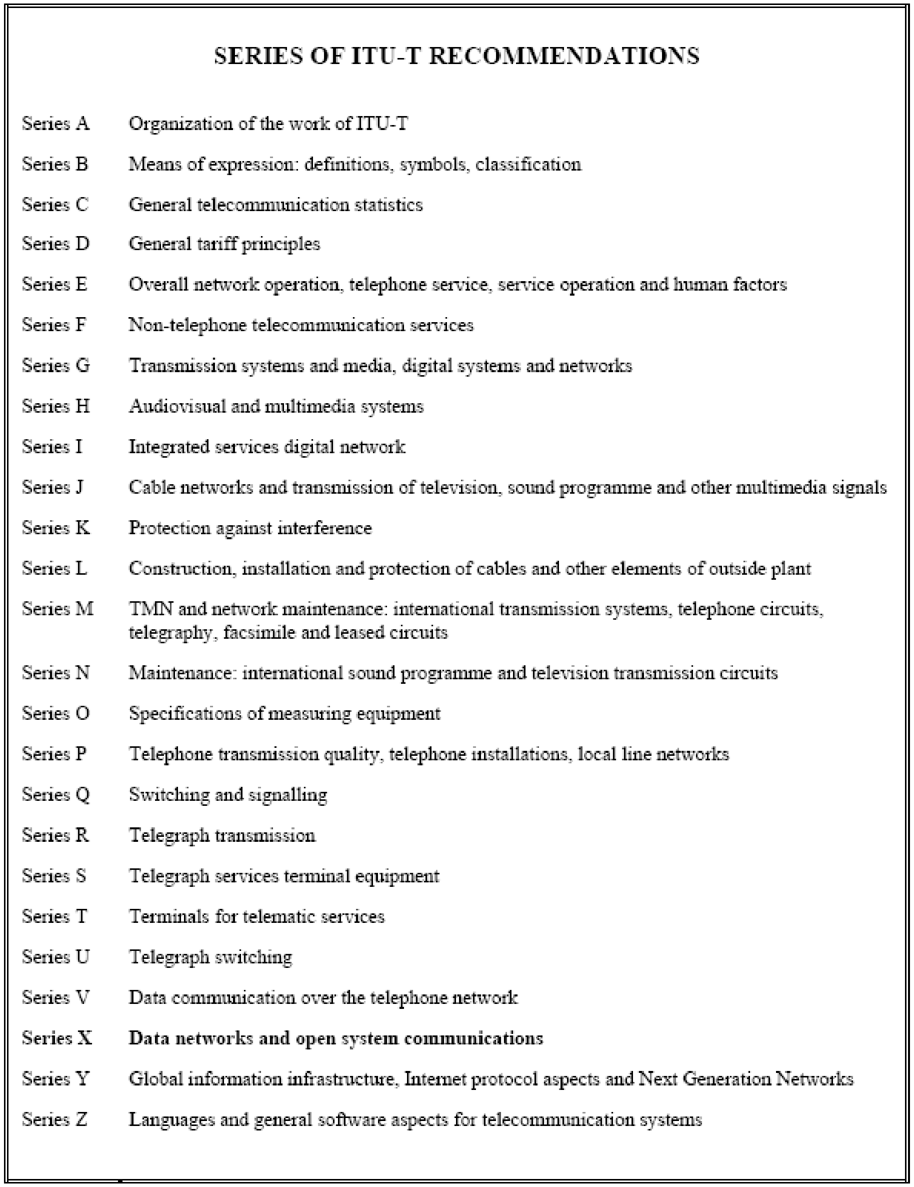
- The ITU Technical Families of Security Standards (from A to Z Series) are extremely comprehensive and span practically all technical aspects of government and enterprise cybersecurity systems and architectures.
- The standards are also being continuously developed and upgraded by professional specialists from the ICT Industry, Government & Academia
  - *X.805 –* Security Architecture for End-to-End Communications
  - *X.1121* – Security Technologies for Mobile Data Communications
  - *X1191 –* Functional Requirements for IPTV Security Agents
  - *X.1205 –* Overview of Cybersecurity and General Guidelines
  - *X.1250 –* Security Standards for Identity Management
  - *X.509 –* Public Key Infrastructure & Certificate Frameworks
  - *H.323* – Multimedia Communications Systems Security
  - *J.170 –* Security Specifications for TV & Multimedia Cable Networks

  *…….We'll be focusing primary on the **X.800** and **X.1200** Series of Standards*

- The ITU security standards can be freely downloaded from the ITU website

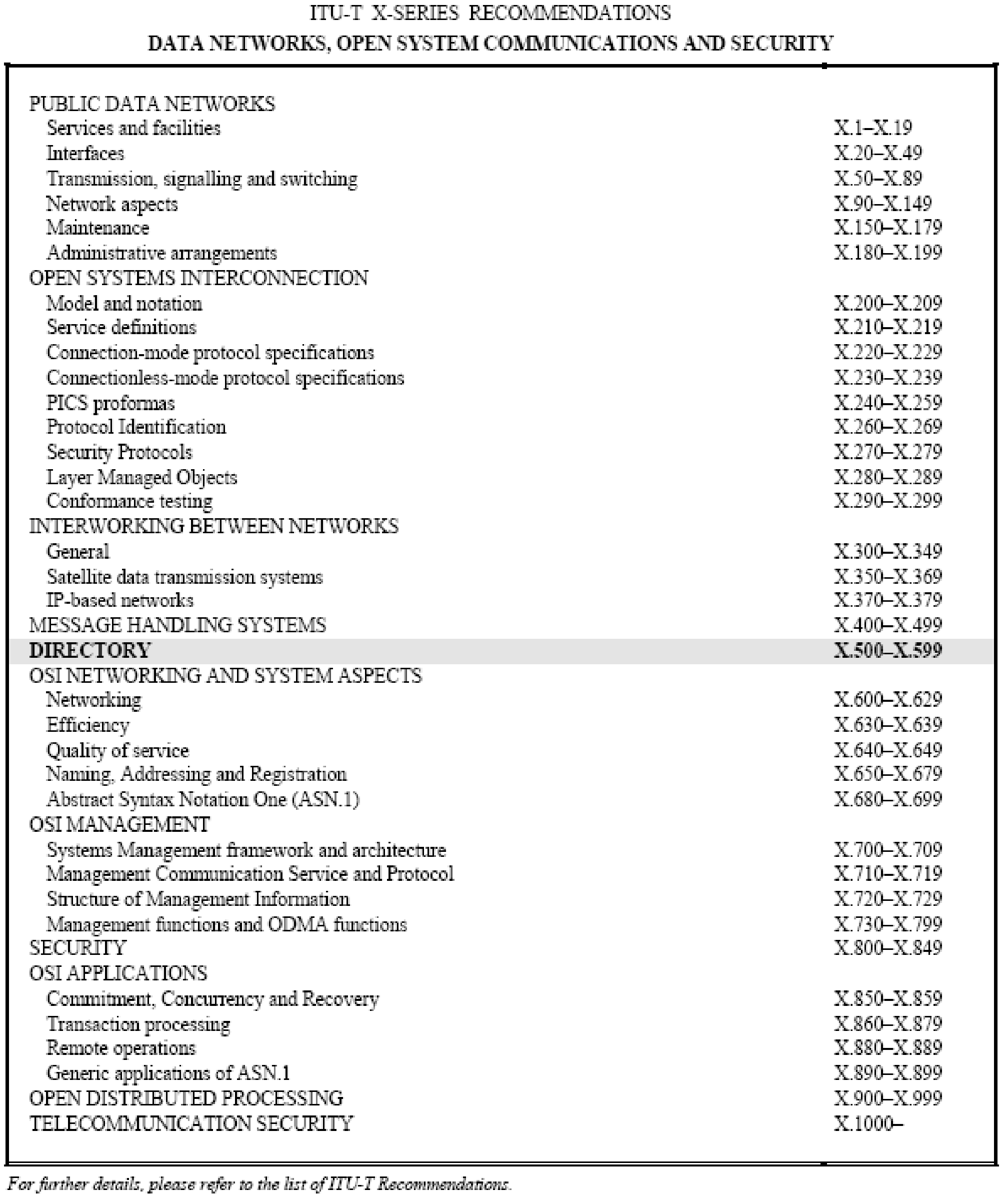
Download Link: **www.itu.int/rec/T-REC/**

ITU-T X-Series – *Data Nets, OSI and Security*



SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks and open system communications**
Series Y	Global information infrastructure, Internet protocol aspects and Next Generation Networks
Series Z	Languages and general software aspects for telecommunication systems



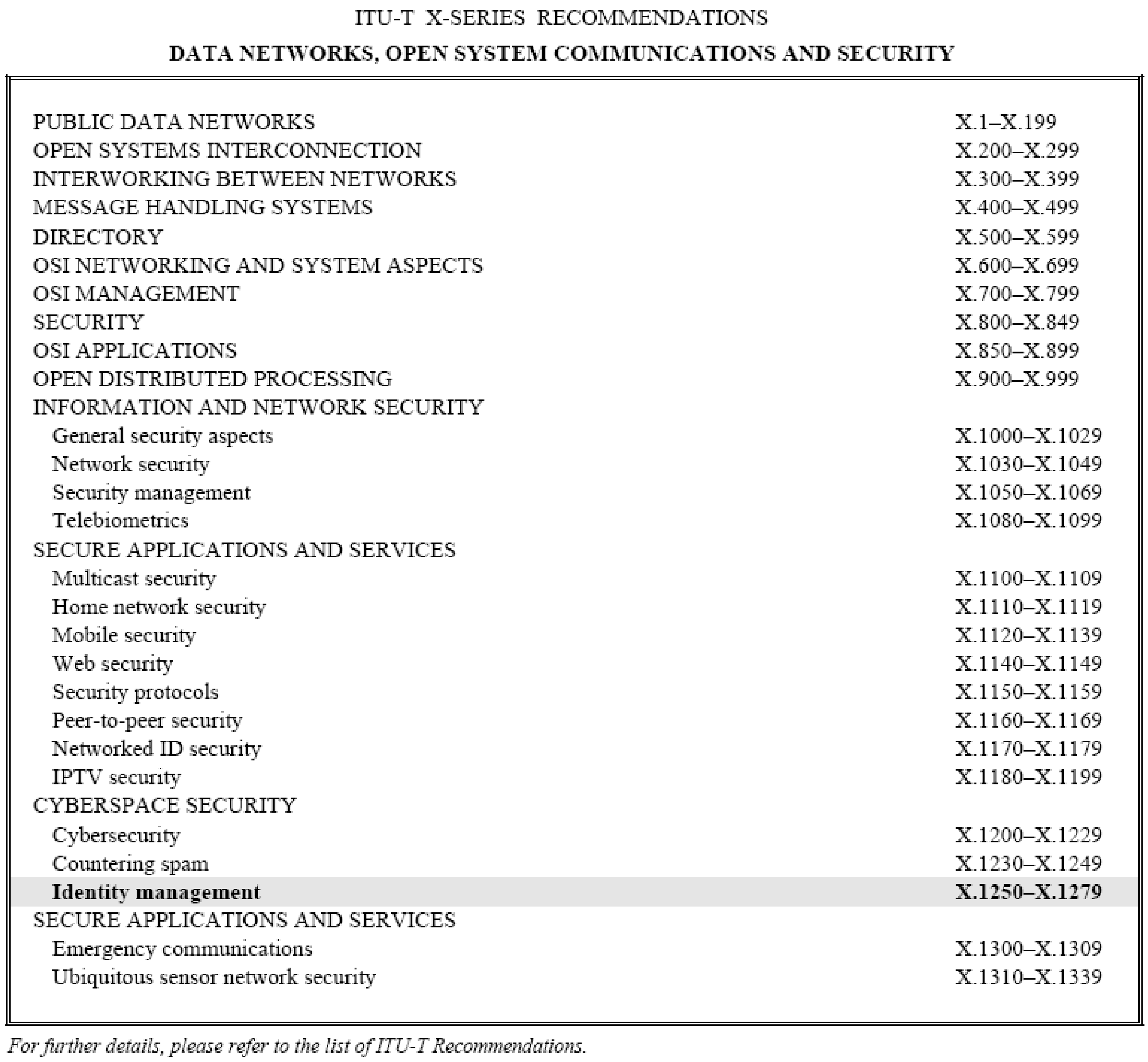
ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	**X.500–X.599**
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	X.1000–

For further details, please refer to the list of ITU-T Recommendations.

ITU-T X-Series *Security* Recommendations



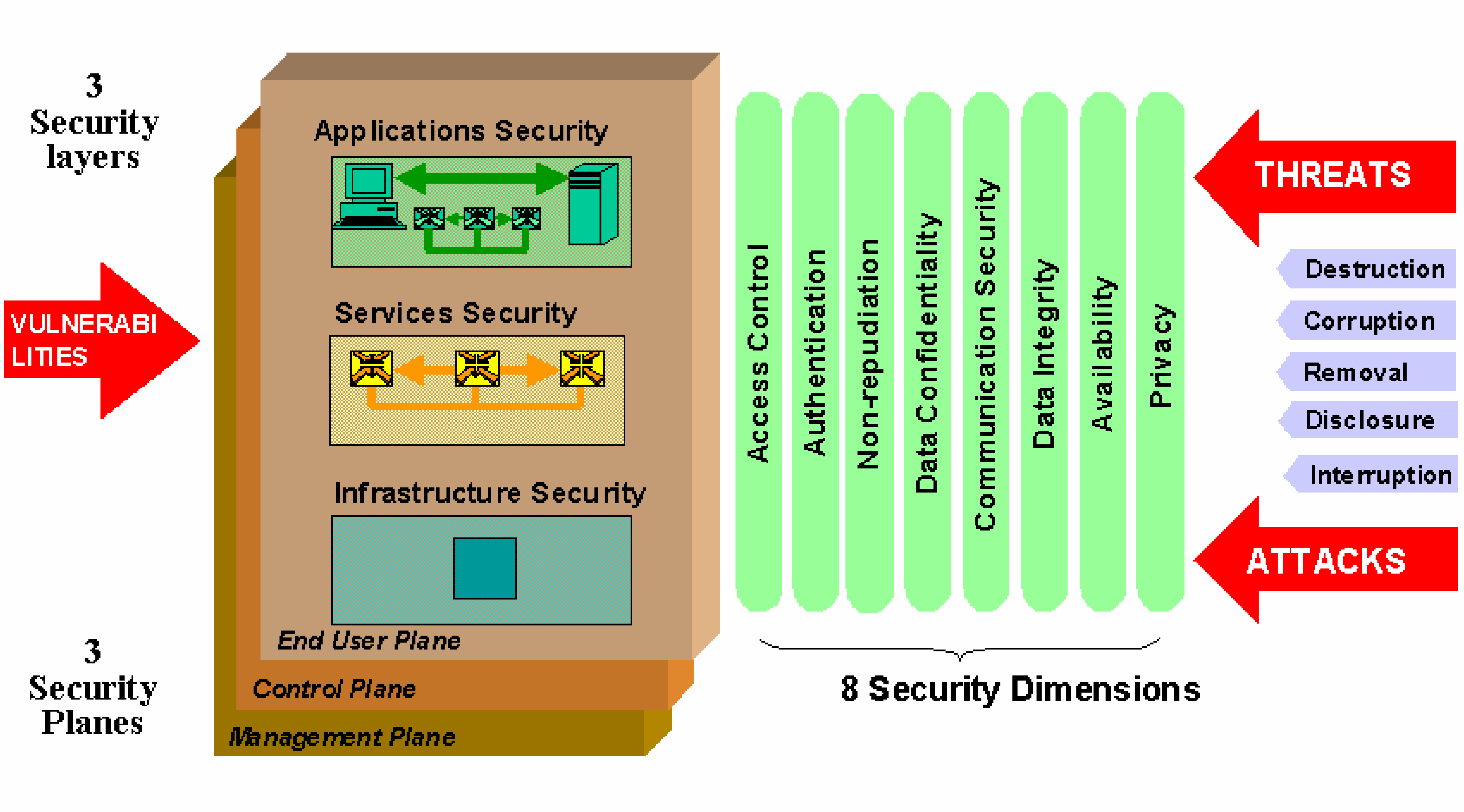
ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	**X.1250–X.1279**
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339

For further details, please refer to the list of ITU-T Recommendations.

UN/ITU – X.805 *Cybersecurity Architecture*



UN/ITU - X.805 Cybersecurity Architecture:

Mapping Security Dimensions to Threats

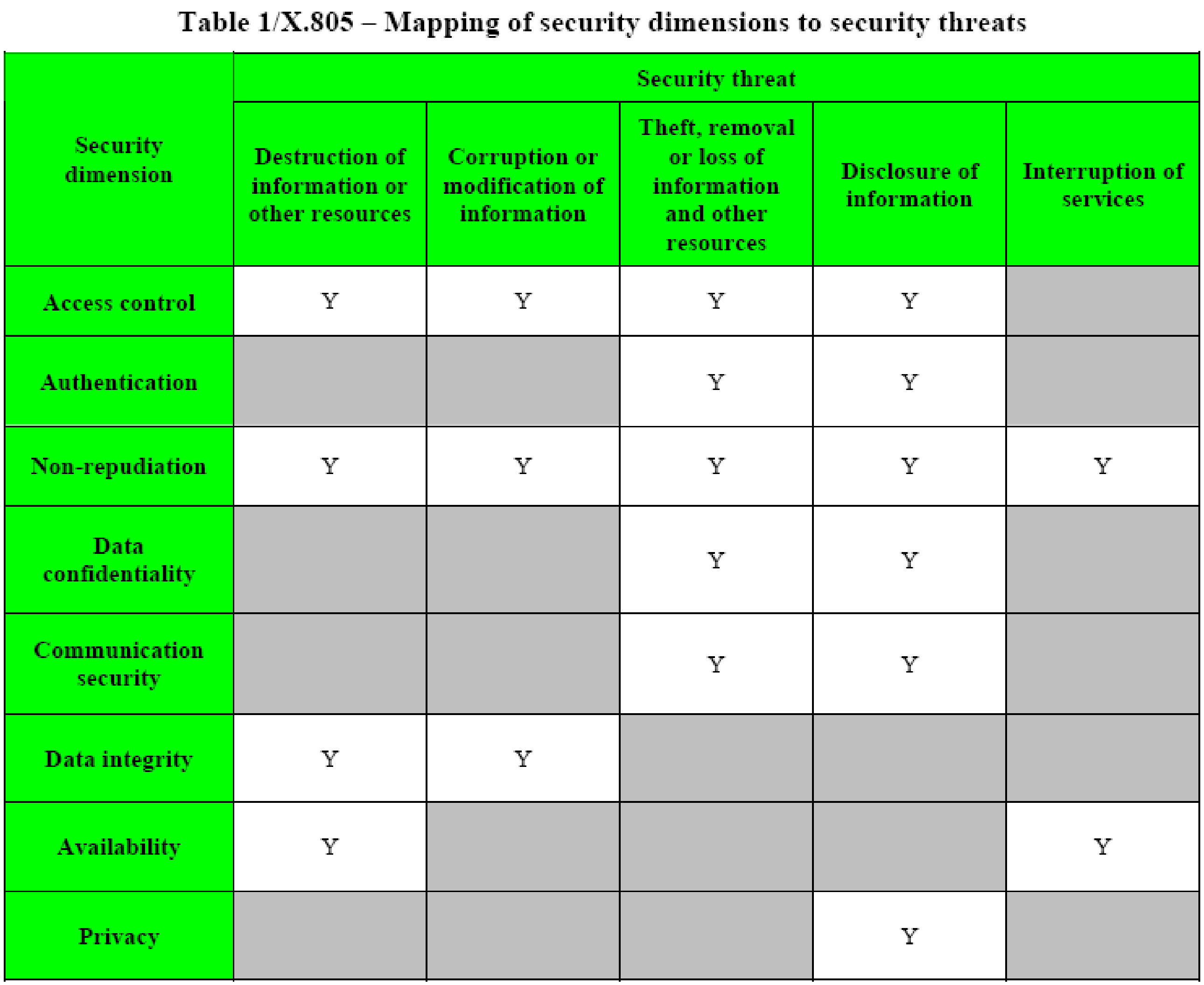
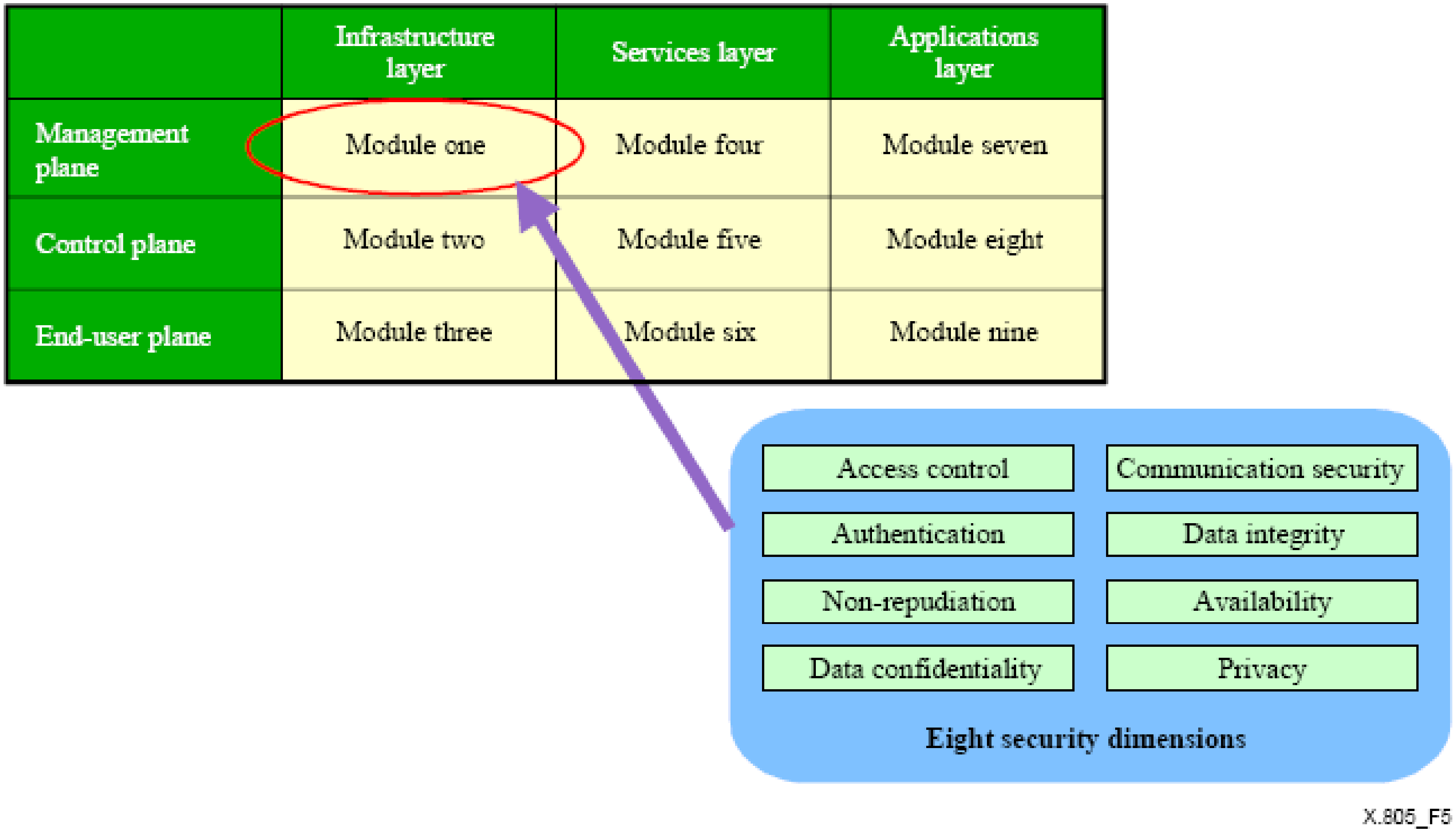


Table 1/X.805 – Mapping of security dimensions to security threats

Security dimension	Security threat				
	Destruction of information or other resources	Corruption or modification of information	Theft, removal or loss of information and other resources	Disclosure of information	Interruption of services
Access control	Y	Y	Y	Y	
Authentication			Y	Y	
Non-repudiation	Y	Y	Y	Y	Y
Data confidentiality			Y	Y	
Communication security			Y	Y	
Data integrity	Y	Y			
Availability	Y				Y
Privacy				Y	

UN/ITU - X.805 : Cybersecurity Architecture

Mapping out the Eight Security Dimensions



	Infrastructure layer	Services layer	Applications layer
Management plane	Module one	Module four	Module seven
Control plane	Module two	Module five	Module eight
End-user plane	Module three	Module six	Module nine

Figure 5/X.805 – Security architecture in a tabular form

UN/ITU - X.805: Security Module 4

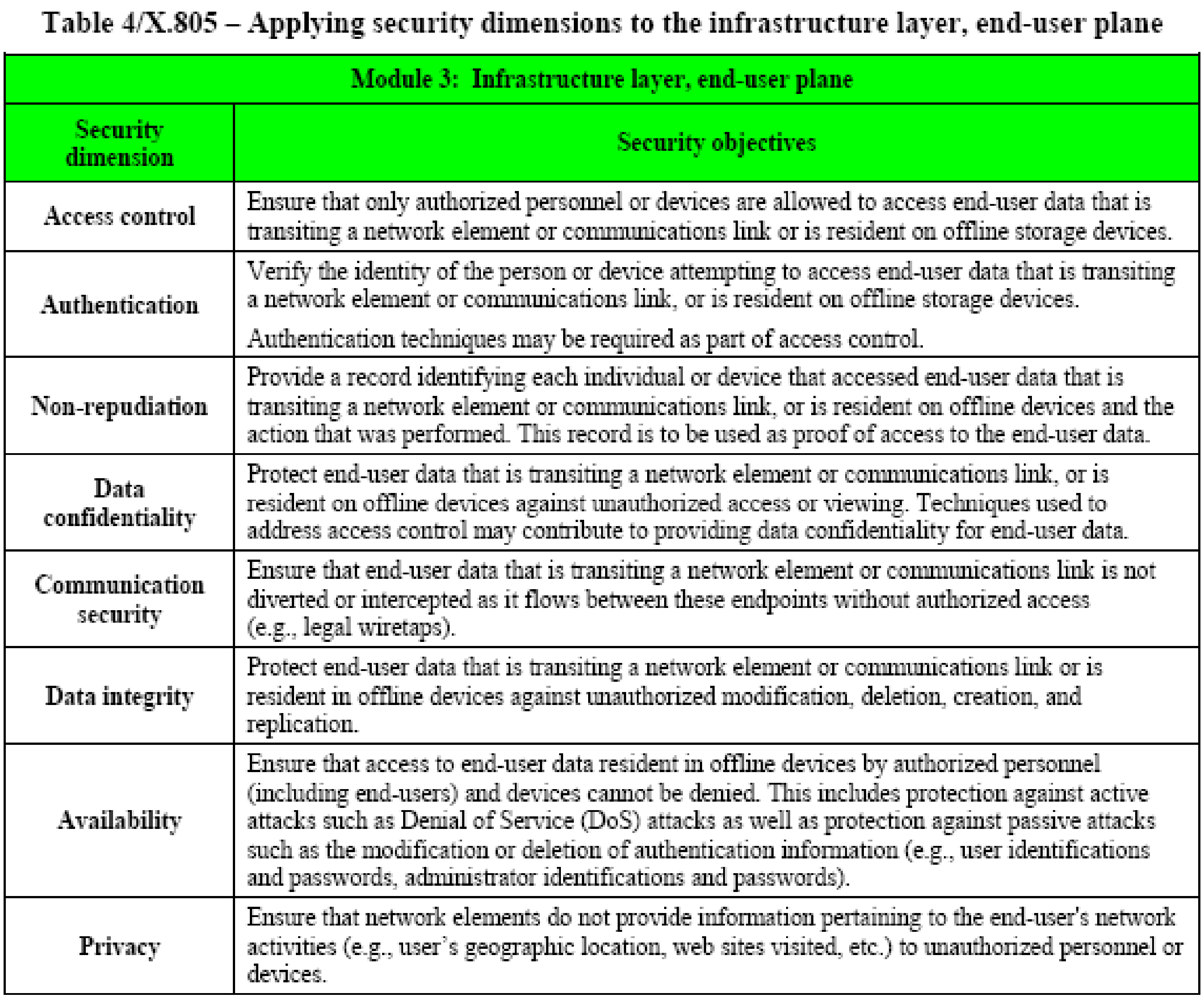


Table 4/X.805 – Applying security dimensions to the infrastructure layer, end-user plane

Module 3: Infrastructure layer, end-user plane	
Security dimension	**Security objectives**
Access control	Ensure that only authorized personnel or devices are allowed to access end-user data that is transiting a network element or communications link or is resident on offline storage devices.
Authentication	Verify the identity of the person or device attempting to access end-user data that is transiting a network element or communications link, or is resident on offline storage devices. Authentication techniques may be required as part of access control.
Non-repudiation	Provide a record identifying each individual or device that accessed end-user data that is transiting a network element or communications link, or is resident on offline devices and the action that was performed. This record is to be used as proof of access to the end-user data.
Data confidentiality	Protect end-user data that is transiting a network element or communications link, or is resident on offline devices against unauthorized access or viewing. Techniques used to address access control may contribute to providing data confidentiality for end-user data.
Communication security	Ensure that end-user data that is transiting a network element or communications link is not diverted or intercepted as it flows between these endpoints without authorized access (e.g., legal wiretaps).
Data integrity	Protect end-user data that is transiting a network element or communications link or is resident in offline devices against unauthorized modification, deletion, creation, and replication.
Availability	Ensure that access to end-user data resident in offline devices by authorized personnel (including end-users) and devices cannot be denied. This includes protection against active attacks such as Denial of Service (DoS) attacks as well as protection against passive attacks such as the modification or deletion of authentication information (e.g., user identifications and passwords, administrator identifications and passwords).
Privacy	Ensure that network elements do not provide information pertaining to the end-user's network activities (e.g., user's geographic location, web sites visited, etc.) to unauthorized personnel or devices.

International Cybersecurity Standards: *Players*

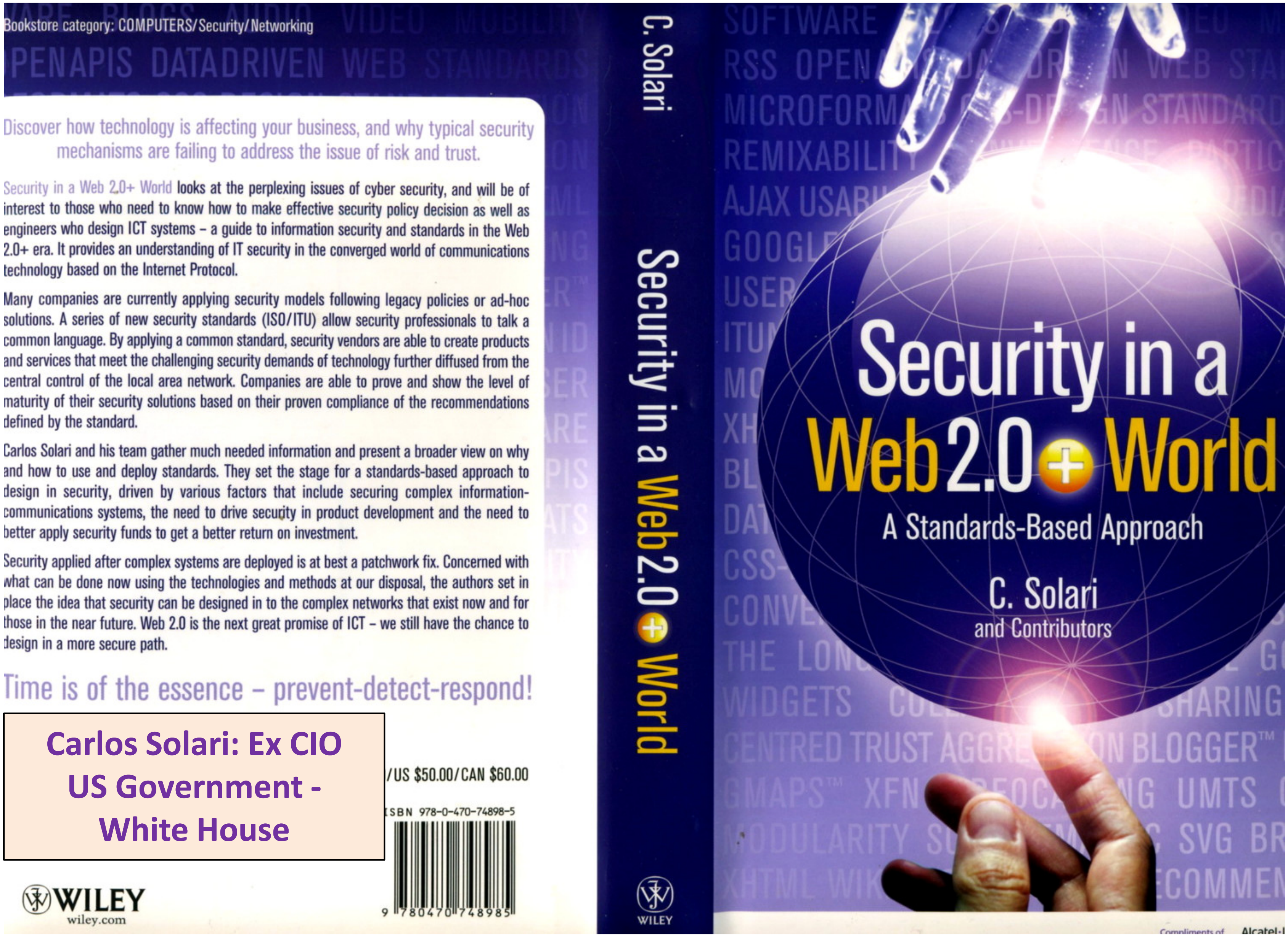
- *Multiple Players:* There are multiple international and national organisations that define and publish standards relating to physical and cyber security. In general these standards, recommendations and guidelines are complementary

- *UN/ITU:* We shall be focusing in this session of the technical security standards & recommendations published by the ITU as their X-Series as well as H-Series

- *Partnerships:* The ITU works closely in partnership with many other organisations, particularly for emerging Telecommunications. Multimedia, Mobile & IP Networking:
  - *ENISA* – European Network and Information Security Agency
  - *ISO* – International Standards Organisation
  - *IETF* – Internet Engineering Task Force
  - *ETSI* – European Telecommunications Standards Institute
  - *IEEE* – Institute of Electrical and Electronic Engineers
  - *ATIS* – Alliance for Telecommunications Industry Solutions
  - *3GPP* – 3rd Generation Partnership Project
  - *ANSI* – American National Standards Institute
  - *NIST* – National Institute of Standards and Technology
  - *ISF* – Information Security Forum

Recommended Book: Security in a Web2.0 World –

- A Standards Based Approach(UN/ITU - X.805) – Author: C. Solari -



Bookstore category: COMPUTERS/Security/Networking

Discover how technology is affecting your business, and why typical security mechanisms are failing to address the issue of risk and trust.

Security in a Web 2.0+ World looks at the perplexing issues of cyber security, and will be of interest to those who need to know how to make effective security policy decision as well as engineers who design ICT systems – a guide to information security and standards in the Web 2.0+ era. It provides an understanding of IT security in the converged world of communications technology based on the Internet Protocol.

Many companies are currently applying security models following legacy policies or ad-hoc solutions. A series of new security standards (ISO/ITU) allow security professionals to talk a common language. By applying a common standard, security vendors are able to create products and services that meet the challenging security demands of technology further diffused from the central control of the local area network. Companies are able to prove and show the level of maturity of their security solutions based on their proven compliance of the recommendations defined by the standard.

Carlos Solari and his team gather much needed information and present a broader view on why and how to use and deploy standards. They set the stage for a standards-based approach to design in security, driven by various factors that include securing complex information-communications systems, the need to drive security in product development and the need to better apply security funds to get a better return on investment.

Security applied after complex systems are deployed is at best a patchwork fix. Concerned with what can be done now using the technologies and methods at our disposal, the authors set in place the idea that security can be designed in to the complex networks that exist now and for those in the near future. Web 2.0 is the next great promise of ICT – we still have the chance to design in a more secure path.

Time is of the essence – prevent-detect-respond!

Carlos Solari: Ex CIO US Government - White House

/US $50.00/CAN $60.00

ISBN 978-0-470-74898-5

WILEY
wiley.com

C. Solari

Security in a Web2.0+ World

WILEY

Security in a Web 2.0+ World

A Standards-Based Approach

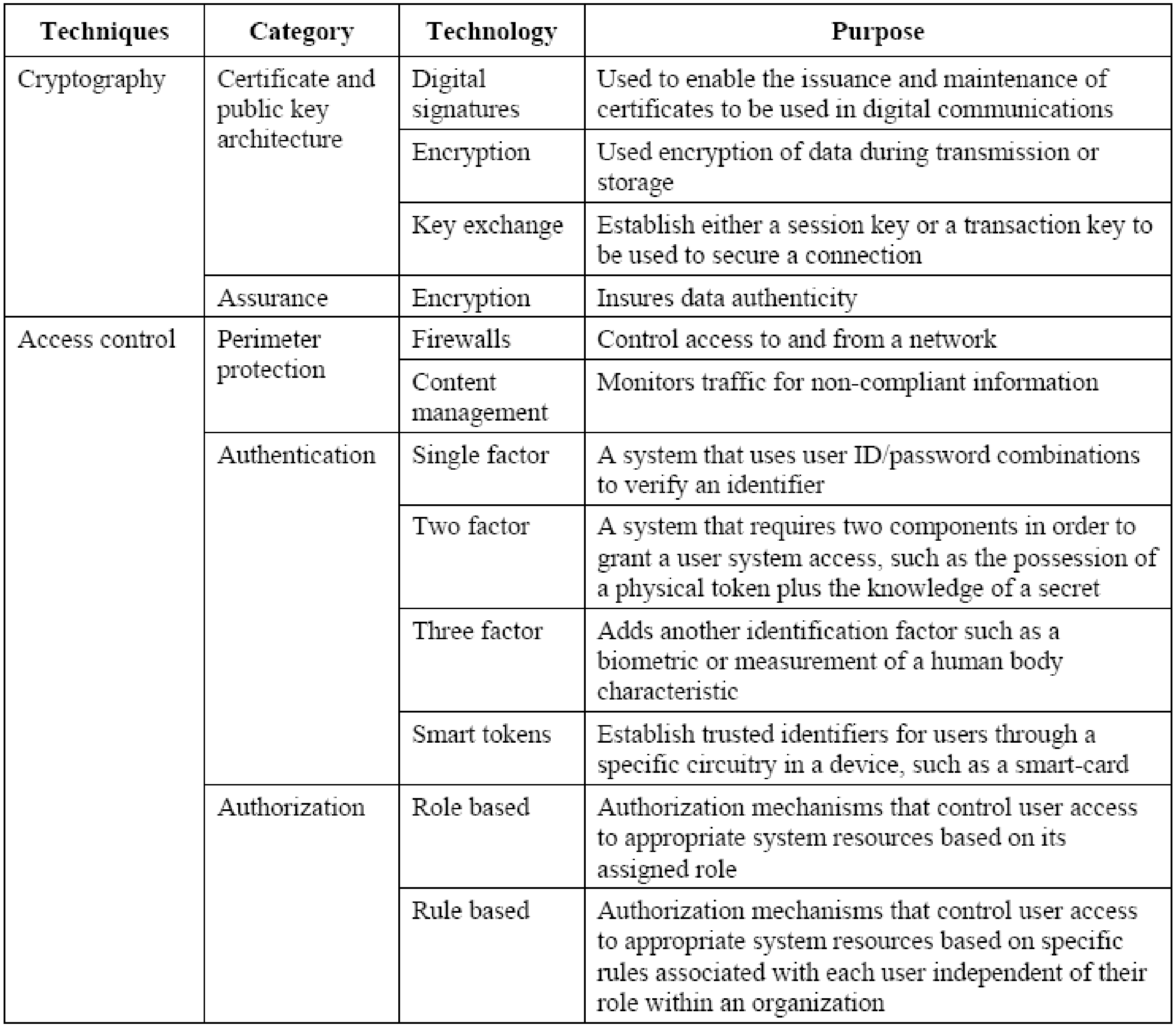
C. Solari
and Contributors

Compliments of Alcatel-

UN/ITU: X.1200 Security Standard Series

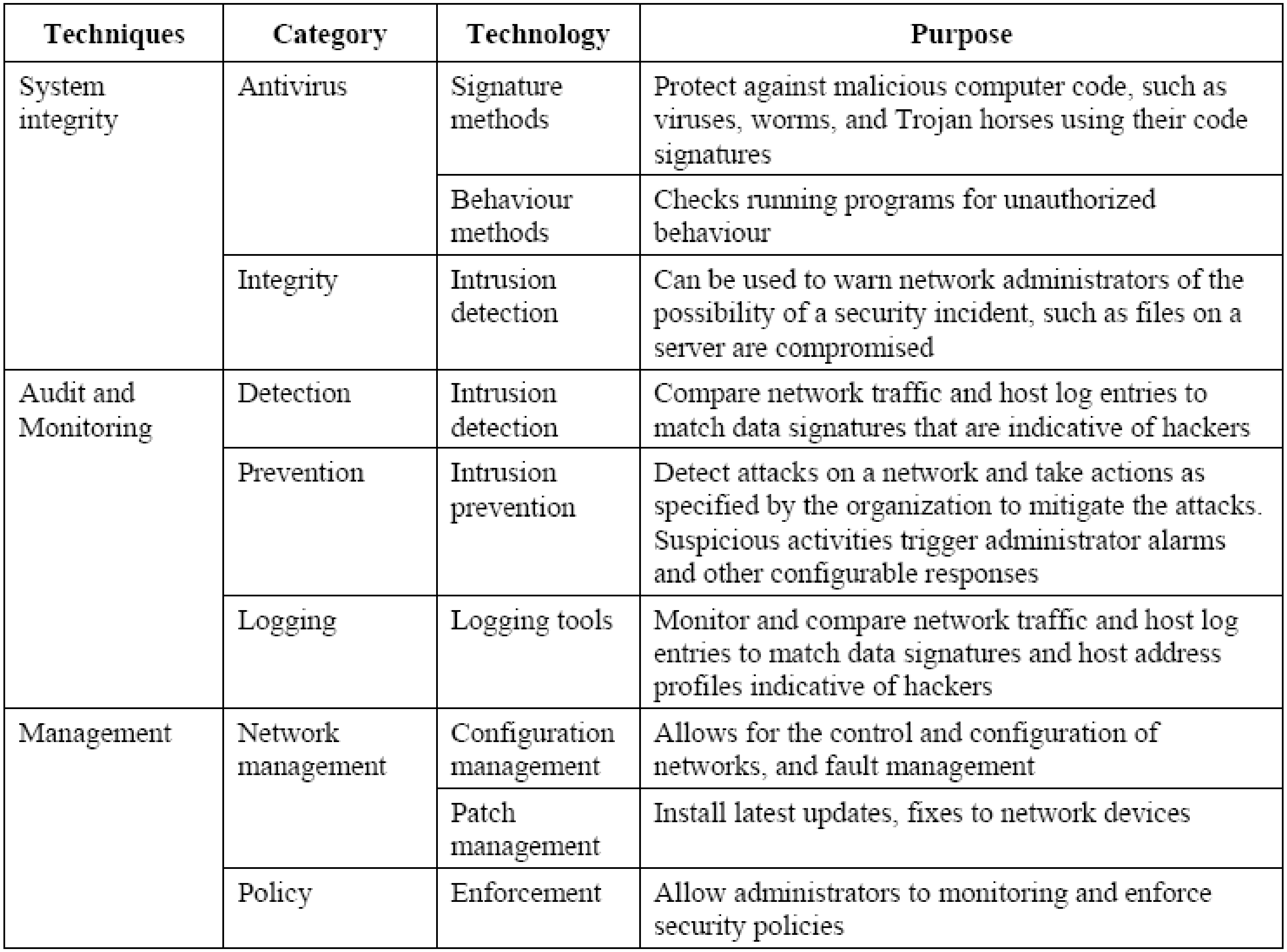
- *X.1205* provides a full definition and overview of most technology aspects of cybersecurity, building upon the X.805 architecture
- *X.1240/X.1241* provide technical strategies for countering spam email
- *X.1242* provides SMS spam filtering system based on user-rules
- *X.1244* provides ways of countering spam in IP Multimedia Systems
- *X.1251/X.1252* provide frameworks and technical models for the secure management of on-line digital identity
- *….Here we shall provide an overview of X.1205 and X.1251/X.1252*

X.1205 *Cybersecurity* Technologies (1)



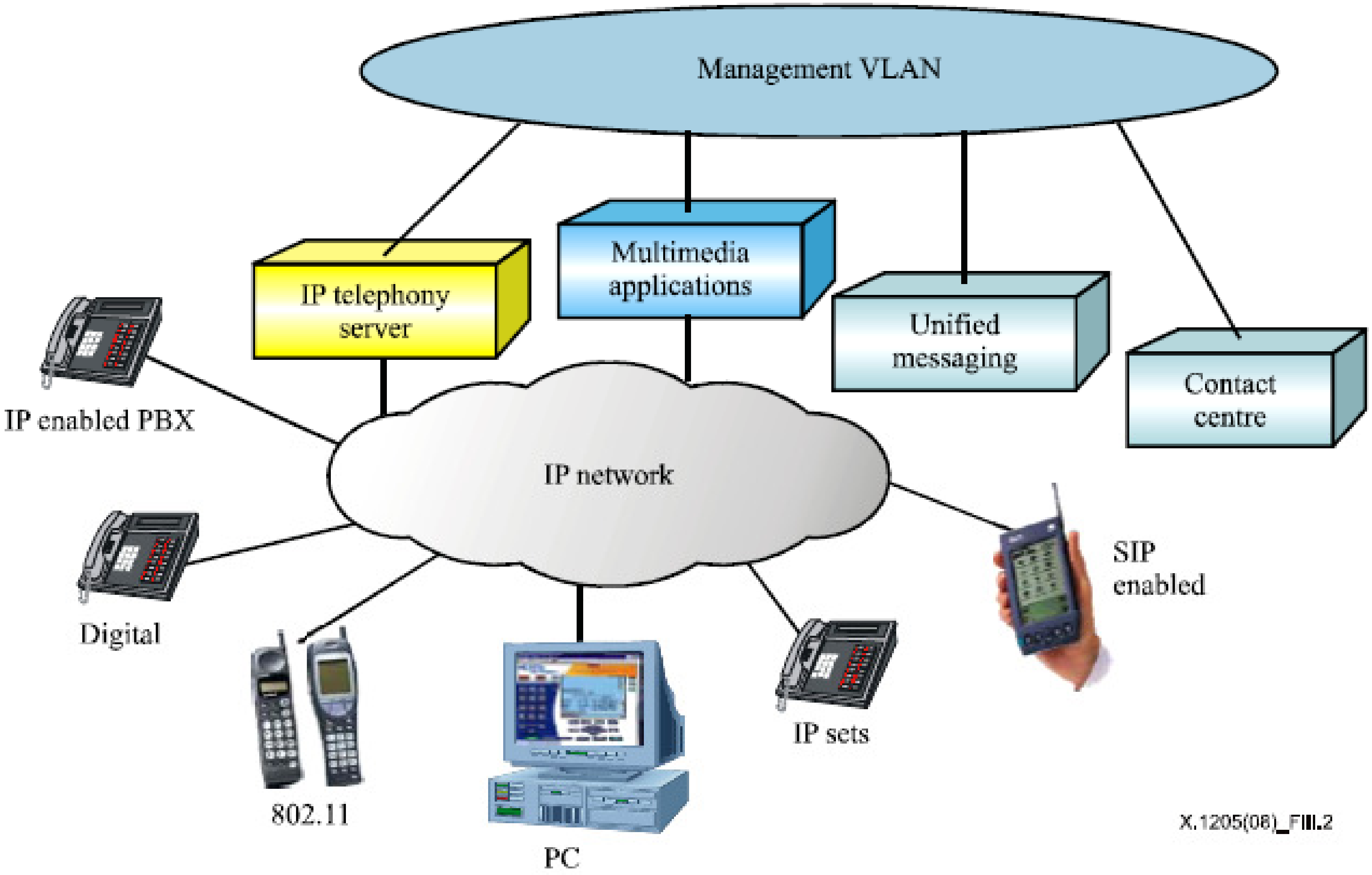
Techniques	Category	Technology	Purpose
Cryptography	Certificate and public key architecture	Digital signatures	Used to enable the issuance and maintenance of certificates to be used in digital communications
		Encryption	Used encryption of data during transmission or storage
		Key exchange	Establish 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

Securing VoIP – IP Telephony – X.1205

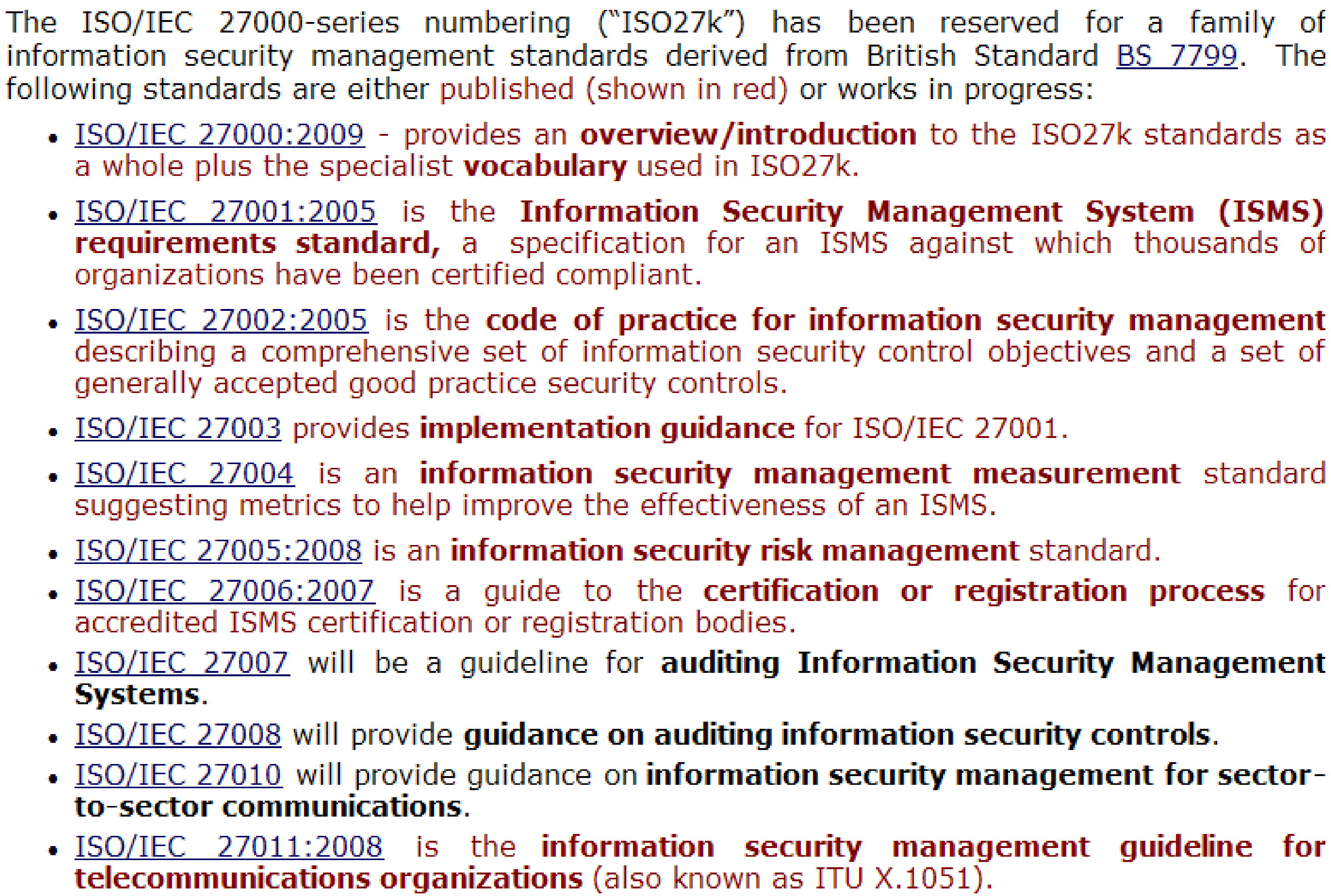


Other Cyber & Physical Security Standards:

- ISO/IEC, NIST, ENISA, ISF, IEEE -

- *ISO/IEC:* These are often adopted as “best practice” for operational aspects of security including the ISO27001 – Information Security Management System, and the ISO27002 – ISMS Code of Practice
- *NIST:* The comprehensive publications of the “800 Series” from the Computer Security Division are complementary to the ITU standards
- *ENISA:* The European Networks Security Agency publishes many detailed security studies and recommendations, with some useful work and guidelines for the establishment of national CERTs
- *ISF* – Information Security Forum – Founded 1989 to provide research, analysis and methodologies for Information Security and Risk Management
- *IEEE:* An important global player in ICT standards, and a key ITU partner in the development of new standards for open network cybersecurity

ISO/IEC 27000/2- *Info Security Management*

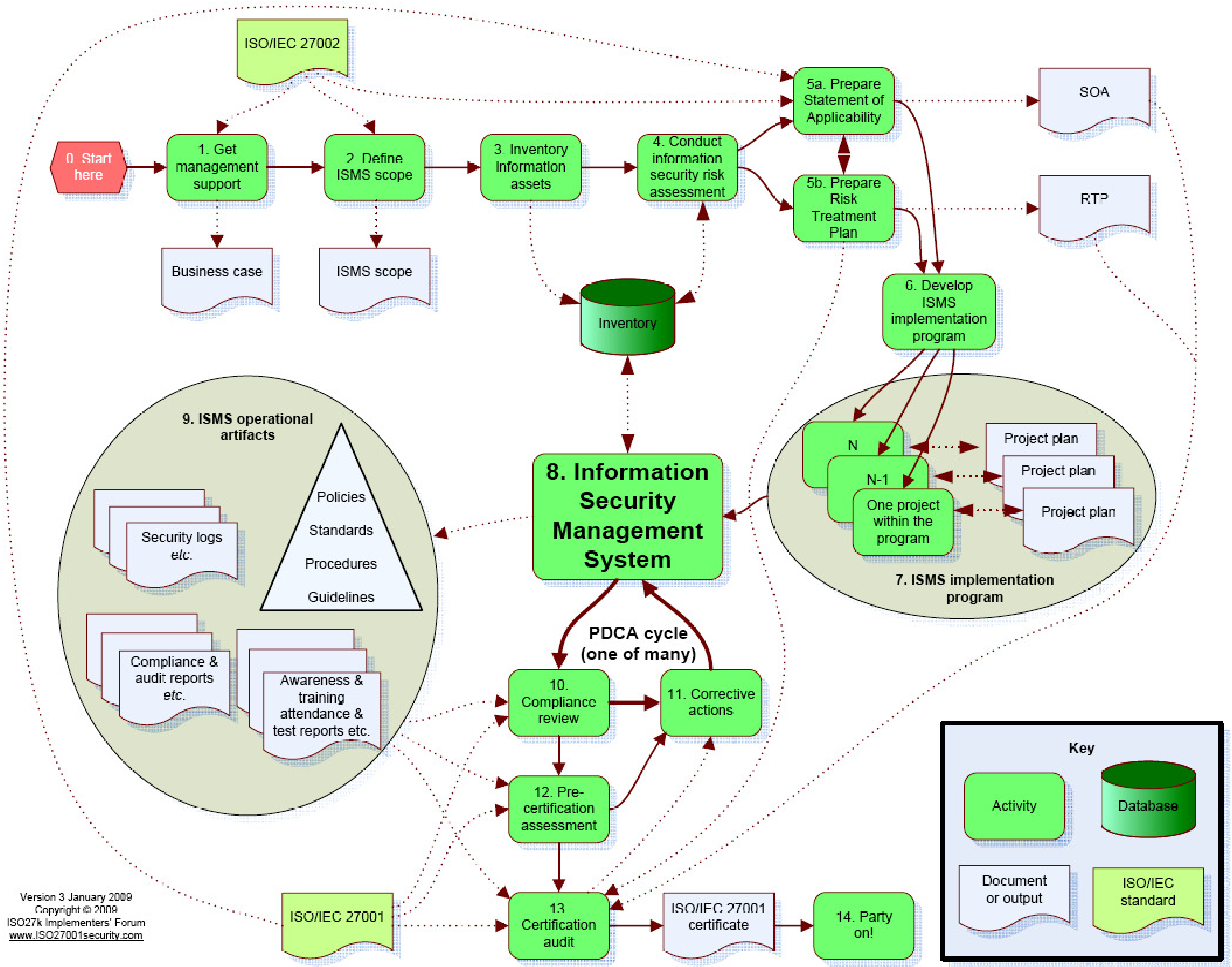


The ISO/IEC 27000-series numbering ("ISO27k") has been reserved for a family of information security management standards derived from British Standard BS 7799. The following standards are either published (shown in red) or works in progress:

- ISO/IEC 27000:2009 - provides an **overview/introduction** to the ISO27k standards as a whole plus the specialist **vocabulary** used in ISO27k.
- ISO/IEC 27001:2005 is the **Information Security Management System (ISMS) requirements standard,** a specification for an ISMS against which thousands of organizations have been certified compliant.
- ISO/IEC 27002:2005 is the **code of practice for information security management** describing a comprehensive set of information security control objectives and a set of generally accepted good practice security controls.
- ISO/IEC 27003 provides **implementation guidance** for ISO/IEC 27001.
- ISO/IEC 27004 is an **information security management measurement** standard suggesting metrics to help improve the effectiveness of an ISMS.
- ISO/IEC 27005:2008 is an **information security risk management** standard.
- ISO/IEC 27006:2007 is a guide to the **certification or registration process** for accredited ISMS certification or registration bodies.
- ISO/IEC 27007 will be a guideline for **auditing Information Security Management Systems.**
- ISO/IEC 27008 will provide **guidance on auditing information security controls**.
- ISO/IEC 27010 will provide guidance on **information security management for sector-to-sector communications**.
- ISO/IEC 27011:2008 is the **information security management guideline for telecommunications organizations** (also known as ITU X.1051).

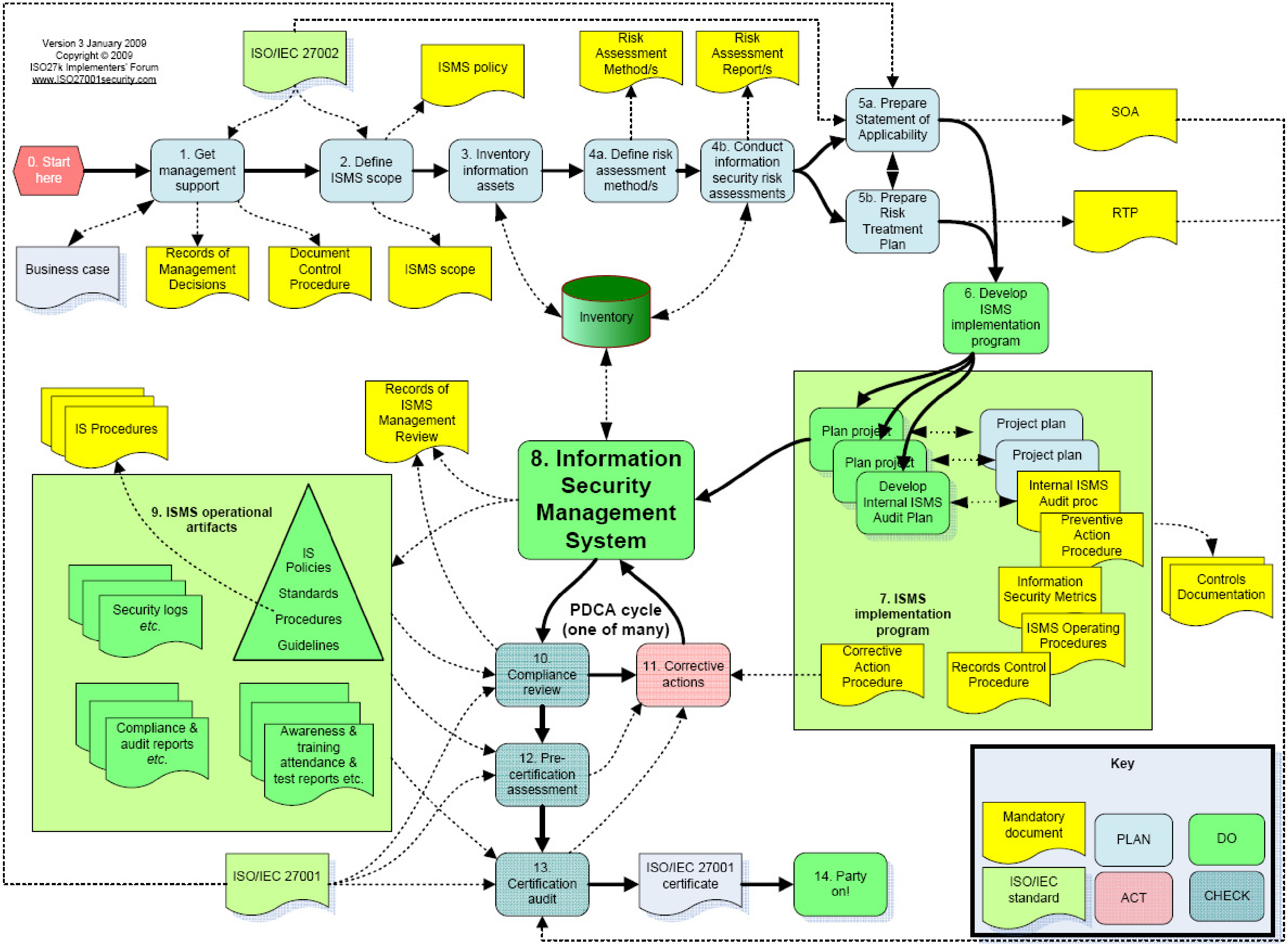
Information Security Management System:

Implementation Process: ISO27001/2

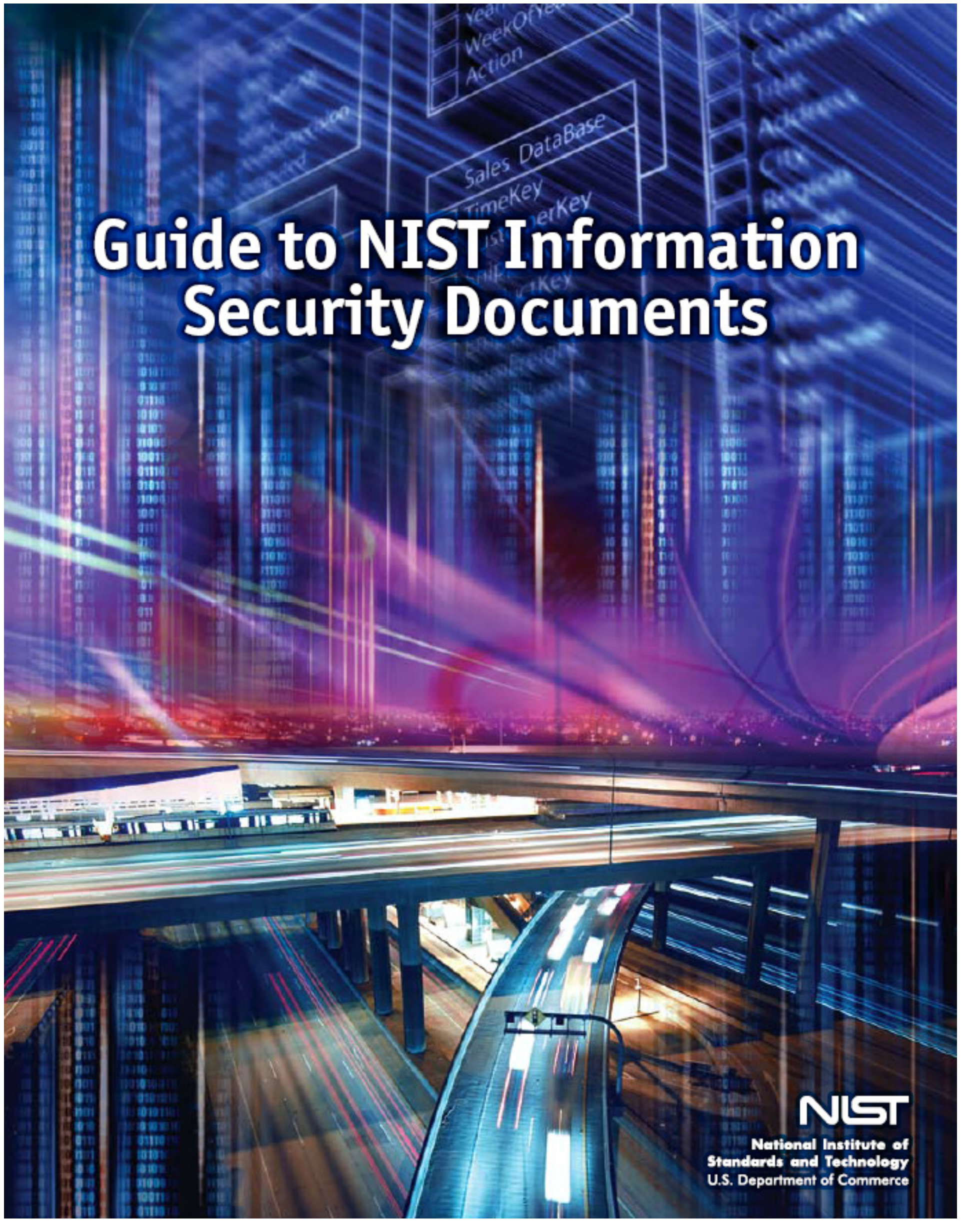

ISO/IEC 27002
0. Start here
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4. Conduct information security risk assessment
5a. Prepare Statement of Applicability
5b. Prepare Risk Treatment Plan
SOA
RTP
Business case
ISMS scope
Inventory
6. Develop ISMS implementation program
9. ISMS operational artifacts
Policies
Standards
Procedures
Guidelines
Security logs etc.
Compliance & audit reports etc.
Awareness & training attendance & test reports etc.
8. Information Security Management System
N
N-1
One project within the program
Project plan
Project plan
Project plan
7. ISMS implementation program
PDCA cycle (one of many)
10. Compliance review
11. Corrective actions
12. Pre-certification assessment
13. Certification audit
ISO/IEC 27001
ISO/IEC 27001 certificate
14. Party on!
Key
Activity
Database
Document or output
ISO/IEC standard

Version 3 January 2009
Copyright © 2009
ISO27k Implementers' Forum
www.ISO27001security.com

Flow-Chart: Route to *ISO27001/2* Certification


Version 3 January 2009
Copyright © 2009
ISO27k Implementers' Forum
www.ISO27001security.com
ISO/IEC 27002
ISMS policy
Risk Assessment Method/s
Risk Assessment Report/s
5a. Prepare Statement of Applicability
SOA
0. Start here
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4a. Define risk assessment method/s
4b. Conduct information security risk assessments
5b. Prepare Risk Treatment Plan
RTP
Business case
Records of Management Decisions
Document Control Procedure
ISMS scope
Inventory
6. Develop ISMS implementation program
IS Procedures
Records of ISMS Management Review
8. Information Security Management System
Plan project
Plan project
Develop Internal ISMS Audit Plan
Project plan
Project plan
Internal ISMS Audit proc
Preventive Action Procedure
Controls Documentation
9. ISMS operational artifacts
IS Policies
Standards
Procedures
Guidelines
Security logs etc.
PDCA cycle (one of many)
Information Security Metrics
7. ISMS implementation program
ISMS Operating Procedures
Corrective Action Procedure
Records Control Procedure
10. Compliance review
11. Corrective actions
Compliance & audit reports etc.
Awareness & training attendance & test reports etc.
12. Pre-certification assessment
Key
Mandatory document
PLAN
DO
ISO/IEC 27001
13. Certification audit
ISO/IEC 27001 certificate
14. Party on!
ISO/IEC standard
ACT
CHECK

NIST Security Publications: “800 Series”



Guide to NIST Information Security Documents

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

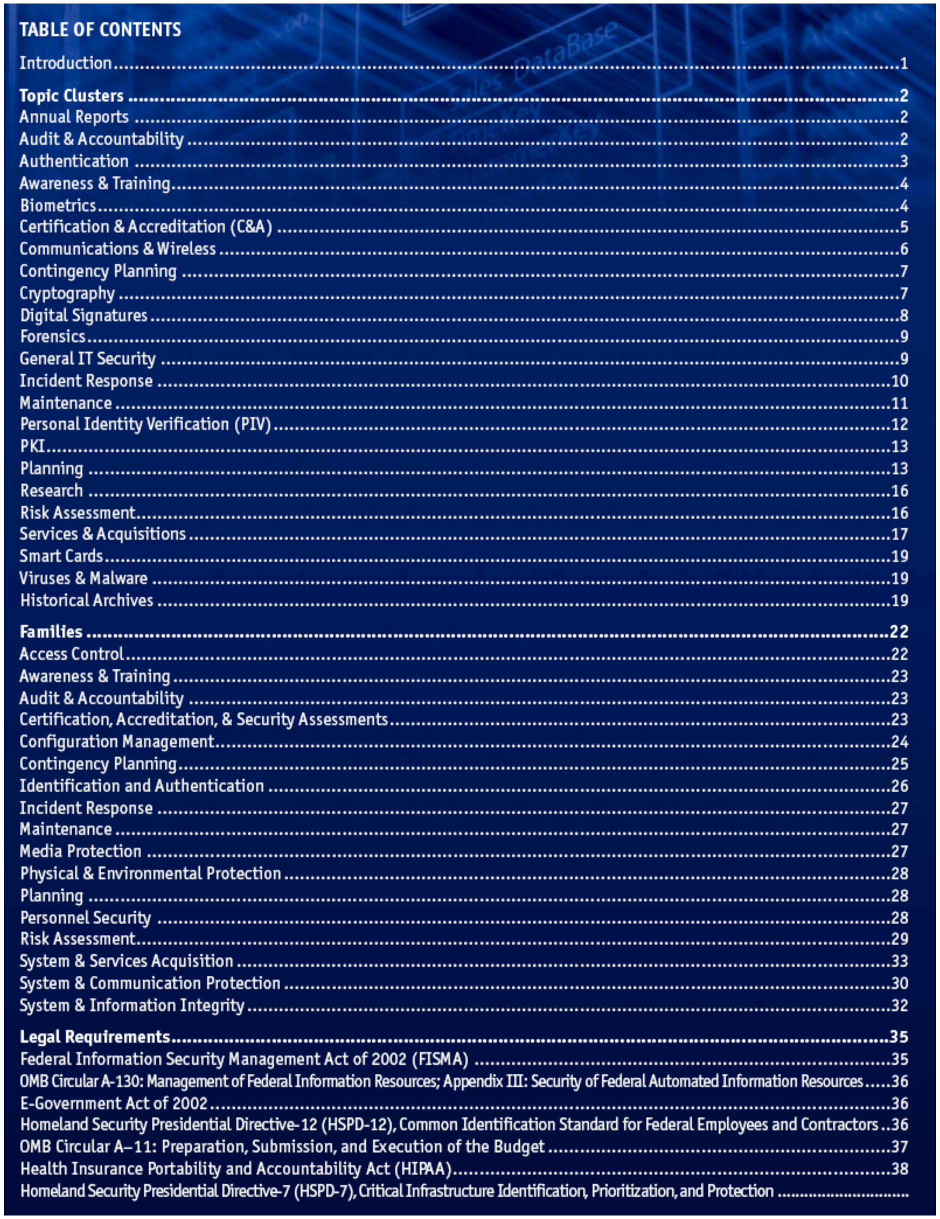
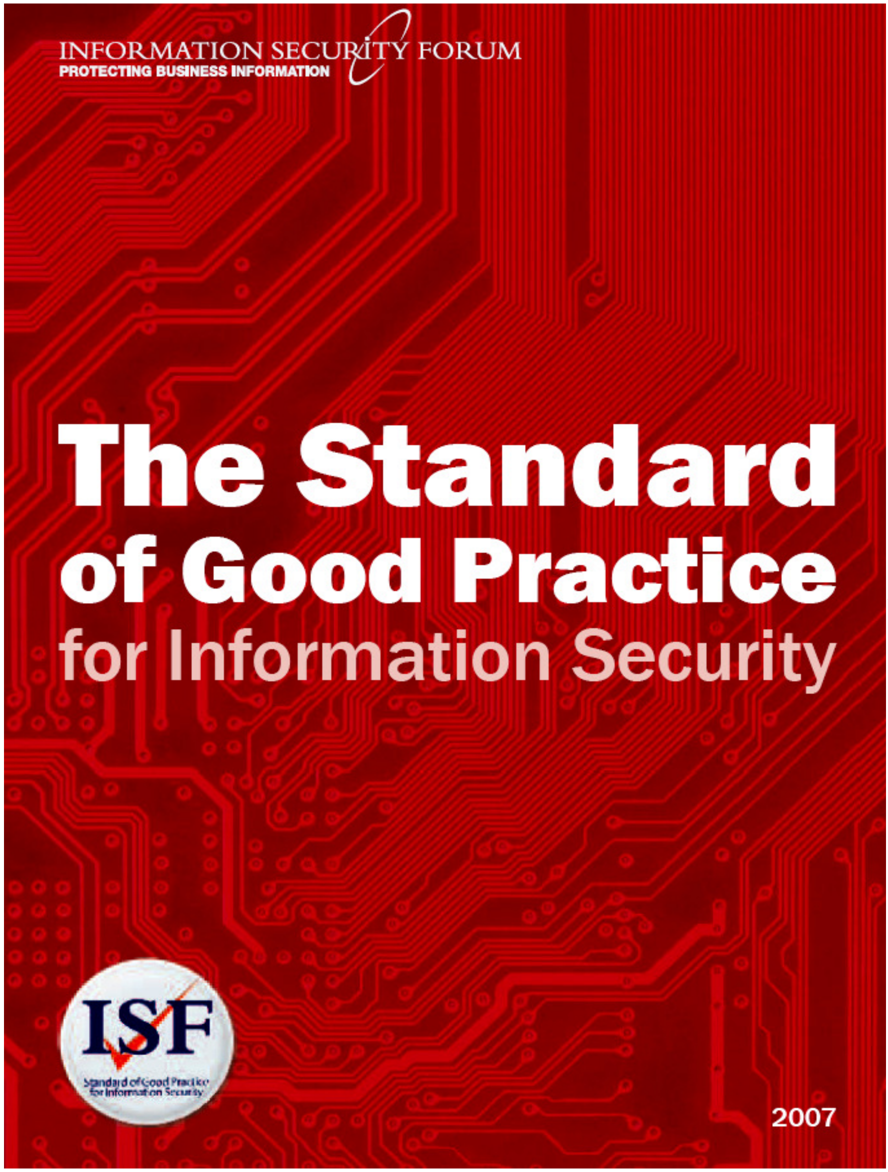
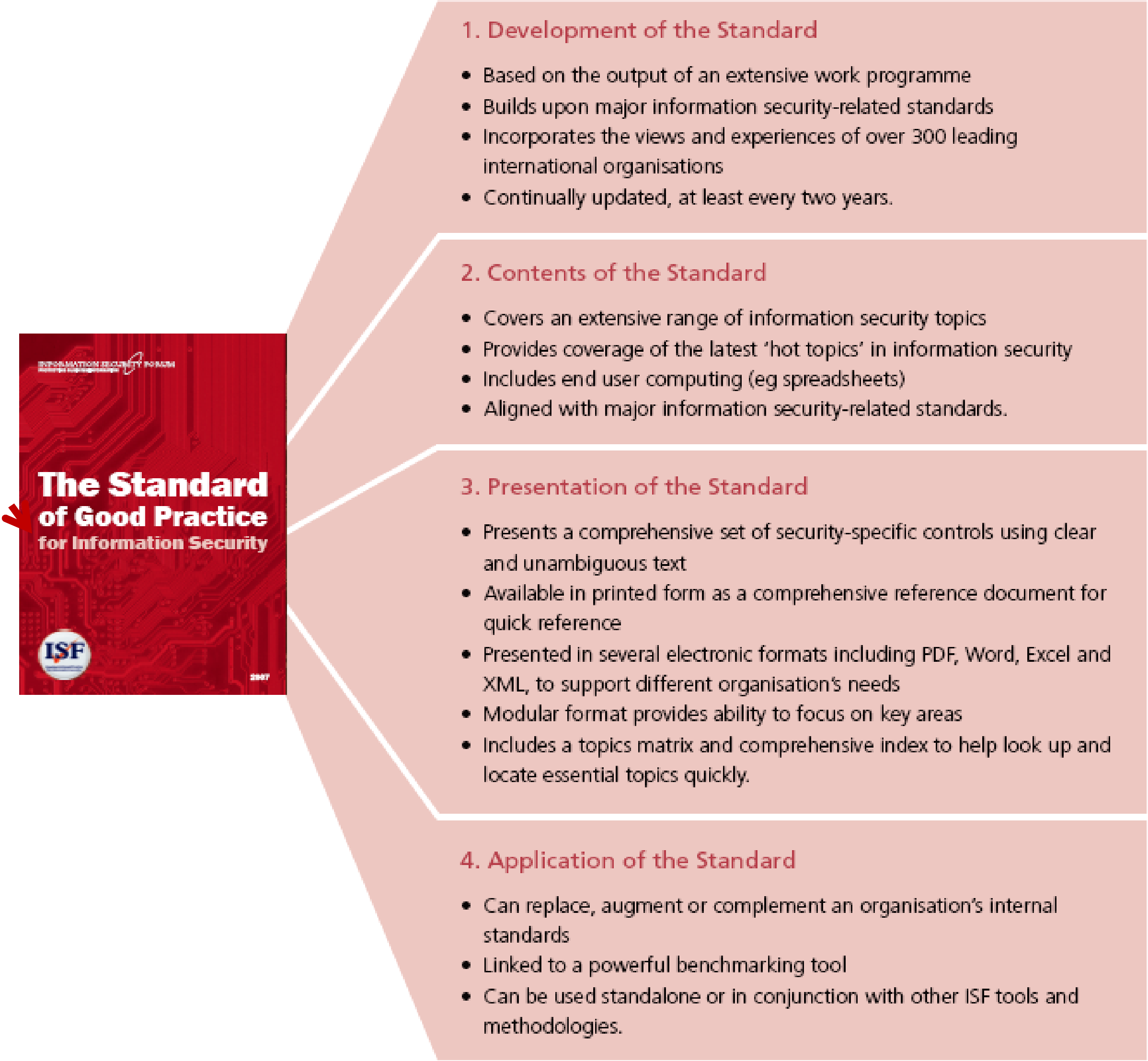


TABLE OF CONTENTS

ISF: Information Security Forum

(25th Anniversary - Founded 1989)


INFORMATION SECURITY FORUM
PROTECTING BUSINESS INFORMATION
The Standard of Good Practice for Information Security
ISF
Standard of Good Practice for Information Security
2007



1. Development of the Standard

- Based on the output of an extensive work programme
- Builds upon major information security-related standards
- Incorporates the views and experiences of over 300 leading international organisations
- Continually updated, at least every two years.

2. Contents of the Standard

- Covers an extensive range of information security topics
- Provides coverage of the latest 'hot topics' in information security
- Includes end user computing (eg spreadsheets)
- Aligned with major information security-related standards.

3. Presentation of the Standard

- Presents a comprehensive set of security-specific controls using clear and unambiguous text
- Available in printed form as a comprehensive reference document for quick reference
- Presented in several electronic formats including PDF, Word, Excel and XML, to support different organisation's needs
- Modular format provides ability to focus on key areas
- Includes a topics matrix and comprehensive index to help look up and locate essential topics quickly.

4. Application of the Standard

- Can replace, augment or complement an organisation's internal standards
- Linked to a powerful benchmarking tool
- Can be used standalone or in conjunction with other ISF tools and methodologies.

Implementation of ITU’s GCA *Cybersecurity* Framework

- The Implementation of the *ITU GCA* Framework can be significantly accelerated using the *National CERT* as a key programme catalyst:
    - *Legislation, Laws & Regulations* – Many CERTs support their government legal professionals in the definition, drafting & review of new cyberlaws & regulations
    - *Technical & Procedural Measures* – CERTs will usually have the most professional technical & operational cyber skills that can be replicated within critical sectors
    - *Organisational Structures* – The CERT may work with both public & private sector as the catalyst to support the creation of a national cybersecurity agency
    - *Capacity Building* – CERTs may work with the Educational Sector (Universities, Colleges & Schools), as well as Specialised Cybersecurity Businesses to organise and staff in-depth professional cybersecurity workshops and training courses
    - *International Collaboration* – The ITU already partners with many International and National CERT organisations including IMPACT, FIRST, US-CERT & ENISA.

…..In summary, the ITU encourages & supports countries to establish CERTs/CSIRTs and to further leverage these skills in the provision of a national cybersecurity strategy

Special Cybersecurity Technical Organisations

- Effective national and enterprise cybersecurity requires the implementation of professionally staffed technical organisations that are dedicated to security operations
- Here 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*
  - NCCU/eCrime Unit: National CyberCrime Unit (NCCU)– *We'll use the UK National Cyber Crime 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 UN/ITU and Interpol. We'll present some of the programmes that may be relevant to YOUR own Government, Institutions and Commercial Enterprises*

Professional *CERT/CSIRT* Organisations

- *Benefits:* Every national government, and major multi-site enterprise should consider the economic benefits of establishing a CERT/CSIRT.

- *Origins:* The original CERTs were established in the early 1990s following the arrival of the first computer viruses, worms & trojans.

- *CERT.org:* Carnegie Mellon University formed the 1st National CERT under contract from the US Government, and now runs www.CERT.org as a global partnership of national and regional CERTs.

- *ENISA:* Within European, the TERENA organisation (Trans-European Education and Research Networks Association) works with ENISA to manage the network of European CERTs, including skills training.

CERT/CSIRT Operations Alert Centre

- *Alerts:* A Fundamental Process within any CERT is the management and classification of “incidents”, and their routing to provide a response

- *Triage:* Some “incidents” may actually be due to some unusual statistical traffic patterns rather than an actual alert, “hack” or cybercrime

- *Risk:* Once an incident is classified the CERT will need to assign staff responsibility to assess the event risk and potential impact & damage

- *Communicate:* The CERT will communicate their analysis with relevant stakeholders, that may include government agencies, business stakeholders, and those responsible for critical information infrastructure

- *Neutralise:* CERT will work with partners to minimise the disruptive risk & damage in order to neutralise the cyber attack and any future threat

CERT/CSIRT – Information Process Flow

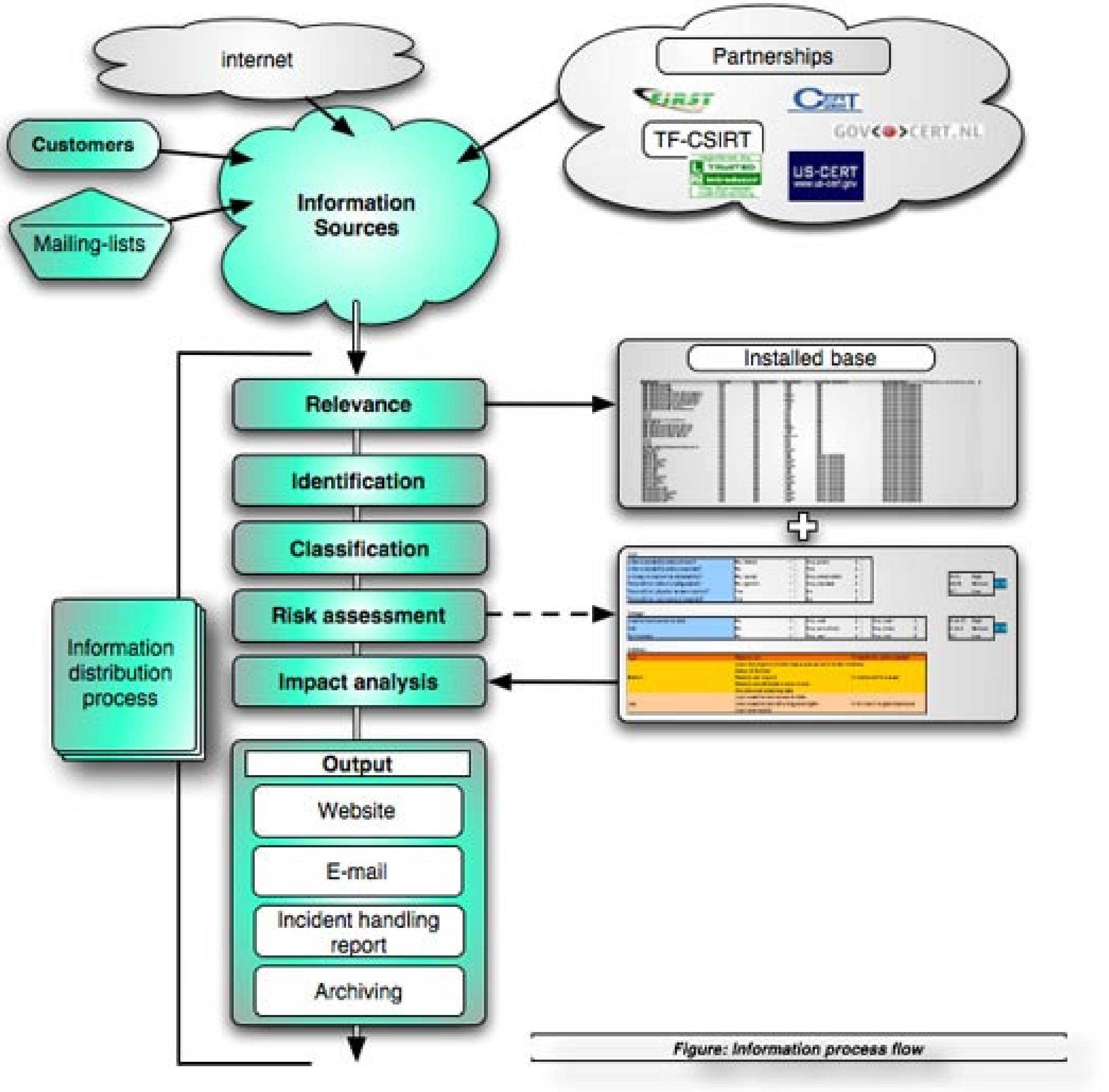
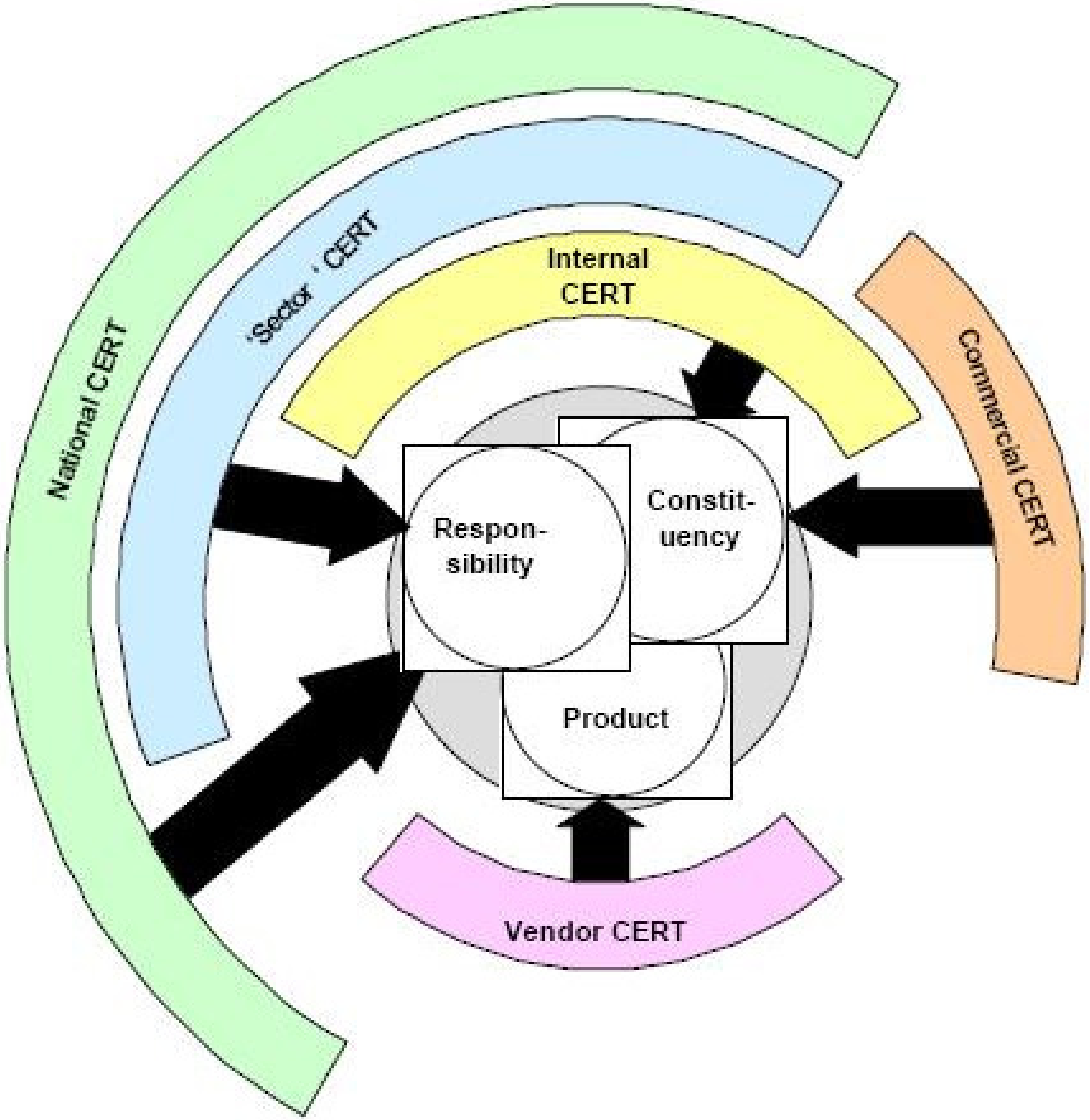
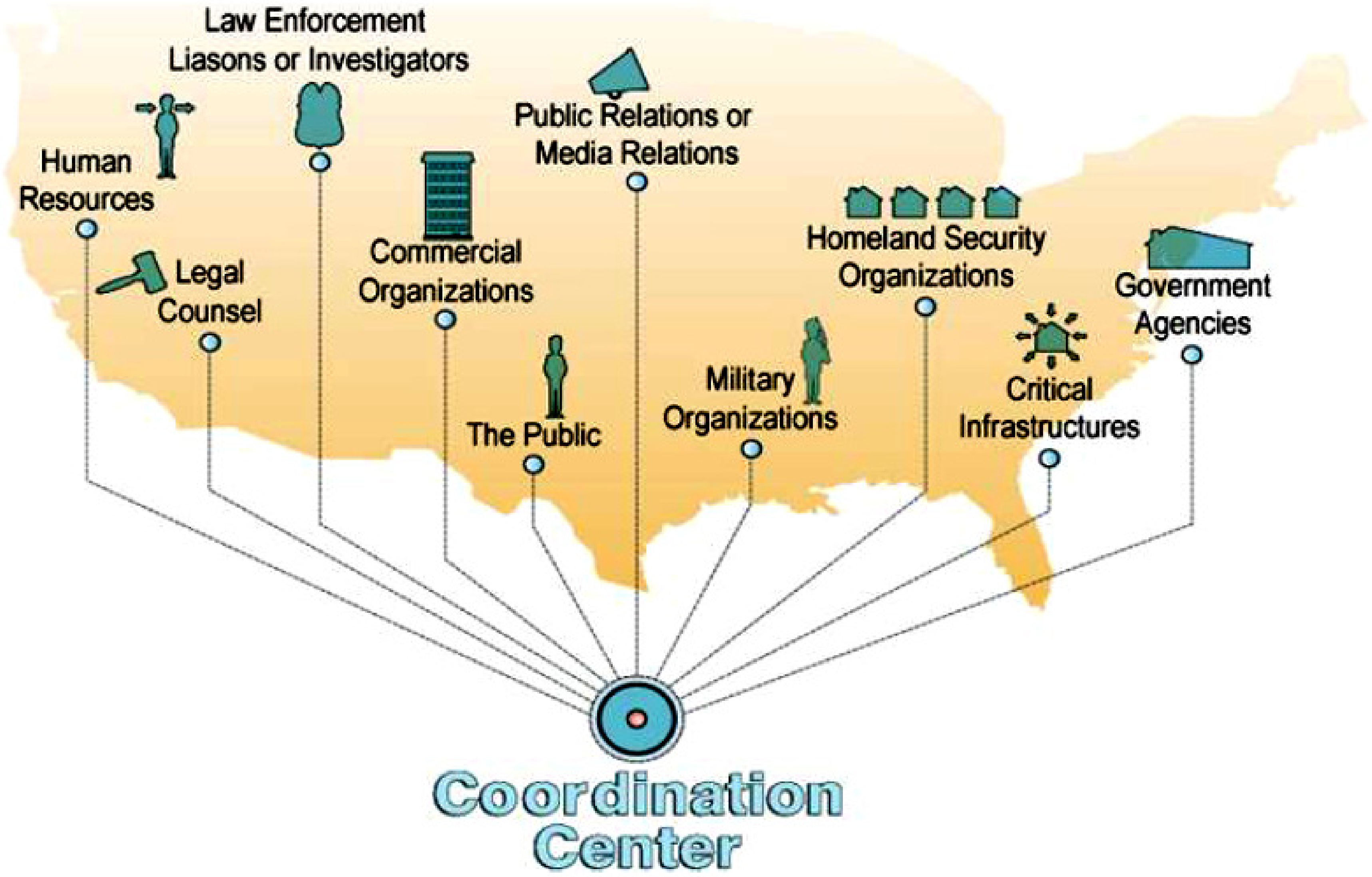


Figure: Information process flow

Networks of Public & Private *CERTs/CSIRTs*



Working with Major Stakeholders to create *your* *National CERT/CSIRT*



CERT/CSIRT Roll-Out Action Plan

- Government and Business may upgrade their CERT/CSIRT capability using the excellent on-line guidebooks from Carnegie Mellon University (CMU) & the European EU/ENISA

- These comprehensive step-by-step guides cover all aspects of the start-up action plan including:

  - *Business Case:* Development of the CERT/CSIRT Business Case
  - *Stakeholders:* Recruiting and Partnering with National Stakeholders
  - *Staff Training:* Recruitment and training of professional CERT staff
  - *Operations:* Establishing the Operational and Technical Procedures
  - *Incident Response:* Documented Process for classifying and responding to alerts

- Establishing a fully functional national CERT/CSIRT will probably take between 12 to 18 months depending on the scope of initial operations

- CERTs will need to continuously evolve, adapt and be trained to respond to new cyberthreats and potential attacks, and will to undergo annual compliance audits

ENISA: European *CERT* Exercises & Pilots

ENISA CERT Exercises pilots

November | 2009

Field Report

ENISA CERT Exercises – A field report from the pilots

Pilot 1: Chisinau, Moldova, Fighting cyber attacks

Pilot 2: Kyoto, Japan, Investigating infected computers

enisa
European Network
and Information
Security Agency

CERT Exercises

Handbook

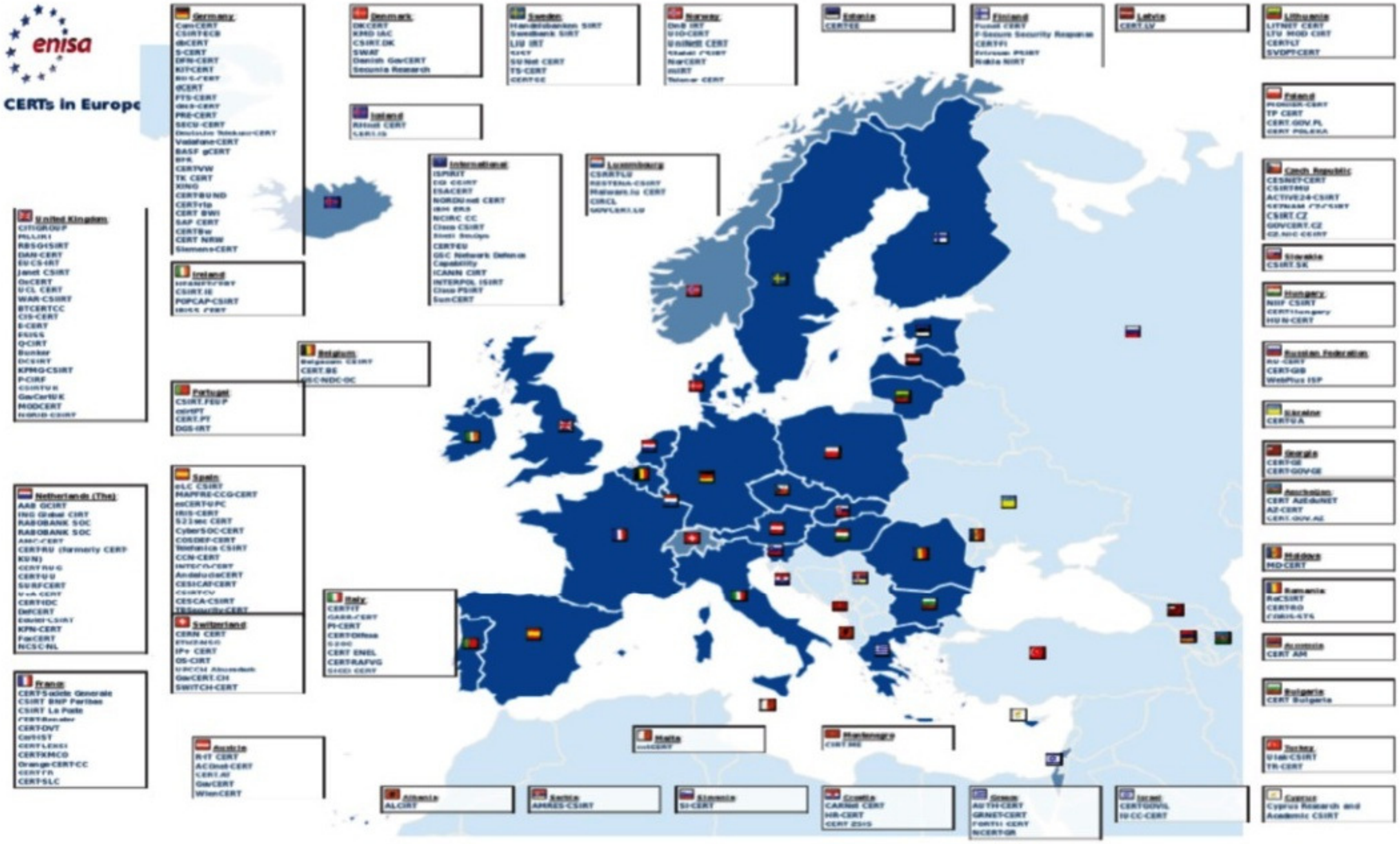
December | 08

enisa
European Network
and Information
Security Agency

www.enisa.europa.eu

Download: www.enisa.europa.eu/act/cert/

ENISA – *Latest CERT Inventory* – June 2014



CERTs in Europe Interactive Map, 2012 v3.0 © European Network and Information Security Agency (ENISA)

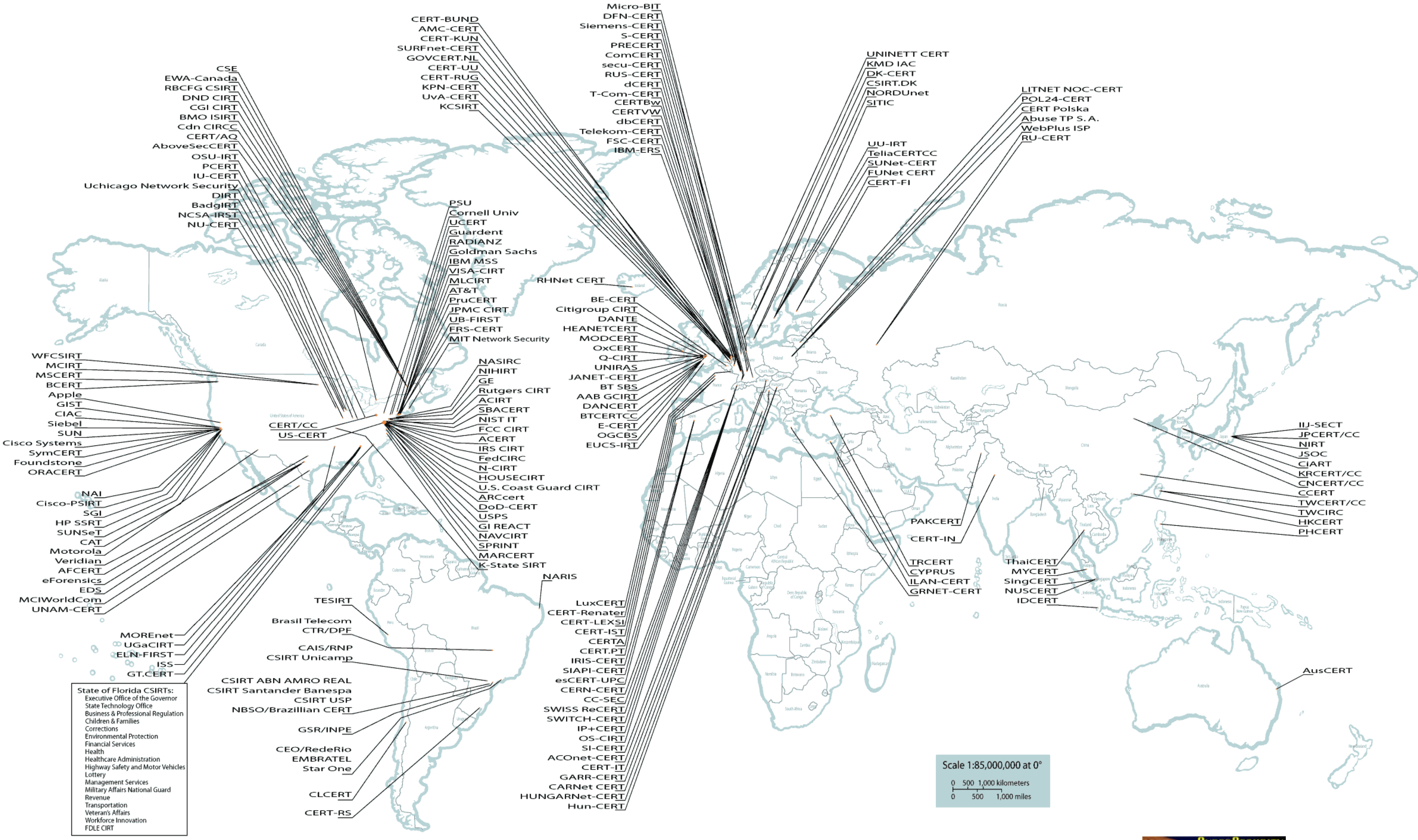
ENISA – CERT Inventory

Inventory of CERT teams and activites in Europe

Version 2.13, June 2014

Incident Response Teams Around the World

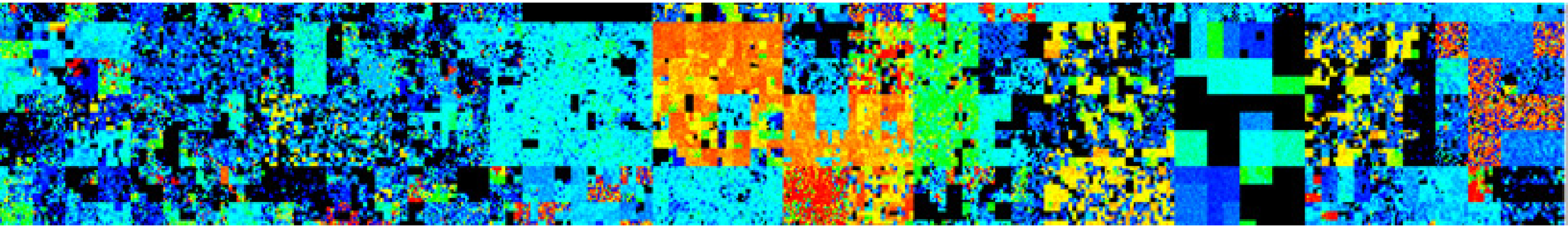
International cooperation speeds response to Internet security breaches.



State of Florida CSIRTs:
Executive Office of the Governor
State Technology Office
Business & Professional Regulation
Children & Families
Corrections
Environmental Protection
Financial Services
Health
Healthcare Administration
Highway Safety and Motor Vehicles
Lottery
Management Services
Military Affairs National Guard
Revenue
Transportation
Veteran's Affairs
Workforce Innovation
FDLE CIRT

National Cybersecurity Strategy, Roadmap & Actions

1 – Our Global Cybersecurity Challenge	2 – Developing the UN Cyber Framework	3 – National Cybersecurity Case Studies
4 – Dimensions of National Cybersecurity	5 – The UN Global Cyber Agenda (GCA)	6 – Technology, Standards & Operations
7 – New Legislation, Training & Partners	8 – National Roadmap - "Shopping List"	9 – Implementing YOUR Action Plan!



UN/ITU *Cybercrime* Toolkit

- *ITU Toolkit:* An excellent toolkit for countries to review and update legislation to reflect all aspects of cybercrime & cyberterrorism. Successive sections of the ITU toolkit consider:

- *Substantive Provisions:* Acts Against Computers, Computer Systems, Networks, Computer Data, Content Data, and Traffic Data

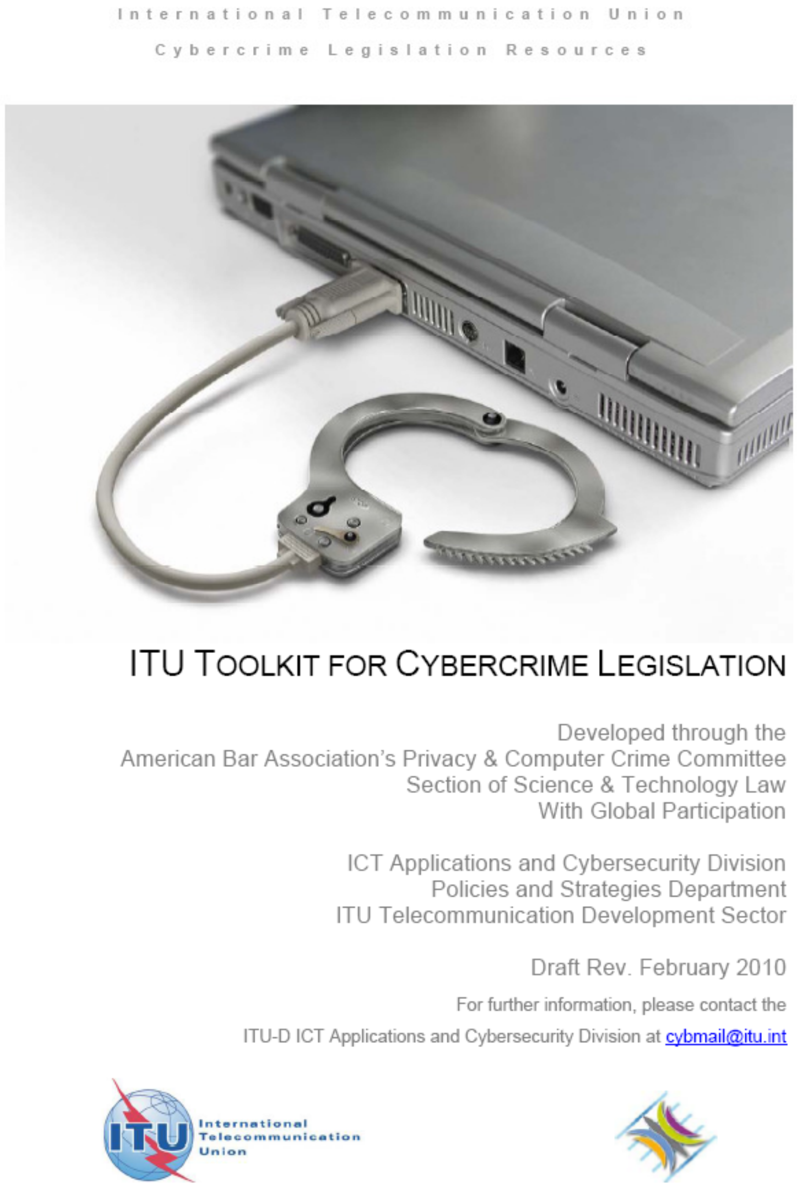
- *Procedural Provisions:* for Criminal Investigations and Proceedings for Offenses within both revised and new Legislation related to Cybercrime and Cybersecurity

- *Jurisdictional Provisions* and International Cooperation

- *Country Work Sheets:* In-Depth Templates that comprehensively span most of the conceivable cybercrime activities & attacks that may occur

- *International Comparisons:* Matrix of Provisions of the Cybercrime Laws that were reviewed from major countries as the basis for the toolkit

UN/ITU Toolkits: *Cybercrime Legislation* & *Cybercrime Guide* for Developing Countries



International Telecommunication Union

Cybercrime Legislation Resources

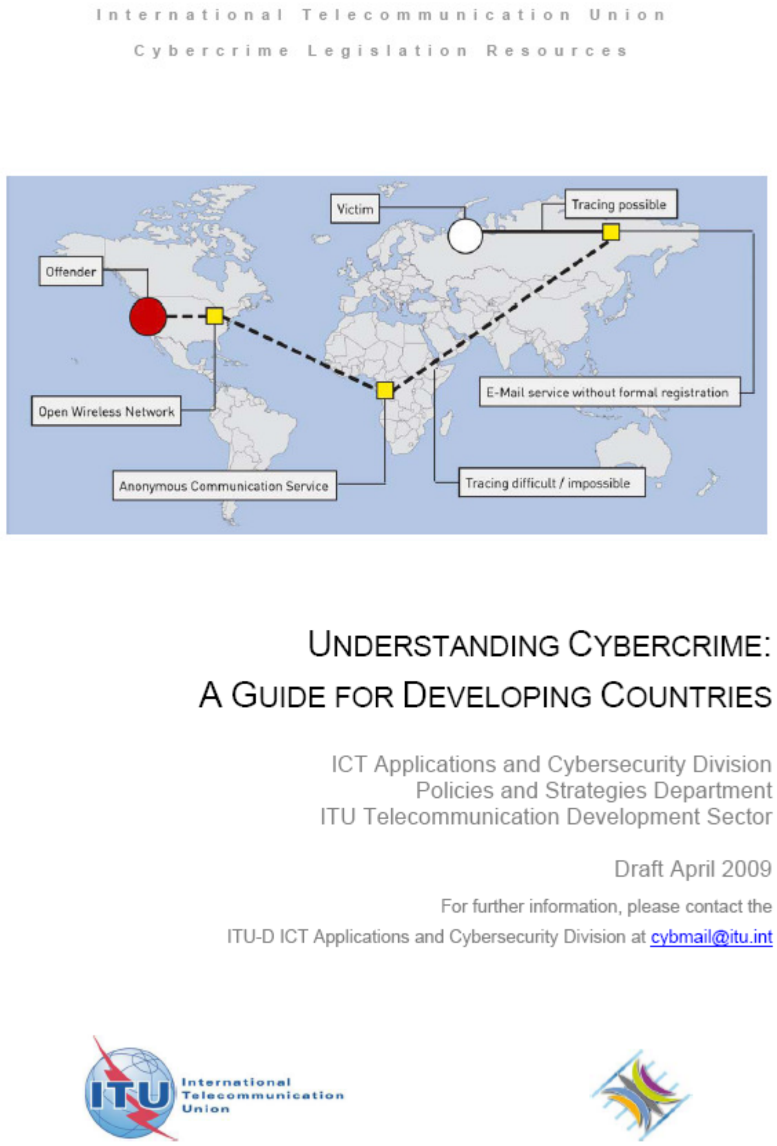
ITU TOOLKIT FOR CYBERCRIME LEGISLATION

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

Victim
Tracing possible
Offender
Open Wireless Network
E-Mail service without formal registration
Anonymous Communication Service
Tracing difficult / impossible
ITU
International
Telecommunication
Union

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

Summary of the UN/ITU Cybercrime Toolkit for *Cybersecurity Laws* & New Legislation

ITU CYBERCRIME TOOLKIT LEGISLATIVE REQUIREMENTS
Acts Against Computers, Computer Systems, Networks, Computer Data, Content Data, and Traffic Data
Section 1: Definition of Terms
Section 2: Unauthorized Access to Computers, Computer Systems, and Networks
Section 3: Unauthorized Access to or Acquisition of Computer Data, Content Data, Traffic Data
Section 4: Interference and Disruption
Section 5: Interception
Section 6: Misuse and Malware
Section 7: Digital Forgery
Section 8: Digital Fraud, Procure Economic Benefit
Section 9: Extortion
Section 10: Aiding, Abetting, and Attempting
Section 11: Corporate Liability
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

Jurisdictional Provisions
Section 21: Jurisdiction
International Cooperation
Section 22: International Cooperation: General Principles
Section 23: Extradition Principles
Section 24: Mutual Assistance: General Principles
Section 25: Unsolicited Information
Section 26: Procedures for Mutual Assistance
Section 27: Expedited Preservation of Stored Computer Data, Content Data, or Traffic Data
Section 28: Expedited Disclosure of Preserved Content Data, Computer Data or Traffic
Section 29: Mutual Assistance Regarding Access to Stored Computer Data, Content Data, or Traffic Data
Section 30: Trans Border Access to Stored Computer Data, Content Data, or Traffic Data
Section 31: Mutual Assistance In Real Time Collection of Traffic Data
Section 32: Mutual Assistance Regarding Interception of Content Data or Computer Data

UK *Cybercrime* Legislation

UK CYBERCRIME LEGISLATION
1. The Official Secrets Acts - 1911 to 1989
2. The Public Records Acts - 1958 to 1967
3. The Data Protection Act - 1998
4. The Freedom of Information Act - 2000
5. The Human Rights Act - 1998
6. The Computer Misuse Act 1990
7. The Copyright Designs and Patents Act 1988
8. The Civil Evidence Act 1968
9. The Police and Criminal Evidence Act 1984
10. The Wireless Telegraphy Act 1949 - 2006
11. The Communications Act 2003
12. The Regulation of Investigatory Powers Act 2000 (RIPA)
13. The Telecommunications Regulations 2000 (Interception)
14. The Civil Contingencies Act 2004
15. The Anti-Terrorism, Crime and Security Act 2001
16. The Forgery and Counterfeiting Act 1981
17. The Fraud Act 2006
18. Police Justice Act 2006
19. The Theft Act - 1978 to 1996
20. The Cybersecurity Strategy - Cabinet Office - June 2009

1. UK Official Secrets Acts 1911 to 1989

- **Official Secrets Acts 1911 to 1989**
  - *Unauthorised Disclosure of Official Informatio*n

➢ Under the Official Secrets Act 1989, it is an offence for a Crown servant or government contractor to disclose official information in any of the protected categories if the disclosure is made without lawful authority and is damaging to the national interest. It is also an offence if a member of the public, or any other person who is not a Crown servant or government contractor under the Act, has in his or her possession, official information in one of the protected categories, and the information has been disclosed without lawful authority, or entrusted by a Crown servant or government contractor on terms requiring it to be held in confidence.

➢ *Cybersecurity Relevance: Covers all electronic communications, documents and media whatever format.*

6. Communications and Information Systems Computer Misuse Act 1990 – (CMA)

6. Communications and Information Systems Computer Misuse Act 1990 – (CMA)

- This deals with the rights of computer owners against the unauthorised use of a computer by any party, making offences of attempted or actual penetration or subversion of computer systems. Under the terms of Section 3 of the Computer Misuse Act it is a criminal offence to introduce unauthorised software into a computer system with the intention of impairing the operation of the computer system or the integrity of any data or program stored within the computer system. Updated through the Police and Justice Act (2006)

- *- Cybersecurity Relevance: This is a key act that makes it illegal to penetrate or hack computer systems, as well as to install malicious codes, "bots", trojans or any other unauthorized software or device.*

15. The UK Anti-Terrorism, Crime & Security Act 2001

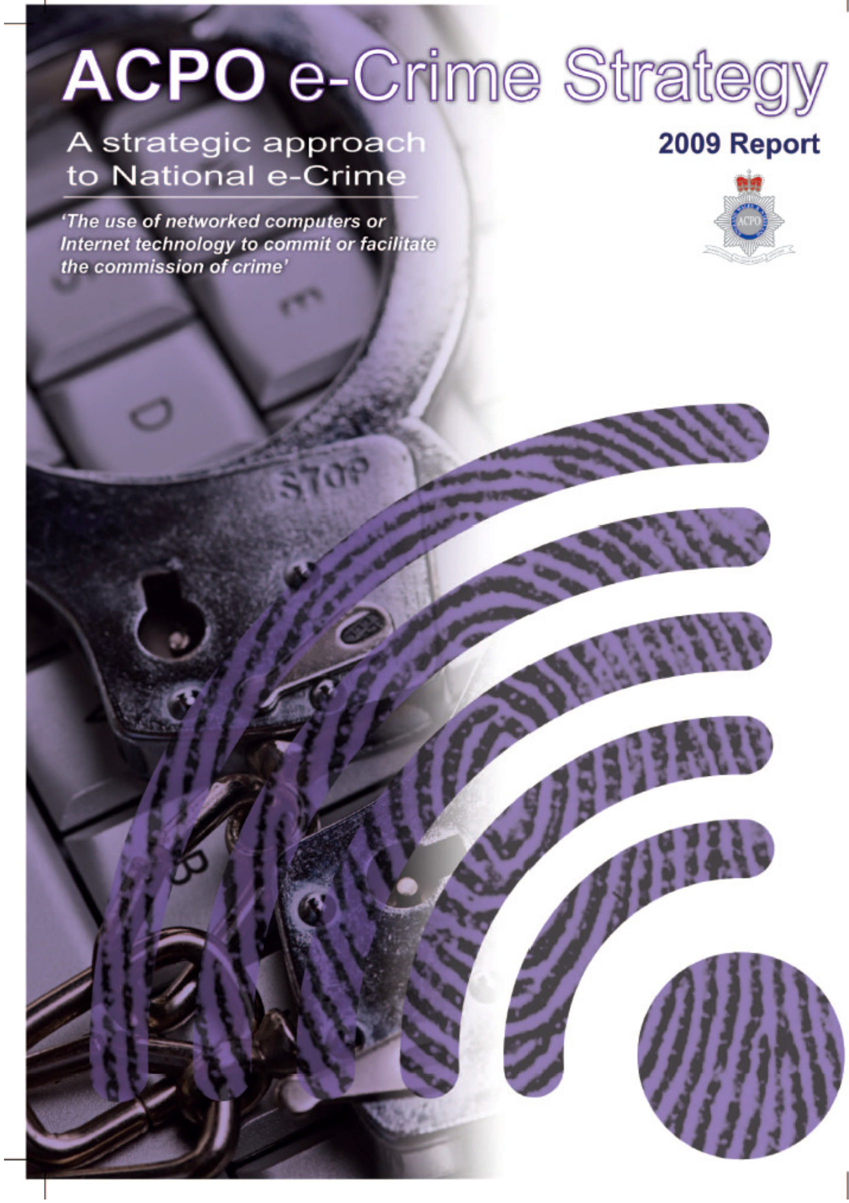
15. The Anti-Terrorism, Crime and Security Act 2001

- This relatively recent act includes electronic evidence as well as covering other aspects of 21st Century threats, risks and challenges that are closely related to cyberattacks and cybercrime.

- *Cybersecurity Relevance: Establishes the right of the authorities to take away electronic evidence and assets such as laptops, storage & networking device that may then be used as criminal evidence in court.*

A Strategic Approach to e-Crime Unit Strategy

Since 2013: UK National Cyber Crime Unit – NCCU (PCeU & SOCA Cyber)

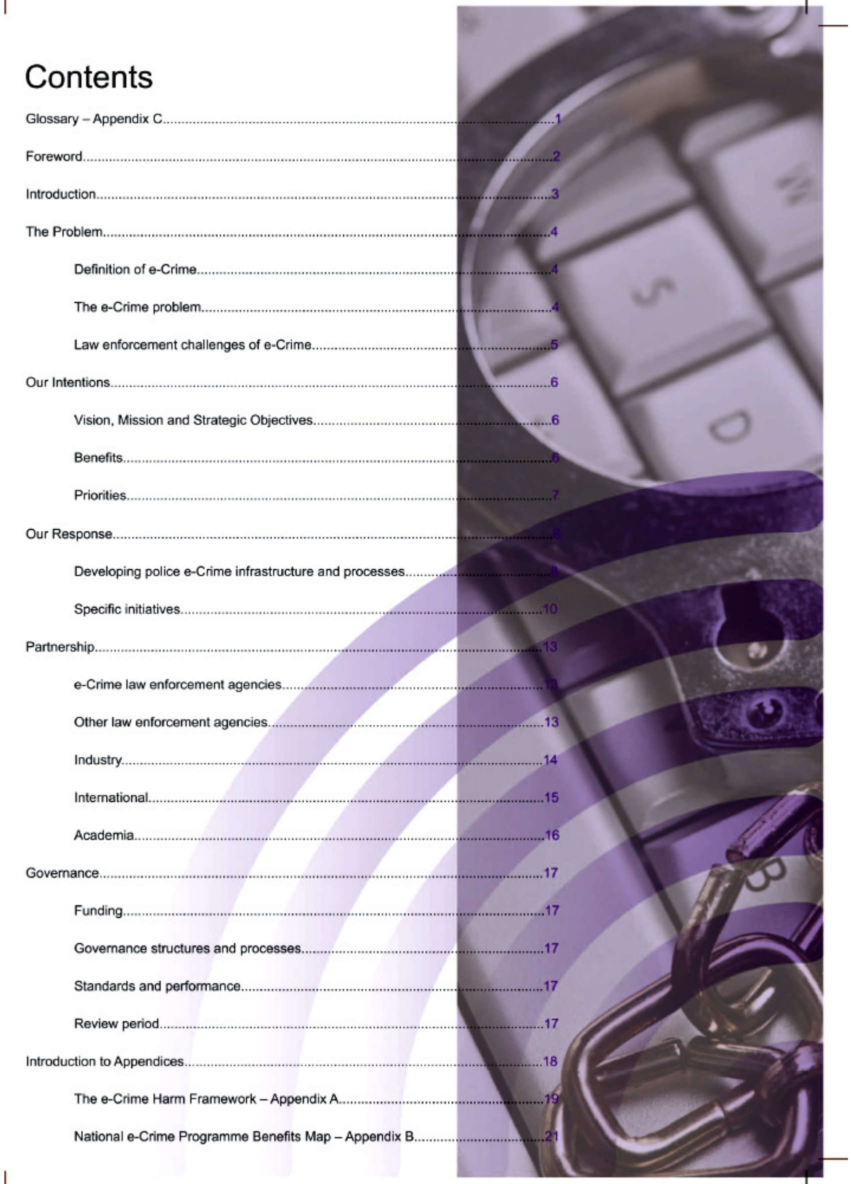


ACPO e-Crime Strategy

A strategic approach
to National e-Crime

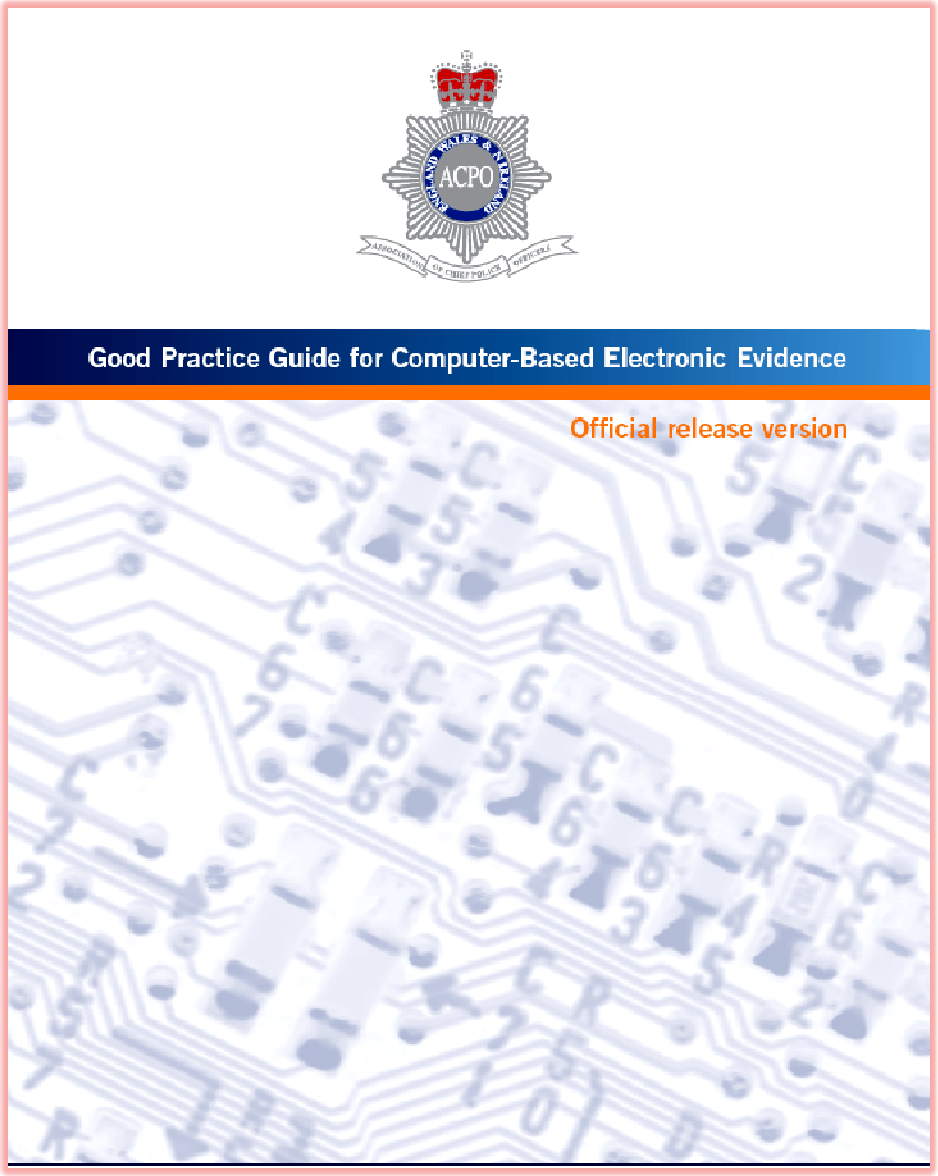
'The use of networked computers or Internet technology to commit or facilitate the commission of crime'

2009 Report



Contents

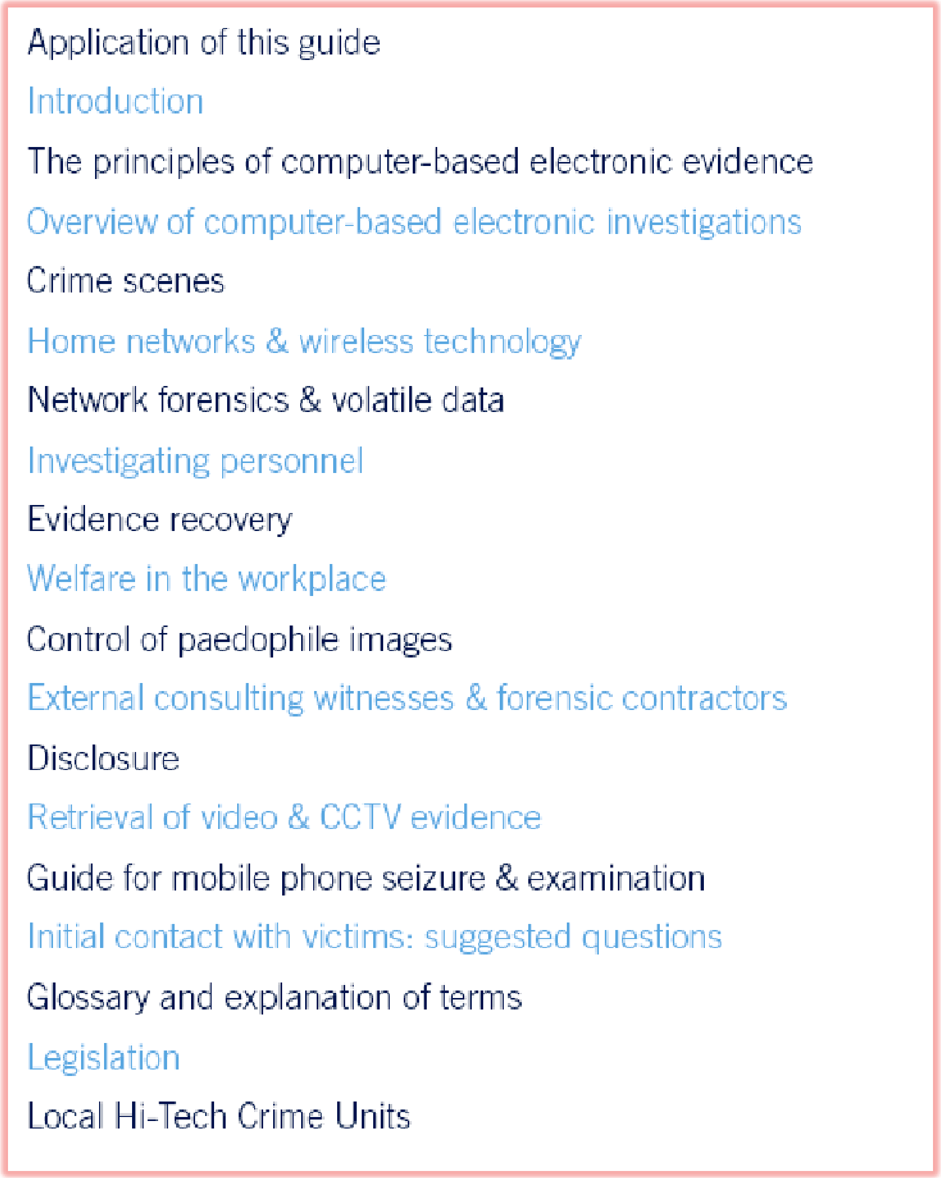
UK Guide to Computer-Based *Electronic Evidence*



ACPO

Good Practice Guide for Computer-Based Electronic Evidence

Official release version

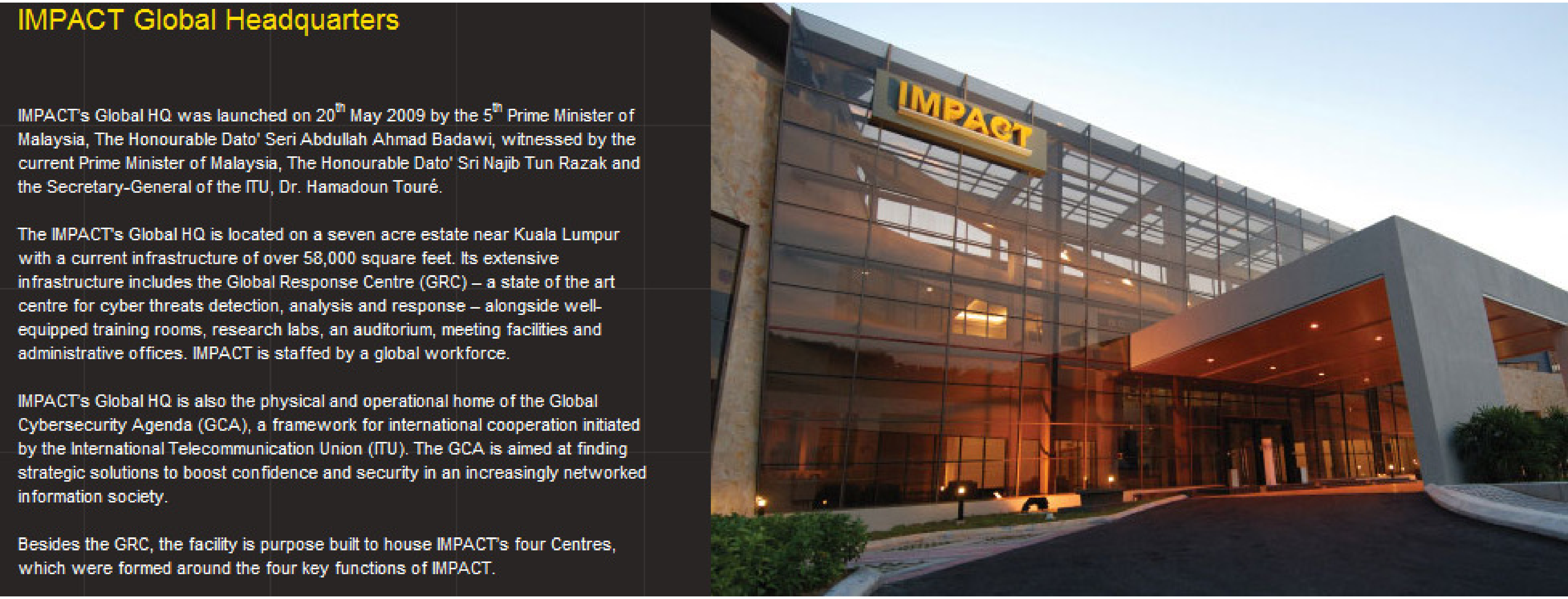


- Application of this guide
- Introduction
- The principles of computer-based electronic evidence
- Overview of computer-based electronic investigations
- Crime scenes
- Home networks & wireless technology
- Network forensics & volatile data
- Investigating personnel
- Evidence recovery
- Welfare in the workplace
- Control of paedophile images
- External consulting witnesses & forensic contractors
- Disclosure
- Retrieval of video & CCTV evidence
- Guide for mobile phone seizure & examination
- Initial contact with victims: suggested questions
- Glossary and explanation of terms
- Legislation
- Local Hi-Tech Crime Units

ITU: Cybersecurity Training – UTECH, Kingston, JAMAICA

Government, Central Bank, Energy, Telecoms Sectors

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.

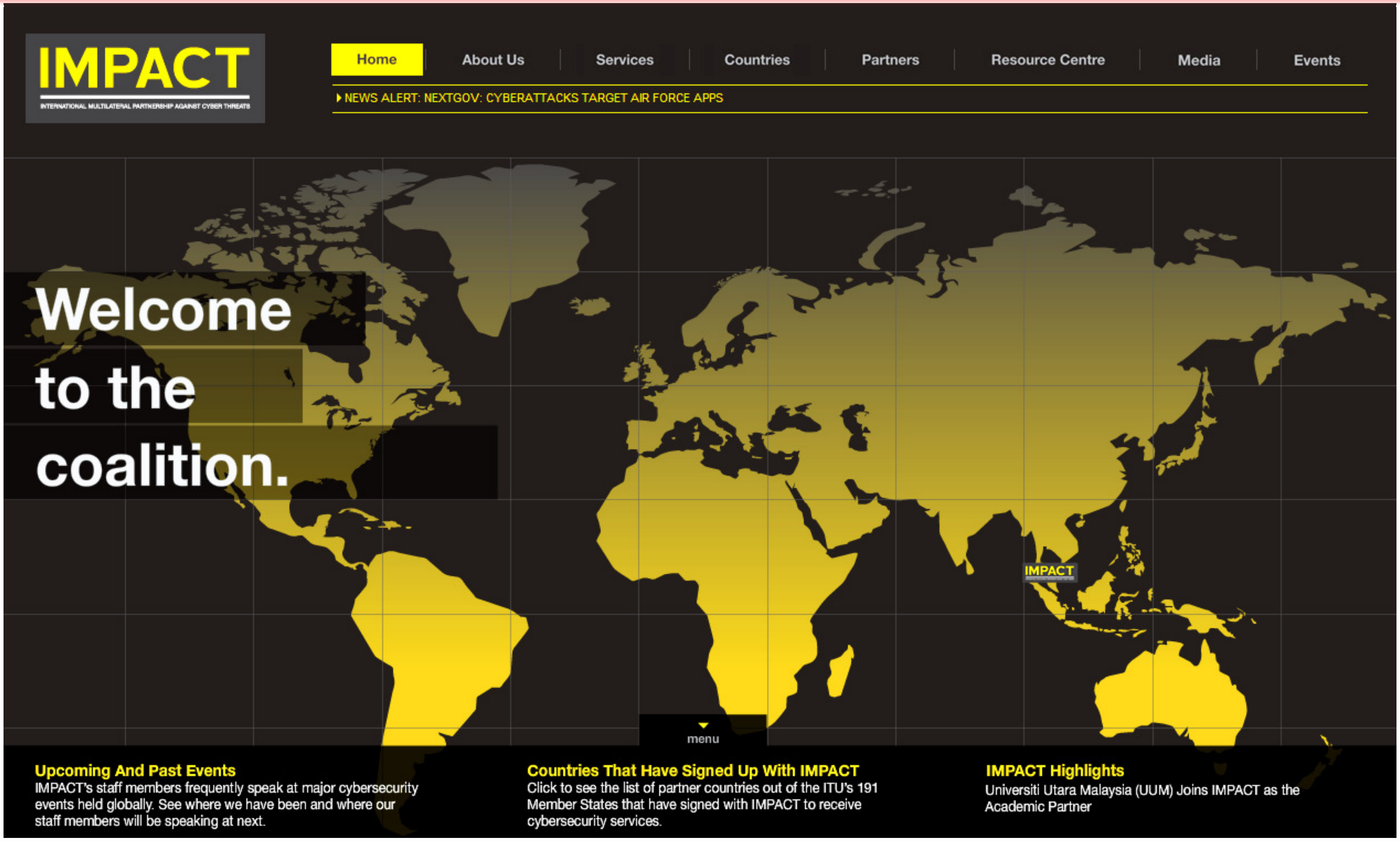
IMPACT's Global HQ is also the physical and operational home of the Global Cybersecurity Agenda (GCA), a framework for international cooperation initiated by the International Telecommunication Union (ITU). The GCA is aimed at finding strategic solutions to boost confidence and security in an increasingly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

IMPACT International Partners: ITU, UN, INTERPOL and CTO



▸ NEWS ALERT: NEXTGOV: CYBERATTACKS TARGET AIR FORCE APPS

Welcome to the coalition.

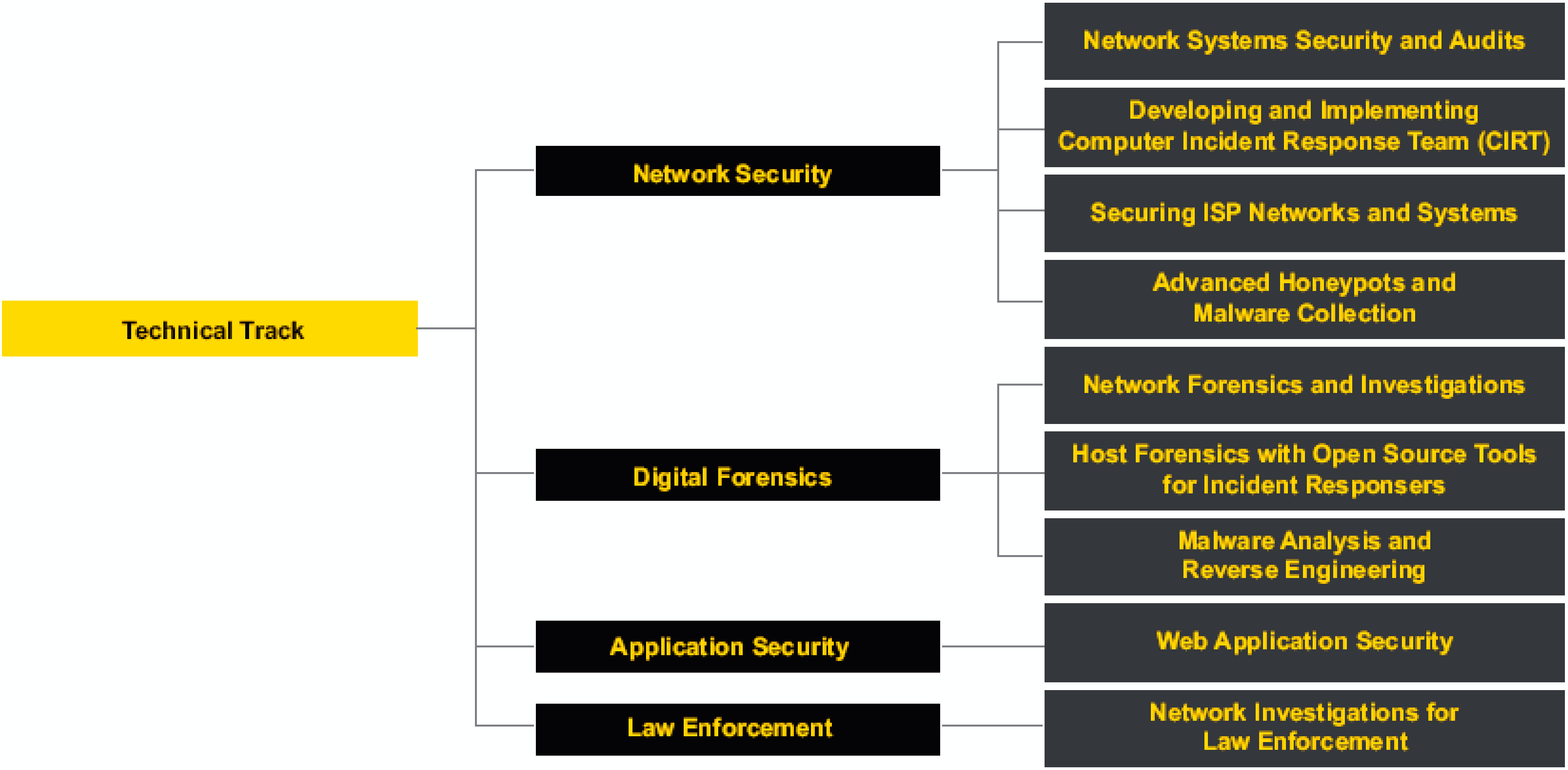
Upcoming And Past Events
IMPACT's staff members frequently speak at major cybersecurity events held globally. See where we have been and where our staff members will be speaking at next.

Countries That Have Signed Up With IMPACT
Click to see the list of partner countries out of the ITU's 191 Member States that have signed with IMPACT to receive cybersecurity services.

IMPACT Highlights
Universiti Utara Malaysia (UUM) Joins IMPACT as the Academic Partner

Industry Partners include: Symantec, Kaspersky Labs, Cisco, Microsoft, (ISC)^2, F-Secure, EC-Council, Iris, GuardTime, Trend Micro and the SANS Institute

IMPACT: *Cybersecurity Technical Training*



Technical Track

Network Security

- Network Systems Security and Audits
- Developing and Implementing Computer Incident Response Team (CIRT)
- Securing ISP Networks and Systems
- Advanced Honeypots and Malware Collection

Digital Forensics

- Network Forensics and Investigations
- Host Forensics with Open Source Tools for Incident Responsers
- Malware Analysis and Reverse Engineering

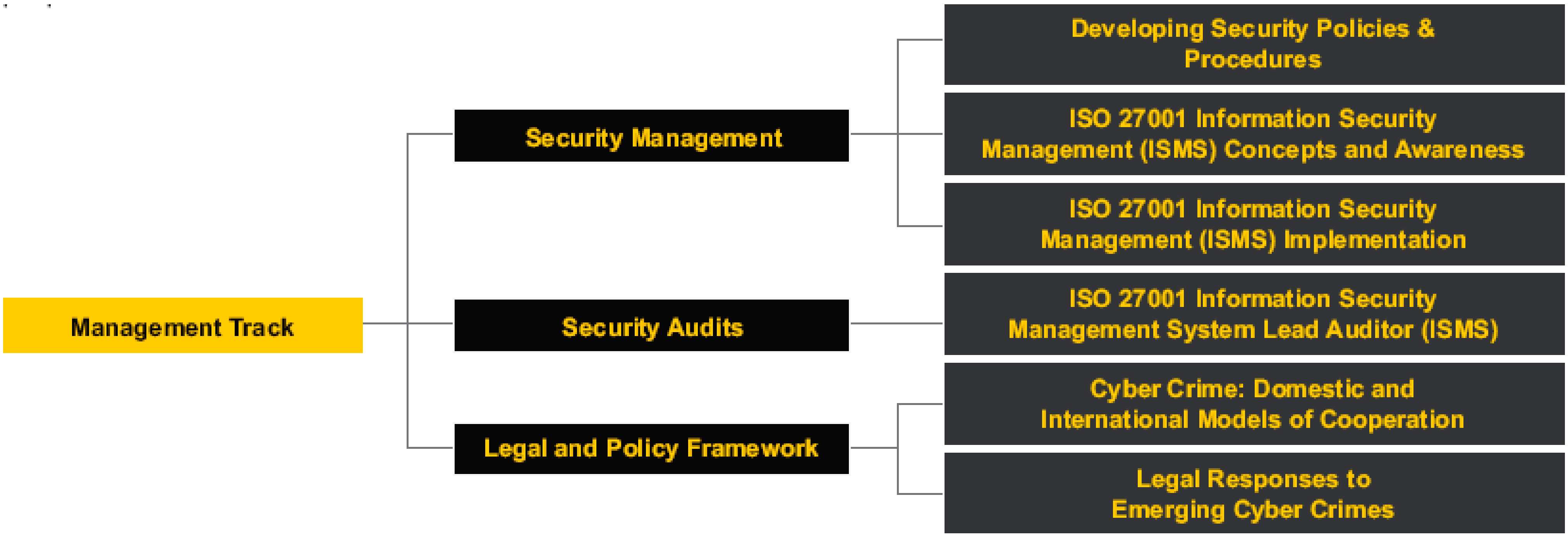
Application Security

- Web Application Security

Law Enforcement

- Network Investigations for Law Enforcement

IMPACT: *Cyber Management Training*



Management Track

Security Management

Security Audits

Legal and Policy Framework

Developing Security Policies & Procedures

ISO 27001 Information Security Management (ISMS) Concepts and Awareness

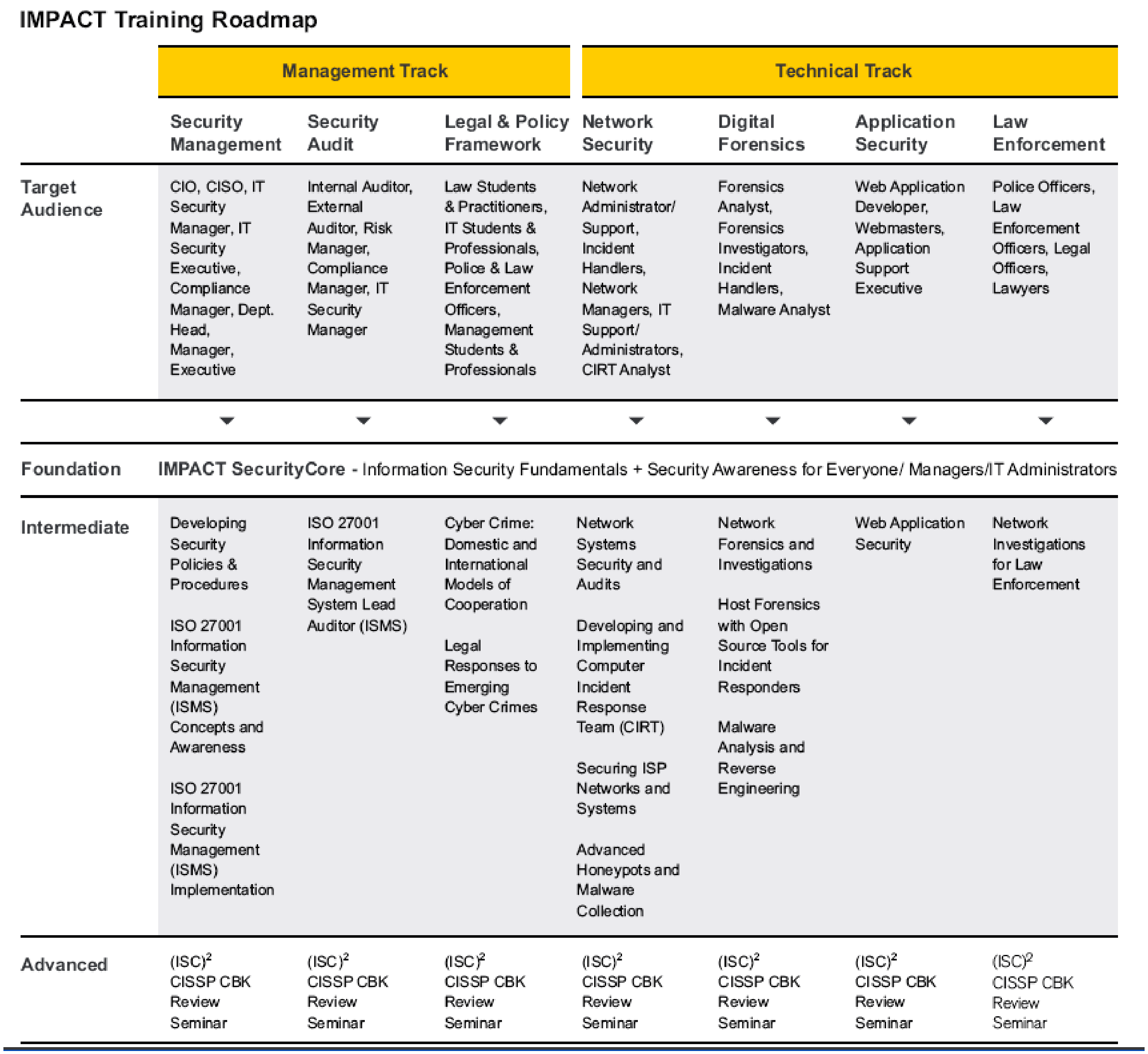
ISO 27001 Information Security Management (ISMS) Implementation

ISO 27001 Information Security Management System Lead Auditor (ISMS)

Cyber Crime: Domestic and International Models of Cooperation

Legal Responses to Emerging Cyber Crimes

IMPACT: *Cybersecurity Training Roadmap*

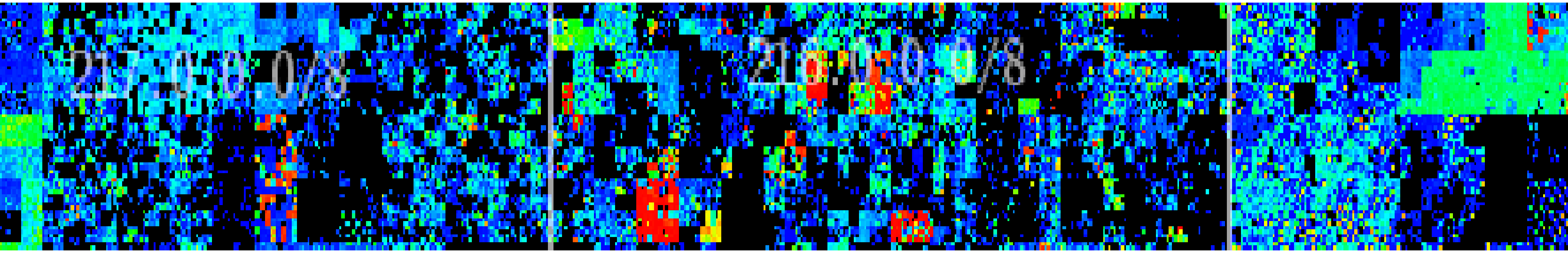


IMPACT Training Roadmap

	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

National Cybersecurity Strategy, Roadmap & Actions

1 – Our Global Cybersecurity Challenge	2 – Developing the UN Cyber Framework	3 – National Cybersecurity Case Studies
4 – Dimensions of National Cybersecurity	5 – The UN Global Cyber Agenda (GCA)	6 – Technology, Standards & Operations
7 – New Legislation, Training and Partners	**8 – National Roadmap – "Shopping List"**	9 – Implementing YOUR Action Plan!



Cybersecurity Benefits: *Government*

- Improved cybersecurity provides significant benefits to the Government & Critical National Utilities & Enterprises including:
  - *eGovernment:* Fully secure & cost effective delivery of on-line services to both citizens and businesses, such as taxes & customs, social welfare, civil & land registries, passports & driving licences
  - *Defence:* Early warning, alerts and defences against cyberattacks through national CERT (Computer Emergency Response Centre)
  - *Cybercrime:* Investigate, Digital Forensics and Prosecution of cybercrimes such ID & Financial Theft, “Computer Misuse, Laundering, On-Line Drug Trafficking & Pornographic Materials
  - *Cyberterrorism:* Ability to assess, predict and prevent potential major cyber terrorist attacks, and to minimise damage during events
  - *Power & Water Utilities:* Prevent malicious damage to control systems
  - *Telecommunications:* Top security of government communications with alternative routings, encryption & protection against cyberattack

National Cybersecurity Strategy : *"The Shopping List"*

Smart Security for Business & Government is a Multi-Year Programme!

1) ***National Cybersecurity Agency***: Establishment of a CERT/CSIRT & National Government Cybersecurity Agency within the Government Ministries
2) ***CNI:*** Long Term Critical National Information Infrastructure Protection (CNI)
3) ***System Upgrades***: Technical Infrastructure Upgrades including Hardware, Software, Databases, Secure Network Links, Biometrics & RFID
4) ***Back-Up***: Disaster Recovery, Business Continuity and Back-Up Systems
5) ***Physical Security***: Physical Security Applications – CCTV, Alarms, Control Centre
6) ***Awareness Campaign***: Government Campaign for Cybersecurity awareness
7) ***Training***: National Cybersecurity Skills & Professional Training Programme
8) ***Encryption***: National User & Systems PKI Authentication Programme
9) ***Laws:*** Programme for Drafting and Enforcing Cyber Laws, Policies & Regulations

……It is also important to develop an in-depth economic "cost-benefit" analysis and Business Case in order to evaluate the "Return on Investment" for Smart Security

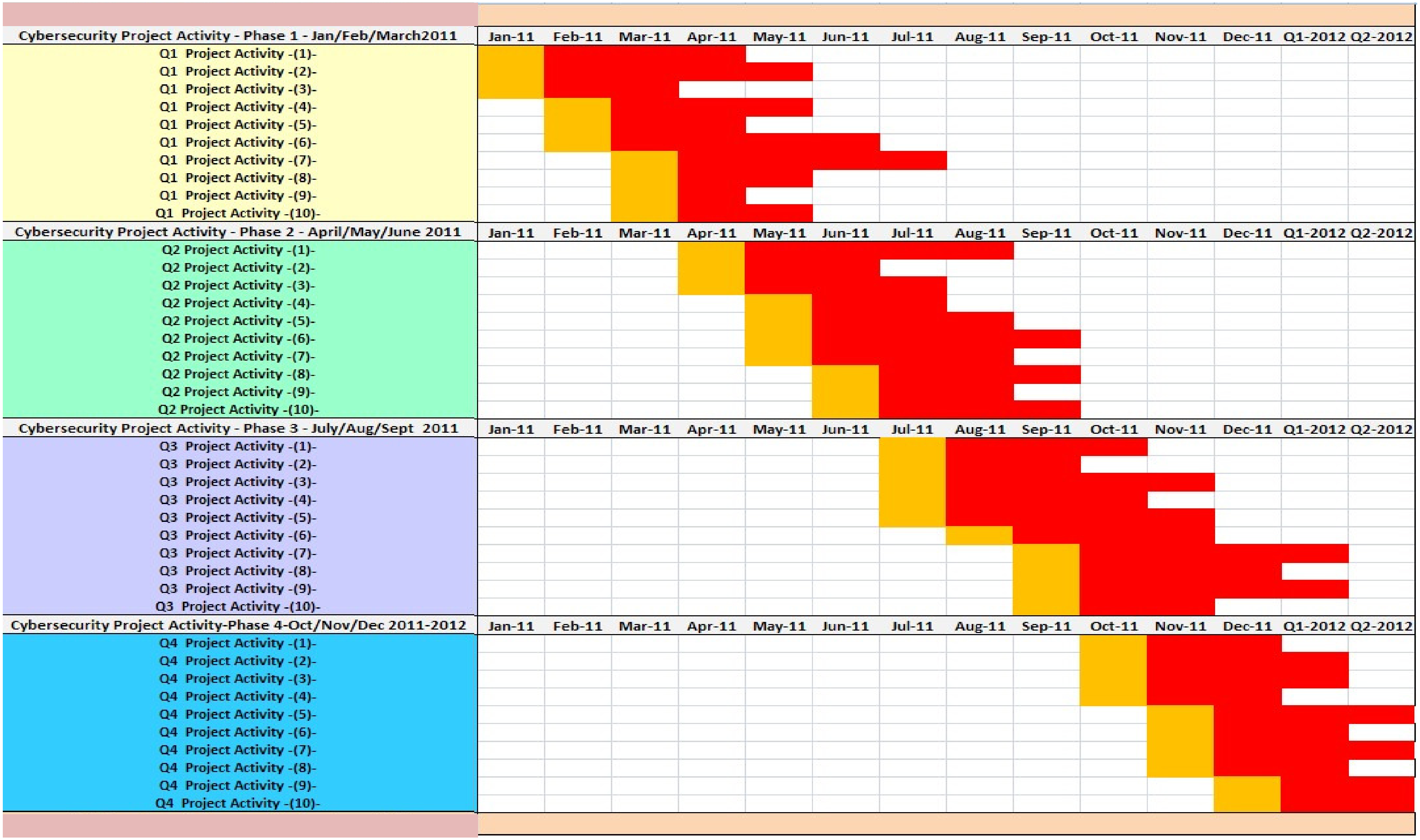
National Cybersecurity *Operational Budgets*

- Managing cybersecurity is an ongoing task with a continuous need for government & business systems upgrades, staff training, and response to emergency cyber events & alerts

- Annual Operational Security Budgets will need to include allowances for:
  - Staff salaries & operational costs for the proposed National Cyber Agency
  - Costs for tackling cybercrime through a possible National Cybercrime Unit
  - Management of cybersecurity by Jamaican Military & Defence Organisation
  - Costs of required annual security audits to ensure ongoing compliance
  - Professional training courses at leading Jamaican Institutions such as UTECH
  - Costs for maintaining "best practice" cybersecurity within each of the critical service sectors within the Jamaican Economy such as Banking, Tourism & Trade
  - Regular Systems, Computing & Communications reviews & upgrades for all secure government computing centres, as well as those for major enterprises
  - On-going costs top support extensive international partnerships & collaboration

National Cybersecurity Project RoadMap:

Spanning the UN/ITU Cybersecurity Framework



Cybersecurity Project Activity - Phase 1 - Jan/Feb/March2011	Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q1 Project Activity -(1)-	🟧	🟥	🟥	🟥										
Q1 Project Activity -(2)-	🟧	🟥	🟥	🟥	🟥									
Q1 Project Activity -(3)-	🟧	🟥	🟥											
Q1 Project Activity -(4)-		🟧	🟥	🟥	🟥									
Q1 Project Activity -(5)-		🟧	🟥	🟥										
Q1 Project Activity -(6)-		🟧	🟥	🟥	🟥	🟥								
Q1 Project Activity -(7)-			🟧	🟥	🟥	🟥	🟥							
Q1 Project Activity -(8)-			🟧	🟥	🟥									
Q1 Project Activity -(9)-			🟧	🟥										
Q1 Project Activity -(10)-			🟧	🟥	🟥									

Cybersecurity Project Activity - Phase 2 - April/May/June 2011	Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q2 Project Activity -(1)-				🟧	🟥	🟥	🟥	🟥						
Q2 Project Activity -(2)-				🟧	🟥	🟥								
Q2 Project Activity -(3)-				🟧	🟥	🟥	🟥							
Q2 Project Activity -(4)-					🟧	🟥	🟥							
Q2 Project Activity -(5)-					🟧	🟥	🟥	🟥						
Q2 Project Activity -(6)-					🟧	🟥	🟥	🟥	🟥					
Q2 Project Activity -(7)-					🟧	🟥	🟥	🟥						
Q2 Project Activity -(8)-						🟧	🟥	🟥	🟥					
Q2 Project Activity -(9)-						🟧	🟥	🟥						
Q2 Project Activity -(10)-						🟧	🟥	🟥	🟥					

Cybersecurity Project Activity - Phase 3 - July/Aug/Sept 2011	Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q3 Project Activity -(1)-							🟧	🟥	🟥	🟥				
Q3 Project Activity -(2)-							🟧	🟥	🟥					
Q3 Project Activity -(3)-							🟧	🟥	🟥	🟥	🟥			
Q3 Project Activity -(4)-							🟧	🟥	🟥	🟥				
Q3 Project Activity -(5)-							🟧	🟥	🟥	🟥	🟥			
Q3 Project Activity -(6)-								🟧	🟥	🟥	🟥			
Q3 Project Activity -(7)-									🟧	🟥	🟥	🟥	🟥	
Q3 Project Activity -(8)-									🟧	🟥	🟥	🟥		
Q3 Project Activity -(9)-									🟧	🟥	🟥	🟥	🟥	
Q3 Project Activity -(10)-									🟧	🟥	🟥			

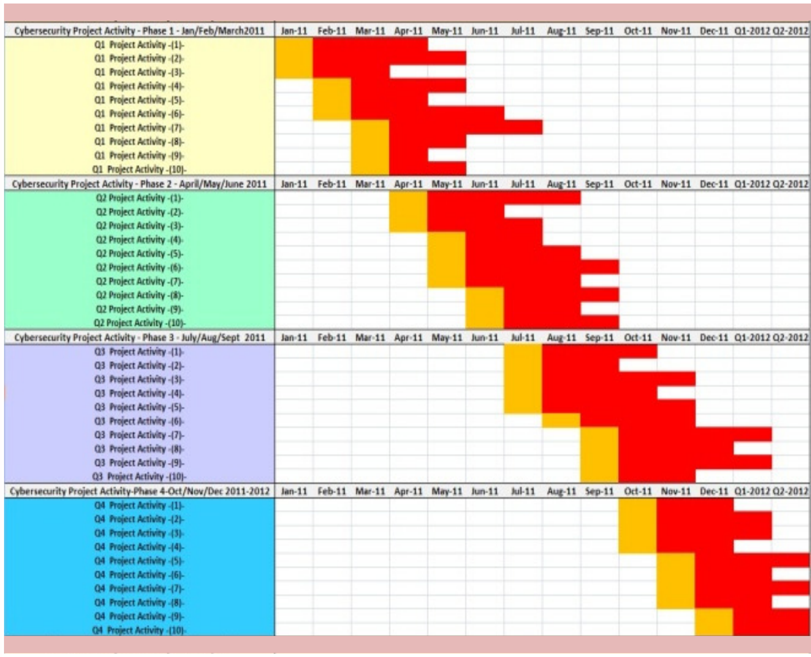
Cybersecurity Project Activity-Phase 4-Oct/Nov/Dec 2011-2012	Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q4 Project Activity -(1)-											🟥	🟥		
Q4 Project Activity -(2)-										🟧	🟥	🟥	🟥	
Q4 Project Activity -(3)-										🟧	🟥	🟥	🟥	
Q4 Project Activity -(4)-										🟧	🟥	🟥		
Q4 Project Activity -(5)-											🟧	🟥	🟥	🟥
Q4 Project Activity -(6)-											🟧	🟥	🟥	
Q4 Project Activity -(7)-											🟧	🟥	🟥	🟥
Q4 Project Activity -(8)-											🟧	🟥	🟥	
Q4 Project Activity -(9)-												🟧	🟥	🟥
Q4 Project Activity -(10)-												🟧	🟥	🟥

Critical Economic Sectors: *Cyber RoadMaps*

Each Critical Service Sector such as Banking & Finance, Civil & National Defence, Telecommunications and Energy will require its own Cyber Strategy, Risk Assessment, Roadmap & Action Plan:

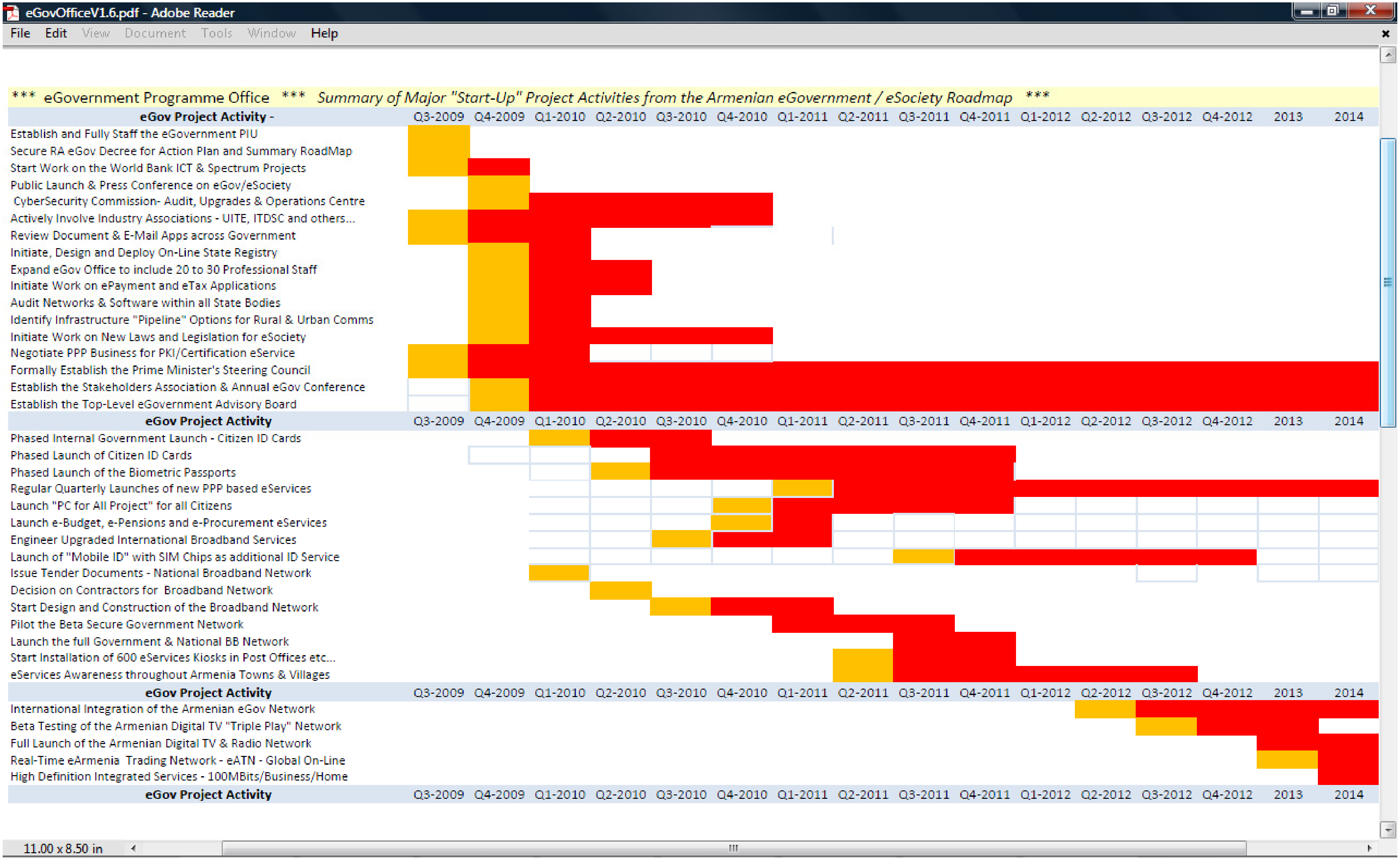
➢Tomorrow I'll discuss the practical ways in which we can develop Strategies, Actions and Activities for Smart Security in each critical sector…

➢ I'll also review the Operational Priorities, and Security Policies that are required to significantly reduce Cybercrime, Cyber terrorism & Attacks…



Cybersecurity Project Activity - Phase 1 - Jan/Feb/March2011	Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q1 Project Activity -(1)-	🟧	🟥	🟥	🟥										
Q1 Project Activity -(2)-	🟧	🟥	🟥	🟥	🟥									
Q1 Project Activity -(3)-	🟧	🟥	🟥											
Q1 Project Activity -(4)-		🟧	🟥	🟥	🟥									
Q1 Project Activity -(5)-		🟧	🟥	🟥										
Q1 Project Activity -(6)-		🟧	🟥	🟥	🟥	🟥								
Q1 Project Activity -(7)-			🟧	🟥	🟥	🟥	🟥							
Q1 Project Activity -(8)-			🟧	🟥	🟥									
Q1 Project Activity -(9)-			🟧	🟥										
Q1 Project Activity -(10)-			🟧	🟥	🟥									
Cybersecurity Project Activity - Phase 2 - April/May/June 2011	Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q2 Project Activity -(1)-				🟧	🟥	🟥	🟥	🟥						
Q2 Project Activity -(2)-				🟧	🟥	🟥								
Q2 Project Activity -(3)-				🟧	🟥	🟥	🟥							
Q2 Project Activity -(4)-					🟧	🟥	🟥							
Q2 Project Activity -(5)-					🟧	🟥	🟥	🟥						
Q2 Project Activity -(6)-					🟧	🟥	🟥	🟥	🟥					
Q2 Project Activity -(7)-					🟧	🟥	🟥	🟥						
Q2 Project Activity -(8)-						🟧	🟥	🟥	🟥					
Q2 Project Activity -(9)-						🟧	🟥	🟥						
Q2 Project Activity -(10)-						🟧	🟥	🟥	🟥					
Cybersecurity Project Activity - Phase 3 - July/Aug/Sept 2011	Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q3 Project Activity -(1)-							🟧	🟥	🟥	🟥				
Q3 Project Activity -(2)-							🟧	🟥	🟥					
Q3 Project Activity -(3)-							🟧	🟥	🟥	🟥	🟥			
Q3 Project Activity -(4)-							🟧	🟥	🟥	🟥				
Q3 Project Activity -(5)-							🟧	🟥	🟥	🟥	🟥			
Q3 Project Activity -(6)-								🟧	🟥	🟥	🟥			
Q3 Project Activity -(7)-									🟧	🟥	🟥	🟥	🟥	
Q3 Project Activity -(8)-									🟧	🟥	🟥	🟥		
Q3 Project Activity -(9)-									🟧	🟥	🟥	🟥	🟥	
Q3 Project Activity -(10)-									🟧	🟥	🟥			
Cybersecurity Project Activity-Phase 4-Oct/Nov/Dec 2011-2012	Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q4 Project Activity -(1)-										🟧	🟥	🟥		
Q4 Project Activity -(2)-										🟧	🟥	🟥	🟥	
Q4 Project Activity -(3)-										🟧	🟥	🟥	🟥	
Q4 Project Activity -(4)-										🟧	🟥	🟥		
Q4 Project Activity -(5)-											🟧	🟥	🟥	🟥
Q4 Project Activity -(6)-											🟧	🟥	🟥	
Q4 Project Activity -(7)-											🟧	🟥	🟥	🟥
Q4 Project Activity -(8)-											🟧	🟥	🟥	
Q4 Project Activity -(9)-												🟧	🟥	🟥
Q4 Project Activity -(10)-												🟧	🟥	🟥

eGovernance/eSecurity Road Map – *2009 to 2014 -*

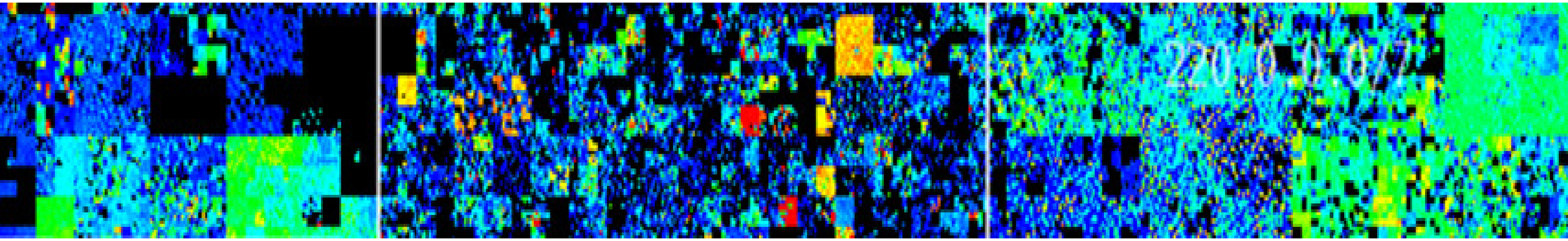


*** eGovernment Programme Office *** *Summary of Major "Start-Up" Project Activities from the Armenian eGovernment / eSociety Roadmap* ***

eGov Project Activity -	Q3-2009	Q4-2009	Q1-2010	Q2-2010	Q3-2010	Q4-2010	Q1-2011	Q2-2011	Q3-2011	Q4-2011	Q1-2012	Q2-2012	Q3-2012	Q4-2012	2013	2014
Establish and Fully Staff the eGovernment PIU	🟨															
Secure RA eGov Decree for Action Plan and Summary RoadMap	🟨															
Start Work on the World Bank ICT & Spectrum Projects	🟨	🟥														
Public Launch & Press Conference on eGov/eSociety		🟨														
CyberSecurity Commission- Audit, Upgrades & Operations Centre		🟨	🟥	🟥	🟥	🟥										
Actively Involve Industry Associations - UITE, ITDSC and others...	🟨	🟥	🟥	🟥	🟥	🟥										
Review Document & E-Mail Apps across Government	🟨	🟥	🟥													
Initiate, Design and Deploy On-Line State Registry		🟨	🟥													
Expand eGov Office to include 20 to 30 Professional Staff		🟨	🟥	🟥												
Initiate Work on ePayment and eTax Applications		🟨	🟥	🟥												
Audit Networks & Software within all State Bodies		🟨	🟥													
Identify Infrastructure "Pipeline" Options for Rural & Urban Comms		🟨	🟥													
Initiate Work on New Laws and Legislation for eSociety		🟨	🟥	🟥	🟥	🟥										
Negotiate PPP Business for PKI/Certification eService	🟨	🟥	🟥													
Formally Establish the Prime Minister's Steering Council	🟨	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Establish the Stakeholders Association & Annual eGov Conference		🟨	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Establish the Top-Level eGovernment Advisory Board		🟨	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
eGov Project Activity	Q3-2009	Q4-2009	Q1-2010	Q2-2010	Q3-2010	Q4-2010	Q1-2011	Q2-2011	Q3-2011	Q4-2011	Q1-2012	Q2-2012	Q3-2012	Q4-2012	2013	2014
Phased Internal Government Launch - Citizen ID Cards			🟨	🟥	🟥											
Phased Launch of Citizen ID Cards					🟥	🟥	🟥	🟥	🟥	🟥						
Phased Launch of the Biometric Passports				🟨	🟥	🟥	🟥	🟥	🟥	🟥						
Regular Quarterly Launches of new PPP based eServices							🟨	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Launch "PC for All Project" for all Citizens						🟨	🟥	🟥	🟥	🟥						
Launch e-Budget, e-Pensions and e-Procurement eServices						🟨	🟥									
Engineer Upgraded International Broadband Services					🟨	🟥	🟥									
Launch of "Mobile ID" with SIM Chips as additional ID Service									🟨	🟥	🟥	🟥	🟥	🟥		
Issue Tender Documents - National Broadband Network			🟨													
Decision on Contractors for Broadband Network				🟨												
Start Design and Construction of the Broadband Network					🟨	🟥	🟥									
Pilot the Beta Secure Government Network							🟥	🟥	🟥							
Launch the full Government & National BB Network									🟥	🟥						
Start Installation of 600 eServices Kiosks in Post Offices etc...								🟨	🟥	🟥						
eServices Awareness throughout Armenia Towns & Villages								🟨	🟥	🟥	🟥	🟥	🟥			
eGov Project Activity	Q3-2009	Q4-2009	Q1-2010	Q2-2010	Q3-2010	Q4-2010	Q1-2011	Q2-2011	Q3-2011	Q4-2011	Q1-2012	Q2-2012	Q3-2012	Q4-2012	2013	2014
International Integration of the Armenian eGov Network												🟨	🟥	🟥	🟥	🟥
Beta Testing of the Armenian Digital TV "Triple Play" Network													🟨	🟥	🟥	
Full Launch of the Armenian Digital TV & Radio Network															🟥	🟥
Real-Time eArmenia Trading Network - eATN - Global On-Line															🟨	🟥
High Definition Integrated Services - 100MBits/Business/Home																🟥
eGov Project Activity	Q3-2009	Q4-2009	Q1-2010	Q2-2010	Q3-2010	Q4-2010	Q1-2011	Q2-2011	Q3-2011	Q4-2011	Q1-2012	Q2-2012	Q3-2012	Q4-2012	2013	2014

National Cybersecurity Strategy, Roadmap & Actions

1 – Our Global Cybersecurity Challenge	2 – Developing the UN Cyber Framework	3 – National Cybersecurity Case Studies
4 – Dimensions of National Cybersecurity	5 – The UN Global Cyber Agenda (GCA)	6 – Technology, Standards & Operations
7 – New Legislation, Training and Partners	8 – National Roadmap - "Shopping List"	9 – Implementing YOUR Action Plan



YOUR Cybersecurity *Action Plan*!...

- **Phase 1:** Define your cybersecurity STRATEGY and OBJECTIVES
- **Phase 2:** Establish, resource & train your cybersecurity ORGANISATION
- **Phase 3:** Agree and communicate technical & operational standards
- **Phase 4:** Review, Audit and Upgrade all ICT Systems during next year
- **Phase 5:** On-Going Operational Management by CSO/CISO, including regular compliance audits and technical upgrades to new Cyber Threats

……In summary, the adoption of international standards for YOUR National & Enterprise ICT systems and Operational Procedures will have a significant impact on cybercrime, & reduce the risk of attacks on critical national infrastructure

Example of National Cybersecurity Action Plan: *Short-Term*

# Action	SHORT-TERM ACTION PLAN: October 2014 – April 2015
1	**Government Cybersecurity Accountability** Consider making cybersecurity one of the Government's main management accountabilities with clear success criteria.
2	**Appoint National Cybersecurity Coordinator** Consider designating a senior Government Aide as National Cybersecurity Coordinator. The official should coordinate cybersecurity activities across the Government and report to the appropriate national bodies
3	**Complete and Promulgate National Cybersecurity Strategy** Consider using the template from the ITU Guidelines as a starting point for the National Cybersecurity Strategy. The Strategy should have clear roles and responsibilities, priorities, timeframes and performance metrics. Thereafter, obtain Government approval for the Cybersecurity Strategy.
4	**Create National Cybersecurity Coordination Agency** In common with other countries, consider creating a multi-agency body as a focal point for all activities dealing with protecting 's cyberspace against threats such as cybercrime.
5	**Define National Cybersecurity Framework** The framework should be flexible to allow stakeholder organisations to achieve the stated goals in the most efficient and effective manner.
6	**Initiate Public-Private Sector Cybersecurity partnership** The process should be transparent and consider all views.
7	**Create Computer Incident Response Team (CIRT)** Consider creating a national CIRT to analyse cyber threat trends, improve response coordination and dissemination of information across the Government, to industry, citizens and international partners.
8	**Strengthen Legal and Regulatory System** Complete the Cybercrime Legislation Programme and enforce the new laws.
9	**Initiate Cybersecurity Awareness and Education campaign** Consider working with the private sector and civil society to explain cyber threats to the citizens and their role in defending cyberspace.
10	**Define and initiate Cybersecurity Skills and Training Programme** Consider the experience of other countries in creating a cybersecurity skills and training programme with periodic measurement of skills.

Example of National Cybersecurity Action Plan: *Mid-Term*

# Action	MID-TERM ACTION PLAN: April 2015 to December 2016
1	Define, localise and communicate Government cybersecurity Standards in areas such as Data Classification and Staff Vetting and Clearance.
2	The National Cybersecurity Agency (NCA) should ensure that cybersecurity policies are in line with the new Cybercrime legislation
3	Launch cybersecurity awareness campaign across Government and NCA website for government, commercial and educational sectors with guidelines, standards and training materials.
4	As National Technical Authority for Information Assurance, the NCA should advise on how to secure eGovernment Services.
5	Use formal channels to organise study trips for NCA Staff to other Cybersecurity Agencies
6	Conduct in-depth cybersecurity review and audit of Government ministries, agencies and associated bodies.
7	Review Physical Security of organisations hosting critical infrastructure.
8	Parliamentary review of the proposed National Cybersecurity Act 2011
9	NCA Programme on Business Continuity and Disaster Recovery
10	Develop and Resource the national CIRT/CERT. In addition, develop national Cyber Incident Response Framework involving public-private stakeholders. Also develop, test and exercise incident response plans for Government emergency communications during natural disasters, cyberattacks, crisis or war as required by the National Security Concept.
11	Implement six to nine months' programme of Operational Cybersecurity upgrades. The activities may extend into 2016 and beyond.
12	Ensure that the Government Communications Network and all new services comply with the agreed Government Authentication Framework.
13	Launch the Cybersecurity Skills and Training Programme for cybersecurity professionals and collaborate with commercial and educational sectors to boost cybersecurity Research and Development.
14	Secure Parliamentary, Cabinet & Government approval of the Cybersecurity Act 2015 and associated Cybercrime legislation.
15	Organise an annual Regional Cybersecurity Conference to communicate progress, share views and promote national Cybersecurity Programme.

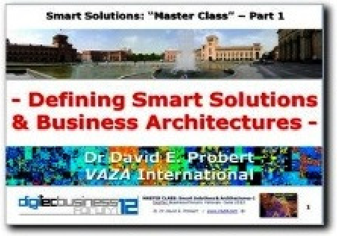
On-Line *Cybersecurity* Resources: UN/ITU

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

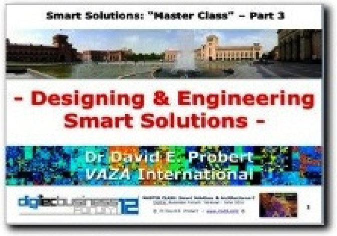
1) Global Cybersecurity Agenda – HLEG Strategic Report – 2008
2) Cybersecurity Guide for Developing Countries – 2009
3) "BotNet" Mitigation Toolkit Guide – 2008
4) National Cybersecurity/CIIP Self-Assessment Tool – 2009
5) Toolkit for Cybersecurity Legislation – 2010
6) Understanding Cybercrime: A Guide for Developing Countries-2009
7) Technical Security Standards & Recommendations – "X-Series" – including X.509 (PKI), X.805 (Architecture), X.1205 (Threats & Solutions)
8) GCA: Global Cybersecurity Agenda: Summary Brochure – 2010
9) National Cybersecurity Strategy Guide – September 2011

- UN/ITU = United Nations – *International Telecommunications Union*

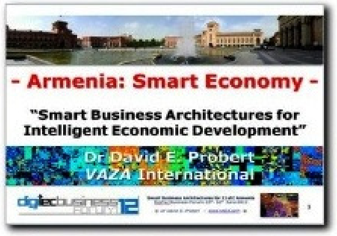
Cybersecurity Resources, Reports and More!...


Smart Solutions: "Master Class" – Part 1
- Defining Smart Solutions & Business Architectures -
Dr David E. Probert
VAZA International

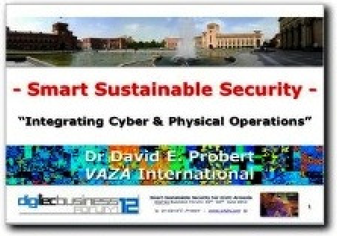
"Master Class - Smart Theory & Practice"


Smart Solutions: "Master Class" – Part 3
- Designing & Engineering Smart Solutions -
Dr David E. Probert
VAZA International

"Master Class 2012 - Smart Design"


- Armenia: Smart Economy -
"Smart Business Architectures for Intelligent Economic Development"
Dr David E. Probert
VAZA International

"21stC Armenia- 2012: Smart Economy"


- Smart Sustainable Security -
"Integrating Cyber & Physical Operations"
Dr David E. Probert
VAZA International

"21stC Armenia - 2012: Smart Security"

- Smart Governance -
"Stimulating Innovation & Economic Growth"
Dr David E. Probert
VAZA International

"21stC Armenia: Smart Governance"

"Real-Time Armenia"
"Securing Government & Financial Enterprise Operations"

"Real-Time Armenia" - White Paper

"Real-Time" ARMENIA!...
...Securing Government & Financial Enterprise Operations
Dr David E Probert
VAZA International

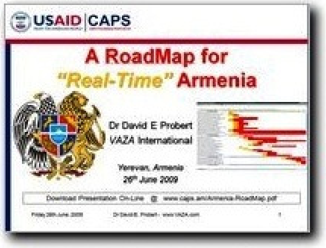
"Real-Time Armenia" - Slides

"Awesome Armenia!"
Photos and Panoramas
Armenia Spring - 2009
Armenia Summer 2009
Armenian Panoramas Summer - 2009

Awesome Armenia: In Photos

"Roadmap for Real-Time Armenia"
"E-Government, E-Commerce and E-Security"
USAID | CAPS

Roadmap for Real-Time Armenia- Report


USAID | CAPS
A RoadMap for "Real-Time" Armenia
Dr David E Probert
VAZA International
Yerevan, Armenia
26th June 2009

RoadMap for Real-Time Armenia- Slides

"Real-Time" Georgia!.....
...Securing Government & Enterprise Operations
Dr David E Probert
VAZA International

"Real-Time Georgia" - GITI 2008 Slides

"Real-Time Georgia"
"Securing Government & Enterprise Operations"

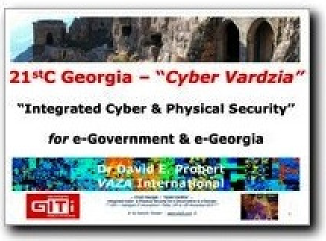
"Real-Time Georgia" - GITI 2008 Paper

"Republic of Georgia"
Photos and Panoramas
Georgian Panoramas Autumn 2007
Georgian Aerial Panoramas
Georgian Panoramas Autumn 2008
Georgia 2008

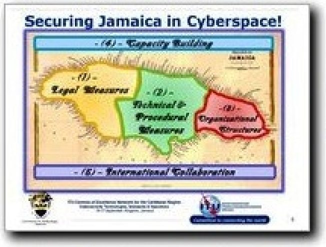
Gorgeous Georgia: In Photos

..."21stC Georgia"...
..."Cyber-Vardzia"...

21stC Georgia: "CyberVardzia" - Paper


21stC Georgia – "Cyber Vardzia"
"Integrated Cyber & Physical Security"
for e-Government & e-Georgia
Dr David E. Probert
VAZA International
GITI

21stC Georgia - "CyberVardzia" - Slides

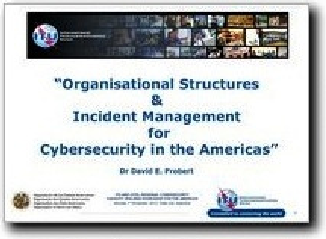

Securing Jamaica in Cyberspace!
- (4) - Capacity Building
- (1) - Legal Measures
- (2) - Technical & Procedural Measures
- (3) - Organizational Structures
- (5) - International Collaboration

Jamaica: Cybersecurity Technology- Slides

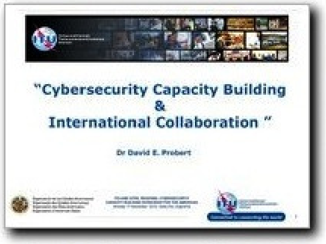
* ITU Cybersecurity Strategy *
"3-Day Workshop Overview"
Workshop Presentations
Group Tasks & Discussions
Workshop Presentations
Group Tasks & Discussions

Jamaica: Cybersecurity Strategy- Slides

"Short Professional Bio"


"Organisational Structures & Incident Management for Cybersecurity in the Americas"
Dr David E. Probert

ITU/CITEL: Cybersecurity in the Americas


"Cybersecurity Capacity Building & International Collaboration "
Dr David E. Probert

ITU/CITEL: Cybersecurity Skills Building

Link: www.valentina.net/vaza/CyberDocs

"National Cybersecurity Strategy, Roadmap and Action Plans"

30th East-West Security Conference – Paris, France

Thank-You!...

Presentation Slides:

www.Valentina.net/East-West2014/

Presentation Slides:

www.Valentina.net/East-West2014/

Thank you for your time!

Professional Profile - *Dr David E. Probert*

- ***Computer Integrated Telephony (CIT)*** – Established and led British Telecom's £25M EIGER Project during the mid-1980s' to integrate computers with telephone switches (PABX's). This resulted in the successful development and launch of CIT software applications for telesales & telemarketing

- ***Blueprint for Business Communities*** – Visionary Programme for Digital Equipment Corporation during late-1980's that included the creation of the "knowledge lens" and "community networks". The Blueprint provided the strategic framework for Digital's Value-Added Networks Business

- ***European Internet Business Group (EIBG***) – Established and led Digital Equipment Corporation's European Internet Group for 5 years. Projects included support for the national Internet infrastructure for countries across EMEA as well as major enterprise, government & educational Intranet deployments. Dr David Probert was a sponsoring member of the European Board for Academic & Research Networking (EARN/TERENA) for 7 years (1991 ➔1998)

- ***Supersonic Car (ThrustSSC)*** – Worked with Richard Noble OBE, and the Mach One Club to set up and manage the 1st Multi-Media and e-Commerce Web-Site for the World's 1st Supersonic Car – ThrustSSC – for the World Speed Record. (Oct 1997), which still stands after 17 years!

- ***Secure Wireless Networking*** – Business Director & VP for Madge Networks to establish a portfolio of innovative fully secure wireless Wi-Fi IEEE802.11 networking products with technology partners from both UK and Taiwan.

- ***Networked Enterprise Security*** - Appointed as the New Products Director (CTO) to the Management Team of the Blick Group plc with overall responsibility for 50+ professional engineers & a diverse portfolio of hi-tech networked security products across global markets.

- ***Georgia*** – Senior Security Adviser – Appointed by the European Union to investigate and then to make recommendations on *all* aspects of IT security, physical security and BCP/DR relating to the Georgian Parliament. Also appointed by the UN/ITU as expert for in-depth cybersecurity audit & roadmap.

- ***Armenia*** – Appointed by USAID/CAPS to develop eGovernance, eSecurity , eSociety Report, Roadmap & Action Plan which has since been implemented

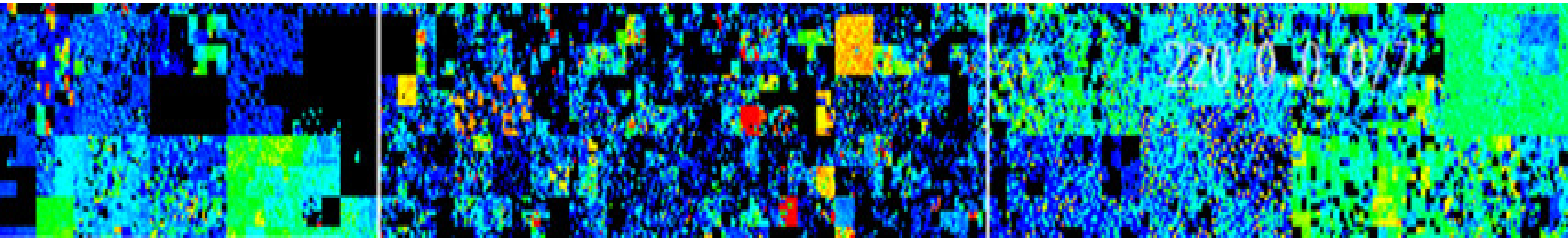
- ***UN/ITU*** – Senior Adviser – Development of Cybersecurity Infrastructure, Standards, Policies, & Organisations in countries within both Europe & Americas

Dr David E. Probert is a Fellow of the Royal Statistical Society. He has a 1st Class Honours Degree in Mathematics (Bristol University) & PhD from Cambridge University in Self-Organising Systems (Evolution of Stochastic Automata) , and his full professional biography is featured in the Marquis Directory of Who's Who in the World: 2007-2015 Editions.

“National Cybersecurity Strategy, Roadmap and Action Plans”

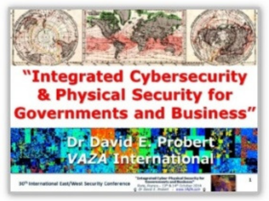
30th East/West Security Conference – Paris, France

BACK-UP SLIDES



Smart Sustainable Security – *"Theme Trilogy"*

Theme (1) – *Smart Security : Integrated Cybersecurity and Physical Security*


"Integrated Cybersecurity & Physical Security for Governments and Business"

Dr David E. Probert
VAZA International

- *Understanding and Mapping the Worldwide Cyber Threats*
- *Transition to Smart Systems : Embedded Networked Intelligence*
- *Emergence of Smart Security: Hybrid Cyber-Physical Applications*

"Operational Convergence " — ***13th Oct: 09:10 – 09:50***

Theme (2) – *National Security : Strategy, Models, and Road Maps*

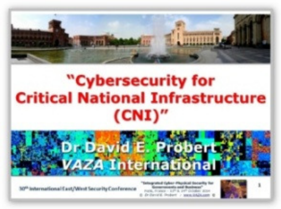
"National Cybersecurity Strategy Roadmap and Action Plan"

Dr David E. Probert
VAZA International

- *UN/ITU – Global Cybersecurity Agenda and Guide*
- *Operations, Technology, Legal, Training, Partnerships*
- *Case Studies of "National Cybersecurity Agencies"*

"Architecture & Standards" — ***13th Oct: 14:30 – 15:10***

Theme (3) - *Critical Security : Sector Threats and Smart Solutions*


"Cybersecurity for Critical National Infrastructure (CNI)"

Dr David E. Probert
VAZA International

- *Smart Security for Critical National Infrastructure (CNI):*
- *Finance, Transportation, ITC, Energy, Defence and more!...*
- *Engineering Smart Technical and Operational Solutions*

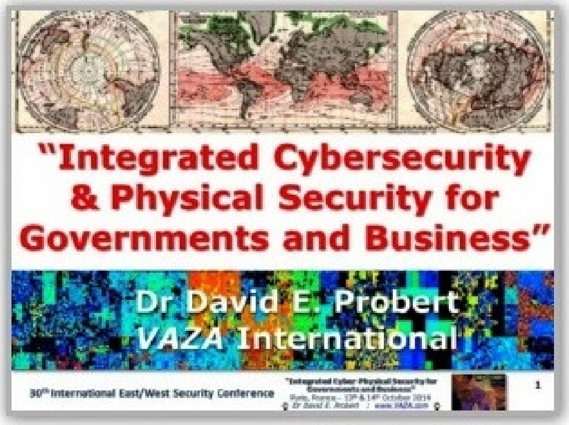
"Intelligent Applications" — ***14th Oct: 11:15 – 11:55***

Download Slides: www.valentina.net/East-West2014/

East-West Security Conference – Paris 2014

- Cybersecurity Presentation Slides (PDF) -

Smart Sustainable Security - "Theme Trilogy"

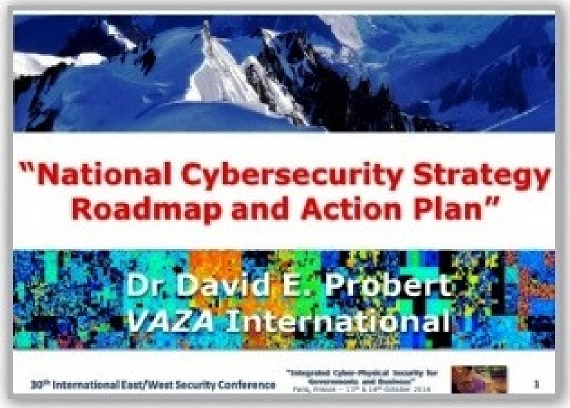


"Integrated Cybersecurity & Physical Security for Governments and Business"

Dr David E. Probert
VAZA International

30th International East/West Security Conference — 1

(1) Smart Security

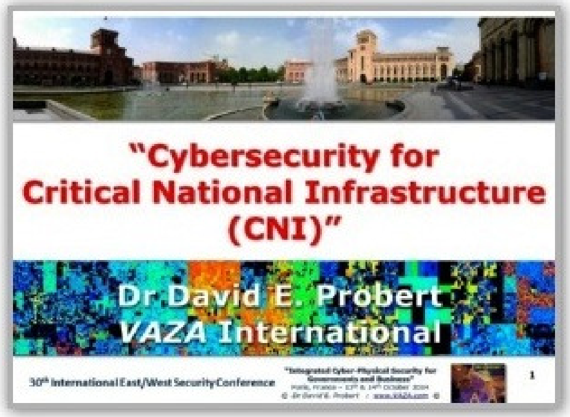


"National Cybersecurity Strategy Roadmap and Action Plan"

Dr David E. Probert
VAZA International

30th International East/West Security Conference — 1

(2) National Security



"Cybersecurity for Critical National Infrastructure (CNI)"

Dr David E. Probert
VAZA International

30th International East/West Security Conference — 1

(3) Critical Security

Download Link: *www.valentina.net/East-West2014/*